HP MSM7xx Controllers

Management and Configuration Guide

HP MSM7xx Controllers

Management and Configuration Guide

Publication Number

5998-1136
January 2011

Applicable Products

See *Products covered on page 1-2*.

Trademark Credits

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the warranty information included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Open Source Software Acknowledgement Statement

This software incorporates open source components that are governed by the GNU General Public License (GPL), version 2. In accordance with this license, HP will make available a complete, machine-readable copy of the source code components covered by the GNU GPL upon receipt of a written request. Send a request to:

Hewlett-Packard Company, L.P.
GNU GPL Source Code
Attn: ProCurve Networking Support
Roseville, CA 95747 USA

Safety and regulatory information

Before installing and operating this product, please read

- *Safety information on page 1-12*.
- *Appendix A: Safety and EMC regulatory statements*

Hewlett-Packard Company
8000 Foothills Boulevard
Roseville, California 95747
www.hp.com/networking/

Contents

1 Introduction

2 Management

3 Network configuration

4 Wireless configuration

5 Working with VSCs

7 Working with VLANs

8 Controller teaming

9 Mobility traffic manager

10 User authentication, accounts, and addressing

11 Authentication services

12 Security

15 Working with RADIUS attributes

16 Working with VPNs

17 LLDP

18 sFlow

19 Working with autonomous APs

20 Maintenance

A Safety and EMC regulatory statements

B Console ports

C Resetting to factory defaults

D NOC authentication

E DHCP servers and Colubris vendor classes

1

Introduction

Contents

About this guide

This guide explains how to configure, and operate the MSM7xx Controllers. It also provides controlled-mode information for MSM3xx and MSM4xx Access Points, and the MSM317 Access Device. For information on the operation of access points that support autonomous mode, see the *MSM3xx/MSM4xx Access Points Management and Configuration Guide*.

Products covered

This guide applies to the following MSM7xx Controller products:

Model	Part
MSM710 (E-MSM710) Access Controller	J9328A
MSM710 (E-MSM710) Mobility Controller	J9325A
MSM730 (E-MSM730) Access Controller	J9329A
MSM730 (E-MSM730) Mobility Controller	J9326A
MSM750 (E-MSM750) Access Controller	J9330A
MSM750 (E-MSM750) Mobility Controller	J9327A
MSM760 (E-MSM760) Access Controller	J9421A
MSM760 (E-MSM760) Mobility Controller	J9420A
MSM765zl (E-MSM765zl) Mobility Controller	J9370A

The product models in the above table include alternative product names in parenthesis. For example, the MSM710 is also known as the E-MSM710. Both names refer to the same product. The original product names (without “E-”) are used throughout this document.

This guide provides controlled-mode information for the following MSM3xx and MSM4xx Access Points (“WW” identifies worldwide versions for the rest of the world):

Model	WW	Americas	Japan	Israel
E-MSM430	J9651A	J9650A	J9652A	J9653A
E-MSM460	J9591A	J9590A	J9589A	J9618A
E-MSM466	J9622A	J9621A	J9620A	

Model	WW	USA	Japan
MSM310 (E-MSM310)	J9379A/B	J9374A/B	J9524A/B
MSM310-R (E-MSM310-R)	J9383A/B	J9380A/B	
MSM320 (E-MSM320)	J9364A/B	J9360A/B	J9527A/B

Model	WW	USA	Japan
MSM320-R (E-MSM320-R)	J9368A/B	J9365A/B	J9528A/B
MSM325 (E-MSM325)	J9373A/B	J9369A/B	
MSM335 (E-MSM335)	J9357A/B	J9356A/B	
MSM410 (E-MSM410)	J9427A/B	J9426A/B	J9529A/B
MSM422 (E-MSM422)	J9359A/B	J9358A/B	J9530A/B
MSM317 Access Device	J9423A	J9422A	

The product models in the table immediately above include alternative product names in parenthesis. For example, the MSM422 is also known as the E-MSM422. Both names refer to the same product. Except for E-MSM430, E-MSM460, and E-MSM466, the original MSM product names (without “E-”) are used throughout this document.

Important terms

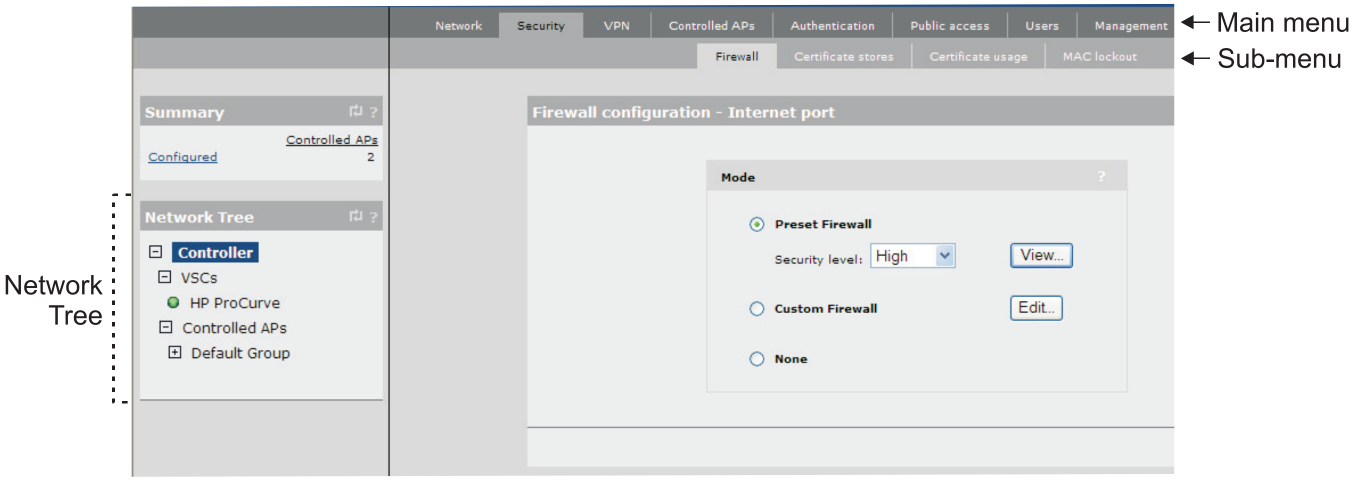
The following terms are used in this guide.

Term	Description
AP	Refers to any HP MSM3xx or MSM4xx Access Point or the MSM317 Access Device which is an AP with integrated Ethernet switch. Specific model references are used where appropriate. Non-HP access points are identified as *third-party APs*. These APs do not support controlled-mode operation.
controller	Refers to any HP MSM7xx Controller, including both Access Controller and Mobility Controller variants. **Controller teams** Most of the concepts discussed in this guide apply equally to both teamed and non-teamed controllers. Any reference to the term controller, also implies controller team unless indicated otherwise.

Conventions

Management tool

This guide uses specific syntax when directing you to interact with the management tool user interface. Key user-interface elements are identified as follows:



● Preset Firewall
Security level: High
○ Custom Firewall
○ None

Example directions in this guide	What to do in the user interface
Select **Controller >> Security > Firewall**.	**On a non-teamed MSM7xx controller** In the Network Tree select the **Controller** element, then on the main menu select **Security,** and then select **Firewall** on the sub-menu. All elements to the left of the double angle brackets **>>** are found in the Network Tree. **On an MSM7xx controller team** In the Network Tree on the team manager, select the **Team [*team-name*]** element, then on the main menu select **Security,** and then select **Firewall** on the sub-menu. All elements to the left of the double angle brackets >> are found in the Network Tree.
Select **Controller > VSCs > [*VSC-name*] >> Configuration**.	**On a non-teamed MSM7xx controller** Expand the **Controller** branch (click its **+** symbol), expand the **VSCs** branch, select a **[*VSC-name*]**, then select **Configuration** on the main menu. **On an MSM7xx controller team** In the Network Tree on the team manager, expand the **Team: [*team-name*]** branch (click its **+** symbol), expand the **VSCs** branch, select a **[*VSC-name*]**, then select **Configuration** on the main menu.
For **Password** specify **secret22**.	In the **Password** field enter the text **secret22** exactly as shown.

Commands and program listings

Monospaced text identifies commands and program listings as follows:

Example	Description
`use-access-list`	Command name. Specify it as shown.
`ip_address`	Items in italics are parameters for which you must supply a value.
`ssl-certificate=`*`URL`*` [%s]`	Items enclosed in square brackets are optional. You can either include them or not. Do not include the brackets. In this example you can either include the "%s" or omit it.
`[ONE	TWO]`	Items separated by a vertical line indicate a choice. Specify only one of the items. Do not include the vertical line.

Warnings and cautions

Do not proceed beyond a WARNING or CAUTION notice until you fully understand the hazardous conditions and have taken appropriate steps.

Warning Identifies a hazard that can cause physical injury or death.

Caution Identifies a hazard that can cause the loss of data or configuration information, create a non-compliant condition, or hardware damage.

New in this release

The following new features and enhancements have been added in releases 5.5.x:

New feature or enhancement	For information see...
New APs	This release supports the following new 802.11n dual-radio access points: E-MSM430, E-MSM460, and E-MSM466. For information, see the *Quickstarts* for these products.
Band steering	*Band steering on page 5-11*
Broadcast filtering	*Broadcast filtering on page 5-11*
Transmission protection	*Tx protection on page 4-30*
Beamforming	*Tx beamforming on page 4-29*
Country configuration per group	*Assigning country settings to a group on page 6-30*
Moving multiple APs between groups	*Moving multiple APs between groups on page 6-29*
Identify RADIUS server by host name	*Primary/Secondary RADIUS server on page 11-9*
User agent filtering	*User agent filtering on page 14-10*
HTTPS proxy support	*Support applications that use on page 14-11*
Improved mobility status pages	*Monitoring the mobility domain on page 9-16*
Manager login credentials reset	*Manager username/password reset on page 2-6*
PayPal support	*PayPal service on page 14-37*
LEAP support	*Supported 802.1X protocols on page 10-9*
MSM317 switch port enhancements ■ Inheritance on a per port basis ■ Port isolation ■ Loop protection ■ Network Policy TLV support ■ Enhanced VLAN support	See the *MSM317 Installation and Getting Started Guide.*

Introducing the MSM7xx Controllers

MSM7xx Controllers provide centralized management and control of intelligent HP MSM APs for a wide range of deployments, from small Internet cafes and businesses, to large corporations and institutions, and even entire towns.

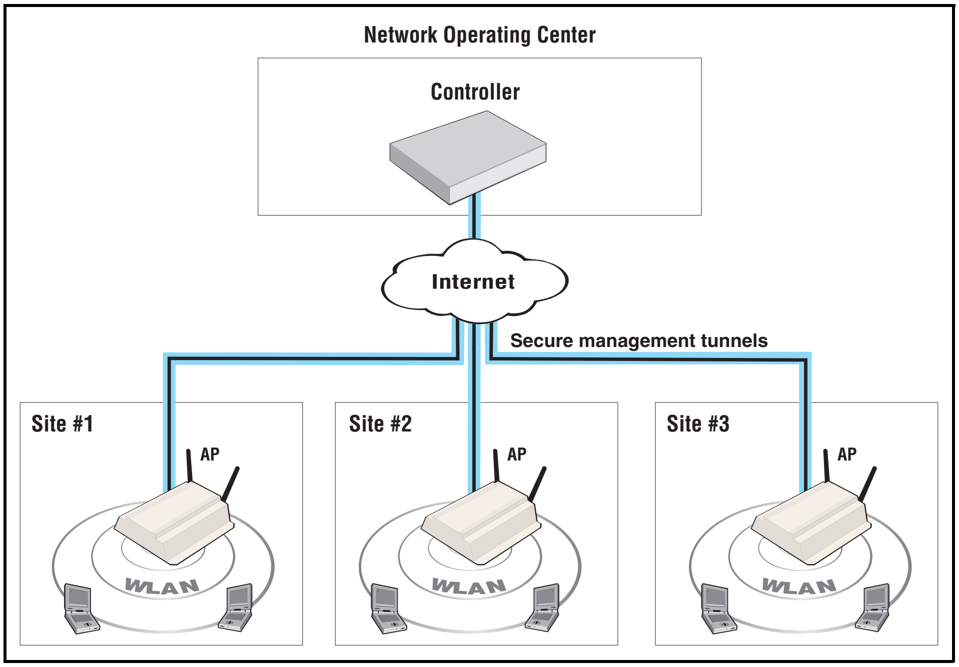
MSM controllers let you take advantage of both distributed and centralized approaches to deploying a wireless networking solution, letting you design a wireless infrastructure that perfectly meets the needs of your users.

Simplified configuration, deployment, and operation

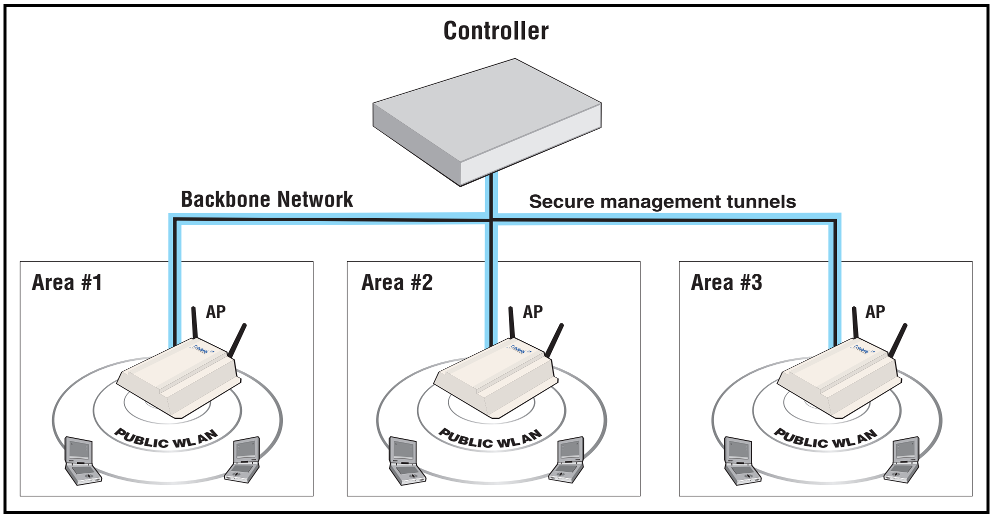
For trouble-free deployment in geographically distributed networks, HP MSM controllers automate discovery, authentication and configuration for all installed APs. Using standard dynamic look-up procedures, APs identify the controller to which they are assigned. Authentication using digital certificates assures security and eliminates the risk of rogue AP connectivity. Once authenticated, the controller establishes a secure management tunnel for the exchange of configuration and control information with the AP.

The controller provides centralized management for all APs. It eliminates time-consuming AP configuration, troubleshooting and maintenance tasks by providing a single management interface for the entire group of APs it manages. The controller automates installation of AP software updates and ensures a consistent set of services are delivered throughout the network. All security, quality of service (QoS), and other policies can be centrally defined through the controller's intuitive and secure Web-based management tool.

Controller managing APs installed in different physical locations

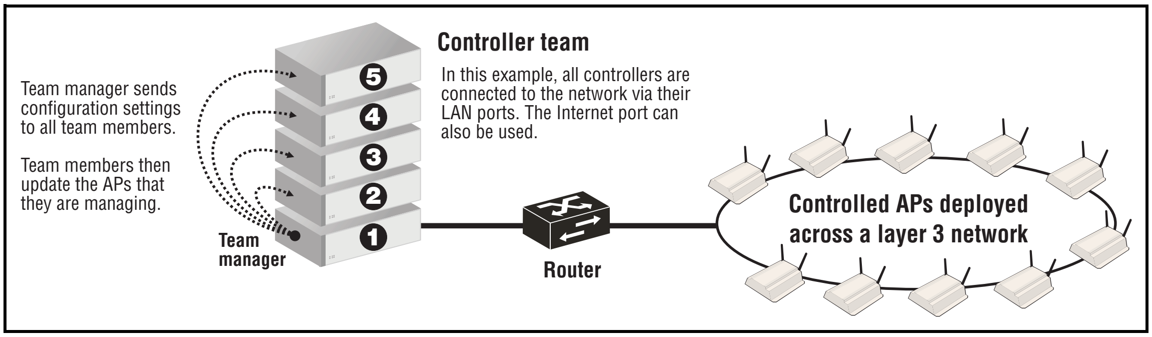


Controller managing APs installed in different areas at a single location



Controller teaming

Controller teaming enables you to easily configure and monitor multiple controllers and their APs. Up to five controllers can be combined into a team providing support for up to 800 APs (four controllers x 200 APs per controller plus one additional controller for backup/ redundancy). For example:


Team manager sends configuration settings to all team members.
Team members then update the APs that they are managing.
5
4
3
2
1
Team manager
Controller team
In this example, all controllers are connected to the network via their LAN ports. The Internet port can also be used.
Router
Controlled APs deployed across a layer 3 network

Key benefits of controller teaming include:

- **Scalability:** Controller teaming enables you to scale up your wireless network as your needs increase. Simply add additional APs, controllers, and licenses to meet the required demand. Up to 800 APs are supported per controller team (four controllers x 200 APs per controller plus one additional controller reserved for backup/redundancy).
- **Redundancy and failover support:** A controller team provides for service redundancy in case of failure. If one of the controllers in a team becomes inoperative (due to network problems, hardware failure, etc.), its APs will automatically migrate to another controller in the team allowing for continuation of services.
- **Centralized management and control:** Configuration and monitoring of all team members and their APs is performed using the management tool on the team manager. The team manager is responsible for handling the addition and deletion of controlled

APs, including newly discovered APs. It also displays status information for all team members and their APs, as well as APs directly connected to the manager.

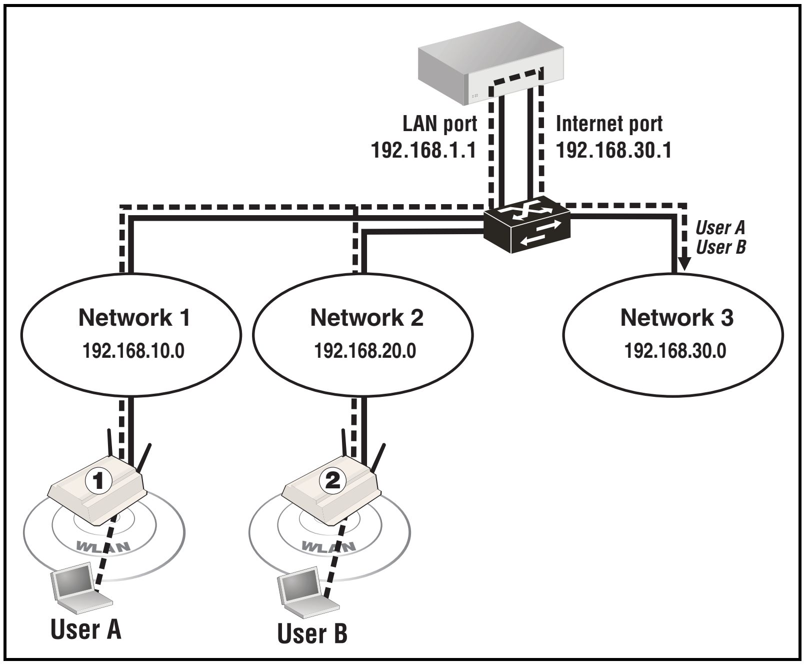
The team manager is responsible for enforcing and updating the firmware of team members. An update to the team manager firmware triggers an update of all members and their controlled APs, ensuring that the entire network is running the same firmware. The synchronization of firmware between controllers and APs alleviates any potential issue regarding software compatibility between deployed devices.

Seamless mobility

The Mobility traffic manager (MTM) feature provides for seamless roaming of wireless users, while at the same time giving you complete control over how wireless user traffic is distributed onto the wired networking infrastructure. MTM enables you to implement a wireless networking solution using both centralized and distributed strategies. Some of the deployment strategies that you can use with MTM include:

- **Centralized wireless traffic:** All traffic from wireless users is tunneled back to a central controller where it is egressed onto the wired infrastructure. Wireless users can be connected to any AP within the layer 3 network serviced by MTM.

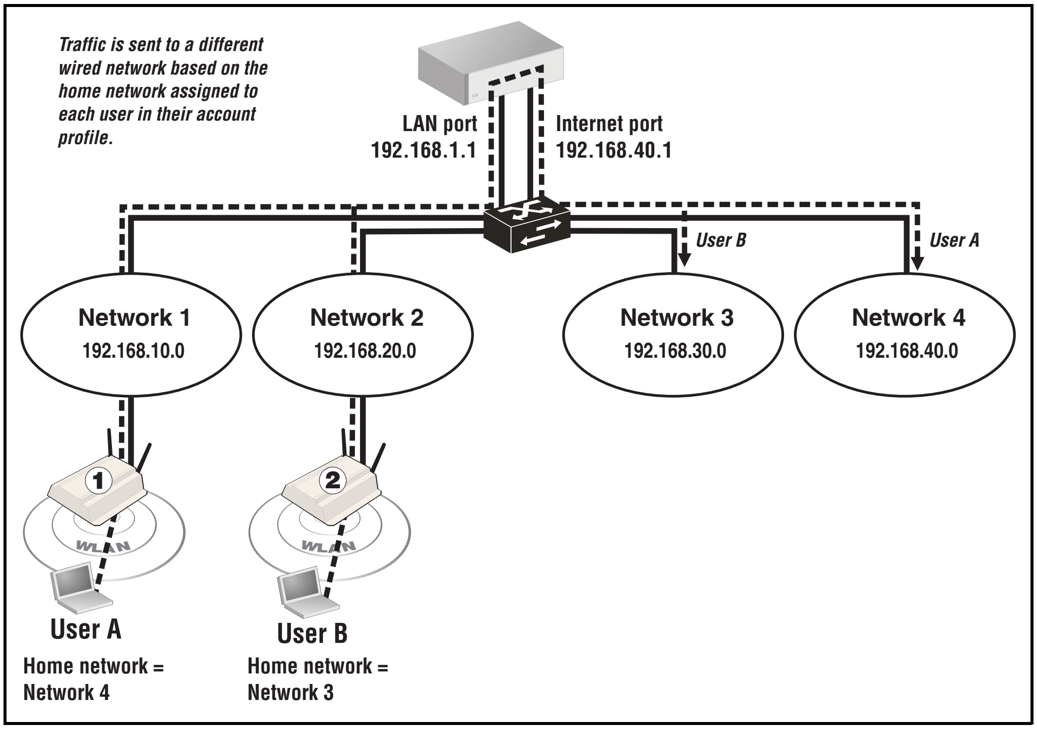
  The following diagram shows a deployment where all wireless traffic is egressed onto a specific network segment (192.168.30.0).



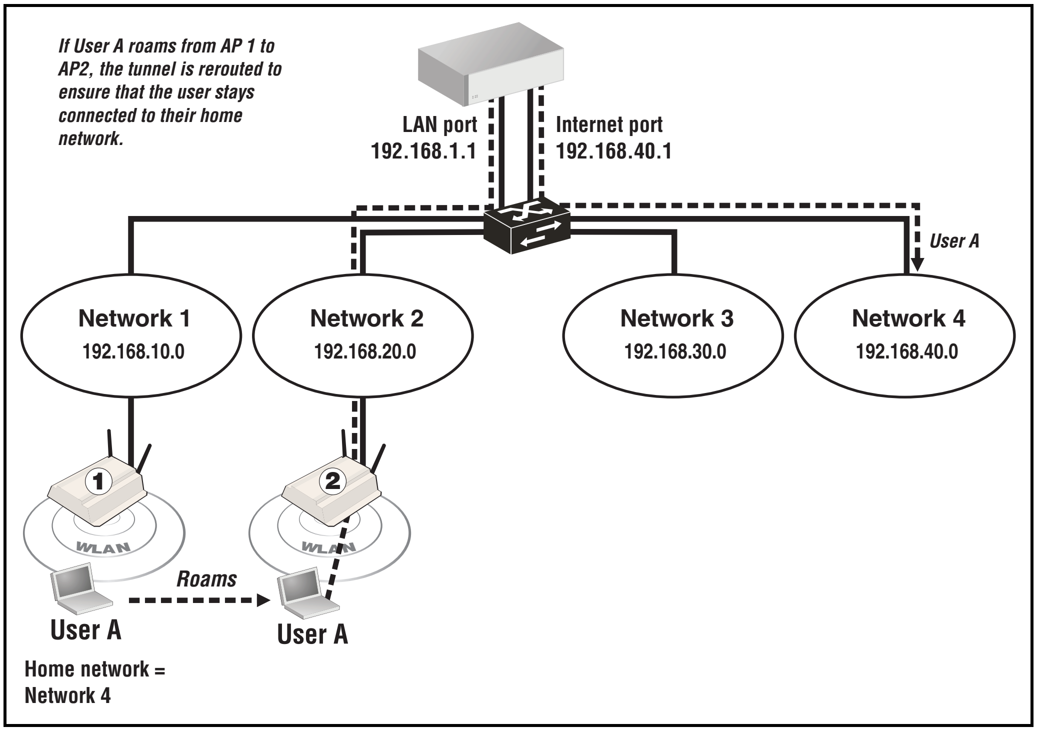
  MTM can also be used to send traffic to different networks or VLANs based on criteria such as username, network location, VSC, or AP group.

- **Traffic distribution using home networks:** A home network can be assigned to each wireless user (via RADIUS, local user accounts, or through a VSC egress). MTM can then be used to tunnel the user’s traffic to their home network, regardless of the AP to which a user connects within the mobility domain.

The following diagram shows a deployment where the wireless traffic for each user is egressed onto a specific network segment by assigning a home network to each user.



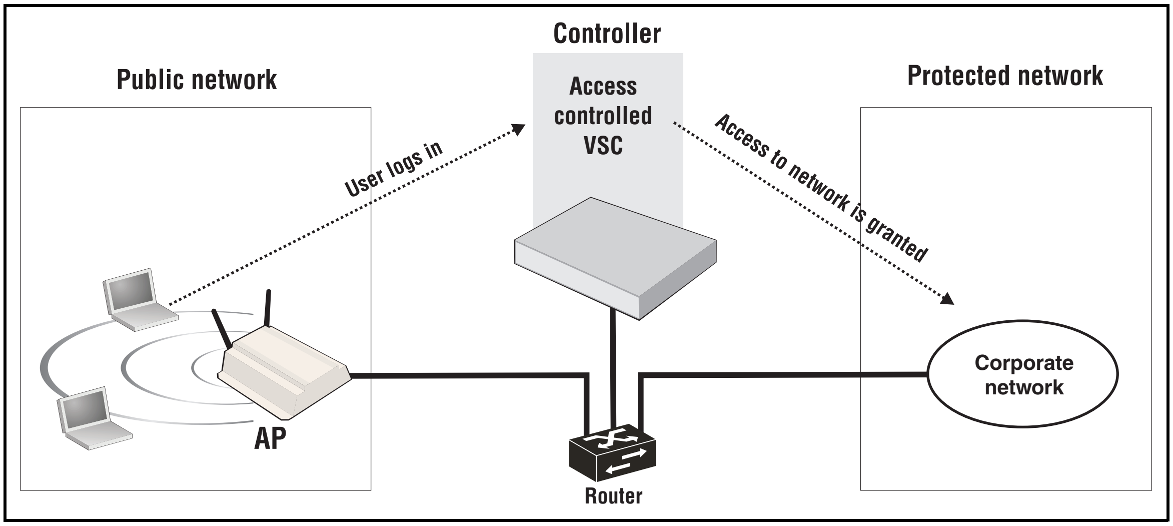
If a user roams between APs, MTM adjusts the tunnel to maintain the user's connection to their home network.



Best-in-class public/guest network access service

Designed to deliver the best possible user experience, the public/guest network access feature adapts to any client device IP address and Web proxy settings, enabling users to connect without reconfiguring their computers.

The public access interface Web pages are fully customizable enabling service providers to create a centrally-managed hotspot network with customized look-and-feel.



Safety information

Warning

Professional Installation Required

Prior to installing or using a controller, consult with a professional installer trained in RF installation and knowledgeable in local regulations including building and wiring codes, safety, channel, power, indoor/outdoor restrictions, and license requirements for the intended country. It is the responsibility of the end user to ensure that installation and use comply with local safety and radio regulations.

Cabling: You must use the appropriate cables, and where applicable, surge protection, for your given region. For compliance with EN55022 Class-B emissions requirements use shielded Ethernet cables.

Country of use: In some regions, you are prompted to select the country of use during setup. Once the country has been set, the controller will automatically limit the available wireless channels, ensuring compliant operation in the selected country. Entering the incorrect country may result in illegal operation and may cause harmful interference to other systems.

Safety: Take note of the following safety information during installation:

- If your network covers an area served by more than one power distribution system, be sure all safety grounds are securely interconnected.
- Network cables may occasionally be subject to hazardous transient voltages (caused by lightning or disturbances in the electrical power grid).
- Handle exposed metal components of the network with caution.
- The MSM7xx Controller and all directly-connected equipment must be installed indoors within the same building (except for outdoor models / antennas), including all PoE-powered network connections as described by Environment A of the IEEE 802.3af standard.

Servicing

There are no user-serviceable parts inside HP MSM7xx products. Any servicing, adjustment, maintenance, or repair must be performed only by trained service personnel.

HP support

For support information, visit www.hp.com/networking/support and for **Product Brand**, select **ProCurve**. Additionally, your HP-authorized networking products reseller can provide you with assistance.

Before contacting support

To make the support process most efficient, before calling your networking dealer or HP Support, you first should collect the following information:

Collect this information	Where to find it
Product identification.	On the rear of the product.
Software version.	The product management tool **Login** page.
Network topology map, including the addresses assigned to all relevant devices.	Your network administrator.

Getting started

Get started by following the directions in the relevant guide as follows:

Product	Guide to use
MSM710, MSM730, MSM750	The provided *Quickstart*.
MSM760, MSM765zl	The provided *Installation and Getting Started Guide*.

Then continue with the next chapter of this guide.

Online documentation

For the latest documentation, visit www.hp.com/networking/support and for **Product Brand**, select **ProCurve**.

Note

The MSM317 Access Device consists of both a controlled-mode-only access point and an integrated Ethernet switch. Where appropriate, this guide makes reference to the *MSM317 Installation and Getting Started Guide* which must be used in conjunction with this guide when working with the MSM317.

2

Management

Contents

Management tool

The management tool is a Web-based interface to the controller that provides easy access to all configuration and monitoring functions.

Management scenarios

For complete flexibility, you can manage the controller both locally and remotely. The following management scenarios are supported:

- Local management using a computer that is connected to the LAN or Internet port on the controller. This may be a direct connection or through a switch.
- Remote management via the Internet with or without a VPN connection. See *Securing controller communications to remote VPN servers on page 16-6* for more information on using the controller integrated VPN clients to create secure remote connections.

Management station

The *management station* refers to the computer that a manager or operator uses to connect to the management tool. To act as a management station, a computer must:

- Have at least Microsoft Internet Explorer 7/8 or Firefox 3.*x*.
- Be able to establish an IP connection with the controller.

Note

Before installation, ensure that TCP/IP is installed and configured on the management station. IP addressing can be either static or DHCP.

Starting the management tool

To launch the management tool, specify the following in the address bar of your browser:

```
https://Controller_IP_address
```

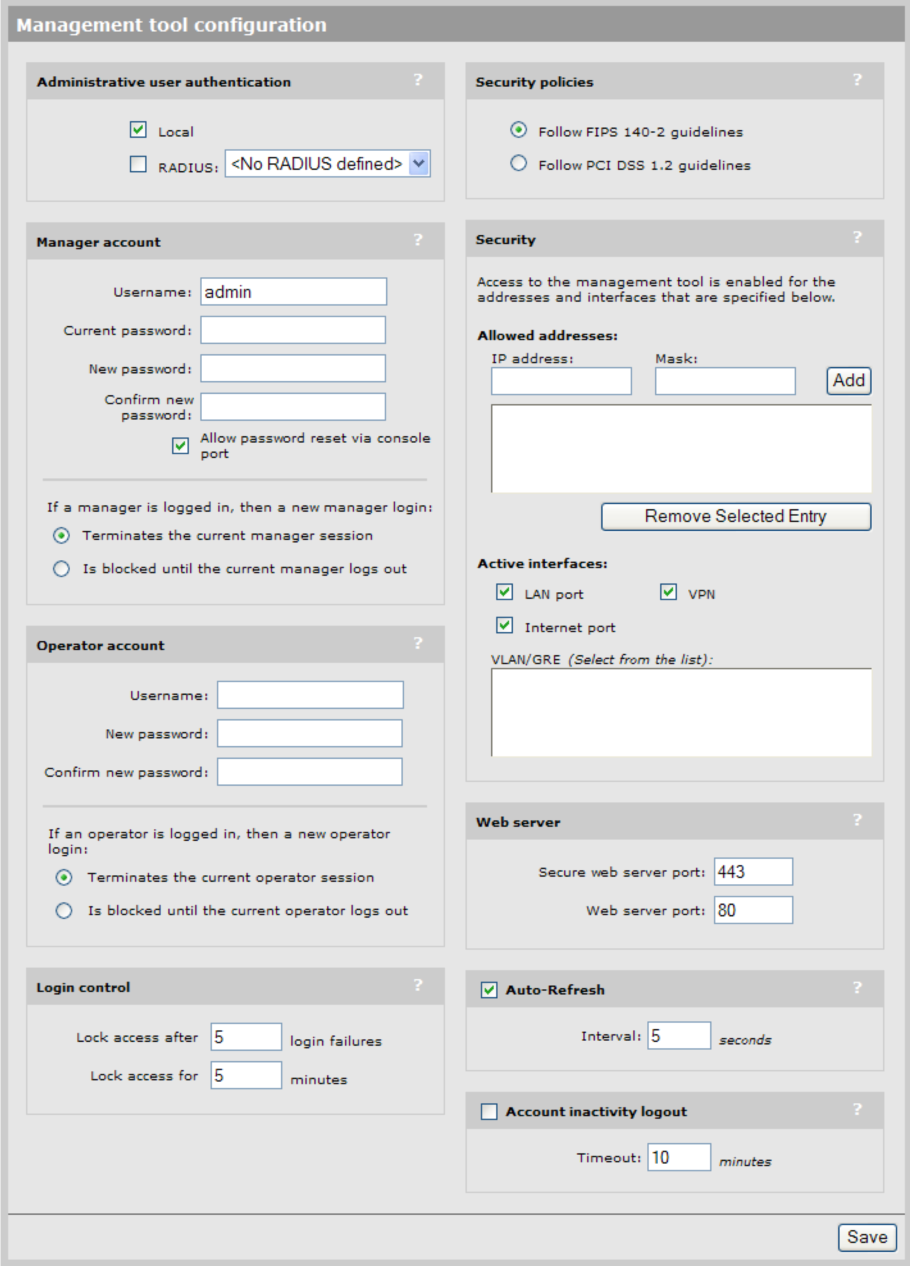
By default, the address 192.168.1.1 is assigned to the LAN port on the controller. For information on starting the management tool for the first time, see the relevant guide as described in *Getting started on page 1-13*.

About passwords

The default username and password is **admin**. New passwords must be 6 to 16 printable ASCII characters in length with at least 4 different characters. Passwords are case sensitive. Space characters and double quotes (“) cannot be used. Passwords must also conform to the selected security policy as described in *Password security policies on page 2-7*.

Customizing management tool settings

To customize management tool settings, select **Controller >> Management > Management tool**.



Management tool configuration

Administrative user authentication

☑ Local

□ RADIUS: <No RADIUS defined>

Manager account

Username: admin

Current password:

New password:

Confirm new password:

☑ Allow password reset via console port

If a manager is logged in, then a new manager login:

● Terminates the current manager session

○ Is blocked until the current manager logs out

Operator account

Username:

New password:

Confirm new password:

If an operator is logged in, then a new operator login:

● Terminates the current operator session

○ Is blocked until the current operator logs out

Login control

Lock access after 5 login failures

Lock access for 5 minutes

Security policies

● Follow FIPS 140-2 guidelines

○ Follow PCI DSS 1.2 guidelines

Security

Access to the management tool is enabled for the addresses and interfaces that are specified below.

Allowed addresses:

IP address:

Mask:

Active interfaces:

☑ LAN port ☑ VPN

☑ Internet port

VLAN/GRE *(Select from the list)*:

Web server

Secure web server port: 443

Web server port: 80

☑ Auto-Refresh

Interval: 5 *seconds*

□ Account inactivity logout

Timeout: 10 *minutes*

Administrative user authentication

Login credentials for administrative users can be verified using local account settings and/or an external RADIUS sever.

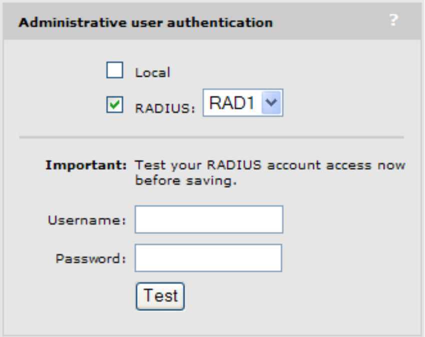
- **Local account settings:** A single manager and operator account can be configured locally under **Manager account** and **Operator account** on this page.
- **RADIUS server:** Using a RADIUS server enables you to have multiple accounts, each with a unique login name and password. Identify manager accounts using the vendor specific attribute **web-administrative-role**. Valid values for this attribute are **Manager** and **Operator**. For attribute information, see *Administrator attributes on page 15-31*. To use a RADIUS server, you must define a RADIUS profile on the **Controller >> Authentication > RADIUS profiles** page.

If both options are enabled, the RADIUS server is always checked first.

Authenticating administrative credentials using an external RADIUS server

Configure RADIUS authentication as follows:

1. Define an account for the administrator on the RADIUS server. See *Administrator attributes on page 15-31*.
2. On the controller, create a RADIUS profile that will connect the controller to the RADIUS server. See *Configuring a RADIUS server profile on the controller on page 11-6*.
3. Under **Administrator authentication**, set **Authenticate via** to the RADIUS profile you created. In this example, the profile is called **Rad1**.



Administrative user authentication

☐ Local

☑ RADIUS: RAD1

Important: Test your RADIUS account access now before saving.

Username:

Password:

4. Test the RADIUS account to make sure it is working before you save your changes. Specify the appropriate username and password and select **Test**.

   (As a backup measure you can choose to enable **Local.** This will allow you to log in using the local account if the connection to the RADIUS server is unavailable.)

Manager and Operator accounts

Two types of administrative accounts are defined: manager and operator.

- The manager account provides full management tool rights.
- The operator account provides read-only rights plus the ability to disconnect wireless clients and perform troubleshooting.

Only one administrator (manager or operator) can be logged in at any given time. Options are provided to control what happens when an administrator attempts to log in while another administrator (or the same administrator in a different session) in already logged in. In every case, the manager's rights supersede those of an operator.

The following options can be used to prevent the management tool from being locked by an idle manager or operator:

- **Terminates the current manager session:** When enabled, an active manager or operator session will be terminated by the login of another manager. This prevents the management tool from being locked by an idle session until the **Account inactivity logout** timeout expires.
- **Is blocked until the current manager logs out:** When enabled, access to the management tool is blocked until an existing manager logs out or is automatically logged out due to an idle session.

  An operator session is always terminated if a manager logs in. An active operator session cannot block a manager from logging in.
- **Terminates the current operator session:** When enabled, an active operator's session will be terminated by the login of another operator. This prevents the management tool from being locked by an idle session until the **Account inactivity logout** timeout expires.

  Operator access to the management tool is blocked if a manager is logged in. An active manager session cannot be terminated by the login of an operator.

  An operator session is always terminated if a manager logs in. An active operator session cannot block a manager from logging in.
- **Login control:** If login to the management tool fails five times in a row (bad username and/or password), login privileges are blocked for five minutes. Once five minutes expires, login privileges are once again enabled. However, if the next login attempt fails, privileges are again suspended for five minutes. This cycle continues until a valid login occurs. You can configure the number of failures and the timeout.
- **Account inactivity logout:** By default, if a connection to the management tool remains idle for more than ten minutes, the controller automatically terminates the session. You can configure the timeout.

Passwords

Passwords must be 6 to 16 printable ASCII characters in length with at least 4 different characters. Passwords are case sensitive. Space characters and double quotes (“) cannot be used. Passwords must also conform to the selected security policy as described below.

Manager username/password reset

Not supported on the MSM-765.

The **Allow password reset via console port** feature provides a secure way to reset the manager login username/password on a controller to factory default values (**admin/admin**), without having to reset the entire controller configuration to its factory default settings. To make use of this feature you must be able to access the controller through its console (serial) port. See *Appendix B: Console ports*.

Important

- This feature is automatically **enabled** after performing a reset to factory default settings.
- This feature is automatically **disabled** after performing a software (firmware) upgrade.

Caution

If you disable this feature and then forget the manager username or password, the only way to gain access the management tool is to reset the controller to its factory default settings. See *Appendix C: Resetting to factory defaults*.

To reset manager credentials on a controller

1. Connect a serial cable from the serial port on your computer to the console port on the controller. (See *Appendix B: Console ports* for information on building a serial cable to connect to your controller.)
2. Configure VT-100 terminal-emulation software on your computer as follows:
   - VT-100 (ANSI) terminal
   - Baud rate of 9600
   - 8 data bits, 1 stop bit, no parity, and no flow control
   - If on Windows, disable the **Use Function, Arrow, and Ctrl Keys for Windows** options.
   - For the Hilgrave HyperTerminal program, select the **Terminal keys** option for the **Function, arrow, and ctrl keys act as** parameter.
3. Open an appropriately-configured terminal session.
4. Power on the controller and wait for the **login** prompt to appear.
5. Type **emergency** and press **Enter**.
6. Type **1** and press **Enter** to reset the manager username and password.

A typical session looks like this:

```
127.0.0.1 login: emergency


--------------------------
      Emergency Menu
--------------------------

  Device information

   Serial number: SG9603P004
       IP address: 16.90.48.186


Select one of the following options:

  1. Reset both the manager username and password to "admin"

  0. Exit

Selection: 1

Trying to reset manager login credentials....

Manager login credentials were successfully reset to:
Username = admin
Password = admin

Press any key to continue.
```

Password security policies

Security policies affect both manager and operator accounts. Select from one of the following options:

- **Follow FIPS 140-2 guidelines:** When selected, implements the following requirements from the FIPS 140-2 guidelines:
  - All administrator passwords must be at least six characters long.
  - All administrator passwords must contain at least four different characters.

  For more information on these guidelines, refer to the *Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules*.
- **Follow PCI DSS 1.2 guidelines:** When selected, implements the following requirements from the PCI DSS 1.2 guidelines:
  - All administrator passwords must be at least seven characters long.
  - All administrator passwords must contain both numeric and alphabetic characters.
  - The settings under **Login control** must be configured as follows:
    - **Lock access after *nn* login failures** must be set to 6 or less.
    - **Lock access for *nn* minutes** must be set to 30 minutes or more.

- The settings under **Account inactivity logout** must be configured as follows:
  - **Timeout** must be set to 15 minutes or less.

For more information on these guidelines, refer to the Payment Card Industry Data Security Standard v1.2 document.

Management tool security features

The management tool is protected by the following security features:

- **Allowed addresses:** You can configure a list of subnets from which access to the management tool is permitted.
- **Active interfaces:** You can enable or disable access to the management tool for each of the following:
  - LAN port
  - Internet port
  - VPN
  - VLAN/GRE.

  These settings also apply when SSH is used to access the command line interface.

Note Changing the security settings may cause you to lose your connection to the management tool.

Web server

You can also configure the Web server ports from which access to the management tool is permitted.

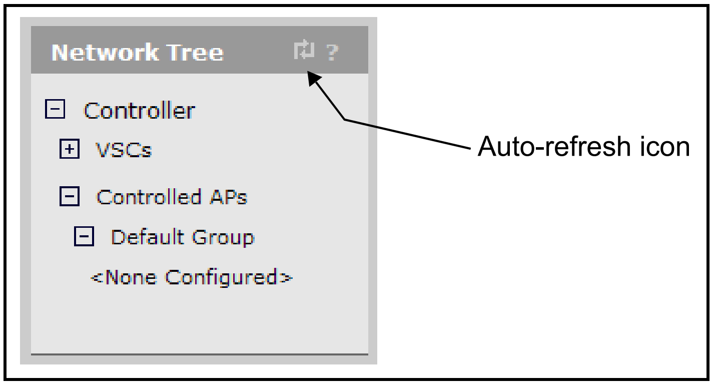
- **Secure web server port**: Specify a port number for the controller to use to provide secure HTTPS access to the management tool**.** Default is 443. Before reaching the management tool login page**,** you must accept a security certificate. The default certificate provided with the controller will trigger a warning message on most browsers because it is self-signed. To remove this warning message, you must replace the default certificate. See *About certificate warnings on page 12-10*.

Note Changing the secure web server port will cause you to lose your connection to the management tool. To reconnect, you will need to specify the following address: https://*Controller_IP_address*:*web_server_Port_number*.

- **Web server port**: Specify a port number for the controller to use to provide standard HTTP access to the management tool**.** These connections are met with a warning, and the browser is redirected to the secure Web server port. Default is 80.

Auto-refresh

This option controls how often the controller updates the information in group boxes that show the auto-refresh icon in their title bar. Under **Interval,** specify the number of seconds between refreshes.



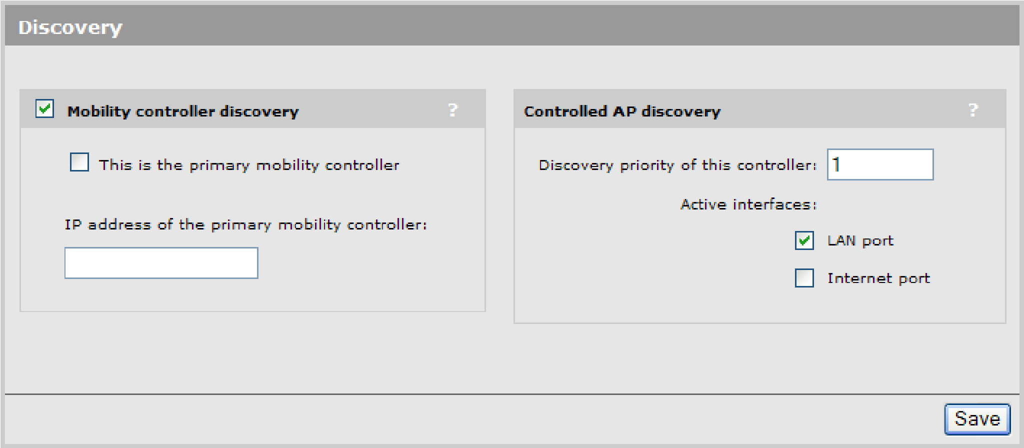
Device discovery

Use this page to define discovery options for:

- Inter-controller discovery when using the wireless mobility feature (*Chapter 9: Mobility traffic manager*)
- Controller discovery by controlled APs (*Chapter 6: Working with controlled APs*)

Select **Controller >> Management > Device discovery** to open the Discovery configuration page.

On a non-teamed controller



Discovery

☑ Mobility controller discovery ?

☐ This is the primary mobility controller

IP address of the primary mobility controller:

Controlled AP discovery ?

Discovery priority of this controller: 1

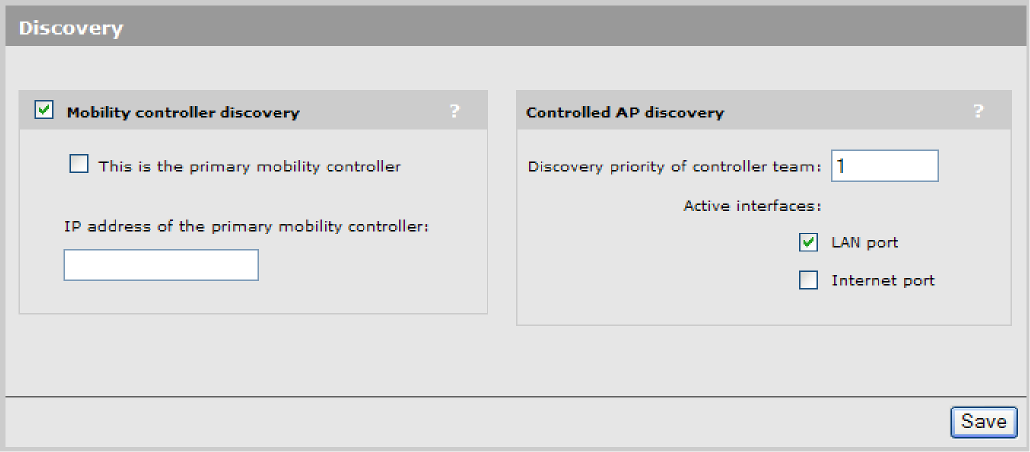
Active interfaces:

☑ LAN port

☐ Internet port

Save

On a controller team



☑ Mobility controller discovery

☐ This is the primary mobility controller

IP address of the primary mobility controller:

Controlled AP discovery

Discovery priority of controller team: 1

Active interfaces:

☑ LAN port

☐ Internet port

Mobility controller discovery

The wireless mobility feature defines a mobility domain, which is an interconnection between multiple controllers for the purpose of exchanging mobility information on wireless users. For more information, see *Chapter 9: Mobility traffic manager*.

For the controllers to interconnect, each must have the **Mobility controller discovery** option enabled. In addition, one controller must be defined as the primary mobility controller. It acts as the central site for distribution of mobility information.

There can only be one primary controller for each mobility domain. On all other controllers set **IP address of primary controller** to the IP address of the primary controller.

Note

- All controllers in the mobility domain must be running the same software version. This means that the first two numbers in the software revision must be the same. For example: All controllers running 5.4.x, or all controllers running 5.5.x.
- Discovery automatically takes place on both the LAN port and Internet port. **VLANs are not supported.**

Network requirements

The network that interconnects the controllers and APs that make up a mobility domain must not block any of the following ports/protocols:

- UDP port 1194
- UDP port 12141
- UDP port 3000
- UDP port 3001
- UDP port 3518
- TCP port 5432
- Internet protocol number 47 (GRE)

Controller discovery and teaming

When teaming is active, several configuration scenarios are possible:

- **Teamed controllers operating in conjunction with one or more non-teamed controllers:** Set the team as the primary mobility controller. On the other controllers, set the **IP address of primary mobility controller** parameter to the team IP address.
- **A single team of controllers:** Enable the **This is the primary mobility controller** option on the team manager.
- **Multiple teamed and non-teamed controllers:** Set one team as the primary mobility controller. On the other teams and controllers, set the **IP address of primary mobility controller** parameter to the team IP address of the primary mobility controller.

This is the primary mobility controller

Enable this option to designate this controller as the primary mobility controller. The primary controller is responsible for the coordination and discovery of all other controllers in the mobility domain.

IP address of primary mobility controller

Enter the IP address of the primary mobility controller.

Controlled AP discovery

Discovery priority of this controller
Discovery priority of controller team

Sets the priority for this controller or team when discovered by a controlled AP. A value of 1 indicates the highest priority. A value of 16 indicates the lowest priority.

If multiple controllers or teams are discovered by a controlled AP, the AP will establish a control channel with the controller or team that has the highest priority setting first. If that controller or team is already managing the maximum number of controlled APs, the AP will choose the controller or team with the next highest priority.

Each controller or team must have a different priority setting, otherwise AP discovery will fail with the diagnostic **Priority conflict**. See *Viewing all discovered APs on page 6-14*.

See *Discovery of controllers by controlled APs on page 6-6* for more detailed information on the discovery process.

Important note when your network also contains controller teams
Non-teamed controllers are always higher priority than controller teams. Therefore, if your network contains both controller teams and non-teamed controllers, APs first attempt to establish a secure management tunnel with discovered non-teamed controllers in order of their discovery priority. Only if all non-teamed controllers are already managing the maximum number of controlled APs will the AP then consider controller teams in the order of their priority.

The following table shows how discovery would occur for several teamed and non-teamed controllers.

Controller or Team	Configured discovery priority setting	Actual order of discovery by APs
Controller 1	1	1
Controller 2	2	2
Controller 3	3	3
Team 1	1	4
Team 2	2	5
Team 3	3	6

Active interfaces

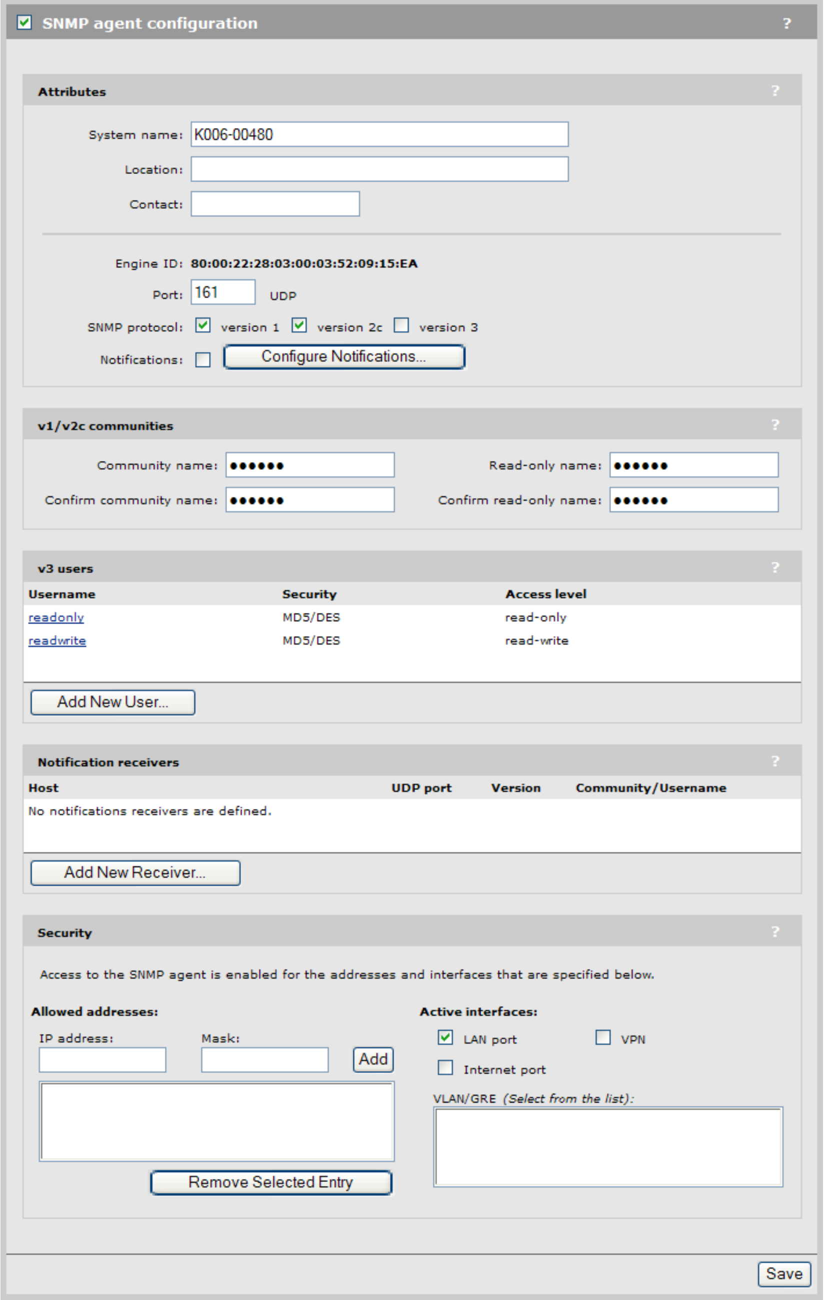
Select the physical interfaces on which the controller or team manager will listen for discovery requests from controlled APs. The control channel to an AP is always established on the interface on which it is discovered.

SNMP

The controller provides a SNMP implementation supporting both industry-standard and custom MIBs. For information on supported MIBs, see the *MSM SNMP MIB Reference Guide*.

Configuring the SNMP agent

Select **Controller >> Management > SNMP** to open the SNMP agent configuration page. By default, the SNMP agent is enabled (**SNMP agent configuration** in title bar is checked) and is active on the LAN port. If you disable the agent, the controller will not respond to SNMP requests.



☑ SNMP agent configuration

Attributes

System name: K006-00480
Location:
Contact:

Engine ID: 80:00:22:28:03:00:03:52:09:15:EA
Port: 161 UDP
SNMP protocol: ☑ version 1 ☑ version 2c □ version 3
Notifications: □ Configure Notifications...

v1/v2c communities

Community name: •••••• Read-only name: ••••••
Confirm community name: •••••• Confirm read-only name: ••••••

v3 users

Username	Security	Access level
readonly	MD5/DES	read-only
readwrite	MD5/DES	read-write

Add New User...

Notification receivers

Host	UDP port	Version	Community/Username
No notifications receivers are defined.			

Add New Receiver...

Security

Access to the SNMP agent is enabled for the addresses and interfaces that are specified below.

Allowed addresses:
IP address: Mask: Add
Remove Selected Entry

Active interfaces:
☑ LAN port □ VPN
□ Internet port
VLAN/GRE *(Select from the list)*:

Save

Attributes

System name
Specify a name to identify the controller. By default, this is set to the serial number of the controller.

Location
Specify a descriptive name for the location where the controller is installed.

Contact
Contact information for the controller.

Port
Specify the UDP port and protocol the controller uses to respond to SNMP requests. Default port is 161.

SNMP protocol
Select the SNMP versions that the controller will support. Default is **Version 1** and **Version 2c**.

Notifications
Select the SNMP versions that the AP will support. Default is **Version 1** and **Version 2c**.

Notifications
When this feature is enabled, the controller sends notifications to the hosts that appear in the **Notifications receivers** list.

The controller supports the following MIB II notifications:

- coldStart
- linkUp
- linkDown
- authenticationFailure

In addition, the controller supports a number of custom notifications. Select **Configure Notifications**. For a descriptions of these notifications, see the online help.

v1/v2 communities

Community name
Specify the password, also known as the read/write name, that controls read/write access to the SNMP agent. A network management program must supply this name when attempting to set or get SNMP information from the controller. By default, this is set to **private**.

Read-only name
This is the password that controls read-only access to the SNMP agent. A network management program must supply this name when attempting to get SNMP information from the controller. By default, this is set to **public**.

v3 users

This table lists all defined SNMP v3 users. To add a new user, select **Add New User**. Up to five users are supported. To edit a user, select its link in the **Username** column.

Username
The SNMP v3 username.

Security
Security protocol defined for the user. Authentication type and encryption type are separated by a slash. For example, **MD5/DES** indicates **MD5** authentication and **DES** encryption.

Access level
Type of access assigned to the user:

- **Read-only:** The user has read and notify access to all MIB objects.
- **Read-write:** The user has read, write, and notify access to all MIB objects.

Notification receivers

This table lists all defined SNMP notification receivers. SNMP notifications are sent to all receivers in this list. To add a new receiver, select **Add New Receiver**. Up to five receivers are supported. To edit a receiver, select its link in the **Host** column.

Host
The domain name or IP address of the SNMP notifications receiver to which the controller will send notifications.

UDP port
The port on which the controller will send notifications.

Version
The SNMP version (1, 2c, 3) for which this receiver is configured.

Community/Username

- For SNMP v1 and v2c, the SNMP Community name of the receiver.
- For SNMP v3, the SNMP v3 Username of the receiver.

Security

Use these settings to control access to the SNMP interface.

- **Allowed addresses**: List of IP address from which access to the SNMP interface is permitted. To add an entry, specify the **IP address** and appropriate **Mask**, and then select **Add.**

  When the list is empty, access is permitted from any IP address.

- **Active interfaces**: Enable the checkboxes that correspond to the interfaces from which to allow access to the SNMP agent. For VLAN, GRE, or Mesh, select from the list. Use Ctrl-click to select multiple objects.

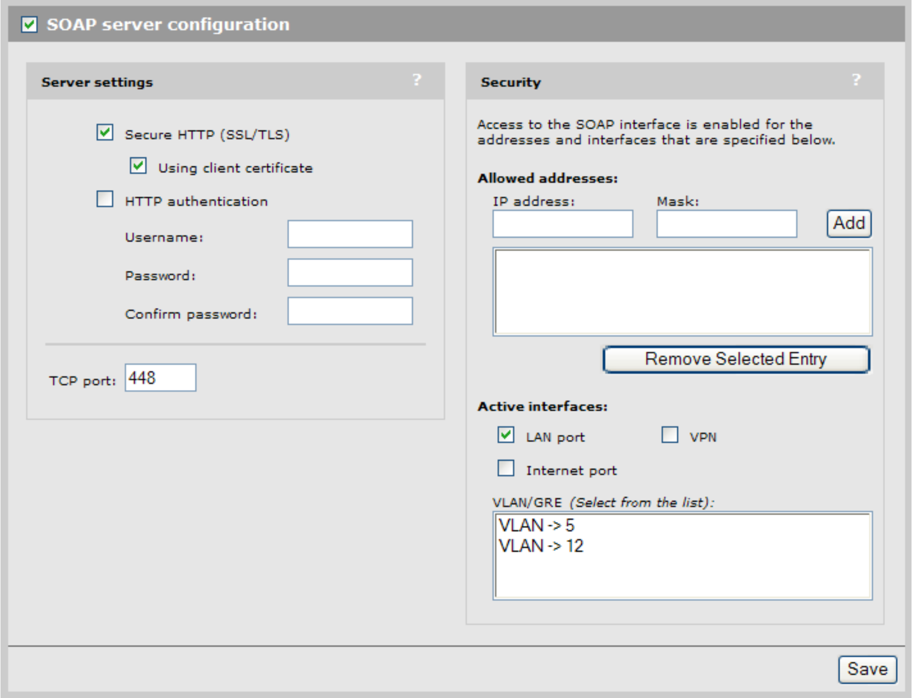
SOAP

The controller provides a SOAP interface that can be used by SOAP-compliant client applications to perform configuration and management tasks.

An MSM SOAP/XML SDK zip file is available at www.hp.com/networking/SOAP-XML-SDK. Look for the file corresponding to your MSM software version.

Configuring the SOAP server

Select **Controller >> Management > SOAP** to open the SOAP server configuration page. By default, the SOAP server is enabled (**SOAP server configuration** in title bar is checked).



☑ **SOAP server configuration**

Server settings

☑ Secure HTTP (SSL/TLS)

☑ Using client certificate

□ HTTP authentication

Username:

Password:

Confirm password:

TCP port: 448

Security

Access to the SOAP interface is enabled for the addresses and interfaces that are specified below.

Allowed addresses:

IP address: Mask:

Active interfaces:

☑ LAN port □ VPN

□ Internet port

VLAN/GRE *(Select from the list)*:

VLAN -> 5
VLAN -> 12

Server settings

Secure HTTP (SSL/TLS)

Enable this option to configure the SOAP server for SSL/TLS mode. When enabled, the Secure Sockets Layer (SSL) protocol must be used to access the SOAP interface.

Using client certificate

When enabled, the use of an X.509 client certificate is mandatory for SOAP clients.

HTTP authentication

When enabled, access to the SOAP interface is available via HTTP with the specified username and password.

TCP port

Specify the number of the TCP port that SOAP uses to communicate with remote applications. Default is 448.

Security

Use these settings to control access to the SOAP interface.

- **Allowed addresses**: List of IP address from which access to the SOAP interface is permitted. To add an entry, specify the **IP address** and appropriate **Mask**, and then select **Add.**

  When the list is empty, access is permitted from any IP address.

- **Active interfaces**: Enable the checkboxes that correspond to the interfaces from which to allow access to the SOAP interface.

Security considerations

- The SOAP server is configured for SSL/TLS mode, and the use of an X.509 client certificate is mandatory for SOAP clients.
- The SOAP server is configured to trust all client certificates signed by the default SOAP CA installed on the controller.
- Users should generate and install their own SOAP CA private key/public key certificate to protect their devices from unauthorized access. This is important because the default SOAP CA and a valid client certificate are provided as an example to all customers. (See *Working with certificates on page 12-5*.)

CLI

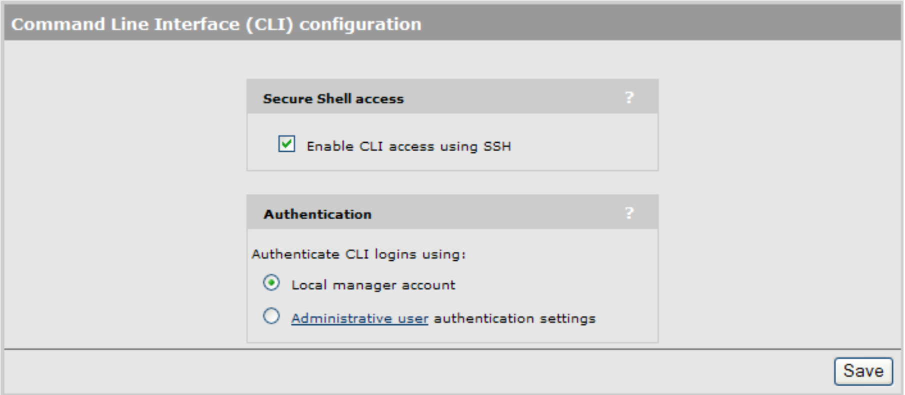
The controller provides a command line interface that can be used to perform configuration and management tasks via the serial port or an IP connection on any of the controller interfaces, including the LAN port, Internet port, or VPN/GRE tunnel.

For information on using the CLI, see the *CLI Reference Guide*.

A maximum of three concurrent CLI sessions are supported regardless of the connection type.

Configuring CLI support

Select **Controller >> Management > CLI** to open the Command Line Interface (CLI) configuration page.



Command Line Interface (CLI) configuration

Secure Shell access

☑ Enable CLI access using SSH

Authentication

Authenticate CLI logins using:

● Local manager account

○ Administrative user authentication settings

Secure shell access

Enable this option to allow access to the CLI via an SSH session. The CLI supports SSH on the standard TCP port (22).

SSH connections to the CLI can be made on any active interface. Support for each interface must be explicitly enabled under **Security.**

Lockout

After 10 unsuccessful login attempts via SSH, login to the CLI is locked for 5 minutes. After the lockout expires, each subsequent unsuccessful login attempt re-activates the lockout period. This behavior repeats until a successful login is completed.

Note Depending on your SSH configuration, your client may make several login attempts with each connection attempt.

Supported clients

The following SSH clients have been tested with the CLI. Others may work as well:

- OpenSSH
- Tectia
- SecureCRT
- Putty

Authenticate CLI logins using

The CLI validates login credentials (username and password) using the settings defined on the **Controller >> Management > Management tool** page.

Local manager account

The login username and password are the same as those defined for the **local manager account**. If this account is disabled, the last known username and password for this account are used.

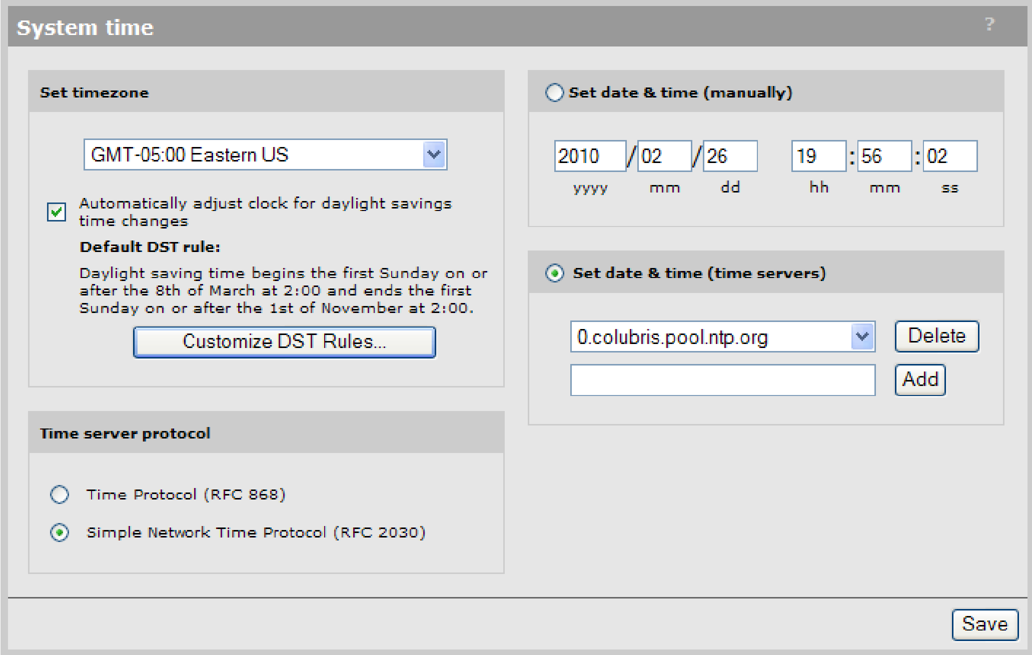
Administrative user authentication settings

The login username and password use the same settings (**Local** and/or **RADIUS**) as defined for the manager account under **Administrative user authentication**.

System time

Select **Controller >> Management > System time** to open the **System time** page. This page enables you to configure the time server and set time zone information.

Note The system time page on the MSM765zl is a read-only page that displays the current time configured on the chassis. This may or may not be the current time.



System time

Set timezone

GMT-05:00 Eastern US

☑ Automatically adjust clock for daylight savings time changes

Default DST rule:

Daylight saving time begins the first Sunday on or after the 8th of March at 2:00 and ends the first Sunday on or after the 1st of November at 2:00.

Time server protocol

○ Time Protocol (RFC 868)

● Simple Network Time Protocol (RFC 2030)

○ **Set date & time (manually)**

2010 / 02 / 26 19 : 56 : 02
yyyy mm dd hh mm ss

● **Set date & time (time servers)**

0.colubris.pool.ntp.org

Note Setting the correct time is important when the controller is managing controlled APs, as the time configured on the controller is used on all controlled APs. Synchronization and certificate problems can occur if the controller time is not accurate.

Note Correct time is also important when the controller is using Active Directory to authenticate users.

Set timezone

Select the time zone in which the controller is located. If you change the time zone setting, the new value does not take effect until you restart the controller.

Automatically adjust clock for daylight savings time changes
Enable this option to automatically update the clock based on the specified daylight savings time (DST) rule.

- **Default DST rule:** This is the currently active daylight savings time rule.
- **Customize DST rules:** Select this button to define your own DST rule.

Time server protocol

Select the protocol that will be used to communicate with the time server.

Set date and time (manually)

Use this option to manually set the system date and time.

Set date and time (time servers)

Select this option to have the controller periodically contact a network time server to update its internal clock. By default, the list contains two ntp vendor zone pools that are reserved for HP devices. By using these pools, you will get better service and keep from overloading the standard ntp.org server. For more information refer to: pool.ntp.org.

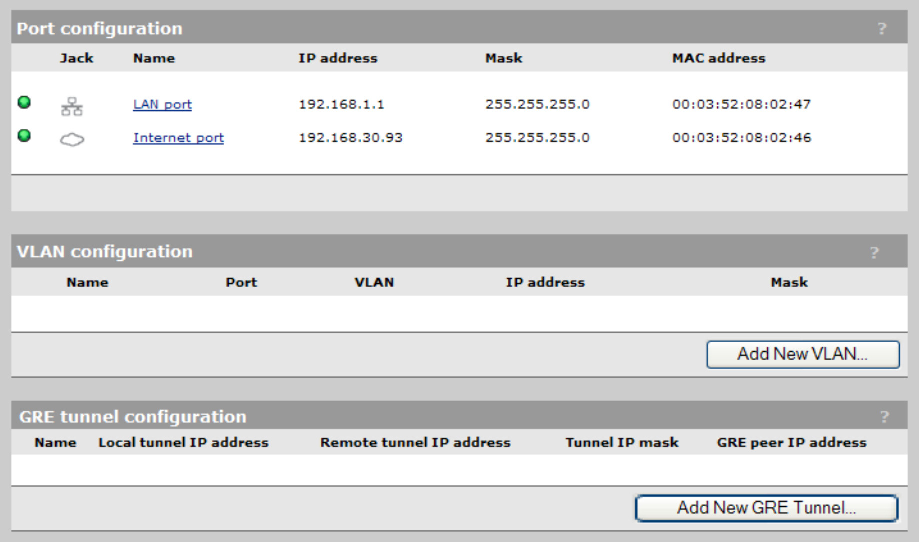
3

Network configuration

Contents

Port configuration

The **Port configuration** page displays summary information about all ports, VLANs, and GRE tunnels. Open this page by selecting **Controller >> Network > Ports**.



Port configuration

	Jack	Name	IP address	Mask	MAC address
●		LAN port	192.168.1.1	255.255.255.0	00:03:52:08:02:47
●		Internet port	192.168.30.93	255.255.255.0	00:03:52:08:02:46

VLAN configuration

Name	Port	VLAN	IP address	Mask

GRE tunnel configuration

Name	Local tunnel IP address	Remote tunnel IP address	Tunnel IP mask	GRE peer IP address

Port configuration information

- **Status indicator:** Operational state of each port, as follows:
  - **Green:** Port is properly configured and ready to send and receive data.
  - **Red:** Port is not properly configured or is disabled.
- **Name**: Identifier for the port. To configure a port, select its name.
- **IP address**: IP addresses assigned to the port. An address of **0.0.0.0** means that no address is assigned.
- **Mask**: Subnet mask for the IP address.
- **MAC address**: MAC address of the port.

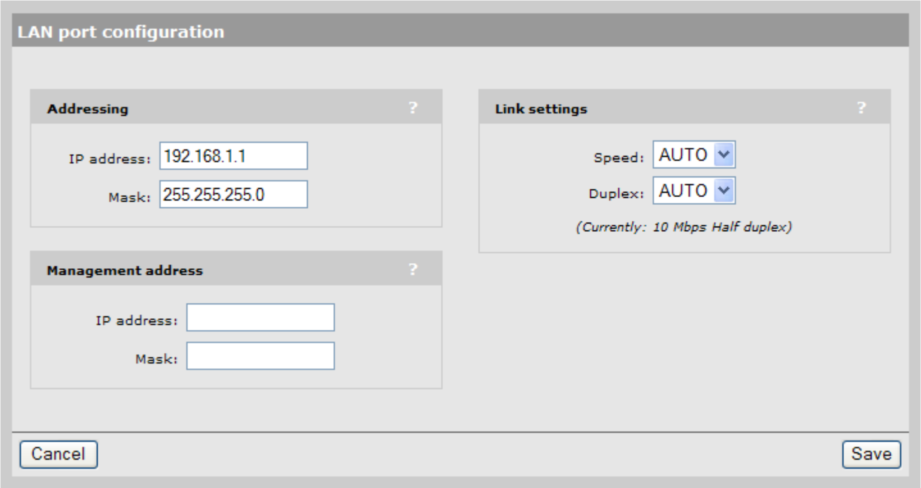
Default port settings

By default, ports are configured as follows:

Port	Default IP address	Default DHCP server status
LAN	192.168.1.1	Disabled.
Internet	DHCP client	This feature is not available on the Internet port.

LAN port configuration

The LAN port is used to connect the controller to a wired network. To verify and possibly adjust LAN port configuration, select **Controller >> Network > Ports > LAN port**.



LAN port configuration

Addressing

IP address: 192.168.1.1

Mask: 255.255.255.0

Management address

IP address:

Mask:

Link settings

Speed: AUTO

Duplex: AUTO

(Currently: 10 Mbps Half duplex)

Addressing options

The LAN port must be configured with a static IP address, because the controller cannot function as a DHCP client on the LAN port. By default it is set to the address 192.168.1.1

For information on configuring address allocation on the LAN port via DHCP server or DHCP relay agent, see *Address allocation on page 3-13*.

Management address

Use this option to assign a second IP address to the LAN port. This address provides a simple way to separate management traffic from user traffic without using VLANs.

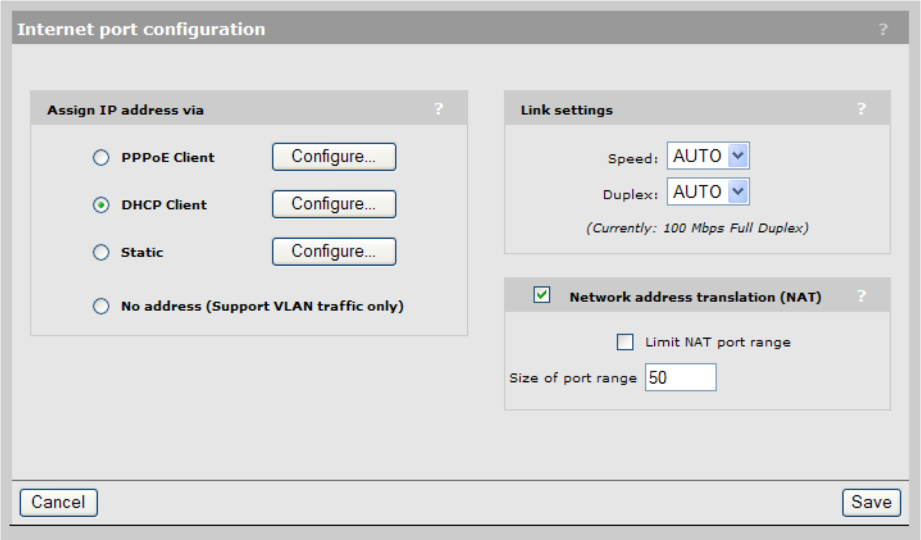
For example, by default the LAN port is set to 192.168.1.1 and all client devices obtain an address on this subnet from the controller's DHCP server. With this feature you can add another address, say 192.168.2.1/255.255.255.0. APs can then be assigned to this subnet using static IP addressing. Now all management traffic exchanged between the controller and the APs is on a separate subnet.

Link settings

By default, the controller automatically adjusts link settings based on the type of equipment the port is connected to. If needed, you can force the port to operate at a particular speed or duplex setting.

Internet port configuration

To verify and possibly adjust Internet port configuration, select **Controller >> Network > Ports > Internet port**.



Internet port configuration

Assign IP address via

○ PPPoE Client

● DHCP Client

○ Static

○ No address (Support VLAN traffic only)

Link settings

Speed: AUTO

Duplex: AUTO

(Currently: 100 Mbps Full Duplex)

☑ Network address translation (NAT)

□ Limit NAT port range

Size of port range 50

Addressing options

The Internet port supports the following addressing options:

- *PPPoE client on page 3-6*
- *DHCP client on page 3-8* (default setting)
- *Static addressing on page 3-9*
- No address.

By default, the Internet port operates as a DHCP client. Select the addressing option that is required by your ISP or network administrator and then select **Configure**.

Link settings

By default, the controller automatically adjusts link settings based on the type of equipment the port is connected to. If needed, you can force the port to operate at a particular speed or duplex setting.

Network address translation

Enable this option to permit all the computers on the network to simultaneously share the connection on the Internet port. See *Network address translation (NAT) on page 3-30*.

Limit NAT port range

When enabled, the controller reserves a range of TCP and UDP ports for each authenticated, access-controlled user starting at port 5000, and maps all outgoing traffic for the user within the range.

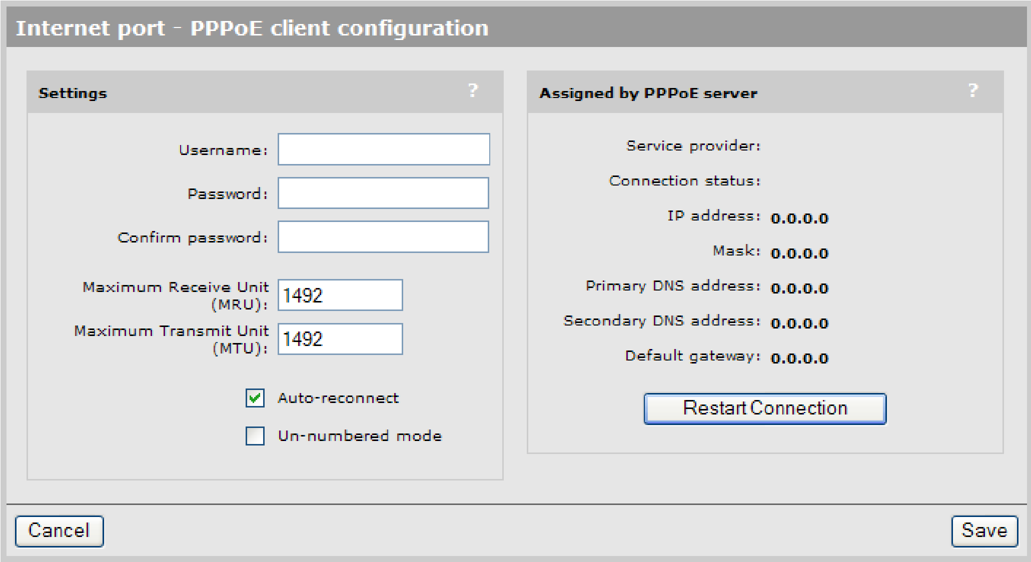
Note If you enable this feature you should not assign static NAT mappings in the range 5000 to 10000.

Size of port range

Sets the number of TCP and UDP ports reserved for each user.

PPPoE client

To configure the PPPoE client on the Internet port, select **Controller >> Network > Ports** and then select **PPPoE** and then **Configure.**



Internet port - PPPoE client configuration

Settings ?

Username:
Password:
Confirm password:
Maximum Receive Unit (MRU): 1492
Maximum Transmit Unit (MTU): 1492
☑ Auto-reconnect
☐ Un-numbered mode

Assigned by PPPoE server ?

Service provider:
Connection status:
IP address: 0.0.0.0
Mask: 0.0.0.0
Primary DNS address: 0.0.0.0
Secondary DNS address: 0.0.0.0
Default gateway: 0.0.0.0

Settings

Username

Specify the username assigned to you by your ISP. The controller will use this username to log on to your ISP when establishing a PPPoE connection.

Password/Confirm password

Specify the password assigned to you by your ISP. The controller will use this password to log on to your ISP when establishing a PPPoE connection.

Maximum Receive Unit (MRU)

Maximum size (in bytes) of a PPPoE packet when receiving. Changes to this parameter only should be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.

Maximum Transmit Unit (MTU)

Maximum size (in bytes) of a PPPoE packet when transmitting. Changes to this parameter should only be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.

Auto-reconnect

The controller will automatically attempt to reconnect if the connection is lost.

Un-numbered mode
This feature is useful when the controller is connected to the Internet and NAT is not being used. Instead of assigning two IP addresses to the controller, one to the Internet port and one to the LAN port, both ports can share a single IP address.

This is especially useful when a limited number of IP addresses are available to you.

Assigned by PPPoE server

These settings are assigned to the controller by your service provider PPPoE server. The Internet connection is not active until this occurs.

Service provider
Identifies your Internet service provider. Not all ISPs provide this information.

Connection status
Indicates the state of the PPPoE connection. If the connection is not active, a message indicates why.

IP address
Identifies the IP address assigned to the controller by the ISP.

Mask
Identifies the subnet mask that corresponds to the assigned IP address.

Primary DNS address
Identifies the IP address of the main DNS server the controller will use to resolve DNS requests.

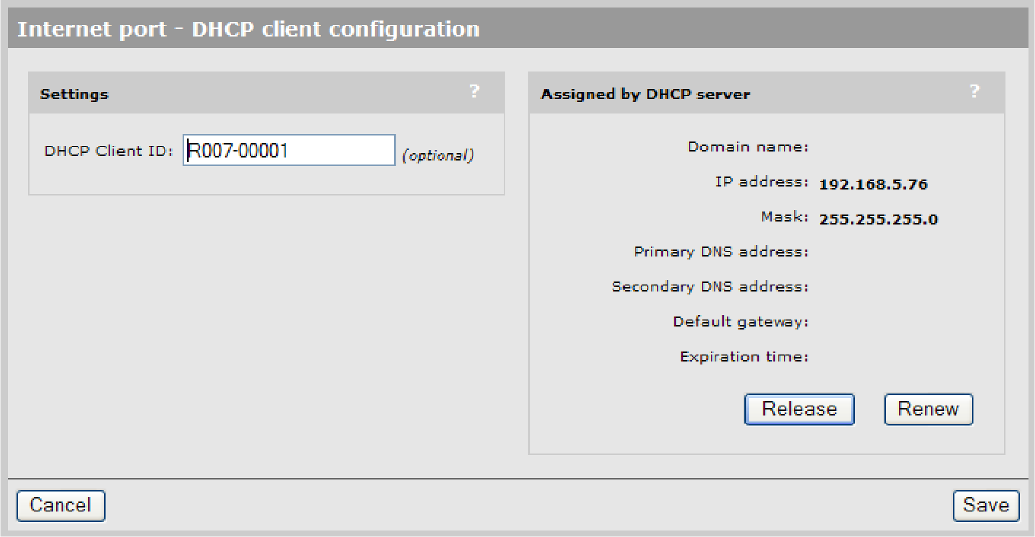
Secondary DNS address
Identifies the IP address of the backup server the controller will use to resolve DNS requests.

Default gateway
Identifies the IP address of the gateway the controller will forward all outbound traffic to.

Restart Connection
Select this button to manually establish the PPPoE connection. During normal operation, you will not need to do this because the controller will automatically reconnect if the PPPoE connection is interrupted. However, for certain types of connection failures, the controller may not be able to re-establish the connection, even after several retries. When this occurs, the cause of the failure is shown in the **Connection** status field and you must select **Restart Connection** to manually establish the connection.

DHCP client

To configure the PPPoE client on the Internet port, select **Controller >> Network > Ports** and then select **DHCP Client** and then **Configure.**



Internet port - DHCP client configuration

Settings

DHCP Client ID: R007-00001 *(optional)*

Assigned by DHCP server

Domain name:
IP address: 192.168.5.76
Mask: 255.255.255.0
Primary DNS address:
Secondary DNS address:
Default gateway:
Expiration time:

Settings

DHCP client ID

Specify an ID to identify the controller to the DHCP server.

Assigned by DHCP server

These settings are assigned to the controller by your service provider DHCP server. The Internet connection is not active until this occurs.

Domain name

Identifies the domain the DHCP server is operating in.

IP address

Identifies the IP address assigned to the controller by the DHCP server.

Mask

Identifies the subnet mask that corresponds to the assigned IP address.

Primary DNS address

Identifies the IP address of the main DNS server the controller will use to resolve DNS requests.

Secondary DNS address

Identifies the IP address of the backup server the controller will use to resolve DNS requests.

Default gateway

Identifies the IP address of the gateway the controller will forward all outbound traffic to.

Expiration time

Indicates how long the address is valid.

Release

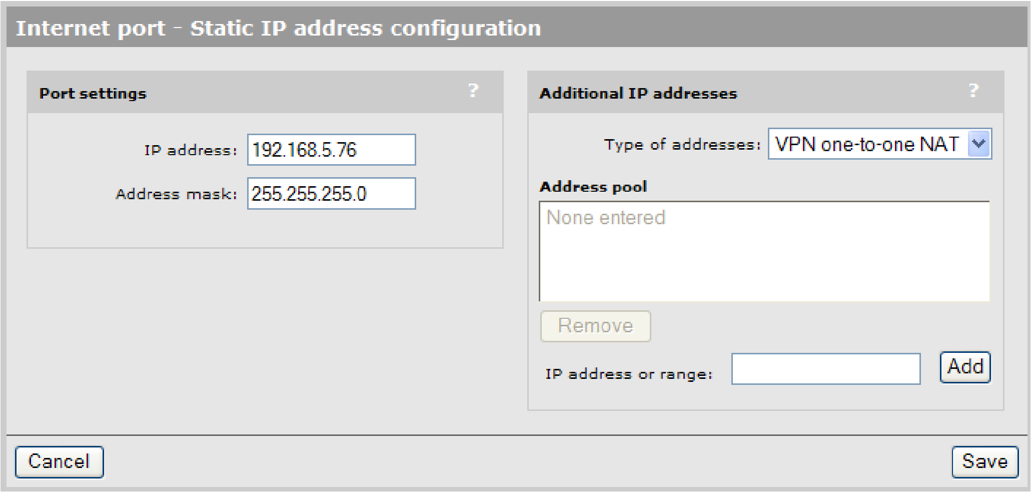
Select to release the controller IP address.

Renew

Select to renew the controller IP address.

Static addressing

To configure the PPPoE client on the Internet port, select **Controller >> Network > Ports** and then select **Static** and then **Configure.**



Internet port - Static IP address configuration

Port settings

IP address: 192.168.5.76

Address mask: 255.255.255.0

Additional IP addresses

Type of addresses: VPN one-to-one NAT

Address pool

None entered

IP address or range:

Port settings

IP address

Specify the static IP address you want to assign to the port.

Address mask

Select the appropriate mask for the IP address you specified.

Additional IP addresses

Use these options to define additional IP addresses for use by either the VPN one-to-one NAT feature or the public IP address feature. Only one of these features can be active.

Type of addresses

Select either the **VPN one-to-one NAT** or **Public IP address** option.

VPN one-to-one NAT

When this feature is enabled, the controller can assign a unique IP address to each IPSec or PPTP VPN connection made by a user to a remote server via the Internet port. Addresses are assigned as defined in the **Address pool**.

This feature can only be used with authenticated, access-controlled users.

To reduce the number of addresses that need to be defined, the controller will use the same address for multiple users as long as they are establishing a connection with different VPN servers.

Use this feature when all of the following conditions are true:

- Users intend to make IPSec or PPTP VPN connections with a remote site via the Internet port on the controller.
- NAT is enabled on the controller. (In its default configuration, NAT translates all IP address on the local network to a single public IP address; the address assigned to the Internet port on the controller. As a result, all user sessions to an external resource appear to originate from the same IP address. This can cause a problem with remote VPN servers that require a unique IP address for each user session.)
- The remote VPN server requires that each user have a unique IP address.

Note External devices cannot initiate connections with users via the address assigned by this feature.

Assigning addresses to users

To make use of this feature, each user account must have the **VPN one-to-one NAT** option enabled. Do this as follows:

- If using the local user accounts (defined on the **Controller >> Users** menu), enable the **VPN one-to-one NAT** option in the account profile or subscription plan that is assigned to the user. See *Defining account profiles on page 10-32* and *Defining subscription plans on page 10-35*.
- If using Active Directory, enable the **VPN one-to-one NAT** option in the account profile (see *Defining account profiles on page 10-32*) that is assigned to an Active Directory group (see *Configuring an Active Directory group on page 11-13*).
- If using a RADIUS server, add the following Colubris AV-Pair value to the user's account: `one-to-one-nat=1`. For more information on setting attributes, see *Default user one-to-one NAT on page 15-53* and *One-to-one NAT on page 15-69*.

Address pool

The address pool contains all the IP addresses that can be assigned to users. You can define up to 30 addresses.

Addresses must be valid for the network to which the Internet port is connected. Specify a single address or an address range as follows: *address1-address2*. For example, the following defines a range of 20 addresses: 192.168.1.1-192.168.1.20

Public IP address

This feature enables the integrated DHCP server on the controller to assign public IP addresses to users. A user with a public IP address is visible on the protected network connected to the Internet port, instead of being hidden by the controller's NAT feature. This makes it possible for external devices to create connections with a user's computer on the internal network.

Public IP addresses are assigned by the integrated DHCP server using the addresses specified in the **Address pool**. Whenever possible, this feature will assign the same public IP address to a user each time they connect.

When you enable public IP address support in a subscription plan, an additional setting is available called **Reserve public IP address**. When this option is enabled, the public IP assigned to a user is reserved until the user's subscription plan expires. This means that the address is reserved, even if the user is not logged in.

When a public IP address is assigned to a user:

- The user cannot access any VLANs, VPNs, or GRE tunnels configured on the controller.
- The user cannot establish more than one concurrent session.

Note

If a user's account is configured for public IP address support and there is no free public IP address in the pool when the user tries to login, the login is refused.

Assigning public IP addresses to users

To obtain a public IP address, a user's account must have its **Public IP address** option enabled. Do this as follows:

- If using the local user accounts (defined on the **Controller >> Users** menu), enable the **Public IP address** option in the account profile or subscription plan that is assigned to the user. See *Defining account profiles on page 10-32* and *Defining subscription plans on page 10-35*.
- If using Active Directory, enable the **Public IP address** option in the account profile (see *Defining account profiles on page 10-32*) that is assigned to an Active Directory group. To set up an Active Directory group, see *Configuring an Active Directory group on page 11-13*.
- If using a RADIUS server, add the following Colubris AV-Pair value to the user's account: `use-public-ip-subnet=1`. For more information, see *Default user public IP address on page 15-54* and *Public IP address on page 15-70*.

DHCP server lease time

Use this setting to define the amount of time the public IP address lease will be valid. This setting only applies to public IP addresses. It overrides the DHCP lease time set by selecting **Controller >> Network > Address allocation > DHCP server**.

Address pool

The address pool contains all the public IP addresses that can be assigned to users. You can define up to 30 addresses.

Addresses must be valid for the network to which the Internet port is connected. Specify a single address or an address range as follows: *address1-address2*. For example, the following defines a range of 20 addresses: 192.168.1.1-192.168.1.20

Network profiles

Network profiles let you define the characteristic of a network and assign a friendly name to it. Profiles make it easy to configure the same settings in multiple places on the controller.

For example, if you define a profile with a VLAN ID of 10, you could use that profile to:

- Configure VLAN 10 on the controller’s Internet or LAN port using the **Controller >> Network > Ports** page.
- Configure VLAN 10 as the egress network for a group of APs when binding them to a VSC using the **Controlled APs > [*group*] >> VSC bindings** page.
- Configure VLAN 10 as the local network for an AP using the **Controlled APs >> Configuration > Local network** page.

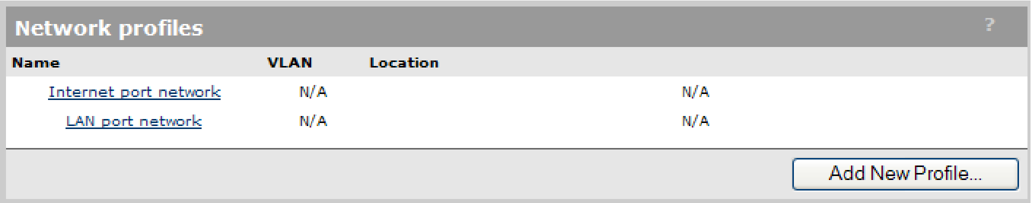
About the default network profiles

Two network profiles are created by default: **LAN port network** and **Internet port network**. These profiles are associated with the two physical Ethernet ports on the controller. You can rename these profiles, but you cannot assign a VLAN to them or delete them. You can use these profiles to send untagged traffic to a specific port on the controller.

Both ports are considered to be local networks on the controller, which means that they automatically map the network that is assigned to each physical port as a local network on the controller. However, the LAN and Internet port network profiles can also be assigned as a local network on an AP (for example, using the **Controlled APs >> Configuration > Local networks** page). When this is done, both profiles refer to the untagged Ethernet port on the AP.

To define a network profile

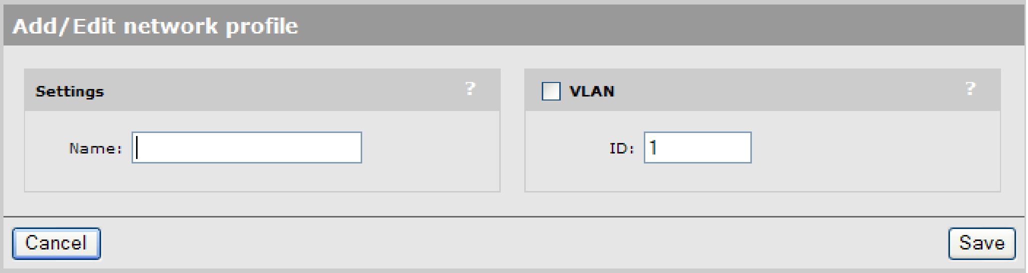
1. Select **Controller >> Network > Network profiles**.



Network profiles

Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A

2. Select **Add New Profile**.



Name:
□ VLAN
ID: 1

3. Configure profile settings as follows:

   - Under **Settings**, specify a **Name** for the profile.
   - To assign a VLAN, select **VLAN** and then specify an **ID**.

     If the profile will be used on an Ethernet port, you can also define a range of VLANs. This enables a single VLAN definition to span a large number of contiguously assigned VLANs. Specify the range in the form X-Y, where X and Y can be 1 to 4094. For example: 50-60.

     An IP address cannot be assigned to a VLAN range.

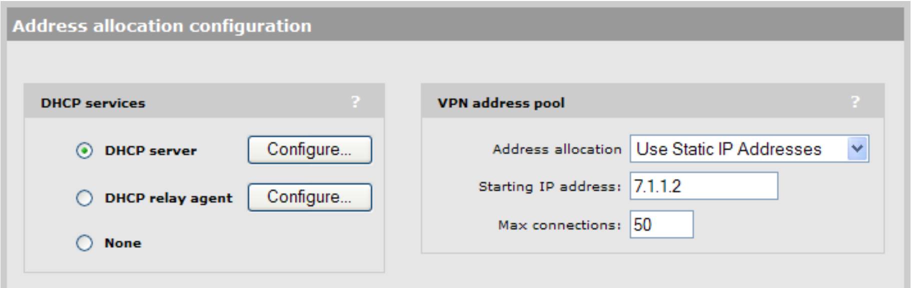
     You can define more than one VLAN range by using multiple profiles. Each range must be distinct and contiguous.

4. Select **Save**.

Address allocation

The controller can operate as a DHCP server or DHCP relay agent on the LAN port. This enables it to assign IP addresses to downstream devices connected to the LAN port.

By default, address allocation is disabled. To configure address allocation settings, select **Controller >> Network > Address allocation**.



● DHCP server
○ DHCP relay agent
○ None

Address allocation: Use Static IP Addresses
Starting IP address: 7.1.1.2
Max connections: 50

For information on VPN address pool, see *Configure an IPSec profile for wireless client VPN on page 16-4*.

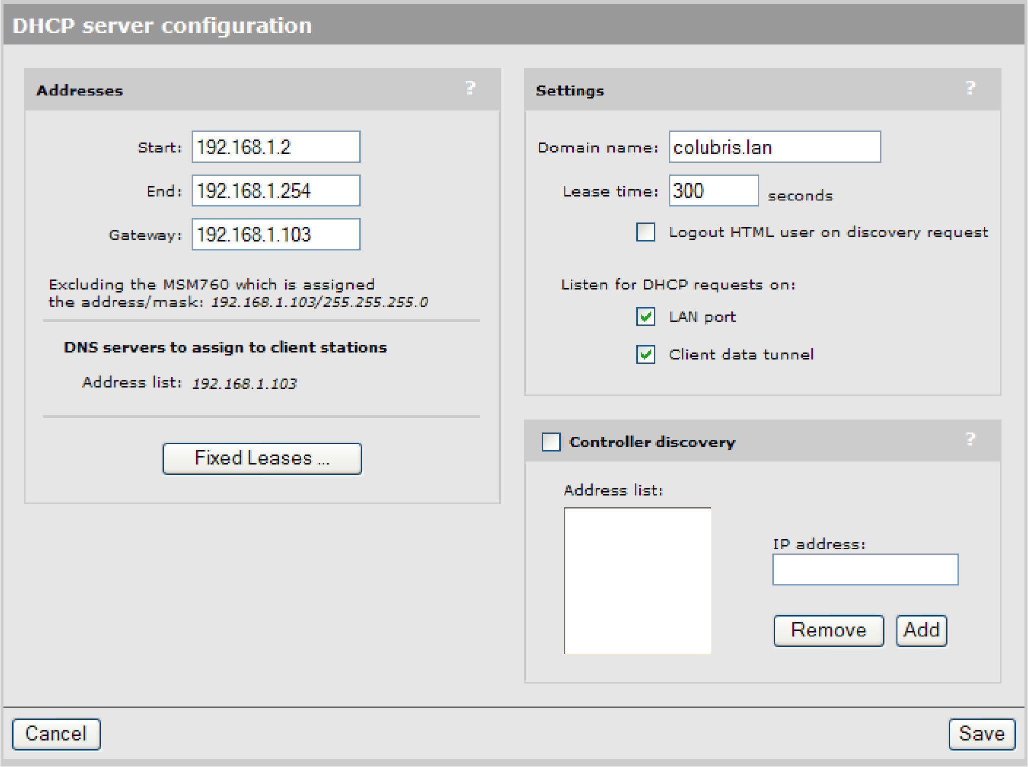
DHCP server

The DHCP server can be used to automatically assign IP addresses to devices that are connected to the controller via the LAN port or client data tunnel.

Note

- Do not enable the DHCP server if the LAN port is connected to a network that already has an operational DHCP server.
- When the DHCP server is active, users can still connect using static IP addresses assigned on different subnets. To configure this feature, select **Public access > Access control** and under **Client options**, select **Allow any IP address**.
- The DHCP settings on this page are always used by the default VSC. For additional flexibility, separate DHCP servers can enabled on other access-controlled VSCs to assign addresses to users. See *DHCP server on page 5-30*.
- The DHCP server feature is not supported when controller teaming is active.

To configure the internal DHCP server, select **Controller >> Network > Address allocation,** select **DHCP server**, and then **Configure.**



Start: 192.168.1.2
End: 192.168.1.254
Gateway: 192.168.1.103

Excluding the MSM760 which is assigned the address/mask: *192.168.1.103/255.255.255.0*

DNS servers to assign to client stations
Address list: *192.168.1.103*

Domain name: colubris.lan
Lease time: 300 seconds
☐ Logout HTML user on discovery request

Listen for DHCP requests on:
☑ LAN port
☑ Client data tunnel

☐ Controller discovery

Addresses

Start / End

Specify the starting and ending IP addresses that define the range of addresses the DHCP server can assign to client stations. The address assigned to the controller is automatically excluded from the range.

Gateway

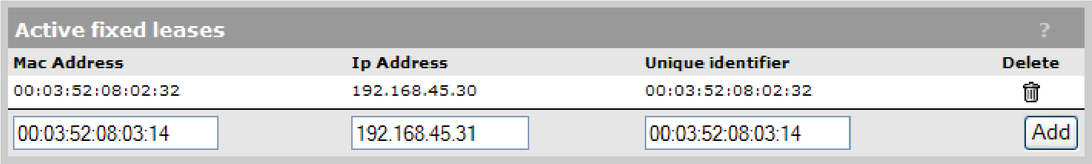
Specify the IP address of the default gateway the controller will assign to DHCP users. In most cases you will specify the IP address of the controller LAN port as the **Gateway**.

DNS servers to assign to client stations

Lists the IP addresses of the DNS servers that the controller will assign to users. You can define DNS options by selecting **Network > DNS.**

Fixed leases

Use this feature to permanently reserve an IP addresses lease for a specific device. This ensures that the device is always reachable at the same address on the network, but does not require a static address to be set directly on the device itself. This table lists all permanently reserved addresses. Up to 255 fixed leases can be defined.



Active fixed leases

Mac Address	Ip Address	Unique identifier	Delete
00:03:52:08:02:32	192.168.45.30	00:03:52:08:02:32	🗑
00:03:52:08:03:14	192.168.45.31	00:03:52:08:03:14	Add

To assign a specific IP address to a client station specify the following and select **Add**:

- **MAC address**: MAC address of the client station in the format: nn:nn:nn:nn:nn:nn.
- **IP address**: IP address that will be assigned to the client station in the format: nnn.nnn.nnn.nnn.
- **Unique identifier**: A number that identifies the device. Must be unique to all DHCP clients on the network. Generally set to the MAC address of the client station. This parameter is optional unless MAC masquerading is being performed by the client station.

Settings

Domain name

Specify the domain name the controller will return to DHCP users. Typically, this will be your corporate domain name.

The host name in the currently installed SSL certificate is automatically assigned as the domain name of the controller. The factory default SSL certificate that is installed on the controller has the host name **wireless.colubris.com**.

You do not have to add this name to your server for it to be resolved. The controller intercepts all DNS requests it receives. It resolves any request that matches the certificate host name by returning the IP address assigned to the Internet port. All other DNS requests are forwarded to the appropriate DNS servers as configured on the **Controller > Network > DNS** page.

To summarize, this means that by default, any DNS request by a user that matches **wireless.colubris.com** will return the IP address of the controller's Internet port.

Lease time
Specify the lease time (in seconds) that the controller will assign to all assigned addresses. As long as a user remains connected their address is automatically renewed when the lease time expires. If a user disconnects without releasing their address, then the address remains reserved until the lease time expires. If you have a small address pool and a large user turnover, setting a long lease time may cause you to run out of addresses even though they are not really in use.

Logout HTML user on discovery request
When enabled, the controller will log out a client station if a DHCP discovery request is received from the client station while a DHCP address lease is currently assigned.

This feature is useful when multiple users share the same client station. If a user forgets to log out before turning off the client station, the next user will have to wait until the lease expires before being able to log in.

Listen for DHCP requests on
Select the port on which the controller will listen for DHCP requests from client stations.

- **LAN port:** Listen for requests on the LAN port.
- **Client data tunnel:** Enable this option when the client data tunnel feature is active on one or more VSCs, and you want tunneled client stations to be able to receive an IP address from the controller's DHCP server.

Controller discovery

Use this option to define controller discovery information for controlled APs. See *DHCP discovery on page 6-8*.

Add the IP address for each controller that is active on the network. When working with a controller team you should add the IP address of each team member.

This list is sent to all devices that request an IP address, encoded as DHCP option 43 (Vendor-specific information). However, this information is only interpreted by HP ProCurve APs that are operating in controlled mode. Controlled mode APs use these addresses to connect with the controllers in the order that they appear in the list.

DHCP relay agent

The controller provides a flexible DHCP relay implementation. It can listen for requests on the LAN port or client data tunnel and forward them to a DHCP via any of the controller's physical or logical interfaces.

Note

For additional flexibility, separate DHCP relay agents can be enabled on access-controlled VSCs. See *DHCP relay agent on page 5-31*.

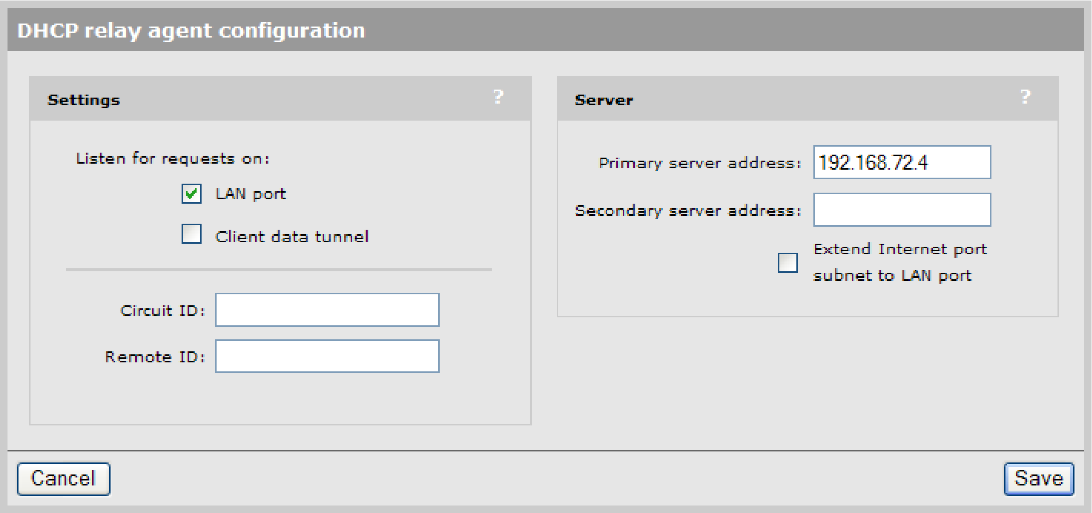
Use the following guidelines when configuring DHCP relay:

- Routes must be defined on the DHCP server, so that the DHCP server can successfully send DHCP response packets back to the DHCP relay agent running on the controller. These should be static and persistent HOST routes that must identify the IP address assigned to the controller's LAN port or additional VSC relay IP address, (i.e. 192.168.1.1). On Windows, such a static route would look like this:

  route add 192.168.1.1 mask 255.255.255.255 10.10.10.22 metric 1 –p

- DHCP relay is not supported via the Internet port when it is operating as a PPPoE client.
- DHCP relay cannot work via the Internet port if the internal firewall is set to High and NAT is enabled on the Internet port. The DHCP server must be able to ping the assigned address to prevent duplicate assignments.

To configure the internal DHCP server, select **Controller >> Network > Address allocation,** select **DHCP relay agent**, and then **Configure.**



DHCP relay agent configuration

Settings

Listen for requests on:

☑ LAN port

□ Client data tunnel

Circuit ID:

Remote ID:

Server

Primary server address: 192.168.72.4

Secondary server address:

□ Extend Internet port subnet to LAN port

Settings

Listen for DHCP requests on

Select the port on which the controller will listen for DHCP requests from users.

Listen for requests on

- **LAN port**: Listens for DHCP requests on the LAN port and relay them to the remote DHCP server.
- **Client data tunnel:** Enable this option when the client data tunnel feature is active on one or more VSCs, and you want tunneled users to be able to receive an IP address via the DHCP relay agent. See *Client data tunnel on page 5-13*.

The following two fields let you attach information to the DHCP request (as defined by DHCP relay agent information option 82) which lets the DHCP server identify the controller.

- **Circuit ID:** Use this field to identify the user that issued the DHCP request.
- **Remote ID:** Use this field to identify the controller.

You can use regular text in combination with the following placeholders to create the information in each field. Placeholders are automatically expanded when the request is sent. The following placeholders can be used:

- **%S:** SSID to which the user is associated.
- **%B:** BSSID to which the user is associated.
- **%V:** VLAN to which the user is mapped.

Server

Primary DHCP server address
Specify the IP address of the first DHCP server to which the controller should forward DHCP requests.

Secondary DHCP server address
Specify the IP address of the backup DHCP server to which the controller should forward DHCP requests.

Note

- The DHCP servers must be reachable via one of the ports on the controller.
- Routes must be defined on the DHCP server so that the DHCP server can successfully send DHCP response packets back to the DHCP relay agent running on the controller. These should be static and persistent HOST routes that must identify the IP address assigned to the controller’s LAN port or an additional VSC relay IP address, (i.e. 192.168.1.1). On Windows, such a static route would look like this:

  ```
  route add 192.168.1.1 mask 255.255.255.255 10.10.10.22 metric 1 –p
  ```
- DHCP relay is not supported via the Internet port when it is operating as a PPPoE client.
- DHCP relay cannot work via the Internet port if the internal firewall is set to High and NAT is enabled on the Internet port. The DHCP server must be able to ping the assigned address to prevent duplicate assignments.

Extend Internet port subnet to LAN port
When enabled, the controller will alter the DHCP address requests from client stations so that they appear to originate from the network assigned to the Internet port on the controller. This will cause the DHCP server to assign IP addresses on this network to all client stations. The controller handles all mapping between the two subnets internally.

For L2 connected APs operating in controlled mode:

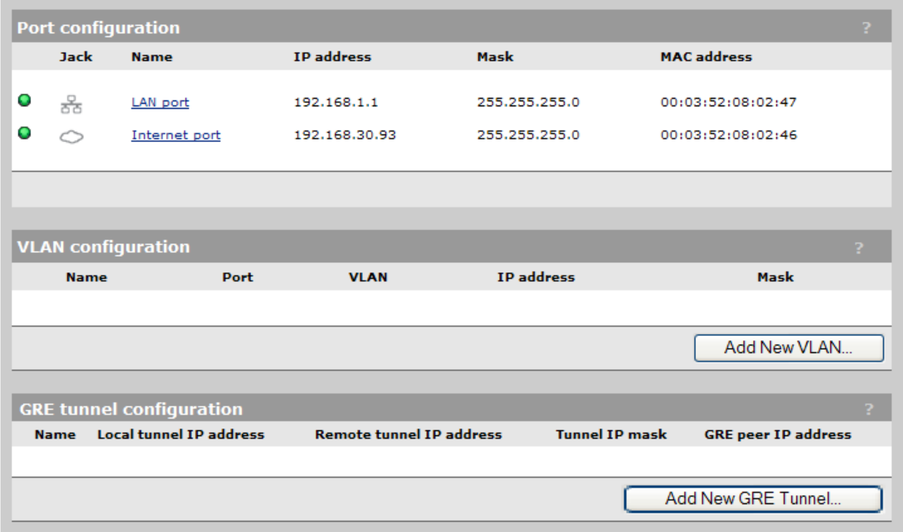
- Enable the **Client data tunnel** option under **Settings.** (If teaming is active, the client data tunnel is automatically used.)
- Enable the **Always tunnel client traffic** option on the VSC profile page under **Virtual AP > Client data tunnel**.

VLAN support

VLAN configuration is discussed in *Chapter 7: Working with VLANs*.

GRE tunnels

To view and configure GRE tunnel definitions, select **Controller >> Network > Ports**. Initially, no GRE tunnels are defined.



Port configuration

	Jack	Name	IP address	Mask	MAC address
●		LAN port	192.168.1.1	255.255.255.0	00:03:52:08:02:47
●		Internet port	192.168.30.93	255.255.255.0	00:03:52:08:02:46

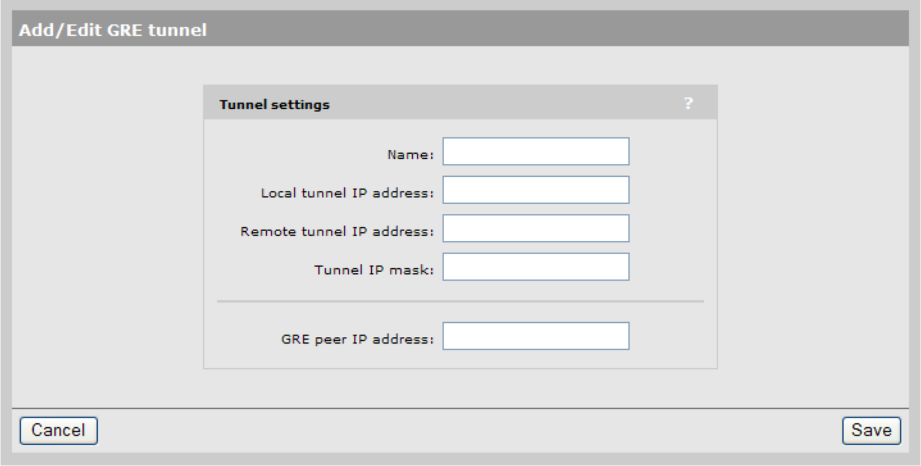
VLAN configuration

Name	Port	VLAN	IP address	Mask

GRE tunnel configuration

Name	Local tunnel IP address	Remote tunnel IP address	Tunnel IP mask	GRE peer IP address

To add a tunnel**,** select **Add New GRE Tunnel.** The **Add/Edit GRE tunnel** page opens.



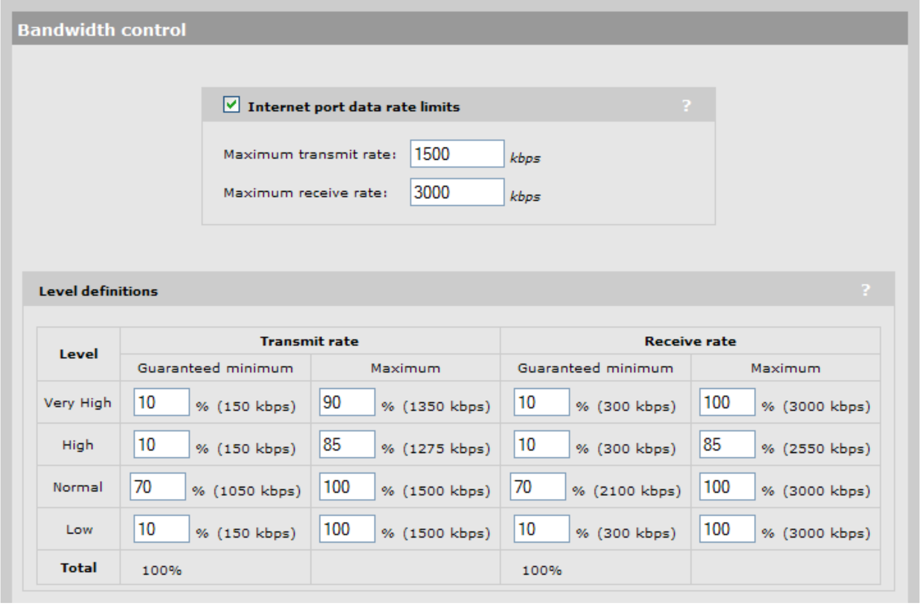
Define tunnel settings as follows:

- **Name:** Tunnel name.
- **Local tunnel IP address:** Specify the IP address of the controller inside the tunnel.
- **Remote tunnel IP address:** Specify the IP address of the remote device inside the tunnel.
- **Tunnel IP mask:** Specify the mask associated with the IP addresses inside the tunnel.
- **GRE peer IP address:** Specify the IP address of the remote device that terminates the tunnel.

Bandwidth control

The controller incorporates a bandwidth management feature that enables control of all user traffic flowing through the controller.

To configure Bandwidth management, select **Controller >> Network > Bandwidth Control.**



Bandwidth control

☑ **Internet port data rate limits** ?

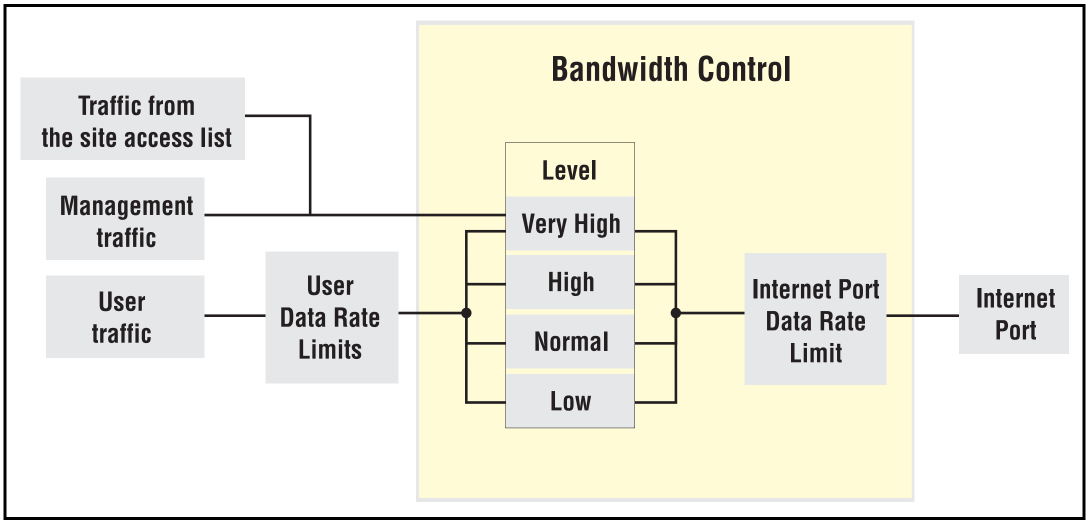
Maximum transmit rate: 1500 *kbps*

Maximum receive rate: 3000 *kbps*

Level definitions ?

Level	**Transmit rate**		**Receive rate**	
	Guaranteed minimum	Maximum	Guaranteed minimum	Maximum
Very High	10 % (150 kbps)	90 % (1350 kbps)	10 % (300 kbps)	100 % (3000 kbps)
High	10 % (150 kbps)	85 % (1275 kbps)	10 % (300 kbps)	85 % (2550 kbps)
Normal	70 % (1050 kbps)	100 % (1500 kbps)	70 % (2100 kbps)	100 % (3000 kbps)
Low	10 % (150 kbps)	100 % (1500 kbps)	10 % (300 kbps)	100 % (3000 kbps)
Total	100%		100%	

Bandwidth control has two separate components: *Internet port data rate limits* and *bandwidth levels*. They interact with the data stream as follows:



Internet port data rate limits

These settings enable you to limit the total incoming or outgoing data rate on the Internet port. If traffic exceeds the rate you set for short bursts, it is buffered. Long overages will result in data being dropped.

To utilize the full available bandwidth, the **Maximum transmit rate** and **Maximum receive rate** should be set to match the incoming and outgoing data rates supported by the connection established on the Internet port.

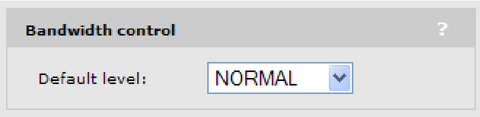
Bandwidth levels

The controller provides four levels of traffic priority that you can use to manage traffic flow: *Very High*, *High*, *Normal*, and *Low*. The settings for each level are customizable, allowing performance to be tailored to meet a wide variety of scenarios.

Assigning traffic to a bandwidth level

Traffic can be assigned to a specific bandwidth level for each VSC and for each user. For bandwidth control to be operational, you must first enable the **Internet port data rate limits** option. Once this is done, you can assign traffic to bandwidth levels as follows:

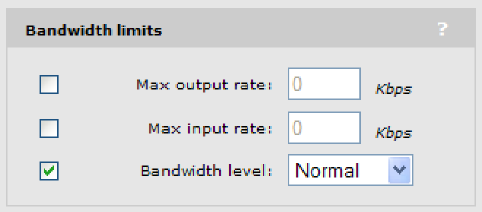
- In a VSC, select the default level for all user traffic in the **Bandwidth control** box. This level applies to users who do not have a specific assignment in their user account.



Bandwidth control

Default level: NORMAL

- In a user's account profile, set the **Bandwidth level** in the **Bandwidth limits** box.



Bandwidth limits

□ Max output rate: 0 Kbps

□ Max input rate: 0 Kbps

☑ Bandwidth level: Normal

- Or if you are using a RADIUS server to validate user logins, set the bandwidth level using a Colubris AV-Pair value. See *Bandwidth level on page 15-68*.

To control the default bandwidth level for all users, see *Default user bandwidth level on page 15-51*.

Note

- Management traffic (which includes RADIUS, SNMP, and administrative sessions) is assigned to bandwidth level **Very High** and cannot be changed.
- All traffic assigned to a particular bandwidth level shares the allocated bandwidth for that level across all VSCs. This means that if you have three VSCs all assigning user traffic to High, all users share the bandwidth allocated to the High level.

Customizing bandwidth levels

Bandwidth levels are arranged in order of priority from Very High to Low. Priority determines how free bandwidth is allocated once the minimum rate is met for each level. Free bandwidth is always assigned to the higher priority levels first.

Bandwidth rates for each level are defined by taking a percentage of the maximum transmit and receive rates defined for the Internet port. Each bandwidth level has four rate settings:

- Transmit rate - guaranteed minimum: Minimum amount of bandwidth that will be assigned to a level as soon as outgoing traffic is present on the level.
- Transmit rate - maximum: Maximum amount of outgoing bandwidth that can be consumed by the level. Traffic in excess is buffered for short bursts, and dropped for sustained overages.
- Receive rate - guaranteed minimum: Minimum amount of bandwidth that will be assigned to a level as soon as incoming traffic is present on the level.
- Receive rate - maximum: Maximum amount of incoming bandwidth that can be consumed by the level. Traffic in excess is buffered for short bursts, and dropped for sustained overages.

Example

For example, assume that transmit bandwidth is configured as follows:

	Transmit rates	
	Min	**Max**
Very High	20	20
High	40	100
Normal	20	100
Low	20	20

Next, assume the following bandwidth requirement occurs on transmitted user data:

- High requires 70%, which is 30% more than its minimum.
- Normal requires 50%, which is 30% more than its minimum.
- There is no traffic on Very High or Low.

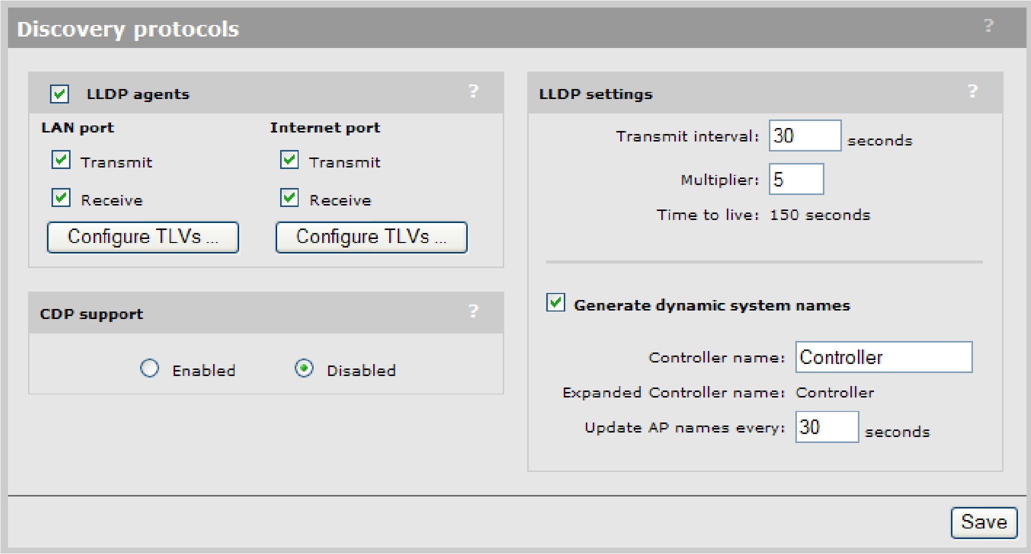
Since both High and Normal require bandwidth in excess of their guaranteed minimum, each is allocated their guaranteed minimum. This leaves 40% of the bandwidth free to be assigned on a priority basis. High has more priority than Normal, so it takes as much bandwidth as needed. In this case it is 30%, which brings High up to 70%. This leaves 10% for Normal, which is not enough. Traffic is buffered for a short period, and then dropped.

If at the same time Very High traffic is sent, this level immediately steals 20% from the lower levels. In this case, 10% is taken from Normal, returning it to its minimum guaranteed level, and 10% is taken from High.

Discovery protocols

The controller supports two protocols (LLDP and CDP) that provide a mechanism for devices on a network to exchange information with their neighbors.

To these protocols, select **Controller >> Network > Discovery protocols.**



Discovery protocols

☑ LLDP agents

LAN port
☑ Transmit
☑ Receive

Internet port
☑ Transmit
☑ Receive

CDP support
○ Enabled ● Disabled

LLDP settings
Transmit interval: 30 seconds
Multiplier: 5
Time to live: 150 seconds

☑ Generate dynamic system names
Controller name: Controller
Expanded Controller name: Controller
Update AP names every: 30 seconds

LLDP agents

For a complete discussion of all LLDP options, see *Chapter 17: LLDP on page 17-1*.

CDP

The controller can be configured to transmit CDP (Cisco Discovery Protocol) information on the LAN and Internet ports. This information is used to advertise controller information to third-party devices, such as CDP-aware switches. Network managers can retrieve this information allowing them to determine the switch ports to which different controllers are connected.

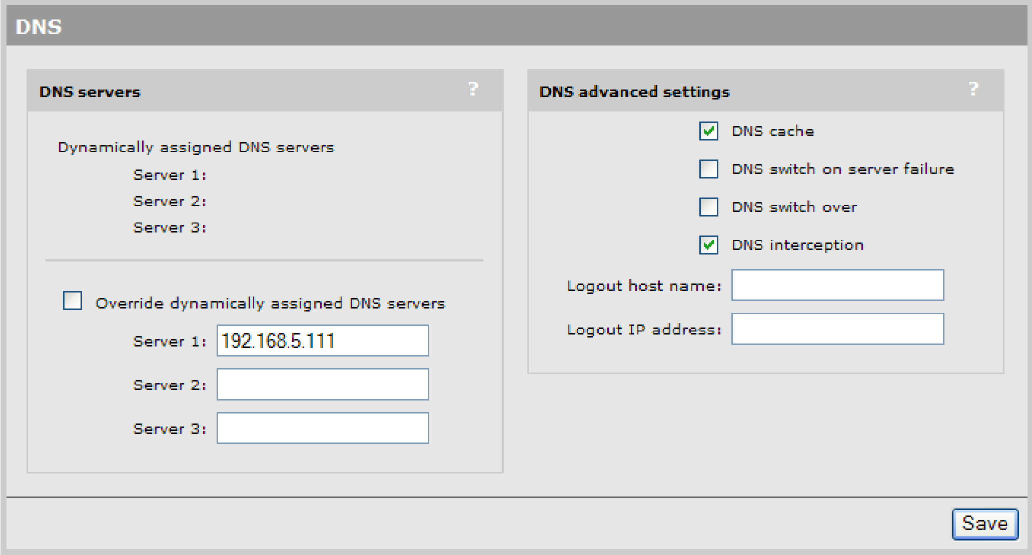
The controller always listens for CDP information on the LAN and Internet ports, even when this option is disabled, to build a list of autonomous APs. CDP information from third-party devices and controlled APs is ignored.

Note Controlled APs always send CDP information.

DNS

The controller provides several options to customize DNS handling. To configure these options, select **Controller >> Network > DNS.** The configuration options on this page change depending on the address option that is active on the Internet port.

When the Internet port is configured to obtain an IP address via PPPoE or DHCP



DNS

DNS servers

Dynamically assigned DNS servers
Server 1:
Server 2:
Server 3:

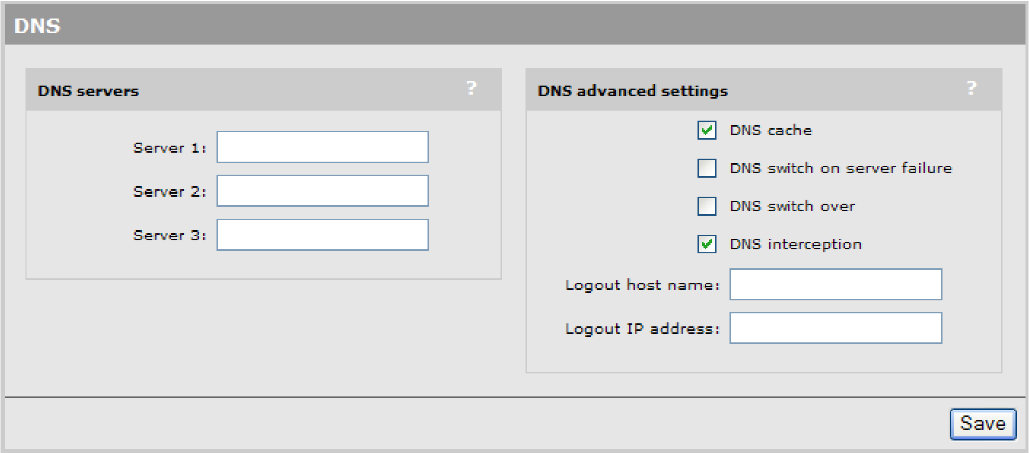
□ Override dynamically assigned DNS servers
Server 1: 192.168.5.111
Server 2:
Server 3:

DNS advanced settings

☑ DNS cache
□ DNS switch on server failure
□ DNS switch over
☑ DNS interception

Logout host name:
Logout IP address:

When the Internet port is configured to use a static IP address



DNS

DNS servers

Server 1:
Server 2:
Server 3:

DNS advanced settings

☑ DNS cache
□ DNS switch on server failure
□ DNS switch over
☑ DNS interception

Logout host name:
Logout IP address:

Note When using Active Directory for user authentication, set the DNS servers to be the Active Directory servers or the devices that provide SRV records.

DNS servers

Dynamically assigned servers

Shows the DNS servers that are dynamically assigned to the controller when PPPoE or DHCP is used to obtain an IP address on the Internet port.

Override dynamically assigned DNS servers

Enable this checkbox to use the DNS servers that you specify on this page to replace those that are assigned to the controller.

Server 1

Specify the IP address of the primary DNS server for the controller to use.

Server 2

- Specify the IP address of the secondary DNS server for the controller to use.

Server 3

- Specify the IP address of the tertiary DNS server for the controller to use.

DNS advanced settings

DNS cache

Enable this checkbox to activate the DNS cache. Once a host name is successfully resolved to an IP address by a remote DNS server, it is stored in the cache. This speeds up network performance, because the remote DNS server does not have to be queried for subsequent requests for this host.

An entry stays in the cache until one of the following is true:

- An error occurs when connecting to the remote host.
- The time to live (TTL) of the DNS request expires.
- The controller restarts.

DNS switch on server failure

Controls how the controller switches between servers:

- When enabled, the controller switches servers if the current server replies with a DNS server failure message.
- When disabled, the controller switches servers if the current server does not reply to a DNS request.

DNS switch over

Controls how the controller switches back to the primary server.

- When enabled, the controller switches back to the primary server once the primary server becomes available again.
- When disabled, the controller switches back to the primary server only when the secondary server becomes unavailable.

DNS interception

When enabled, the controller intercepts all DNS requests and relays them to the configured DNS servers. DNS interception must be enabled to support:

- Redirection of users to the public access interface login page when the controller cannot resolve the domain requested by the user. For example, if the user is using a private or local domain as the default home page in its browser.
- Users configured to use HTTP proxy.
- Users with static IP addresses when the **Allow any IP address** option is enabled on the **Public access > Access control** page.

  When disabled, the controller does not intercept any DNS requests, enabling devices to use a DNS server other than the controller. To support this option, you must set **Network > Address allocation** to **DHCP relay agent** or **Static**.

Note

When **Network > Address allocation** is set to **DHCP Server** the controller always returns its own address as the DNS server.

IP routes

The routing module on the controller provides the following features:

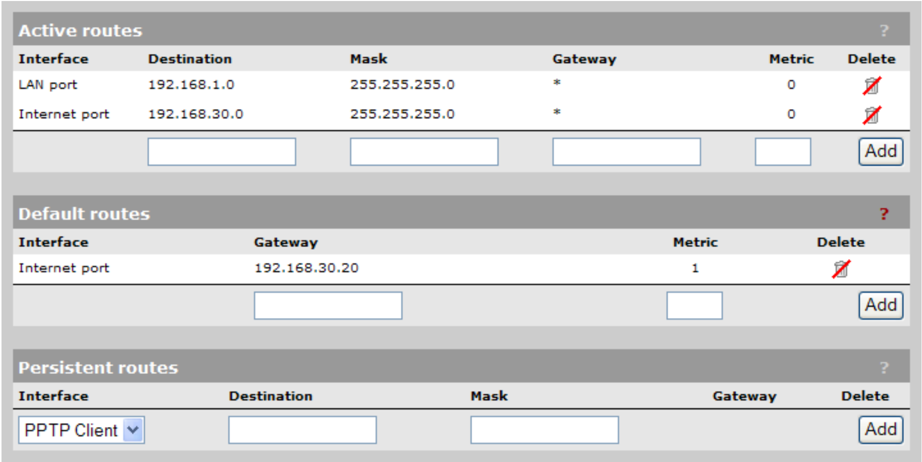
- Compliance with RFC 1812, except for multicast routing
- Supports Classless Inter Domain Routing (CIDR)
- Supports Routing Internet Protocol (RIP) versions 1 and 2 in active or passive mode.

Output from the router is sent to the appropriate logical interface based on the target address of the traffic. Supported logical interfaces include:

- VLAN
- Untagged
- IPSec client
- PPTP client
- GRE tunnel

Configuration

To view and configure IP routes, select **Controller >> Network > IP routes**.



Active routes

Interface	Destination	Mask	Gateway	Metric	Delete
LAN port	192.168.1.0	255.255.255.0	*	0	✗
Internet port	192.168.30.0	255.255.255.0	*	0	✗
					Add

Default routes

Interface	Gateway	Metric	Delete
Internet port	192.168.30.20	1	✗
			Add

Persistent routes

Interface	Destination	Mask	Gateway	Delete
PPTP Client				Add

Active routes

This table shows all active routes on the controller. You can add routes by specifying the appropriate parameters and then selecting **Add.**

The routing table is dynamic and is updated as needed. This means that during normal operation the controller adds routes to the table as required. You cannot delete these system routes.

The following information is shown for each active route:

- **Interface**: The port through which traffic is routed. When you add a route, the controller automatically determines the interface to be used based on the **Gateway** address.
- **Destination**: Traffic addressed to this IP address or subnet is routed.
- **Mask**: Number of bits in the destination address that are checked for a match.
- **Gateway**: IP address of the gateway to which the controller forwards routed traffic (known as the next hop).

  An asterisk is used by system routes to indicate a directly connected network.

  Routes cannot be manually specified for IPSec. These routes are automatically added by the system based on the settings for the IPSec security association.
- **Metric**: Priority of a route. If two routes exist for a destination address, the controller chooses the one with the lower metric.

Default routes

The **Default routes** table shows all default routes on the controller. Default routes are used when traffic does not match any route in the Active routes table. You can add routes by specifying the appropriate parameters and then selecting **Add.**

The routing table is dynamic and is updated as needed. If more than one default route exists, the first route in the table is used.

The following information is shown for each default route:

- **Interface**: The port through which traffic is routed. When you add a route, the controller automatically determines the interface to be used based on the **Gateway** address.
- **Gateway**: IP address of the gateway to which the controller forwards routed traffic (known as the next hop).

  An asterisk is used by system routes to indicate a directly connected network.
- **Metric**: Priority of a route. If two routes exist for a destination address, the controller chooses the one with the lower metric.

Persistent routes

Persistent routes are automatically deleted and then restored each time the interface they are associated with is closed and opened. When the routes are active, they also appear in the Active routes table.

PPTP client

The controller provides an **Auto-route discovery** option to enable it to automatically discover and add routes for IP addresses on the other side of a Point-to-Point Tunnelling Protocol (PPTP) tunnel. The addresses must be part of the remote domain as specified on the **Controller >> VPN > PPTP client** page. Routes are added only when an attempt is made to access the target addresses.

About PPTP client routes (Internet port)

If you disabled the **Auto-route discovery** option (**VPN > PPTP client**), or if you need to access IP addresses that are not part of the specified domain, you must define the appropriate persistent routes.

About PPTP server routes (Internet port)

Activation of the route can be triggered by a specific username. When a user establishes a connection with the controller PPTP server, its username is checked against the persistent routes list and if a match is found, the route is enabled.

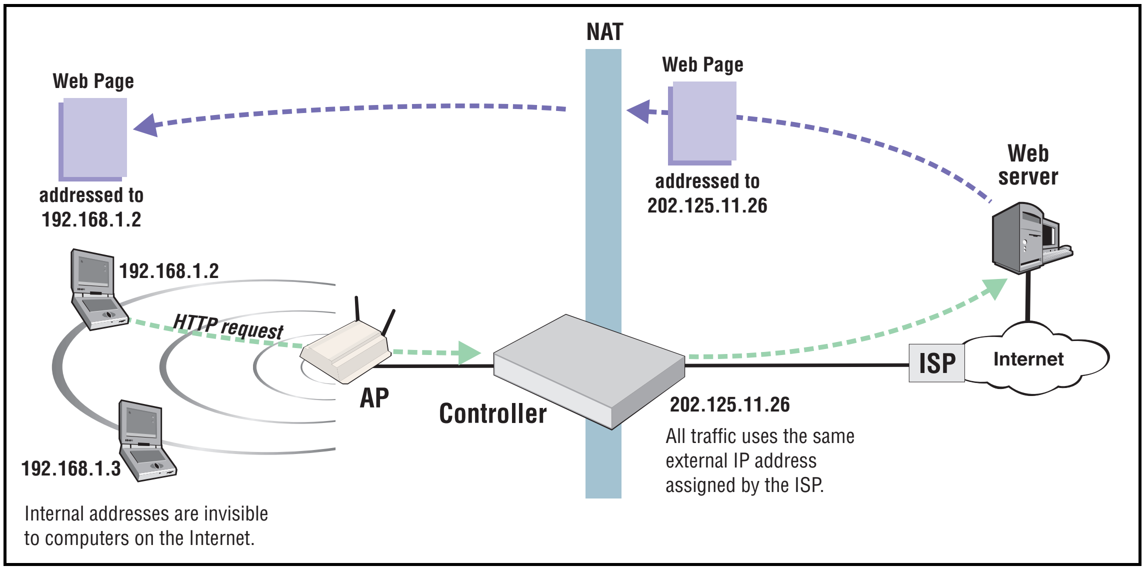
Network address translation (NAT)

Network address translation is an address mapping service that enables one set of IP addresses to be used on an internal network, and a second set to be used on an external network. NAT handles the mapping between the two sets of addresses.

Generally NAT is used to map all addresses on an internal network to a single address for use on an external network like the Internet. The main benefits are that NAT:

- Enables several devices to share a single connection
- Effectively hides the IP addresses of all devices on the internal network from the external network.

This is illustrated as follows:



NAT can be useful in conjunction with virtual private network (VPN) connections. When two networks are connected through a VPN tunnel, it may be desirable to obscure the address of local computers for security reasons.

NAT security and static mappings

One of the benefits of NAT is that it effectively hides the IP addresses of all devices on the internal network an external network. In some cases, however, it is useful to make a computer on the internal network accessible externally. For example, a Web server or FTP server.

Static NAT mapping addresses this problem. Static NAT mapping enables you to route specific incoming traffic to an IP address on the internal network. For example, to support a Web server, you can define a static NAT mapping to route traffic on TCP port 80 to an internal computer running a Web server.

A static NAT mapping allows only one internal IP address to act as the destination for a particular protocol (unless you map the protocol to a nonstandard port). For example, you can run only one Web server on the internal network.

Note

- If you use a NAT static mapping to enable a secure (HTTPS) Web server on the internal network on TCP port 443, remote access to the **management tool** is no longer possible, as all incoming HTTPS requests are routed to the internal Web server and not to the **management tool. You can change the default management port (TCP 443) to an alternate unused TCP port in this case.**
- If you create a static mapping, the firewall is automatically opened to accept the traffic. However, this firewall rule is not visible on the Firewall configuration page (it is maintained internally by the controller).

Common applications are affected by NAT as follows:

Application	NAT
FTP (passive mode)	Requires a static mapping to function.
FTP (active mode)	Requires a static mapping to function.
NetMeeting	Requires a static mapping to function.
Telnet	Requires a static mapping to function.
Windows networking	No effect

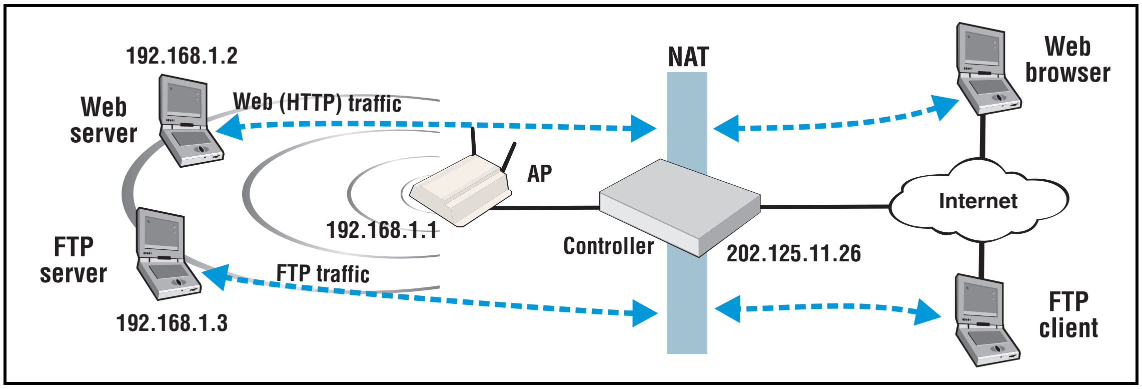
The controller provides pre-configured static mappings for most common applications, which you can enable as needed.

Most Web browsers use FTP in active mode. Some browsers provide a configuration option that enables you to alter this. Use the following steps to change this behavior in Microsoft Internet Explorer.

1. Select **Tools > Internet options** to open the **Internet options** dialog.
2. Select the **Advanced** tab.
3. Under **Browsing,** enable the **Use Passive FTP for compatibility with some firewalls and DSL modems** checkbox.

NAT example

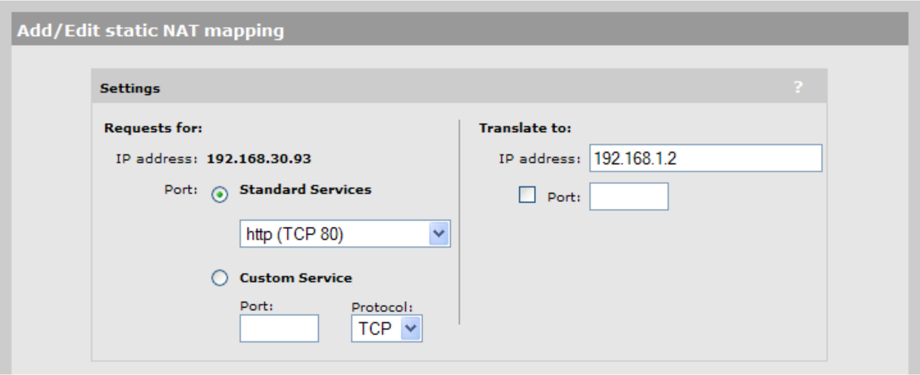
The following example shows you how to configure static NAT mappings to run a Web server and an FTP server on the internal network. This scenario might occur if you use the controller in an enterprise environment.



By creating static NAT mappings, FTP and HTTP (Web) traffic can be routed to the proper user. Note that the addresses of these stations are still not visible externally. Remote computers send their requests to 202.125.11.26, and the controller routes them to the proper client.

Use the following steps to configure the controller to support this example,.

1. Select **Controller >> Network > NAT** > **Add New Static NAT Mapping**.
2. On the NAT mappings page, select **Add New Static NAT Mapping**.
3. Under **Requests for**, select **Standard Services**, and then select **http (TCP 80).**
4. Under **Translate to**, specify the IP address of the Web server, for example **192.168.1.2.** The Settings box should now look similar to this:



Add/Edit static NAT mapping

Settings

Requests for:

IP address: **192.168.30.93**

Port: ● **Standard Services**

http (TCP 80)

○ **Custom Service**

Port: Protocol: TCP

Translate to:

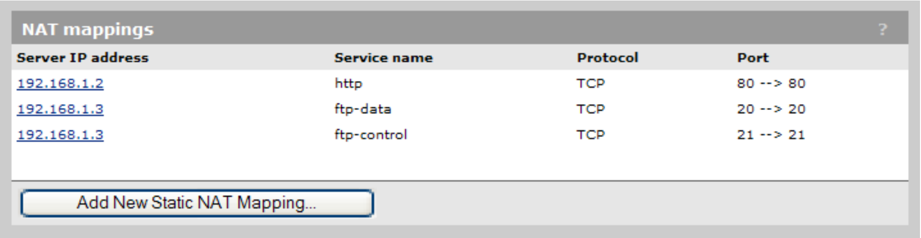
IP address: 192.168.1.2

□ Port:

5. Select **Add** to save your changes and return to the NAT mappings page. The new mapping is added to the table.

6. To support the FTP server, create two additional mappings with the following values:
   - Set **Standard Services** to **ftp-data (TCP 20)** and set **IP address** to **192.168.1.3**.
   - Set **Standard Services** to **ftp-control (TCP 21)** and set **IP address** to **192.168.1.3**.

   The NAT mappings table should now show all three mappings:



NAT mappings

Server IP address	Service name	Protocol	Port
192.168.1.2	http	TCP	80 --> 80
192.168.1.3	ftp-data	TCP	20 --> 20
192.168.1.3	ftp-control	TCP	21 --> 21

VPN One-to-one NAT

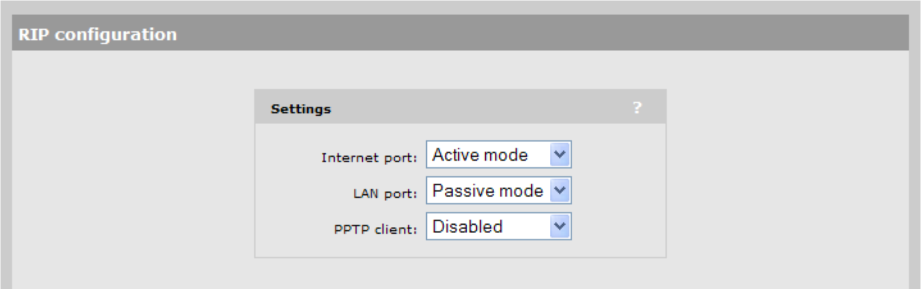
This feature can only be used with authenticated, access-controlled users. It is only supported when a static IP address is assigned to the Internet port. It is configured by selecting **Network > Ports > Internet port > Static > Additional IP addresses**. See *VPN one-to-one NAT on page 3-9*.

RIP

The controller supports Routing Information Protocol (RIP) versions 1 and 2. RIP can operate in one of two modes on the interfaces you select.

- **Passive mode**: The controller listens for routing broadcasts to update the routing table, but does not broadcast its own routes.
- **Active mode**: The controller listens for routing broadcasts to update the routing table, and also broadcast its own routes.

For example:



RIP configuration

Settings

Internet port: Active mode
LAN port: Passive mode
PPTP client: Disabled

Note RIP is not supported if you are using PPPoE on the Internet port.

IP QoS

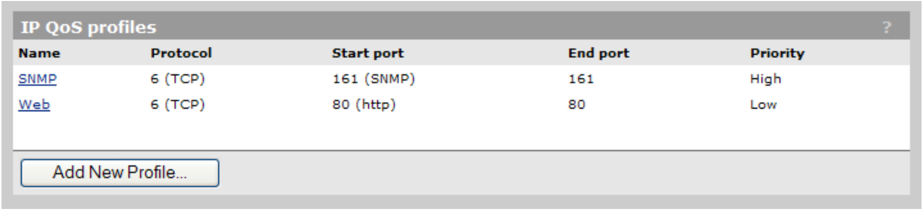
To ensure that critical applications have access to the required amount of wireless bandwidth, you can classify packets destined for the wireless interface into priority queues based on a number of criteria. For example, you can use any of the following to place data packets in one of four priority queues for transmission onto the wireless interface:

- TCP source port
- UDP source port
- Destination port
- Port ranges

You configure IP quality of service (QoS) by creating IP QoS profiles that you can then associate with VSCs or use for global wireless settings. You can configure as many as 32 IP QoS profiles on the controller. You can associate as many as 10 IP QoS profiles with each VSC.

Configuration

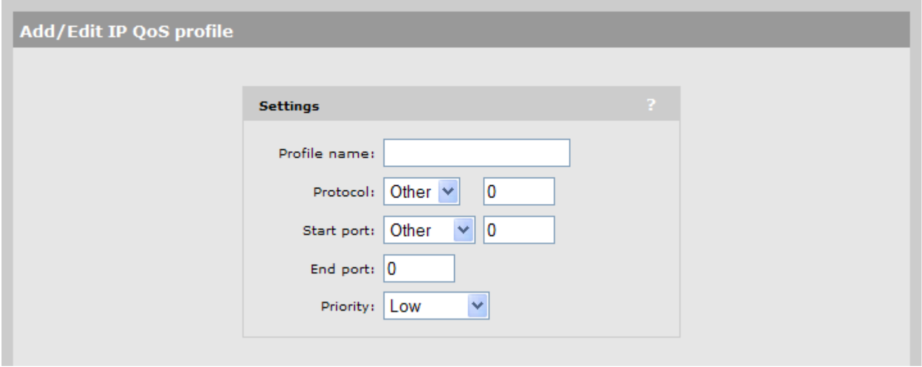
To view and configure IP QoS profiles, select **Controller >> Network > IP QoS**. Initially, no profiles are defined.



IP QoS profiles

Name	Protocol	Start port	End port	Priority
SNMP	6 (TCP)	161 (SNMP)	161	High
Web	6 (TCP)	80 (http)	80	Low

To create an IP QoS profile select **Add New Profile**.



Add/Edit IP QoS profile

Settings

Profile name:
Protocol: Other 0
Start port: Other 0
End port: 0
Priority: Low

Settings

- **Profile name:** Specify a unique name to identify the profile.
- **Protocol:** Specify an IP protocol to use to classify traffic by specifying its Internet Assigned Numbers Authority (IANA) protocol number. Protocol numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually. You can find IANA-assigned protocol numbers on the Internet.
- **Start port/ End port:** Optionally specify the first and last port numbers in the range of ports to which this IP QoS profile applies. To specify a single port, specify the same port number for both **Start port** and **End port.** Port numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually.

Note To accept traffic on all ports for a specified protocol, set **Start port** to **Other** and **0.** Also set **End port** to 65535.

- **Priority:** Select the priority level that will be assigned to traffic that meets the criteria specified in this IP QoS profile.

Note It is strongly recommended that you reserve **Very high** priority for voice applications.

Example

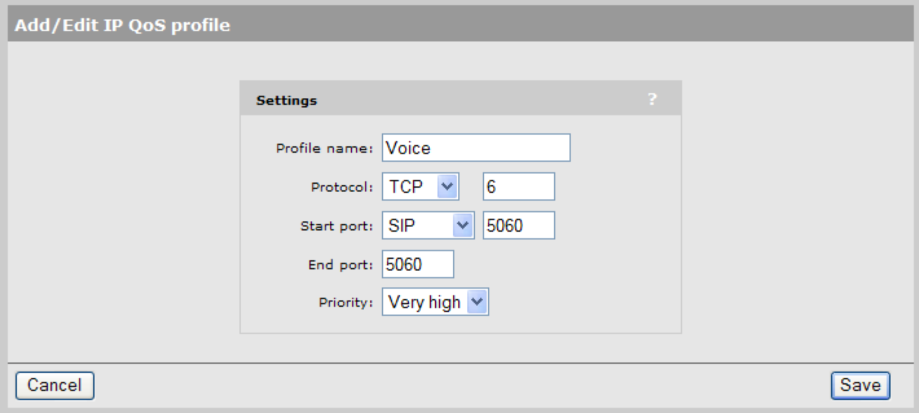
This example shows how to create two IP QoS profiles and associated them with a VSC. The two profiles are:

- **Voice**: Provides voice traffic with high priority.
- **Web:** Provides HTTP traffic with low priority.

Create the profiles

1. Select **Network > IP QoS,** and then **Add New Profile.** The **IP QoS Profile** page opens.
2. Under **Profile name,** specify **Voice.**
3. Under **Protocol,** from the drop-down list select **TCP.**
4. Under **Start port,** from the drop-down list select **SIP. Start port** and **End port** are automatically populated with the correct value: **5060.**

5. Under **Priority,** from the drop-down list select **Very High.**



Add/Edit IP QoS profile

Settings

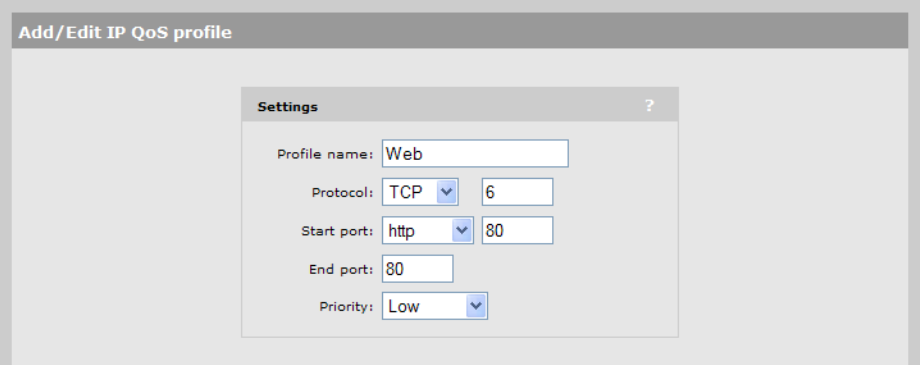
Profile name: Voice
Protocol: TCP 6
Start port: SIP 5060
End port: 5060
Priority: Very high

6. Select **Save.**

Note

You could also create another profile using the same parameters but for UDP to cope with any kind of SIP traffic.

7. On the **IP QoS Profile** page select **Add New Profile.**
8. Under **Profile name,** specify **Web.**
9. Under **Protocol,** from the drop-down list select **TCP.**
10. Under **Start port,** from the drop-down list select **http. Start port** and **End port** are automatically populated with the common HTTP port, **80.**
11. Under **Priority,** from the drop-down list select **Low.**



Add/Edit IP QoS profile

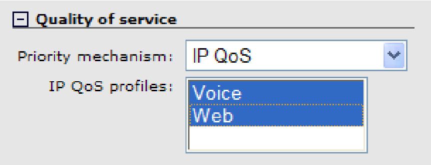
Settings

Profile name: Web
Protocol: TCP 6
Start port: http 80
End port: 80
Priority: Low

12. Select **Save.**

Assign the profiles to a VSC

1. In the **Network Tree** select **VSCs** (if not visible, first select the + symbol to the left of **Controller**), and then select one of the VSC profiles in the **Name** column. Scroll down to the **Quality of service** section of the **Virtual AP** box.



⊟ Quality of service

Priority mechanism: IP QoS

IP QoS profiles: Voice, Web

2. Set **Priority mechanism** to **IP QoS.**
3. In **IP QoS profiles**, Ctrl-click each profile .
4. Select **Save.**

IGMP proxy

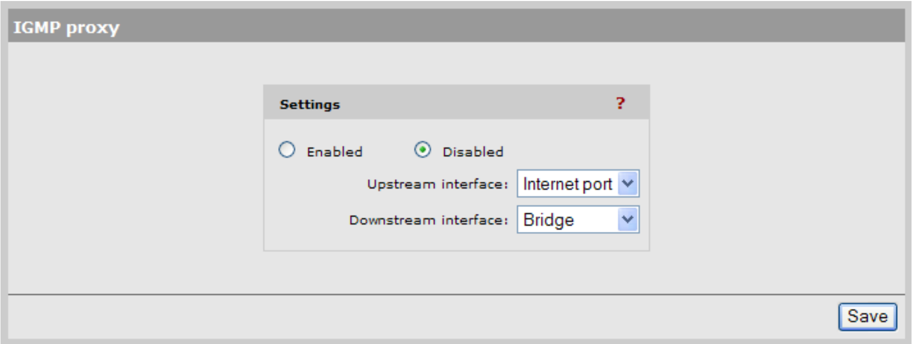
This feature provides support for multicast routing using IGMP (Internet Group Management Protocol), which is typically required by the controller. When enabled, the controller:

- Routes all multicast traffic received on the Upstream interface to the Downstream interface.
- Listens for IGMP host membership reports from authenticated users on the Downstream interface and forwards them to the Upstream interface. IGMP host membership reports from unauthenticated users are ignored.

Note

- An access list definition must be created to accept the multicast traffic (video streams, etc.)
- Due to the nature of multicast traffic, once a user registers for a stream it automatically becomes visible to unauthenticated users as well. However, unauthenticated users are not able to register with the IGMP group.

To view and configure IGMP proxy settings, select **Controller >> Network > IGMP proxy**.



IGMP proxy

Settings

○ Enabled ● Disabled

Upstream interface: Internet port

Downstream interface: Bridge

4

Wireless configuration

Contents

Wireless coverage

As a starting point for planning your network, you can assume that when operating at high power, an AP radio provides a wireless networking area (also called a wireless cell) of up to 300 feet (100 meters) in diameter. Before creating a permanent installation however, you should always perform a site survey (see *Wireless neighborhood on page 4-34*) to determine the optimal settings and location for the AP.

The following sections provide information on wireless coverage. A tool that can help simplify planning a secure wireless network is the HP ProCurve RF Planner. For more information, see the *RF Planner Admin Guide*.

Note Supported wireless modes, operating channels, and power output vary according to the AP model, and are governed by the regulations of the country in which the AP is operating (called the regulatory domain). For a list of all operating modes, see *Radio configuration on page 4-8*. To set the regulatory domain, see *Assigning country settings to a group on page 6-30*.

Factors limiting wireless coverage

Wireless coverage is affected by the factors discussed in this section.

Radio power

More radio power means better signal quality and the ability to create bigger wireless cells. However, cell size should generally not exceed the range of transmission supported by wireless users. If it does, users will be able to receive signals from the AP but will not be able to reply, rendering the connection useless.

Further, when more than one AP operates in an area, you must adjust wireless cell size to reduce interference between APs. An automatic power control feature is available to address this challenge. See *Transmit power control on page 4-32*.

Antenna configuration

Antennas play a large role in determining the shape of the wireless cell and transmission distance. See the specifications for the antennas you use to determine how they affect wireless coverage.

Interference

Interference is caused by other APs or devices that operate in the same frequency band as the AP and can substantially affect throughput. Advanced wireless configuration features are available to automatically eliminate this problem. See *Radio configuration on page 4-8*.

In addition, the several tools are available to diagnose interference problems as they occur.

- Select **Controlled APs >> Wireless > Neighborhood** to view a list of wireless APs operating in the immediate area so that you can effectively set the operating frequencies. See *Wireless neighborhood on page 4-34.*

- Select **Controlled APs >> Overview > Wireless rates** to view information about data rates for all connected client stations. This makes it easy to determine if low-speed clients are affecting network performance. To prevent low-speed clients from connecting, you can use the **Allowed wireless rates** option when defining a VSC. See *Virtual AP on page 5-10*.
- Select **Controlled APs >> Overview > Wireless clients** to view information about each connected wireless client.
- Select **Controlled APs > [*group*] > [*AP*] >> Status > Wireless** to view detailed wireless information for an AP, including: packets sent and received, transmission errors, and other low-level events.

Caution APs that operate in the 2.4 GHz band may experience interference from 2.4 GHz cordless phones and microwave ovens.

Physical characteristics of the location

To maximize coverage of a wireless cell, wireless APs are best installed in an open area with as few obstructions as possible. Try to choose a location that is central to the area being served.

Radio waves cannot penetrate metal; they are reflected instead. A wireless AP can transmit through wood or plaster walls and closed windows; however, the steel reinforcing found in concrete walls and floors may block transmissions or reduce signal quality by creating reflections. This can make it difficult or impossible for a single AP to serve users on different floors in a concrete building. Such installations require a separate wireless AP on each floor.

Configuring overlapping wireless cells

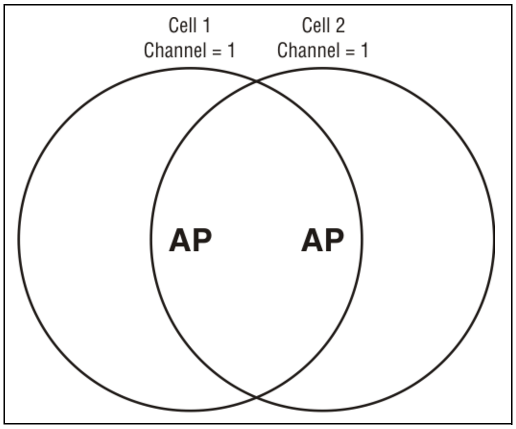
Overlapping wireless cells occur when two or more APs are operating within transmission range of each other. This may be under your control, (for example, when you use several cells to cover a large location), or out of your control (for example, when your neighbors set up their own wireless networks). When APs are operating in the 2.4 GHz band, overlapping wireless cells can cause performance degradation due to insufficient channel separation.

Performance degradation and channel separation

When two wireless cells operating on the same frequency overlap, throughput can be reduced in both cells. Reduced throughput occurs because a wireless user that is attempting to transmit data defers (delays) transmission if another station is transmitting. In a network with many users and much traffic, these delayed transmissions can severely affect performance, because wireless users may defer several times before the channel becomes available. If a wireless user is forced to delay transmission too many times, data can be lost.

Delays and lost transmissions can severely reduce throughput on a network. To view this information about your network, select **Controller > Controlled APs {*group*} > {*AP*} >> Status > Wireless.** For recommendations on using this information to diagnose wireless problems, see the online help for this page.

The following example shows two overlapping wireless cells operating on the same channel (frequency). Since both APs are within range of each other, the number of deferred transmissions can be large.



The solution to this problem is to configure the two AP to operate on different channels. Unfortunately, in the 2.4 GHz band, adjacent channels overlap. So even though APs are operating on different channels, interference can still our. This is not an issue in the 5 GHz band, as all channels are non-overlapping.

Selecting channels in the 2.4 GHz band

In the 2.4 GHz band, the center frequency of each channel is spaced 5 MHz apart (except for channel 14). Each 802.11 channel uses 20 MHz of bandwidth (10 MHz above and 10 MHz below the center frequency), which means that adjacent channels overlap and interfere with each other as follows:

Channel	Center frequency	Overlaps channels
1	2412	2, 3
2	2417	1, 3, 4
3	2422	1, 2, 4, 5
4	2427	2, 3, 5, 6
5	2432	3, 4, 6, 7
6	2437	4, 5, 7, 8
7	2442	5, 6, 8, 9

Channel	Center frequency	Overlaps channels
8	2447	6, 7, 9, 10
9	2452	7, 8, 10, 11
10	2457	8, 9, 11, 12
11	2462	9, 10, 12, 13
12	2467	10, 11, 13
13	2472	11, 12,
14	2484	

To avoid interference, APs in the same area must use channels that are separated by at least 25 MHz (5 channels). For example, if an AP is operating on channel 3, and a second AP is operating on channel 7, interference occurs on channel 5. For optimal performance, the second AP should be moved to channel 8 (or higher).

With the proliferation of wireless networks, it is possible that the wireless cells of APs outside your control overlap your intended area of coverage. To choose the best operating frequency, select **Controlled APs >> Overview > Neighborhood** to view a list of all APs that are operating nearby and their operating frequencies.

The number of channels available for use in a particular country are determined by the regulations defined by the local governing body and are automatically configured by the AP based on the **Country** setting you define. (See *Assigning country settings to a group on page 6-30*.) This means that the number of non-overlapping channels available to you varies by geographical location.

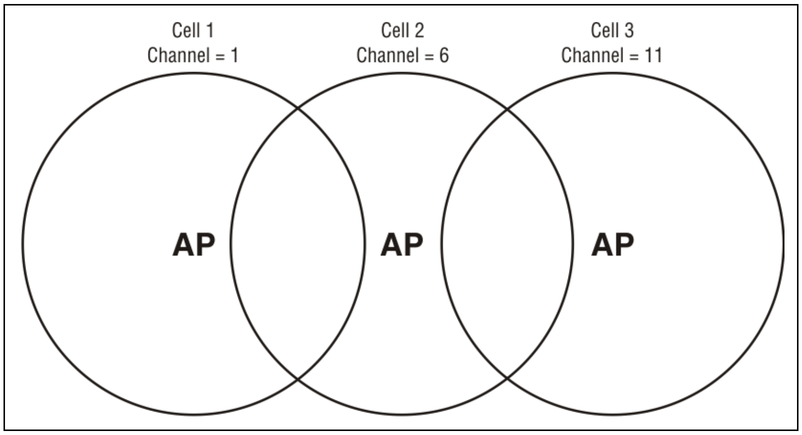
The following table shows the number of channels that are available in North America, Japan, and Europe.

Region	Available channels
North America	1 to 11
Japan	1 to 14
Europe	1 to 13

Since the minimum recommended separation between overlapping channels is 25 MHz (five channels) the recommended maximum number of overlapping cells you can have in most regions is three. The following table gives examples relevant to North America, Japan, and Europe (applies to 22 MHz channels in the 2.4 GHz band).

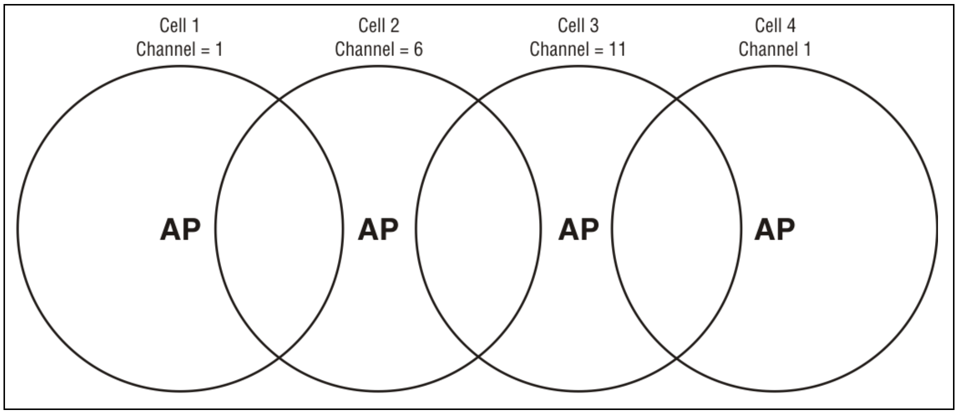
North America	Japan	Europe
■ cell 1 on channel 1 ■ cell 2 on channel 6 ■ cell 3 on channel 11	■ cell 1 on channel 1 ■ cell 2 on channel 7 ■ cell 3 on channel 14	■ cell 1 on channel 1 ■ cell 2 on channel 7 ■ cell 3 on channel 13

In North America you can create an installation as shown in the following figure.



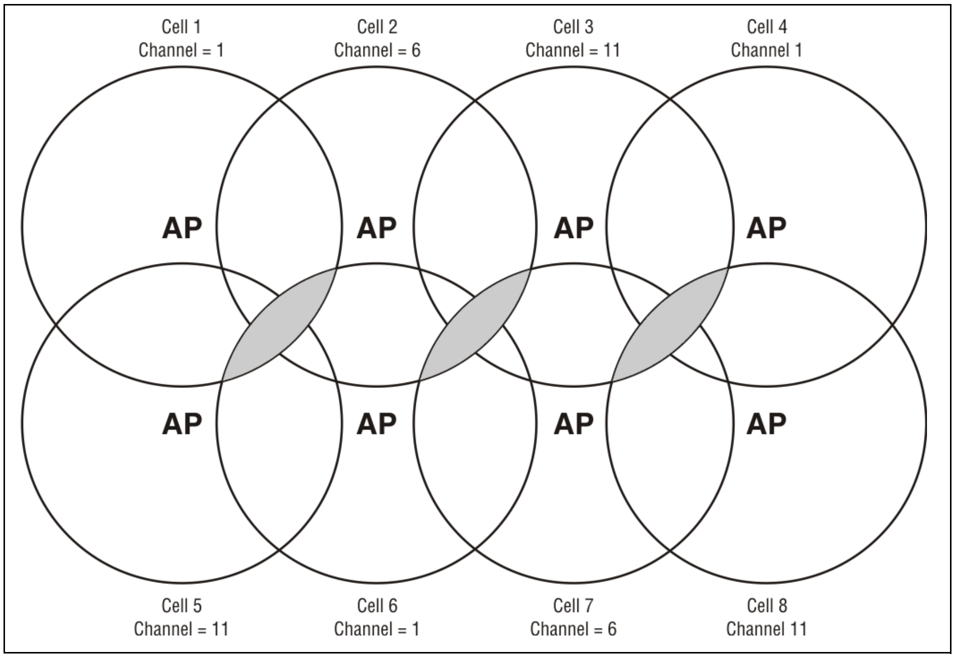
Reducing transmission delays by using different operating frequencies in North America.

Alternatively, you can stagger cells to reduce overlap and increase channel separation, as shown in the following figure.



Using only three frequencies across multiple cells in North America.

This strategy can be expanded to cover an even larger area using three channels, as shown in the following figure.



Using three frequencies to cover a large area in North America. Gray areas indicate overlap between two cells that use the same frequency.

Distance between APs

Not supported on: E-MSM430, E-MSM460, E-MSM466

In environments where the number of wireless frequencies is limited, it can be beneficial to adjust the receiver sensitivity of the AP. To make the adjustment, select **Controlled APS >> Configuration > Radio list > [*radio*]** and set the **Distance between access points** option.

For most installations, **Distance between access points** should be set to **Large.** However, if you are installing several wireless APs and the channels available to you do not provide enough separation, reducing receiver sensitivity can help you to reduce the amount of crosstalk between wireless APs.

Another benefit to using reduced settings is that it improves roaming performance. Wireless users switch between APs more frequently.

Automatic transmit power control

The automatic power control feature enables the AP to dynamically adjust its transmission power to avoid causing interference with neighboring HP ProCurve APs. For information see *Transmit power control on page 4-32*.

Supporting 802.11n and legacy wireless clients

The 802.11n standard is very similar to the 802.11g standard, in that both provide mechanisms to support older wireless standards. In the case of 802.11g, protection mechanisms were created to allow 802.11b and 802.11g wireless devices to co-exist on the same frequencies. The data rates of 802.11g (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) are transmitted using Orthogonal Frequency Division Multiplexing (OFDM) modulation, while the data rates of 802.11b are transmitted using Direct Sequence Spread Spectrum (DSSS) modulation. Since older 802.11b-only clients cannot detect OFDM transmissions, 802.11g clients must “protect” their transmissions by first sending a frame using DSSS modulation. This frame – usually a CTS-to-self or RTS/CTS exchange – alerts 802.11b clients to not attempt to transmit for a specified period of time.

If protection is not used, 802.11b clients may transmit a frame while an 802.11g frame is already being sent. This leads to a collision and both devices need to re-transmit. If there are enough devices in the network, the collision rate will grow exponentially and prevent any useful throughput from the wireless network.

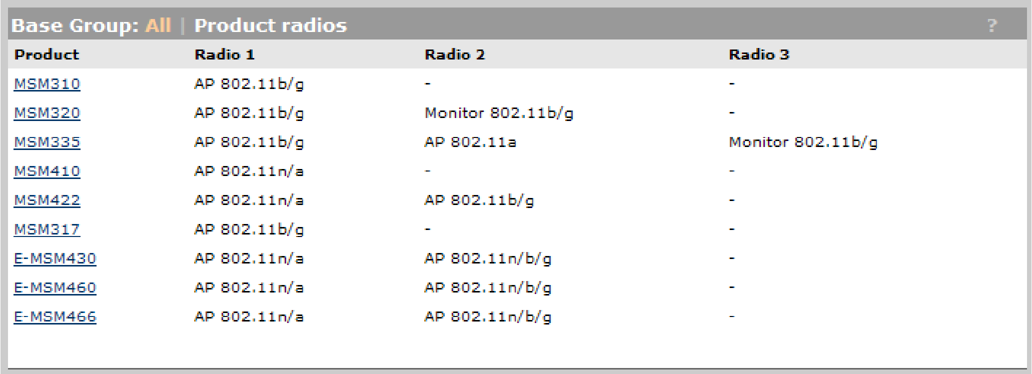
802.11n clients face the same problem as described above – legacy 802.11b clients cannot detect the High Throughput (HT) rates that 802.11n uses. So to avoid causing excessive collisions, 802.11n clients must use the same protection mechanisms when a legacy client is present. Even the most efficient protection mechanism (CTS-to-self) causes a substantial decline in throughput; performance can decline by as much as 50 percent. For this reason, the protection behavior of the E-MSM430, E-MSM460, and E-MSM466 can be configured (see *Tx protection on page 4-30*) to allow network administrators greater flexibility over their deployments.

Note

802.11n clients can only achieve maximum throughput when legacy clients are not present on the same radio.

Radio configuration

To define configuration settings for a radio, select **Controller > Controlled APs >> Configuration > Radio list**. This opens the Product radios page which lists all radios on all AP models. For example:



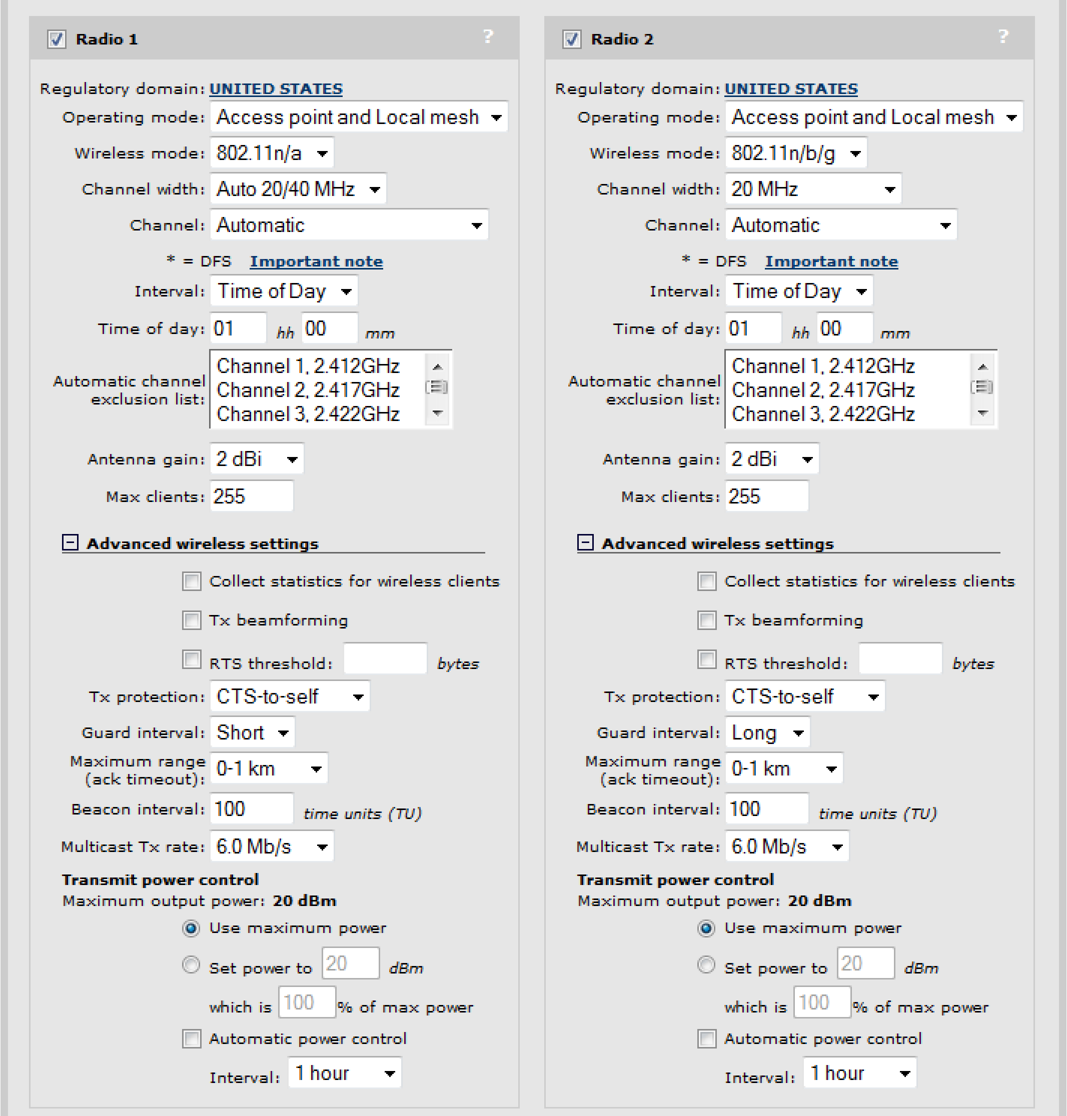
Base Group: All | Product radios

Product	Radio 1	Radio 2	Radio 3
MSM310	AP 802.11b/g	-	-
MSM320	AP 802.11b/g	Monitor 802.11b/g	-
MSM335	AP 802.11b/g	AP 802.11a	Monitor 802.11b/g
MSM410	AP 802.11n/a	-	-
MSM422	AP 802.11n/a	AP 802.11b/g	-
MSM317	AP 802.11b/g	-	-
E-MSM430	AP 802.11n/a	AP 802.11n/b/g	-
E-MSM460	AP 802.11n/a	AP 802.11n/b/g	-
E-MSM466	AP 802.11n/a	AP 802.11n/b/g	-

To configure the radios for a product, select the product in the list. This opens the Radio(s) configuration page. The contents of this page varies depending on the product. The following screen shots show the Radio(s) configuration page for various products.

In each case, **Operating mode** is set to **Access Point and Local Mesh**, and **Advanced wireless settings** has been expanded to show the complete set of configurable settings.

E-MSM466



☑ **Radio 1** ?

Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11n/a
Channel width: Auto 20/40 MHz
Channel: Automatic
* = DFS Important note
Interval: Time of Day
Time of day: 01 *hh* 00 *mm*
Automatic channel exclusion list: Channel 1, 2.412GHz; Channel 2, 2.417GHz; Channel 3, 2.422GHz
Antenna gain: 2 dBi
Max clients: 255

⊟ **Advanced wireless settings**

□ Collect statistics for wireless clients
□ Tx beamforming
□ RTS threshold: *bytes*
Tx protection: CTS-to-self
Guard interval: Short
Maximum range (ack timeout): 0-1 km
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 6.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**
● Use maximum power
○ Set power to 20 *dBm*
which is 100 % of max power
□ Automatic power control
Interval: 1 hour

☑ **Radio 2** ?

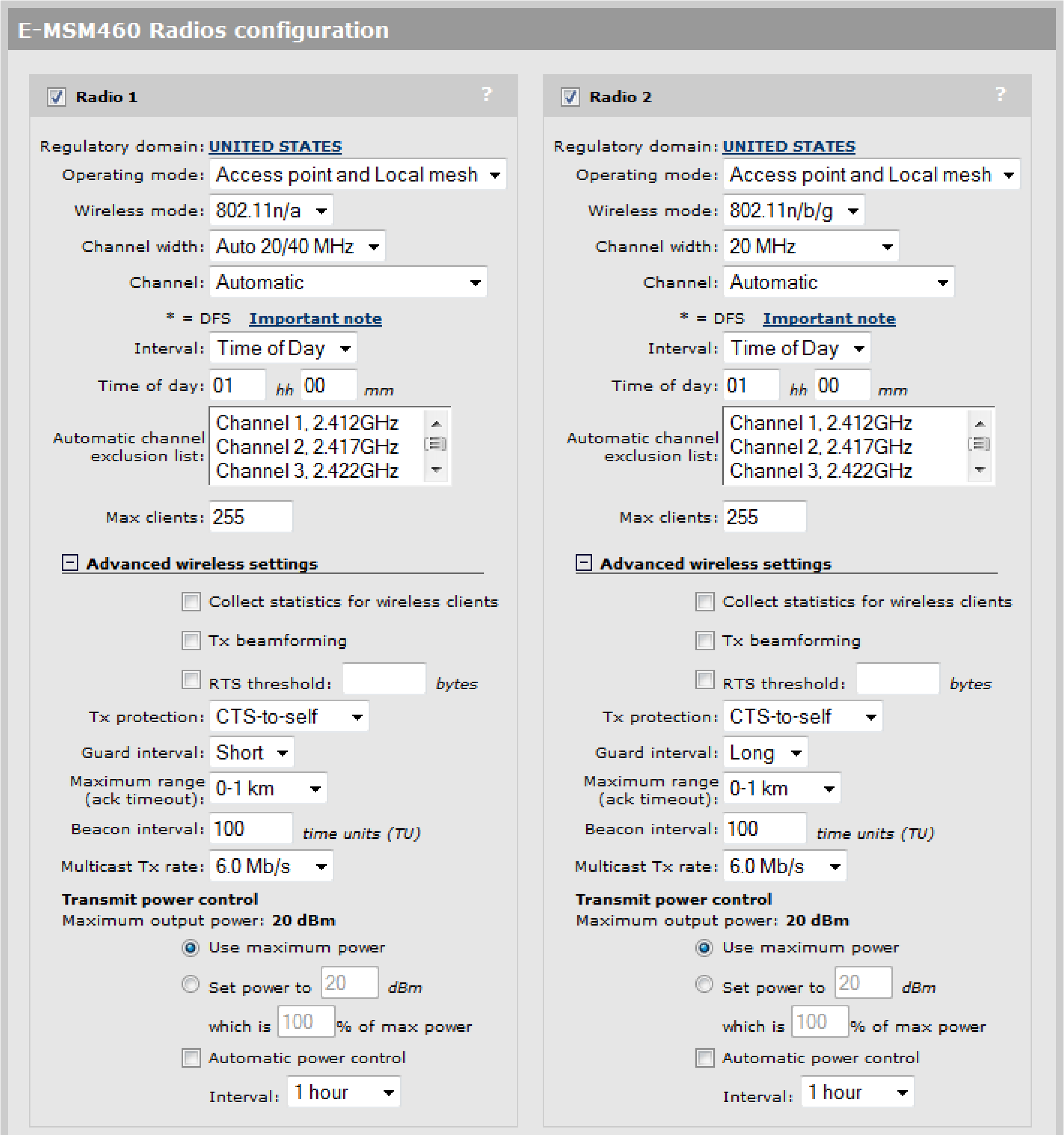
Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11n/b/g
Channel width: 20 MHz
Channel: Automatic
* = DFS Important note
Interval: Time of Day
Time of day: 01 *hh* 00 *mm*
Automatic channel exclusion list: Channel 1, 2.412GHz; Channel 2, 2.417GHz; Channel 3, 2.422GHz
Antenna gain: 2 dBi
Max clients: 255

⊟ **Advanced wireless settings**

□ Collect statistics for wireless clients
□ Tx beamforming
□ RTS threshold: *bytes*
Tx protection: CTS-to-self
Guard interval: Long
Maximum range (ack timeout): 0-1 km
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 6.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**
● Use maximum power
○ Set power to 20 *dBm*
which is 100 % of max power
□ Automatic power control
Interval: 1 hour

E-MSM460 and E-MSM430



E-MSM460 Radios configuration

☑ **Radio 1**

Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11n/a
Channel width: Auto 20/40 MHz
Channel: Automatic
* = DFS Important note
Interval: Time of Day
Time of day: 01 *hh* 00 *mm*
Automatic channel exclusion list: Channel 1, 2.412GHz / Channel 2, 2.417GHz / Channel 3, 2.422GHz
Max clients: 255

⊟ **Advanced wireless settings**

□ Collect statistics for wireless clients
□ Tx beamforming
□ RTS threshold: *bytes*
Tx protection: CTS-to-self
Guard interval: Short
Maximum range (ack timeout): 0-1 km
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 6.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**
● Use maximum power
○ Set power to 20 *dBm*
which is 100 % of max power
□ Automatic power control
Interval: 1 hour

☑ **Radio 2**

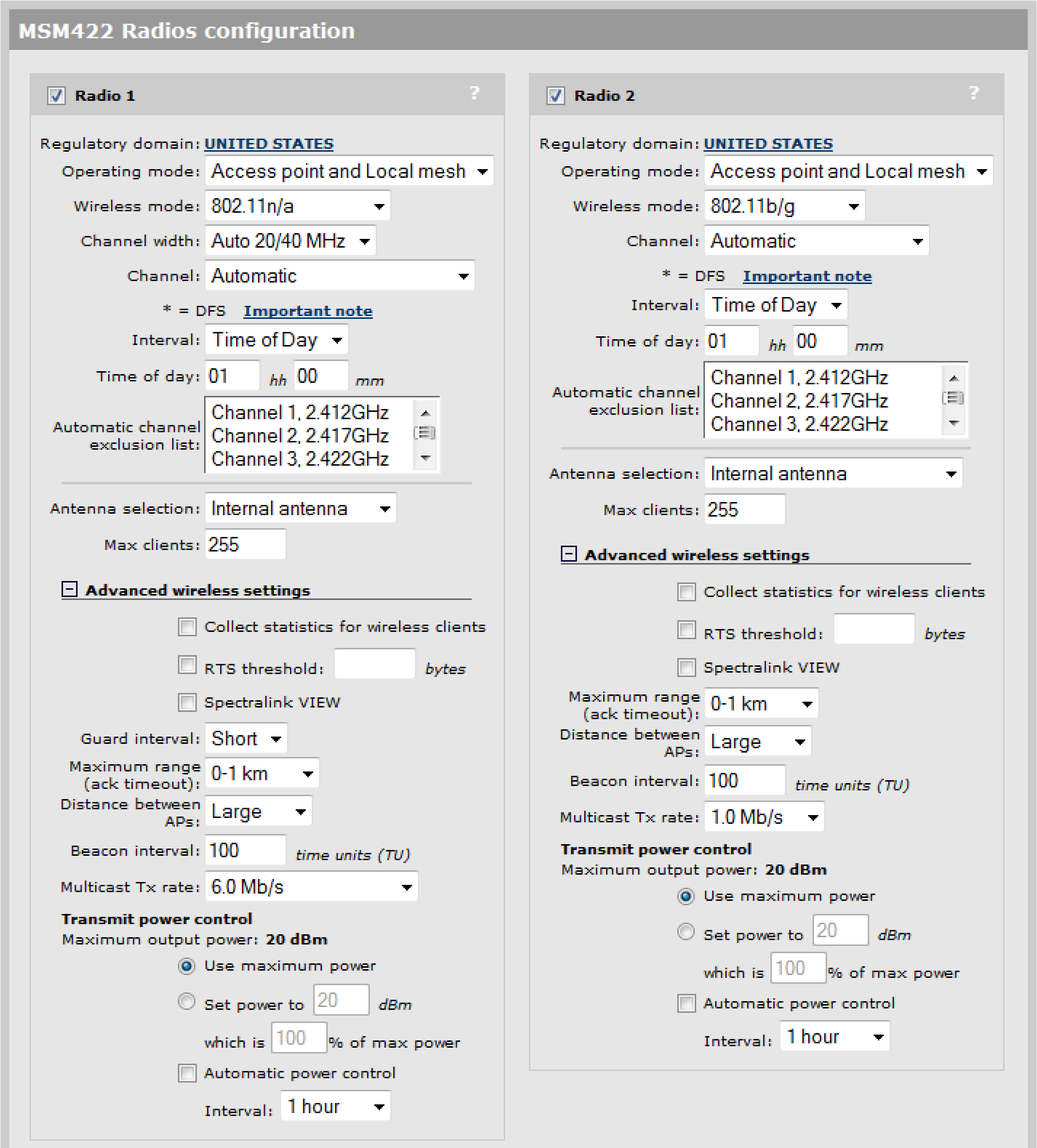
Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11n/b/g
Channel width: 20 MHz
Channel: Automatic
* = DFS Important note
Interval: Time of Day
Time of day: 01 *hh* 00 *mm*
Automatic channel exclusion list: Channel 1, 2.412GHz / Channel 2, 2.417GHz / Channel 3, 2.422GHz
Max clients: 255

⊟ **Advanced wireless settings**

□ Collect statistics for wireless clients
□ Tx beamforming
□ RTS threshold: *bytes*
Tx protection: CTS-to-self
Guard interval: Long
Maximum range (ack timeout): 0-1 km
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 6.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**
● Use maximum power
○ Set power to 20 *dBm*
which is 100 % of max power
□ Automatic power control
Interval: 1 hour

MSM422



MSM422 Radios configuration

☑ **Radio 1**

Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11n/a
Channel width: Auto 20/40 MHz
Channel: Automatic
* = DFS Important note
Interval: Time of Day
Time of day: 01 *hh* 00 *mm*
Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz
Antenna selection: Internal antenna
Max clients: 255

⊟ **Advanced wireless settings**

□ Collect statistics for wireless clients
□ RTS threshold: *bytes*
□ Spectralink VIEW
Guard interval: Short
Maximum range (ack timeout): 0-1 km
Distance between APs: Large
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 6.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**
● Use maximum power
○ Set power to 20 *dBm*
which is 100 % of max power
□ Automatic power control
Interval: 1 hour

☑ **Radio 2**

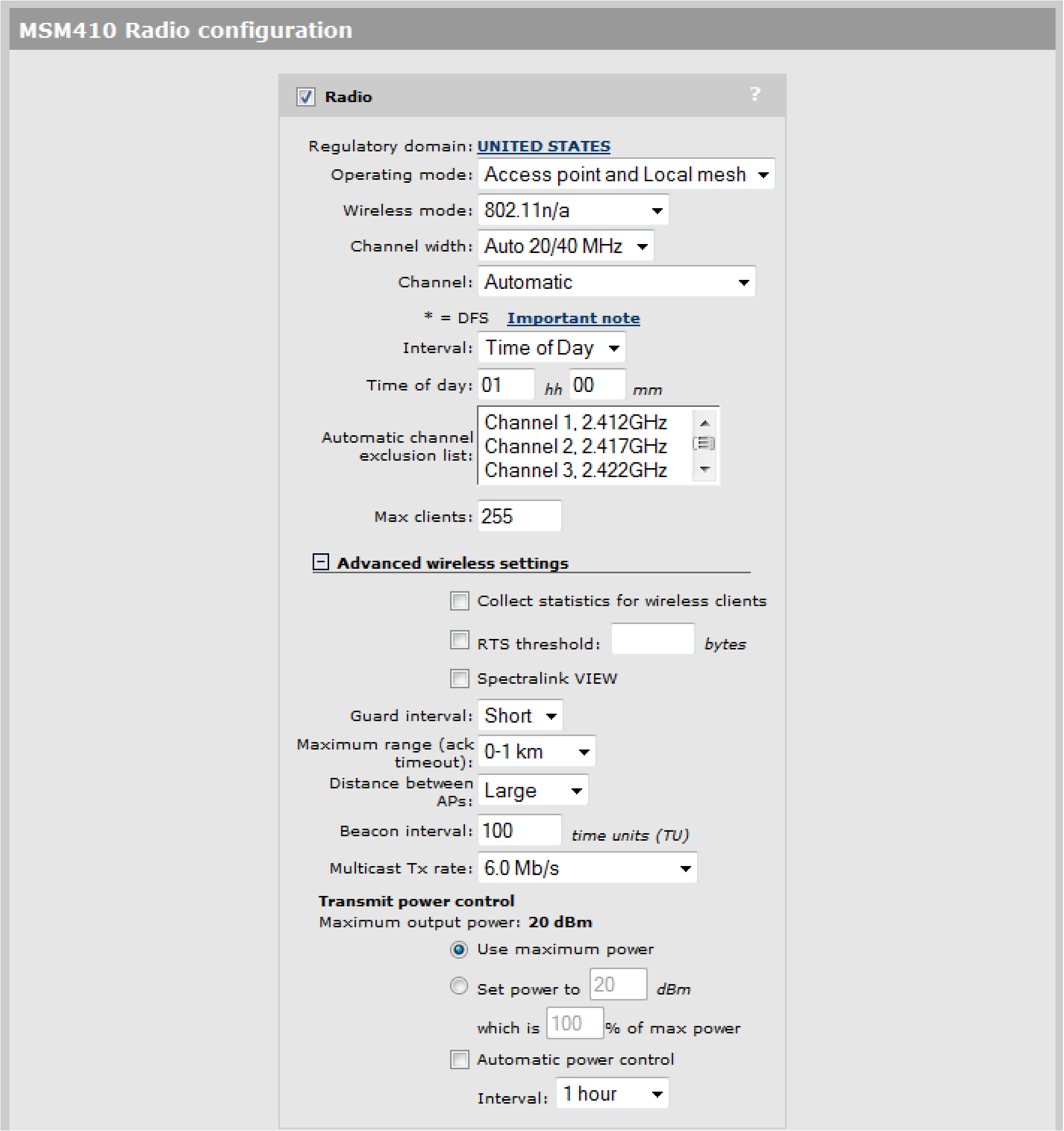
Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11b/g
Channel: Automatic
* = DFS Important note
Interval: Time of Day
Time of day: 01 *hh* 00 *mm*
Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz
Antenna selection: Internal antenna
Max clients: 255

⊟ **Advanced wireless settings**

□ Collect statistics for wireless clients
□ RTS threshold: *bytes*
□ Spectralink VIEW
Maximum range (ack timeout): 0-1 km
Distance between APs: Large
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 1.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**
● Use maximum power
○ Set power to 20 *dBm*
which is 100 % of max power
□ Automatic power control
Interval: 1 hour

MSM410



MSM410 Radio configuration

☑ **Radio** ?

Regulatory domain: UNITED STATES

Operating mode: Access point and Local mesh

Wireless mode: 802.11n/a

Channel width: Auto 20/40 MHz

Channel: Automatic

* = DFS Important note

Interval: Time of Day

Time of day: 01 *hh* 00 *mm*

Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz

Max clients: 255

⊟ **Advanced wireless settings**

□ Collect statistics for wireless clients

□ RTS threshold: *bytes*

□ Spectralink VIEW

Guard interval: Short

Maximum range (ack timeout): 0-1 km

Distance between APs: Large

Beacon interval: 100 *time units (TU)*

Multicast Tx rate: 6.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**

● Use maximum power

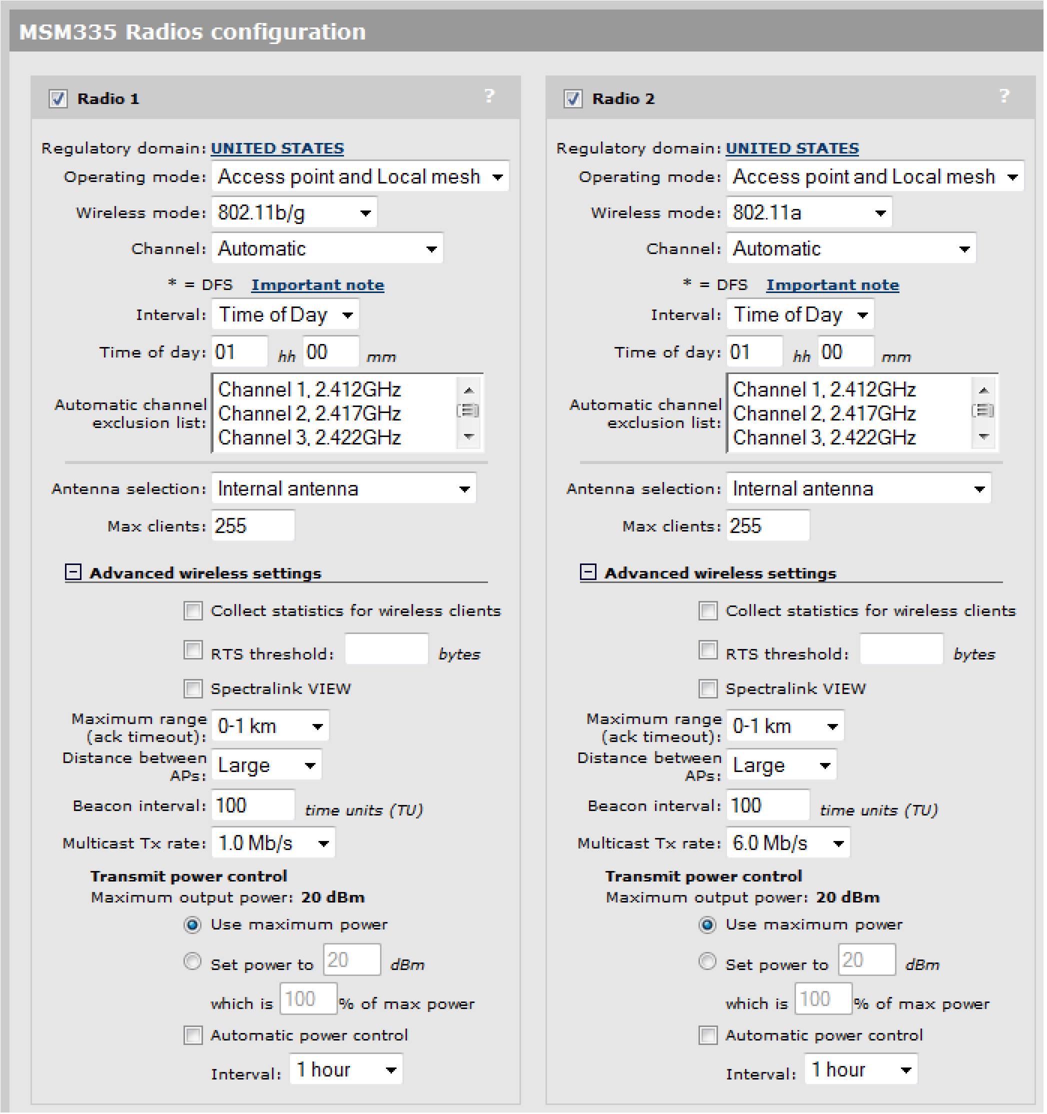
○ Set power to 20 *dBm*

which is 100 % of max power

□ Automatic power control

Interval: 1 hour

MSM335 (radio 1 and 2)



MSM335 Radios configuration

☑ Radio 1

Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11b/g
Channel: Automatic
* = DFS Important note
Interval: Time of Day
Time of day: 01 *hh* 00 *mm*
Automatic channel exclusion list: Channel 1, 2.412GHz / Channel 2, 2.417GHz / Channel 3, 2.422GHz
Antenna selection: Internal antenna
Max clients: 255

⊟ Advanced wireless settings

☐ Collect statistics for wireless clients
☐ RTS threshold: *bytes*
☐ Spectralink VIEW
Maximum range (ack timeout): 0-1 km
Distance between APs: Large
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 1.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**
● Use maximum power
○ Set power to 20 *dBm*
which is 100 % of max power
☐ Automatic power control
Interval: 1 hour

☑ Radio 2

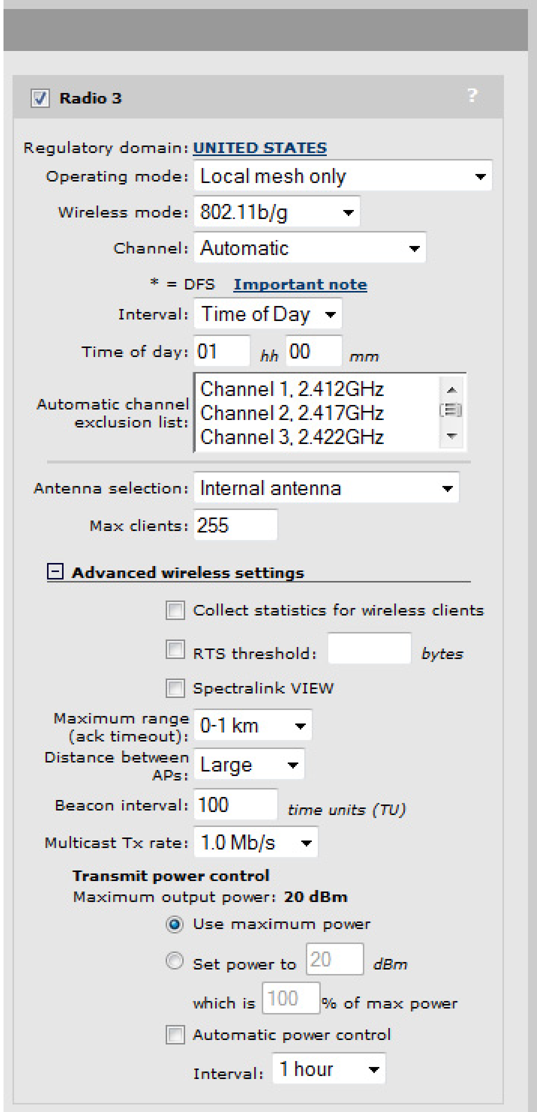
Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11a
Channel: Automatic
* = DFS Important note
Interval: Time of Day
Time of day: 01 *hh* 00 *mm*
Automatic channel exclusion list: Channel 1, 2.412GHz / Channel 2, 2.417GHz / Channel 3, 2.422GHz
Antenna selection: Internal antenna
Max clients: 255

⊟ Advanced wireless settings

☐ Collect statistics for wireless clients
☐ RTS threshold: *bytes*
☐ Spectralink VIEW
Maximum range (ack timeout): 0-1 km
Distance between APs: Large
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 6.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**
● Use maximum power
○ Set power to 20 *dBm*
which is 100 % of max power
☐ Automatic power control
Interval: 1 hour

MSM335 (radio 3)



☑ **Radio 3**

Regulatory domain: UNITED STATES

Operating mode: Local mesh only

Wireless mode: 802.11b/g

Channel: Automatic

* = DFS **Important note**

Interval: Time of Day

Time of day: 01 *hh* 00 *mm*

Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz

Antenna selection: Internal antenna

Max clients: 255

Advanced wireless settings

□ Collect statistics for wireless clients

□ RTS threshold: *bytes*

□ Spectralink VIEW

Maximum range (ack timeout): 0-1 km

Distance between APs: Large

Beacon interval: 100 *time units (TU)*

Multicast Tx rate: 1.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**

● Use maximum power

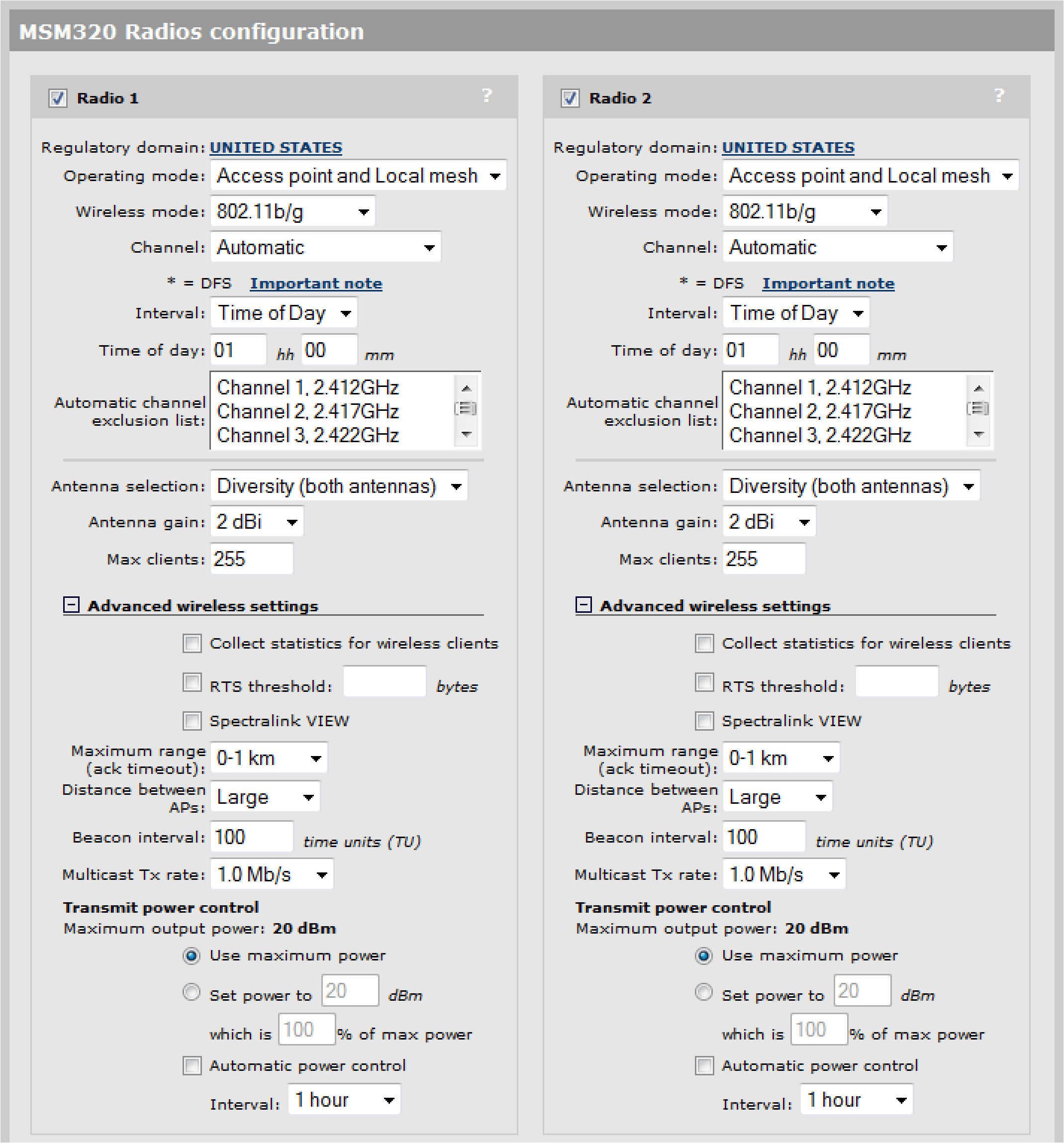
○ Set power to 20 *dBm*

which is 100 % of max power

□ Automatic power control

Interval: 1 hour

MSM320



MSM320 Radios configuration

☑ **Radio 1** ?

Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11b/g
Channel: Automatic
* = DFS Important note
Interval: Time of Day
Time of day: 01 *hh* 00 *mm*
Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz
Antenna selection: Diversity (both antennas)
Antenna gain: 2 dBi
Max clients: 255

⊟ **Advanced wireless settings**

☐ Collect statistics for wireless clients
☐ RTS threshold: *bytes*
☐ Spectralink VIEW
Maximum range (ack timeout): 0-1 km
Distance between APs: Large
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 1.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**
● Use maximum power
○ Set power to 20 *dBm*
which is 100 % of max power
☐ Automatic power control
Interval: 1 hour

☑ **Radio 2** ?

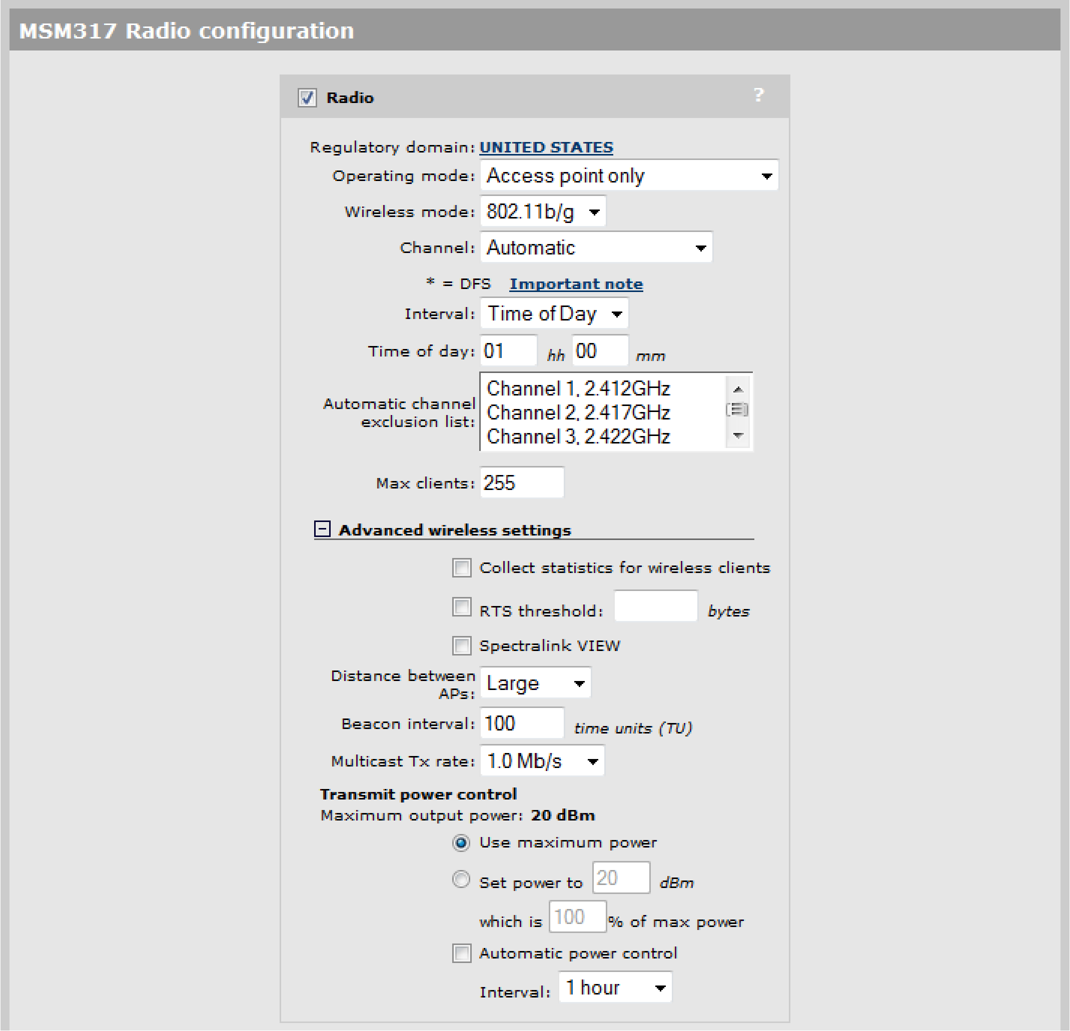
Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11b/g
Channel: Automatic
* = DFS Important note
Interval: Time of Day
Time of day: 01 *hh* 00 *mm*
Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz
Antenna selection: Diversity (both antennas)
Antenna gain: 2 dBi
Max clients: 255

⊟ **Advanced wireless settings**

☐ Collect statistics for wireless clients
☐ RTS threshold: *bytes*
☐ Spectralink VIEW
Maximum range (ack timeout): 0-1 km
Distance between APs: Large
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 1.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**
● Use maximum power
○ Set power to 20 *dBm*
which is 100 % of max power
☐ Automatic power control
Interval: 1 hour

MSM317



MSM317 Radio configuration

☑ Radio

Regulatory domain: UNITED STATES

Operating mode: Access point only

Wireless mode: 802.11b/g

Channel: Automatic

* = DFS Important note

Interval: Time of Day

Time of day: 01 hh 00 mm

Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz

Max clients: 255

Advanced wireless settings

□ Collect statistics for wireless clients

□ RTS threshold: bytes

□ Spectralink VIEW

Distance between APs: Large

Beacon interval: 100 time units (TU)

Multicast Tx rate: 1.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**

● Use maximum power

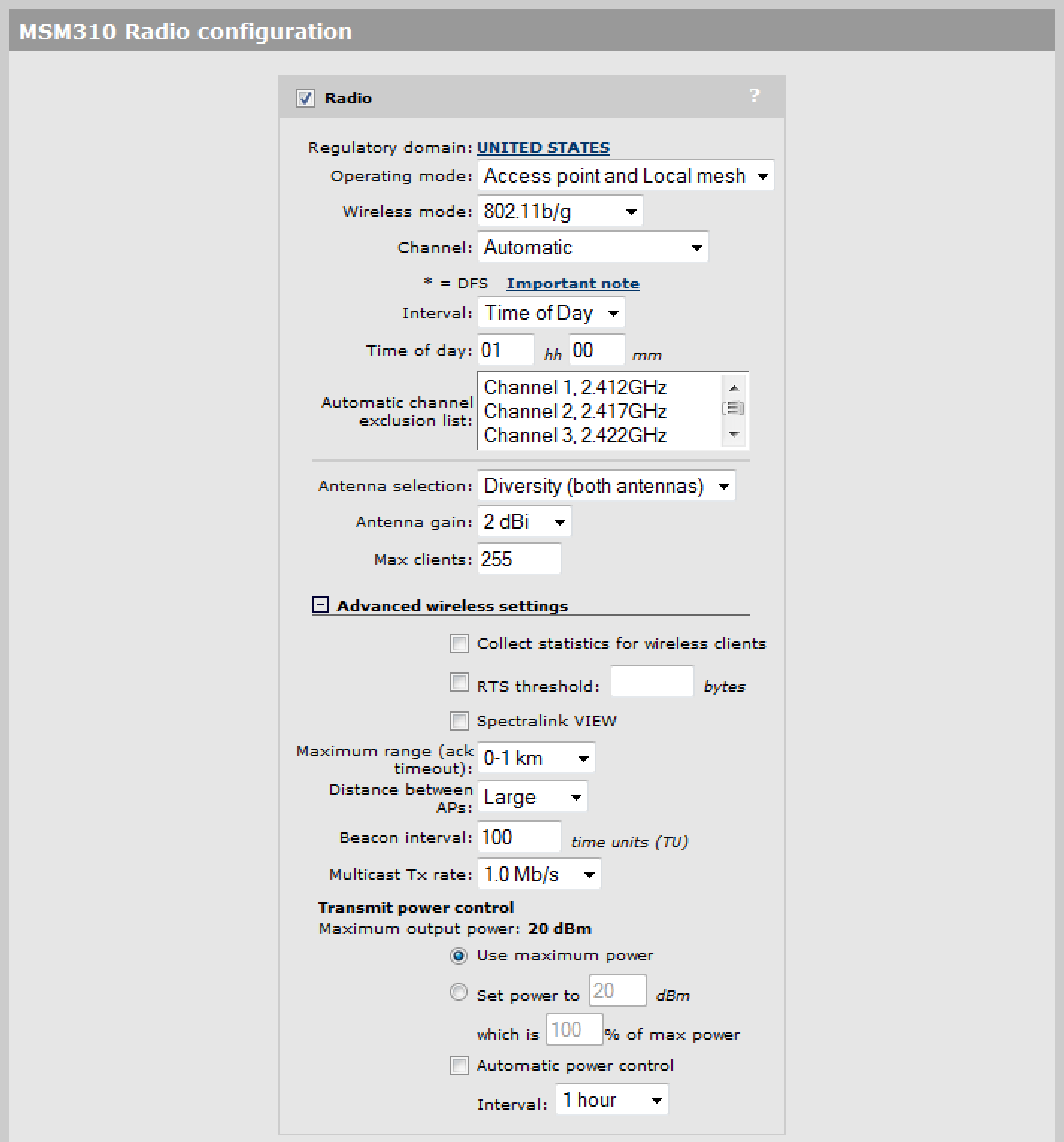
○ Set power to 20 dBm

which is 100 % of max power

□ Automatic power control

Interval: 1 hour

MSM310



MSM310 Radio configuration

☑ Radio

Regulatory domain: UNITED STATES

Operating mode: Access point and Local mesh

Wireless mode: 802.11b/g

Channel: Automatic

* = DFS Important note

Interval: Time of Day

Time of day: 01 *hh* 00 *mm*

Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz

Antenna selection: Diversity (both antennas)

Antenna gain: 2 dBi

Max clients: 255

⊟ **Advanced wireless settings**

☐ Collect statistics for wireless clients

☐ RTS threshold: *bytes*

☐ Spectralink VIEW

Maximum range (ack timeout): 0-1 km

Distance between APs: Large

Beacon interval: 100 *time units (TU)*

Multicast Tx rate: 1.0 Mb/s

Transmit power control

Maximum output power: **20 dBm**

● Use maximum power

○ Set power to 20 *dBm*

which is 100 % of max power

☐ Automatic power control

Interval: 1 hour

Radio configuration parameters

This section provides definitions for all configuration parameters that are present on all products.

Regulatory domain

Indicates the geographical region in which the AP is operating. To set the regulatory domain, see *Assigning country settings to a group on page 6-30*.

Operating mode

Select the operating mode for the radio. Available options are:

- **Access point and Local mesh:** Standard operating mode provides support for all wireless functions. (Not supported on radio 3 on the MSM335.)
- **Access point only:** Only provides AP functionality, local mesh links cannot be created. (Not supported on radio 3 on the MSM335.)
- **Local mesh only:** Only provides local mesh functionality. Wireless client stations cannot connect.
- **Monitor:** Disables AP and local mesh functions. Use this option for continuous scanning across all channels in all wireless modes. See the results of the scans by selecting **Controlled APS >> Overview > Neighborhood**.
- **Sensor:** Enables RF sensor functionality on the radio. HP APs are smart APs, and do not forward broadcast packets when no client stations are connected. Therefore, the RF sensor function will not be able to detect these APs unless they have at least one connected wireless client station. This feature requires that the appropriate license is installed on the AP. See *Licenses on page 20-6*.

The following table shows the operating modes supported for each product.

Product	Access point and Local mesh	Access point only	Local mesh only	Monitor	Sensor
MSM310 MSM310-R	✔	✔	✔	✔	✕
MSM320 MSM320-R	✔	✔	✔	✔	✔
MSM325	✔	✔	✔	✔	✔
MSM335 (Radio 1 + 2)	✔	✔	✔	✔	✔
MSM335 (Radio 3)	✕	✕	✔	✔	✔
MSM410	✔	✔	✔	✔	✕

Product	Access point and Local mesh	Access point only	Local mesh only	Monitor	Sensor
MSM422	✔	✔	✔	✔	✕
MSM317	✕	✔	✕	✔	✕
E-MSM430	✔	✔	✔	✔	✕
E-MSM460	✔	✔	✔	✔	✕
E-MSM466	✔	✔	✔	✔	✕

The following table shows all radio parameters that are configurable for each operating mode.

Parameter	Access point and Local mesh	Access point only	Local mesh only	Monitor	Sensor
Regulatory domain	✔	✔	✔	✔	✔
Wireless mode	✔	✔	✔	✔	✕
Channel width	✔	✔	✔	✔	✕
Channel extension	✔	✔	✔	✔	✕
Channel	✔	✔	✔	✔	✕
Interval	✔	✔	✔	✕	✕
Time of day	✔	✔	✔	✕	✕
Automatic channel exclusion list	✔	✔	✔	✕	✕
Antenna selection	✔	✔	✔	✕	✔
Antenna gain	✔	✔	✔	✕	✕
Max clients	✔	✔	✔	✕	✕
Collect statistics for wireless clients	✔	✔	✔	✕	✕
Tx beamforming	✔	✔	✔	✕	✕
RTS threshold	✔	✔	✔	✕	✕
Spectralink VIEW	✔	✔	✔	✕	✕
Tx protection	✔	✔	✔	✕	✕
Guard interval	✔	✔	✔	✕	✕
Maximum range (ack timeout)	✔	✕	✔	✕	✕
Distance between APs	✔	✔	✔	✕	✕
Beacon interval	✔	✔	✔	✕	✕
Multicast Tx rate	✔	✔	✔	✕	✕
Transmit power control	✔	✔	✔	✕	✕

Certain parameters are not supported on all radios. Refer to the parameter descriptions that follow for details.

Wireless mode

Supported wireless modes are determined by the regulations of the country in which the AP is operating, and are controlled by the country setting on the AP. To configure the country setting, see *Assigning country settings to a group on page 6-30*.

E-MSM430, E-MSM460, and E-MSM466

These products support the following wireless modes.

802.11n/a

Supported on	Radio 1, Radio 2
Frequency band	5 GHz
Data rates	**For 802.11n clients:** Up to 450 Mbps on the E-MSM466 and E-MSM460, and up to 300 Mbps on the E-MSM430. **For 802.11a clients:** Up to 54 Mbps on the E-MSM430, E-MSM460, and E-MSM466.

When operating in this mode, the AP allows both 802.11n and legacy 802.11a clients to associate. The AP advertises protection in the beacon when legacy clients are associated or operating on the same channel. This alerts associated 802.11n clients to use protection when transmitting. The AP also uses protection when necessary when sending 802.11n data. The type of protection is configurable by setting the **Tx protection** parameter.

802.11n/b/g

Supported on	Radio 2
Frequency band	2.4 GHz
Data rates	**For 802.11n clients:** Up to 450 Mbps on the E-MSM466 and E-MSM460 and up to 300 Mbps on the E-MSM430. These values are achievable when using a 40 MHz channel width, which is not recommended in the 2.4 GHz frequency band. **For 802.11g clients:** Up to 54 Mbps on the E-MSM430, E-MSM460, and E-MSM466. **For 802.11b clients:** Up to 11 Mbps on the E-MSM430, E-MSM460, and E-MSM466.

When operating in this mode, the AP allows both 802.11n and legacy 802.11b/g clients to associate. The AP advertises protection in the beacon when legacy clients are associated or operating on the same channel. This alerts associated 802.11n clients to use protection when transmitting. The AP also uses protection when necessary when sending 802.11n data. The type of protection is configurable by setting the **Tx protection** parameter.

MSM310, MSM317, MSM320, MSM335, MSM410, MSM422

These products support the following wireless modes.

802.11n (5 GHz)

Supported on	MSM422 (radio 1), MSM410
Frequency band	5 GHz
Data rates	Up to 300 Mbps.

HP refers to this mode as *Pure 802.11n*. When operating in this mode, the AP does not permit non-802.11n clients to associate. Legacy clients can see the access point, and may attempt to associate, but they will be rejected. The AP makes this determination based on the supported rates that the client presents during its association request. If the rates do not include any of the 802.11n (HT) rates (MCS0-MCS15), the client is not allowed to associate.

The AP also does not use protection mechanisms (RTS/CTS or CTS-to-self when operating in this mode). This can potentially cause problems with other APs/clients operating on the same channel in 802.11a mode, but provides the best throughput for the AP and its 802.11n clients.

The AP will still signal associated clients to use protection when they send data. The AP does this via a field in the beacon that it sends. So clients sending data to the AP will use protection, but data sent from the AP will not be protected.

Note

This mode is sometimes incorrectly called Greenfield. Greenfield is an 802.11n-specific preamble that can be used by clients and APs. HP APs do not support this preamble and therefore do not support Greenfield mode.

When to use this mode

Use this mode when the AP is installed in an area where there is no legacy wireless traffic on the channel that the AP will use, and all potential wireless client devices support 802.11n.

802.11n (2.4 GHz)

Supported on	MSM422 (radio 1), MSM410
Frequency band	2.4 GHz
Data rates	Up to 300 Mbps.

HP refers to this mode as *Pure 802.11n*. When operating in this mode, the AP does not permit non-802.11n clients to associate. Legacy clients can see the access point, and may attempt to associate, but they will be rejected. The AP makes this determination based on the supported rate set that the client presents during its association request. If the rate set does not include any of the 802.11n (HT) rates (MCS0-MCS15), it is not allowed to associate.

The AP does not use protection mechanisms (RTS/CTS or CTS-to-self) when operating in this mode, which provides for the best throughput tor the AP and its 802.11n clients. However, if legacy clients are using the same channel, this can lead to collisions and potentially serious performance deterioration for all traffic (802.11n and legacy a/b/g) on the channel.

The AP will still signal associated clients to use protection when they send data. The AP does this via a field in the beacons that it sends. So clients sending data to the AP will use protection, but data sent from the AP will not be protected.

Note This mode is sometimes incorrectly called Greenfield. Greenfield is an 802.11n-specific preamble that can be used by clients and APs. HP APs do not support this preamble and therefore do not support Greenfield mode.

When to use this mode

Use this mode when the AP is installed in an area where there is no legacy wireless traffic on the channel that the AP will use, and all potential wireless client devices support 802.11n.

802.11n/a

Supported on	MSM410, MSM422 (radio 1)
Frequency band	5 GHz
Data rates	**For 802.11n clients:** Up to 300 Mbps. **For 802.11a clients:** Up to 54 Mbps.

HP refers to this mode as *Compatibility mode* because the AP allows both 802.11n and legacy clients to associate. The AP advertises protection in the beacon when legacy clients are associated or operating on the same channel. This alerts associated 802.11n clients to use protection when transmitting. The AP also uses protection mechanisms (RTS/CTS or CTS-to-self) when sending 802.11n data to prevent disruption to legacy clients associated on the same channel.

802.11n/g

Supported on	MSM410, MSM422 (radio 1)
Frequency band	2.4 GHz
Data rates	**For 802.11n clients:** Up to 130 Mbps. (Up to 300 Mbps when using a 40 MHz channel width, which is not recommended in the 2.4 GHz frequency band.) **For 802.11g clients:** Up to 54 Mbps.

This mode is the same as 802.11n/b/g except that 802.11b clients are prevented from associating. The AP does not advertise 1, 2, 5.5 and 11 Mbps as supported rates in its beacons or Probe-Responses. The AP does not tell 802.11g clients to use protection, and this can cause collisions with any 802.11b clients present on the same channel. However, the AP uses protection mechanisms (RTS/CTS or CTS-to-self) when sending 802.11n data to prevent disruption to legacy (802.11a/b/g) clients associated on the same channel.

802.11n/b/g

Supported on	MSM410, MSM422 (radio 1)
Frequency band	2.4 GHz
Data rates	**For 802.11n clients:** Up to 130 Mbps. (Up to 300 Mbps when using a 40 MHz channel width, which is not recommended in the 2.4 GHz frequency band.) **For 802.11g clients:** Up to 54 Mbps. **For 802.11b clients:** Up to 11 Mbps.

HP refers to this mode as *Compatibility mode* because the AP allows both 802.11n and legacy clients to associate. The AP advertises protection in the beacon when legacy clients are associated or operating on the same channel. This alerts associated 802.11n clients to use protection when transmitting. The AP also uses protection mechanisms (RTS/CTS or CTS-to-self) when sending 802.11n data to prevent disruption to legacy clients associated on the same channel.

802.11b

Supported on	MSM310, MSM317, MSM320, MSM335, MSM410, MSM422
Frequency band	2.4 GHz
Data rates	Up to 11 Mbps.

This is a legacy mode that can be used to support older wireless client stations.

802.11b/g

Supported on	MSM310, MSM317, MSM320, MSM335, MSM410, MSM422
Frequency band	2.4 GHz
Data rates	**For 802.11g clients:** Up to 54 Mbps. **For 802.11b clients:** Up to 11 Mbps.

This is a legacy mode that can be used to support older wireless client stations.

802.11g

Supported on	MSM310, MSM317, MSM320, MSM335, MSM410, MSM422
Frequency band	2.4 GHz
Data rates	Up to 54 Mbps.

This is a legacy mode that can be used to support older wireless client stations.

802.11a

Supported on	MSM310, MSM317, MSM320, MSM335, MSM410, MSM422
Frequency band	5 GHz
Data rates	Up to 54 Mbps.

This is a legacy mode that can be used to support older wireless client stations.

802.11a Turbo

Supported on	MSM310, MSM317, MSM320, MSM335, MSM410, MSM422
Frequency band	5 GHz
Data rates	Up to 108 Mbps.

Provides channel bonding in the 5 GHz frequency band for enhanced performance. Useful to provide increased throughput when creating local mesh links between two APs.

Channel width

Supported on: MSM410, MSM422 (radio 1), E-MSM430, E-MSM460, E-MSM466
Not available in Monitor or Sensor modes.

802.11n allows for the use of the standard channel width of 20 MHz or a double width of 40 MHz. The double width is achieved by using two adjacent channels to send data simultaneously. This results in double the available bandwidth leading to much higher throughput.

Select the **Channel width** that will be used for 802.11n traffic. Available options are:

- **20 MHz:** Uses the standard channel width of 20 MHz. Recommended when the AP is operating in the 2.4 GHz band and multiple networks must co-exist in the same location.
- **Auto 20/40 MHz:** The AP will advertise 40 MHz support to clients, but will use 20 MHz for each client that does not support 40 MHz.

Note

On the E-MSM466, E-MSM460, and E-MSM430, when operating in the 2.4 GHz band, the AP will automatically switch to using a 20 MHz channel width if a legacy 802.11b/g client or AP is detected on the primary channel. When the legacy device is no longer present, the AP will revert back to using a 40 MHz channel width.

The channel selected on the radio page is the primary channel and the secondary (or extension) channel is located adjacent to it. The secondary channel is either above or below depending on which channel was selected as the primary. In the 5 GHz band, the channels are paired: 36 and 40 are always used together, 44 and 48 are always used together, etc. It works slightly differently in the 2.4 GHz band: there you choose whether the extension channel should be above or below the beacon using the **Channel extension** parameter. See the **Channel** parameter for more information.

Channel extension

Supported on: MSM410, MSM422 (radio 1), E-MSM430 (radio 2), E-MSM460 (radio 2), E-MSM466 (radio 2)
Not available in Sensor mode.

This setting only appears when **Wireless mode** is set to **802.11n (2.4 GHz)**, **802.11n/b/g**, or **802.11 n/g** and **Channel width** is set to **Auto 20/40 MHz**.

This setting determines where the second 20 MHz channel is located.

- **Above the beacon (+1):** The secondary channel is located on a channel above the currently selected channel.
- **Below the beacon (-1)**:The secondary channel is located on a channel below the currently selected channel.

Channel

Select channel (frequency) for wireless services. The channels that are available are determined by the radio installed in the AP and the regulations that apply in your country.

Automatic channel selection

Use the **Automatic** option to have the AP select the best available channel. Control how often the channel selection is re-evaluated by setting the **Interval** parameter.

- **On the E-MSM430, E-MSM460, E-MSM466:** Scanning during the channel selection process can cause interruptions to voice calls. This only occurs each time the Interval expires. Therefore, configuring a short **Interval** is not recommended.
- **On the MSM310, MSM320, MSM335, MSM410, MSM422:** Scanning is continuously performed on all the channels in the currently selected **Operating mode**, even though the channel is only re-evaluated each time the **Interval** expires. (If **Interval** is set to **Disabled**, continuous scanning is not performed.) Continuous scanning can cause interruptions to voice calls. On dual-radio APs, you can avoid interruptions by setting one radio to operate in Monitor mode. For example, if radio 1 is set to **Automatic** and radio 2 is in **Monitor** mode, scanning occurs on radio 2 and interruptions on radio 1 do not occur.

Caution

When using the **Automatic** option with an external antenna in the 2.4 GHz band, all channels must be set to the lowest acceptable value for your regulatory domain. See *Transmit power control on page 4-32*.

Manual channel selection

If setting the channel manually, for optimal performance when operating in 2.4 GHz modes, select a channel that differs from other wireless APs operating in neighboring cells by at least 25 MHz. For example, if another AP is operating on channel 1, set the AP to channel 6 or higher. See *Wireless neighborhood on page 4-34* to view a list of APs currently operating in your area. For detailed information on selecting channels when operating at 2.4 GHz, see *Selecting channels in the 2.4 GHz band on page 4-4*.

When operating in 802.11a or 802.11n (5 GHz) modes, channels do not interfere with each other, enabling APs to operate on two adjacent channels without interference.

HP APs support Dynamic Frequency Selection (802.11h) and Transmit Power Control (802.11d) for 802.11a operation in European countries. These options are automatically enabled as required. Channels used by dynamic frequency selection (DFS) for radar avoidance, are identified with an asterisk "*".

- **On the MSM410, MSM422 (radio 1), E-MSM430, E-MSM460, E-MSM466:** When **Wireless mode** is **802.11n (5 GHz)** or **802.11n/a** and **Channel width** is **Auto 20/40 MHz**, the channel numbers in the **Channel** list include either a "**(1)**" or "**(-1)**" to their right. A "(1)" indicates that the 40 MHz channel is formed from the indicated channel plus the next channel. A "-1" indicates that the 40 MHz channel is formed from the indicated channel plus the previous channel.

  With a 40 MHz Channel width in the 5 GHz band, channel selection and usage is as follows for the first four channels:

Channel selected	Channels used
36(1)	36+40
40(-1)	40+36
44(1)	44+48
48(-1)	48+44

Note

The channel selected is the primary channel and the channel above or below it becomes the secondary channel. The AP beacon is transmitted only on the primary channel and all legacy client traffic is carried on the primary channel.

- **On the MSM410, MSM422 (radio 1):** When **Wireless mode** is **802.11n (2.4 GHz)** or **802.11n/g** or **802.11n/b/g**, and **Channel width** is **Auto 20/40 MHz**, the **Channel extension** parameter value affects which channels are shown in the Channel list. Although it is recommended that you use the 5 GHz band for all 802.11n activity, if you insist upon using 802.11n and a 40 MHz Channel width in the crowded 2.4 GHz band, it is best to select channels as follows, according to the number of 2.4 GHz channels available in your region.

Available 2.4 GHz channels	Channel width	Recommended non-overlapping channels
1 to 13	20 MHz	1, 7, 13
1 to 13	40 MHz	1, 13 (If both are used, there will be some performance degradation.)
1 to 11	20 MHz	1, 6, 11
1 to 11	40 MHz	1, 11 (If both are used, there will be some performance degradation.)

Interval

Not available in Monitor or Sensor modes.

When the **Automatic** option is selected for Channel, this parameter determines how often the AP re-evaluates the channel setting. Select **Time of day** to have the channel setting re-evaluated at a specific time of day.

- Select **Time of day** to have the channel setting re-evaluated at a specific time of day. Note that to prevent all APs from re-evaluating their channel at the same time, a random delay between 0 and 2 hours is added to the time of day for each AP.
- Select **Disabled** to have the scan performed once when you select **Save**, and then only when the AP is restarted. This also prevents continuous scanning from being performed on the MSM310, MSM320, MSM335, MSM410, and MSM422.

Time of day

Not available in Monitor or Sensor modes.

When the **Time of day** option is selected for **Interval**, this parameter determines the time of day that the AP re-evaluates the channel setting.

To prevent APs from re-evaluating their channel at the same time, a random delay between 0 and 2 hours is added to the time of day for each AP. For example, if 1AM is selected, the channel with be re-evaluated between 1AM and 3AM.

Automatic channel exclusion list

Not available in Monitor or Sensor modes.

Used when **Automatic** is selected under **Channel**, this parameter determines the channels that are not available for automatic selection. To select more than one channel, hold down **Ctrl** as you select the channel names.

Antenna selection

Supported on: MSM310, MSM320, MSM335, MSM422
Not available in Monitor or Sensor modes.

Select the antenna(s) to use for each radio. Antenna support varies on each AP. For a list of supported external antennas, see *Connecting external antennas* in the *MSM3xx / MSM4xx Access Points Management and Configuration Guide*.

In most APs, antenna diversity is supported. Diversity provides improved signal quality by using multiple antennas on the same radio.

Note

- When using an external antenna, it is your responsibility to make sure that the radio does not exceed the transmit power level for the country of use. See *Transmit power control on page 4-32*.
- When creating a point-to-point local mesh link, it is recommended that you use an external directional antenna.

MSM310, MSM310-R, and MSM320
Select **Diversity**, **Main**, or **Auxiliary** according to the following guidelines:

- For a single antenna, connect one antenna to either Main or Aux and select the corresponding value.
- For maximum wireless coverage, install an omnidirectional antenna on the Main and Aux antenna connectors and select **Diversity**.
- When creating a point-to-point wireless bridge, it is recommended that a single directional antenna be used on either Main or Aux.

MSM320-R
Only two antenna connectors are available on the MSM320-R. To use both radios, connect an antenna to each connector. Diversity is not supported.

MSM335
Select either **Internal** or **External** according to the following guidelines:

- The MSM335 features six internal antennas in its two flaps, providing two antennas for each of its three radios. Radios 1, 2, and 3, have corresponding external antenna connectors A, B, and C for optional external antennas.
- Diversity is supported on all three radios via the internal antennas. but not when using external antennas.

MSM422
Select either **Internal** or **External** according to the following guidelines:

- The MSM422 features three internal antennas in the lower flap for Radio 1 (802.11n/a/b/g) (corresponding to external connectors A, B, and C) and two internal antennas in the upper flap for Radio 2 (801.11a/b/g) (corresponding to external connector D). If desired, install optional antennas via the external connectors.
- Radio 1 supports diversity on its internal and external antennas (connectors A, B, and C). In 802.11n modes, a special form of diversity called MIMO is used.

- For point-to-point local mesh links on Radio 1, install two directional antennas on connectors A and B. Installing a third directional antenna on connector C will increase performance only on the receive side.
- Radio 2 supports diversity via its two internal antennas. but not when using an external antenna.

Antenna gain

Supported on: MSM310. MSM310-R, MSM320, MSM320-R, E-MSM466
Not available in Monitor or Sensor modes.

For optimum performance, this parameter must be set to the gain of the antenna at the selected frequency (DFS channel).

Max clients

Not available in Monitor or Sensor modes.

Specify the maximum number of wireless client stations that can be supported on this radio across all VSCs.

Advanced wireless settings

Collect statistics for wireless clients

Not available in Monitor or Sensor modes.

When this option is enabled, the AP collects statistics for connected wireless client stations. The statistical information can be retrieved via SNMP from the following MIBs:

MIB	Table
COLUBRIS-DEVICE-WIRELESS-MIB.my (controlled mode)	
COLUBRIS-IEEE802DOT11.my (autonomous mode)	coDot11DetectedStationTable

Tx beamforming

Supported on: E-MSM430, E-MSM460, E-MSM466
Not available in Monitor or Sensor modes.

Tx beamforming can be used to help increase throughput by improving the quality of the signal sent to wireless clients

When this option is enabled, APs use beamforming techniques to optimize the signal strength for each individual wireless client station. Beamforming works by changing the characteristics of the transmitter to create a focused beam that can be more optimally received by a wireless station.

HP APs support the following two explicit beamforming techniques:

- Non-compressed beamforming, in which the client station calculates and sends the steering matrix to the AP.
- Compressed beamforming, in which the client station sends a compressed steering matrix to the AP.

Radio calibration is not required to use either of these two methods.

Note Beamforming only works with wireless clients that are configured to support it.

RTS threshold

Not available in Monitor or Sensor modes.

Use this parameter to control collisions on the link that can reduce throughput. If the **Controlled APs > [*group*] > [*AP*] >> Status > Wireless** page shows increasing values for **Tx multiple retry frames** or **Tx single retry frames**, adjust this value until the errors clear. Start with a value of 1024 and decrease to 512 until errors are reduced or eliminated. Note that using a small value for **RTS threshold** can affect throughput. Range: 128 to 1540.

If a packet is larger than the threshold, the AP holds the packet and issues a *request to send* (RTS) message to the client station. The AP sends the packet only when the client station replies with a *clear to send* (CTS) message. Packets smaller than the threshold are transmitted without this handshake.

Spectralink VIEW

Supported on: MSMS310, MSM320, MSM335, MSM410, MSM422
Not available in Monitor or Sensor modes.

Provides support for Spectralink phones using Spectralink Voice Interoperability for Enterprise Wireless (VIEW) extensions.

Tx protection

Supported on: E-MSM430, E-MSM460, E-MSM466
Not available in Monitor or Sensor modes.

When an AP is operating in an 802.11n mode, and legacy (a/b/g) traffic is present on the same channel as 802.11n traffic, this feature can be used to ensure maximum 802.11n throughput.

The following options are available:

- **CTS-to-self:** 802.11n transmissions are protected by sending a Clear To Send (CTS) frame that blocks other wireless clients from accessing the wireless network.
- **RTS/CTS:** 802.11n transmissions are protected by sending a Request To Send (RTS) frame followed by a CTS frame. This is a more robust, but slower, solution than CTS-to-self. However, this method resolves the hidden station problem (where certain legacy stations may not see only a CTS frame).

- **No MAC protection:** This setting gives the best performance for 802.11n clients in the presence of 802.11g or 802.11a legacy clients or APs. No protection frames (CTS-to-self or RTS/CTS) are sent at the MAC layer by the AP. PHY-based protection remains active, which alerts legacy clients to stay off the air while the AP is transmitting data to 802.11n clients. This method of protection is supported by most 802.11g or 802.11a clients, but is not supported for 802.11b-only clients and should not be used if such clients are expected on the network.

Guard interval

Supported on: MSM410, MSM422 (radio 1), E-MSM430, E-MSM460, E-MSM466
Not available in Monitor or Sensor modes.

This parameter is only configurable when **Wireless mode** is set to support an 802.11n option.

On the MSM410 and MSM422, **Guard interval** is automatically set to **Long** when **Channel width** is set to **20 MHz**.

To enhance performance in 802.11n modes, the guard interval can be reduced from its default of 800 nanoseconds to 400.

The guard interval is the intersymbol time period that is used to prevent symbol interference when multiple data streams are used (MIMO). However, symbol interference reduces the effective SNR of the link, so reducing the guard interval may not improve performance under all conditions.

The following settings are available:

- **Short:** Sets the guard interval to 400 nanoseconds which can provide improved throughput (up to 10%) in some environments. The AP remains compatible with clients that only support a long guard interval. Use this setting when **Channel width** is set to **Auto 20/40 MHz** to get the best throughput.
- **Long:** Sets the guard interval to the standard of 800 nanoseconds.

Maximum range (ack timeout)

Only available in modes that support Local Mesh.

Fine tunes internal timeout settings to account for the distance that a link spans. For normal operation, timeout is optimized for links of less than 1 km.

Note This is a global setting that applies to all wireless connection made with the radio. Therefore, adjusting this setting may lower the performance for users with marginal signal strength or when interference is present. (Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)

Distance between APs

Not supported on: E-MSM430, E-MSM460, E-MSM466
Not available in Monitor or Sensor modes.

Use this parameter to adjust the receiver sensitivity of the AP only if:

- You have more than one wireless AP installed in your location.
- You are experiencing throughput problems.

In all other cases use the default setting of **Large**.

If you have installed multiple APs, reducing the receiver sensitivity helps to reduce the amount of cross-talk between the wireless stations to better support roaming clients. It also increases the probability that client stations connect with the nearest AP.

Available settings

- **Large:** Accepts all clients.
- **Medium:** Accepts clients with an RSSI greater than 15 dB.
- **Small:** Accepts clients with an RSSI greater than 20 dB.

Note RSSI (Received Signal Strength Indication) is the difference between the amount of noise in an environment and the wireless signal strength. It is expressed in decibels (dB). The higher the number the stronger the signal.

Beacon interval

Not available in Monitor or Sensor modes.

Sets the number of time units (TUs) that the AP waits between transmissions of the wireless beacon. One TU equals 1024 microseconds. The default interval is 100 TU, which is equal to 102.4 milliseconds. Supported range is from 20 to 500 TU.

Multicast Tx rate

Not available in Monitor or Sensor modes.

Use this parameter to set the transmit rate for multicast and broadcast traffic. This is a fixed rate, which means that if a station is too far away to receive traffic at this rate, the multicast is not be seen by the station.

Transmit power control

Not available in Monitor or Sensor modes.

Use these parameters to control the transmission power of the wireless radio.

Adjustments to the transmission power may be required for two reasons. First, when using an optional external antenna, it may be necessary to reduce power levels to remain in compliance with local regulations. Second, it may be necessary to reduce power levels to avoid interference between APs and other radio devices.

Important
For a list of supported external antennas, see *Connecting external antennas* in the *MSM3xx / MSM4xx Access Points Management and Configuration Guide*.

When using antennas not originally supplied with the AP, it is your responsibility to ensure that the **Transmit power control** settings are configured so that the radio will not exceed permissible power levels for the regulatory domain in which the AP is operating. Depending on the regulatory domain, the specific antenna chosen, the wireless mode, channel width, band or channel selected, you may need to configure the radio with a reduced transmit power setting. When using **Automatic channel selection** with an external antenna in the 2.4 GHz band, all channels must be set to the lowest acceptable value for your regulatory domain.

Caution

For specific power limits according to your regulatory domain, consult the *Antenna Power-Level Settings Guide* available at www.hp.com/networking/support (for **Product Brand**, select **ProCurve** and search for your antenna**)**.

For example, if you install an external 8 dBi directional antenna, and the maximum allowed power level for your country is 15 dBm, you may have to reduce the transmit power level to be in compliance.

If you change the antenna at a later time, you must get the latest version of the *Antenna Power-Level Settings Guide*, and again reassess and possibly adjust radio power settings according to the antenna used.

When setting **Transmit power control** to comply with information in the Antenna Power-Level Settings Guide, always set radio power in dBm, and not as a percentage.

Maximum output power

Shows the maximum output power that can be supported by the radio based on the regulatory domain.

Use maximum power

Select this checkbox to use the maximum available output power.

Set power to

Specify the transmission power in dBm or as a percentage of the maximum output power. When you select **Save**, percentage values are rounded up or down so that the dBm value is always a whole number).

Note that the actual transmit power used by the radio may be less than the specified value. The AP determines the maximum power to be used based on the regulatory domain.

Automatic power control

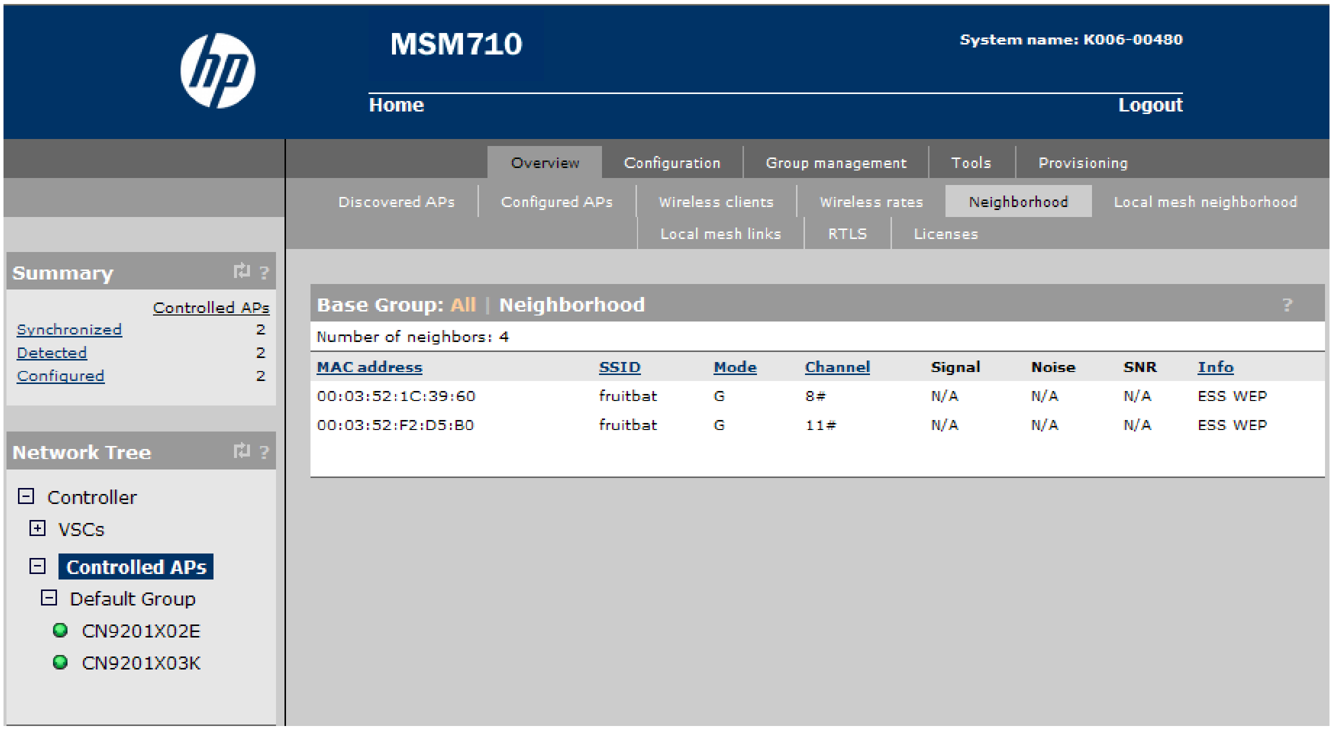
Select this checkbox to have the AP automatically determine the optimal power setting within the defined power limits (i.e., up to the specified percentage/dBm value).

Interval

Specify the interval at which the **Automatic power control** feature adjusts the optimal power setting.

Wireless neighborhood

Select **Controlled APs >> Overview > Neighborhood** to view information on APs operating in your area. This page presents a list of all APs that have been detected by all of the controlled APs. For example:



Summary

	Controlled APs
Synchronized	2
Detected	2
Configured	2

Base Group: All | Neighborhood

Number of neighbors: 4

MAC address	SSID	Mode	Channel	Signal	Noise	SNR	Info
00:03:52:1C:39:60	fruitbat	G	8#	N/A	N/A	N/A	ESS WEP
00:03:52:F2:D5:B0	fruitbat	G	11#	N/A	N/A	N/A	ESS WEP

You can also view the list detected by a specific controlled AP by selecting in the Network Tree.

Scanning modes

The way in which the AP performs scanning depends on the configuration of the wireless radio (**Wireless > Radio** page). The following scanning modes are possible:

- **Monitor mode:** When a radio has its **Operating mode** set to **Monitor**, scanning occurs continuously. The scan switches to a new channel every 200 ms, sequentially covering all supported wireless modes and channels. Use this method to quickly obtain an overview of all APs in your area for site planning, or for initial configuration of the authorized access points list.

  Monitor mode scanning is temporarily disabled when a trace is active (**Tools > Network trace** page).

- **Automatic channel selection:** When the **Automatic channel selection** feature is enabled, scanning occurs as follows:

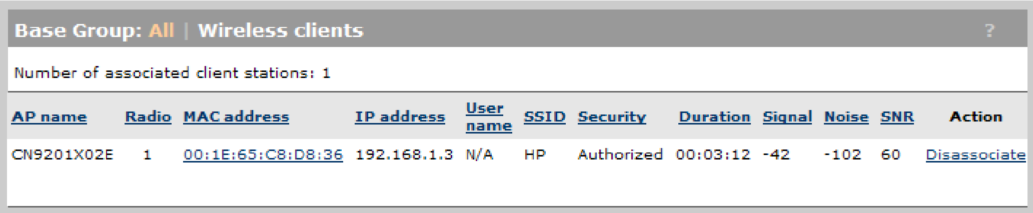
  - **On the E-MSM430, E-MSM460, E-MSM466:** Scanning only occurs when the channel selection interval expires. This may cause interruptions to voice calls. Therefore, configuring a short channel selection interval is not recommended.

- **On the MSM310, MSM320, MSM335, MSM410, MSM422:** Scanning is continuously performed on all the channels in the currently selected **Operating mode**, even though the channel is only re-evaluated each time the channel selection interval expires. (If the interval is set to **Disabled**, continuous scanning is not performed.) Continuous scanning can cause interruptions to voice calls. On dual-radio APs, you can avoid interruptions by setting one radio to operate in monitor mode. For example, if radio 1 is set to automatic channel scanning and radio 2 is in monitor mode, scanning occurs on radio 2 and interruptions on radio 1 do not occur.

Viewing wireless information

Viewing all wireless clients

To view information on all wireless client stations, select **Controlled APs >> Overview > Wireless clients**.



Base Group: All | Wireless clients

Number of associated client stations: 1

AP name	Radio	MAC address	IP address	User name	SSID	Security	Duration	Signal	Noise	SNR	Action
CN9201X02E	1	00:1E:65:C8:D8:36	192.168.1.3	N/A	HP	Authorized	00:03:12	-42	-102	60	Disassociate

This page lists all wireless clients associated with all VSCs.

AP name

Name of the AP the with which the client station is associated.

Radio

Radio on the AP that the client station is using.

MAC Address

MAC address of the client station. Select the MAC address to view more detailed information on the client.

IP address

IP address assigned to the client station.

SSID

SSID assigned to the client station.

Security

Indicates if the client station has been authorized.

Duration

Indicates how long the client station has been authorized.

Signal

Indicates the strength of the radio signal received from client stations. Signal strength is expressed in decibel milliwatt (dBm). The higher the number the stronger the signal.

Noise

Indicates how much background noise exists in the signal path between client stations and the AP. Noise is expressed in decibel milliwatt (dBm). The lower (more negative) the value, the weaker the noise.

SNR

Indicates the relative strength of the client station radio signals versus the radio interference (noise) in the radio signal path.

In most environments, SNR is a good indicator for the quality of the radio link between the client stations and the AP. A higher SNR value means a better quality radio link.

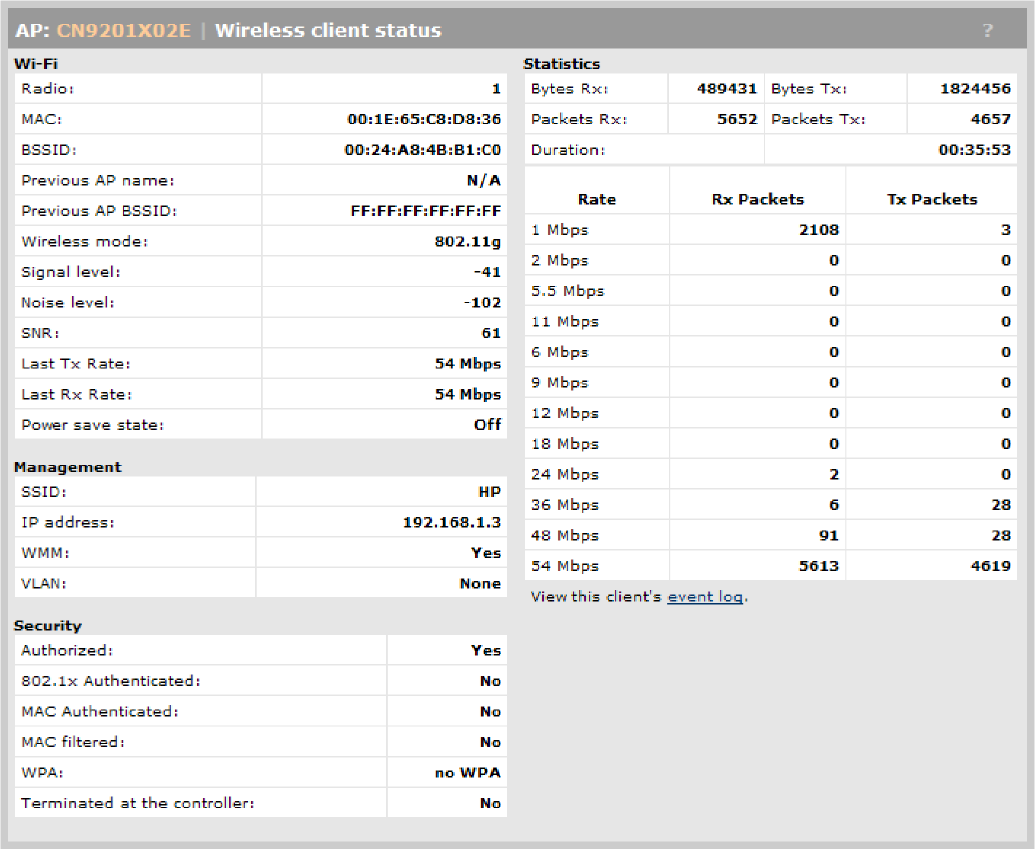
Action

Select **Disassociate** to disconnect a wireless client.

Viewing info for a specific wireless client

To view information on a specific wireless client station, select **Controlled APs >> Overview > Wireless clients,** and then in the table, select the MAC address of the client.

The information you see will vary depending on the AP to which the client is connected. For example, the following shows the status page for a client connected to an MSM317.



AP: CN9201X02E | Wireless client status

Wi-Fi

Radio:	1
MAC:	00:1E:65:C8:D8:36
BSSID:	00:24:A8:4B:B1:C0
Previous AP name:	N/A
Previous AP BSSID:	FF:FF:FF:FF:FF:FF
Wireless mode:	802.11g
Signal level:	-41
Noise level:	-102
SNR:	61
Last Tx Rate:	54 Mbps
Last Rx Rate:	54 Mbps
Power save state:	Off

Management

SSID:	HP
IP address:	192.168.1.3
WMM:	Yes
VLAN:	None

Security

Authorized:	Yes
802.1x Authenticated:	No
MAC Authenticated:	No
MAC filtered:	No
WPA:	no WPA
Terminated at the controller:	No

Statistics

Bytes Rx:	489431	Bytes Tx:	1824456
Packets Rx:	5652	Packets Tx:	4657
Duration:			00:35:53

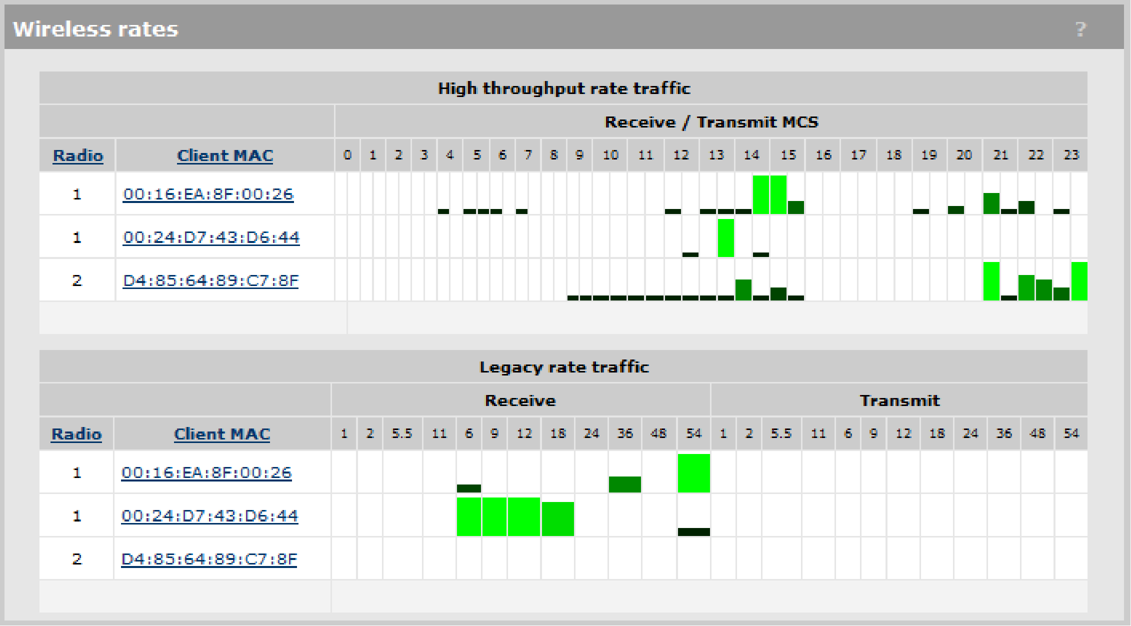
Rate	Rx Packets	Tx Packets
1 Mbps	2108	3
2 Mbps	0	0
5.5 Mbps	0	0
11 Mbps	0	0
6 Mbps	0	0
9 Mbps	0	0
12 Mbps	0	0
18 Mbps	0	0
24 Mbps	2	0
36 Mbps	6	28
48 Mbps	91	28
54 Mbps	5613	4619

View this client's event log.

For a complete description of all fields see the online help.

Viewing wireless client data rates

To view information on all wireless client stations currently connected to the AP, select **Controlled APs >> Overview > Wireless rates**.



High throughput rate traffic

		Receive / Transmit MCS																							
Radio	Client MAC	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	00:16:EA:8F:00:26																								
1	00:24:D7:43:D6:44																								
2	D4:85:64:89:C7:8F																								

Legacy rate traffic

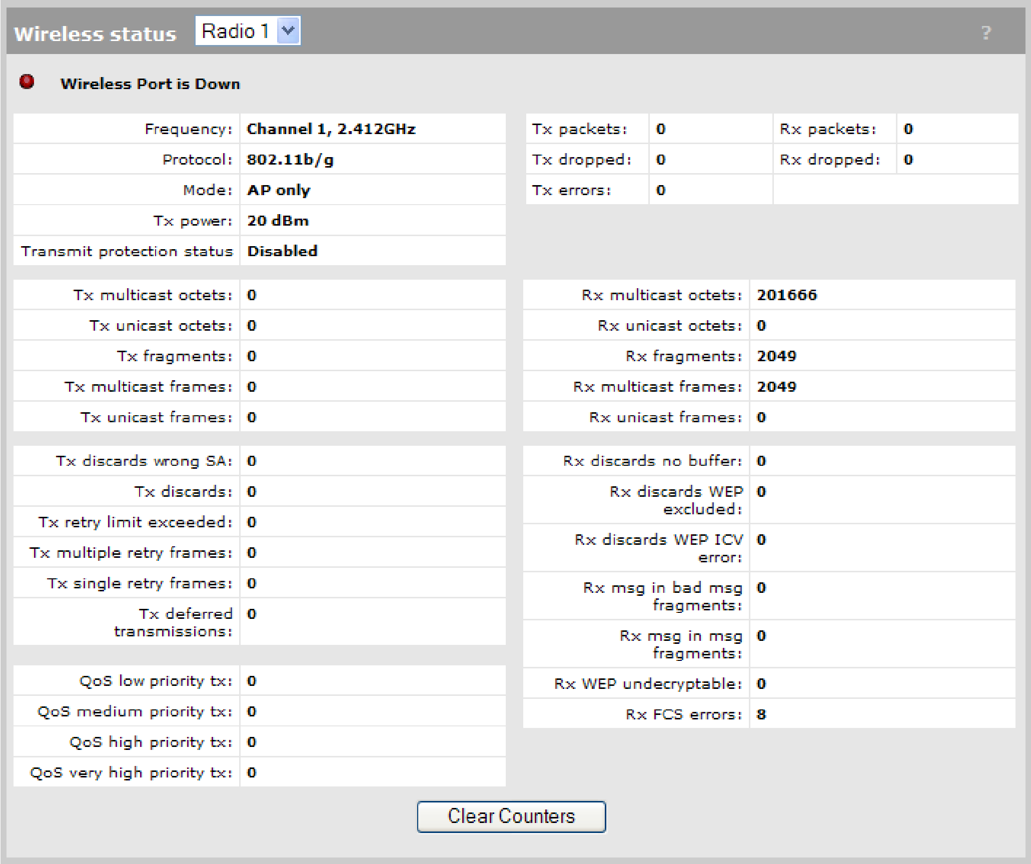
		Receive												Transmit											
Radio	Client MAC	1	2	5.5	11	6	9	12	18	24	36	48	54	1	2	5.5	11	6	9	12	18	24	36	48	54
1	00:16:EA:8F:00:26																								
1	00:24:D7:43:D6:44																								
2	D4:85:64:89:C7:8F																								

This page shows the volume of traffic sent and received at each data rate for each client station. Headings in bold indicate the data rates that are currently active for the wireless mode being used.

Wireless access points

To view wireless information for an AP, select **Controlled APs > [*group*] > [*AP*] >> Status > Wireless**.

The information you see will vary depending on the AP. For example, this is the status page for an MSM317:



● **Wireless Port is Down**

Frequency:	**Channel 1, 2.412GHz**
Protocol:	**802.11b/g**
Mode:	**AP only**
Tx power:	**20 dBm**
Transmit protection status	**Disabled**

Tx packets:	**0**	Rx packets:	**0**
Tx dropped:	**0**	Rx dropped:	**0**
Tx errors:	**0**		

Tx multicast octets:	**0**	Rx multicast octets:	**201666**
Tx unicast octets:	**0**	Rx unicast octets:	**0**
Tx fragments:	**0**	Rx fragments:	**2049**
Tx multicast frames:	**0**	Rx multicast frames:	**2049**
Tx unicast frames:	**0**	Rx unicast frames:	**0**

Tx discards wrong SA:	**0**
Tx discards:	**0**
Tx retry limit exceeded:	**0**
Tx multiple retry frames:	**0**
Tx single retry frames:	**0**
Tx deferred transmissions:	**0**

QoS low priority tx:	**0**
QoS medium priority tx:	**0**
QoS high priority tx:	**0**
QoS very high priority tx:	**0**

Rx discards no buffer:	**0**
Rx discards WEP excluded:	**0**
Rx discards WEP ICV error:	**0**
Rx msg in bad msg fragments:	**0**
Rx msg in msg fragments:	**0**
Rx WEP undecryptable:	**0**
Rx FCS errors:	**8**

Access point status

Wireless port

- **UP:** Port is operating normally.
- **DOWN:** Port is not operating.

Frequency

The current operating frequency.

Protocol

Identifies the wireless protocol used by the AP to communicate with client stations.

Mode

Current operation mode.

Tx power

Current transmission power.

Transmit protection status

- **Disabled:** HT protection / G protection is disabled.
- **B clients:** G protection is enabled because a B client is connected to the AP.
- **B APs:** G protection is enabled because a B client is connected to another AP on the same channel used by the AP.
- **AG clients:** HT protection is enabled because a non-HT client is connected to the AP.
- **AG APs:** HT protection is enabled because a non-HT AP is present on the same channel used by the AP.

Tx multicast octets

The number of octets transmitted successfully as part of successfully transmitted multicast MSDUs. These octets include MAC Header and Frame Body of all associated fragments.

Tx unicast octets

The number of octets transmitted successfully as part of successfully transmitted unicast MSDUs. These octets include MAC Header and Frame Body of all associated fragments.

Tx fragments

The number of MPDUs of type Data or Management delivered successfully; i.e., directed MPDUs transmitted and being ACKed, as well as non-directed MPDUs transmitted.

Tx multicast frames

The number of MSDUs, of which the Destination Address is a multicast MAC address (including broadcast MAC address), transmitted successfully.

Tx unicast frames

The number of MSDUs, of which the Destination Address is a unicast MAC address, transmitted successfully. This implies having received an acknowledgment to all associated MPDUs.

Tx discards wrong SA

The number of transmit requests that were discarded because the source address is not equal to the MAC address.

Tx discards

The number of transmit requests that were discarded to free up buffer space on the AP. This can be caused by packets being queued too long in one of the transmit queues, or because too many retries and defers occurred, or otherwise not being able to transmit (for example, when scanning).

Tx retry limit exceeded

The number of times an MSDU is not transmitted successfully because the retry limit is reached, due to no acknowledgment or no CTS received.

Tx multiple retry frames

The number of MSDUs successfully transmitted after more than one retransmission (on the total of all associated fragments). May be due to collisions, noise, or interference. Excessive retries can indicate that too many computers are using the wireless network or that something is interfering with transmissions.

Tx single retry frames

The number of MSDUs successfully transmitted after one (and only one) retransmission (on the total of all associated fragments). May be due to collisions, noise, or interference. Large numbers of single retries can indicate that too many computers are using the wireless network or that something is interfering with transmissions.

Tx deferred transmissions

The number of MSDUs for which (one of) the (fragment) transmission attempt(s) was one or more times deferred to avoid a collision. Large numbers of deferred transmissions can indicate that too many computers are using the wireless network.

QoS low priority tx

Total number of QoS low priority packets that have been sent.

QoS medium priority tx

Total number of QoS medium priority packets that have been sent.

QoS high priority tx

Total number of QoS high priority packets that have been sent.

QoS very high priority tx

Total number of QoS very high priority packets that have been sent.

Tx packets

(Not shown on the E-MSM460)

The total number of packets transmitted.

Tx dropped

(Not shown on the E-MSM460)

The number of packets that could not be transmitted. This can occur when the wireless configuration is being changed.

Tx errors

(Not shown on the E-MSM460)

The total number of packets that could not be sent due to the following errors: Rx retry limit exceeded and TX discards wrong SA.

Rx packets

(Not shown on the E-MSM460)

The total number of packets received.

Rx dropped

(Not shown on the E-MSM460)

The number of received packets that were dropped due to lack of resources on the AP. This should not occur under normal circumstances. A possible cause could be if many client stations are continuously transmitting small packets at a high data rate.

Rx multicast octets

The number of octets received successfully as part of multicast (including broadcast) MSDUs. These octets include MAC Header and Frame Body of all associated fragments.

Rx unicast octets

The number of octets received successfully as part of unicast MSDUs. These octets include MAC Header and Frame Body of all associated fragments.

Rx fragments

The number of MPDUs of type Data or Management received successfully.

Rx multicast frames

The number of MSDUs, with a multicast MAC address (including the broadcast MAC address), as the Destination Address, received successfully.

Rx unicast frames

The number of MSDUs, with a unicast MAC address as the Destination Address received successfully.

Rx discards no buffer

The number of received MPDUs that were discarded because of lack of buffer space.

Rx discards WEP excluded

The number of discarded packets, excluding WEP-related errors.

Rx discards WEP ICV error

The number of received MPDUs that were discarded due to malformed WEP packets.

Rx MSG in bad msg fragments

The number of MPDUs of type Data or Management received successfully, while there was another reception going on above the carrier detect threshold but with bad or incomplete PLCP Preamble and Header (the message-in-message path #2 in the modem).

Rx MSG in msg fragments

The number of MPDUs of type Data or Management received successfully, while there was another good reception going on above the carrier detect threshold (the message-in-message path #2 in the modem).

Rx WEP undecryptable

The number of received MPDUs, with the WEP subfield in the Frame Control field set to one, that were discarded because it should not have been encrypted or due to the receiving station not implementing the privacy option.

Rx FCS errors

The number of MPDUs, considered to be destined for this station (Address matches), received with an FCS error. Note that this does not include data received with an incorrect CRC in the PLCP header. These are not considered to be MPDUs.

Clear counters

Select this button to reset all counters to zero.

5

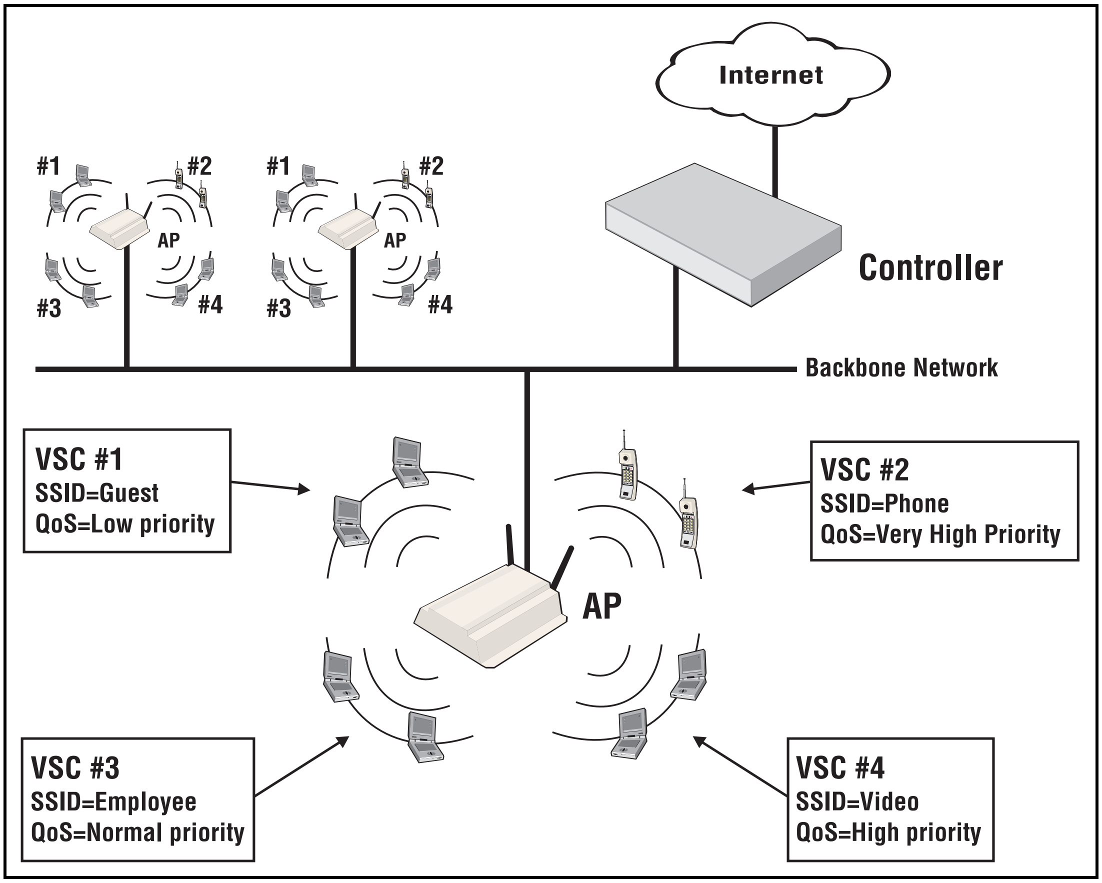
Working with VSCs

Contents

Key concepts

A VSC (virtual service community) is a collection of configuration settings that define key operating characteristics of the controller and controlled APs. In most cases, a VSC is used to define the characteristics of a wireless network and to control how wireless user traffic is distributed onto the wired network.

Multiple VSCs can be active at the same time, allowing for great flexibility in the configuration of services. For example, in the following scenario four VSCs are used to support different types of wireless users. Each VSC is configured with a different wireless network name (SSID), and the quality of service (QoS) feature is used to classify user traffic priority.



Binding VSCs to APs

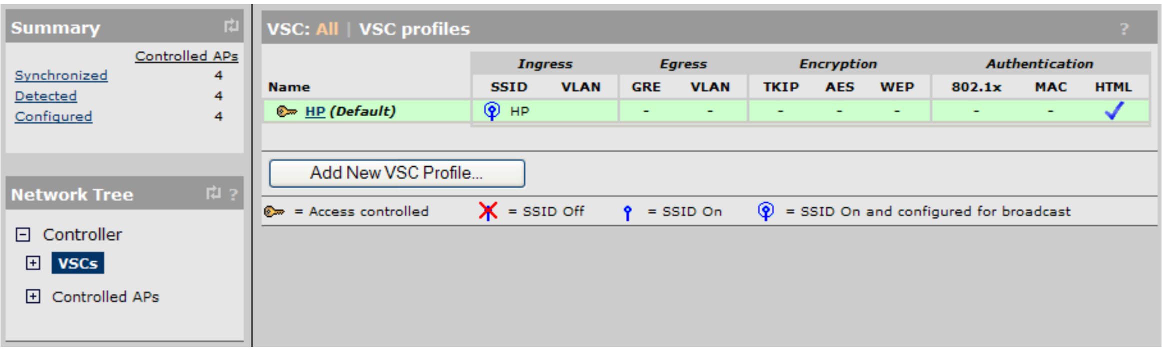
VSCs are defined on the controller, creating a global pool of services. From this pool, specific VSCs are then *bound* to one or more groups (and the APs in the groups), to provide a homogeneous wireless offering. See *Binding VSCs to groups on page 6-23*.

Note

The MSM760 and MSM765 controllers support up to 64 VSCs. Other controllers support up to 16 VSCs. Controlled APs support a maximum of 16 VSCs.

Viewing and editing VSC profiles

The VSC profiles list shows all VSCs are that are currently defined on the controller. To open the list, select **VSCs** in the **Network Tree**.



Summary

	Controlled APs
Synchronized	4
Detected	4
Configured	4

Network Tree

⊟ Controller
⊞ VSCs
⊞ Controlled APs

VSC: All | VSC profiles

	Ingress		Egress		Encryption			Authentication		
Name	SSID	VLAN	GRE	VLAN	TKIP	AES	WEP	802.1x	MAC	HTML
HP (Default)	HP		-	-	-	-	-	-	-	✓

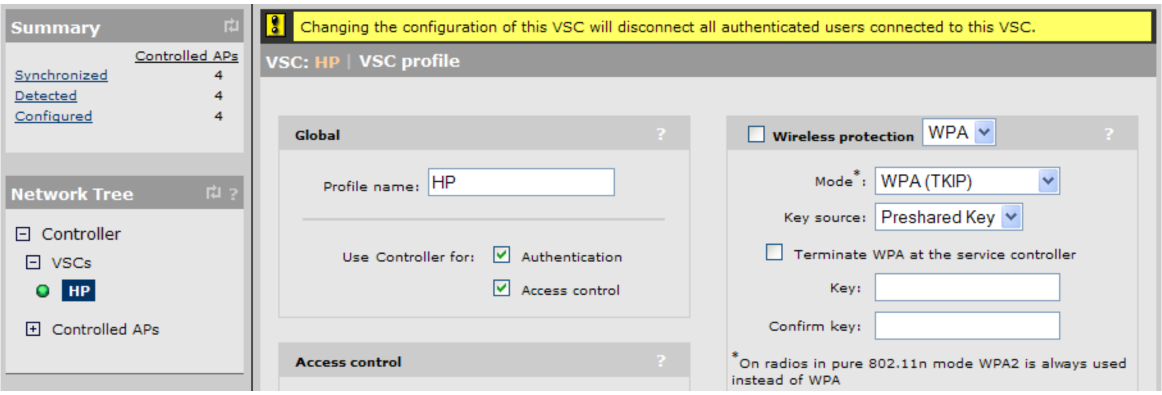
Add New VSC Profile...

= Access controlled   = SSID Off   = SSID On   = SSID On and configured for broadcast

The **HP** VSC profile is defined by default.

- To add a VSC, select **VSCs >> Overview > Add New VSC Profile**.
- To edit a VSC, select its name in the VSC list, or in the Network Tree.

In either case, the VSC profile page opens. In this page sample, only the top of the VSC profile page is shown.



Summary

	Controlled APs
Synchronized	4
Detected	4
Configured	4

Network Tree

⊟ Controller
⊟ VSCs
● HP
⊞ Controlled APs

Changing the configuration of this VSC will disconnect all authenticated users connected to this VSC.

VSC: HP | VSC profile

Global

Profile name: HP

Use Controller for: ☑ Authentication
☑ Access control

Access control

☐ Wireless protection WPA

Mode*: WPA (TKIP)
Key source: Preshared Key
☐ Terminate WPA at the service controller
Key:
Confirm key:

*On radios in pure 802.11n mode WPA2 is always used instead of WPA

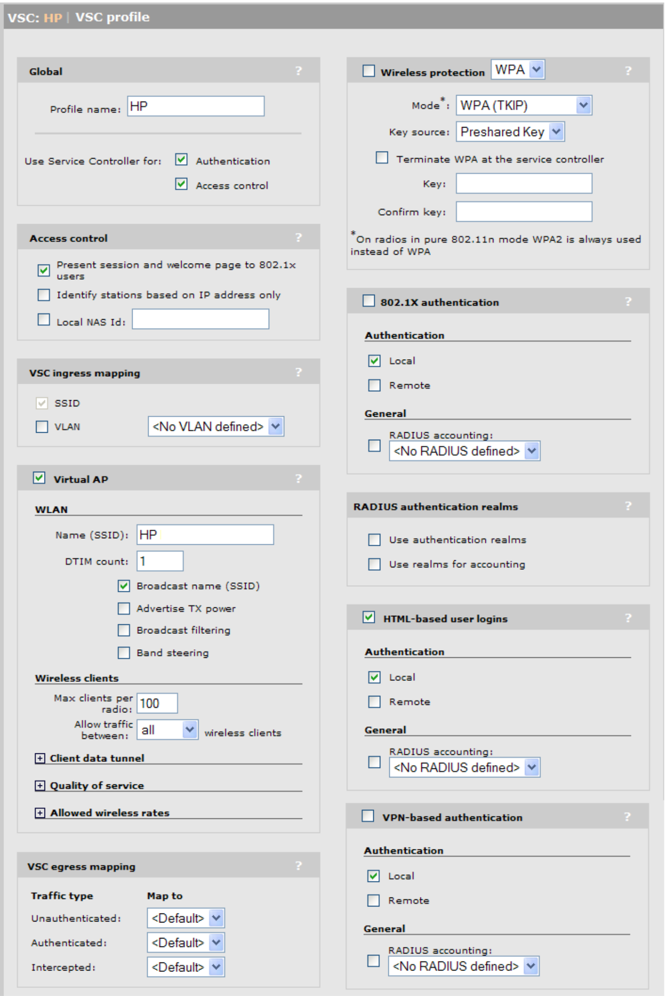
The default VSC

The default VSC is used as a fallback for any traffic that goes through the controller and that cannot be identified as coming from an MSM AP. It is also used to handle all non-VLAN traffic from wired devices connected to the controller's LAN port (i.e., traffic from 3rd-party APs or wired users on the network). See *About the default VSC on page 5-36*.

VSC configuration options

This section provides an overview of all the configuration options available for a VSC. It will give you a good idea on how the features can be used.

The default VSC is pre-configured as described in the following pages. Below, is an overview of the entire VSC configuration page.



VSC: HP | VSC profile

Global

Profile name: HP

Use Service Controller for: ☑ Authentication
☑ Access control

Access control

☑ Present session and welcome page to 802.1x users
☐ Identify stations based on IP address only
☐ Local NAS Id:

VSC ingress mapping

☑ SSID
☐ VLAN <No VLAN defined>

☑ **Virtual AP**

WLAN

Name (SSID): HP
DTIM count: 1
☑ Broadcast name (SSID)
☐ Advertise TX power
☐ Broadcast filtering
☐ Band steering

Wireless clients

Max clients per radio: 100
Allow traffic between: all wireless clients

⊞ Client data tunnel
⊞ Quality of service
⊞ Allowed wireless rates

VSC egress mapping

Traffic type	Map to
Unauthenticated:	<Default>
Authenticated:	<Default>
Intercepted:	<Default>

☐ **Wireless protection** WPA

Mode*: WPA (TKIP)
Key source: Preshared Key
☐ Terminate WPA at the service controller
Key:
Confirm key:

*On radios in pure 802.11n mode WPA2 is always used instead of WPA

☐ **802.1X authentication**

Authentication
☑ Local
☐ Remote

General
☐ RADIUS accounting: <No RADIUS defined>

RADIUS authentication realms

☐ Use authentication realms
☐ Use realms for accounting

☑ **HTML-based user logins**

Authentication
☑ Local
☐ Remote

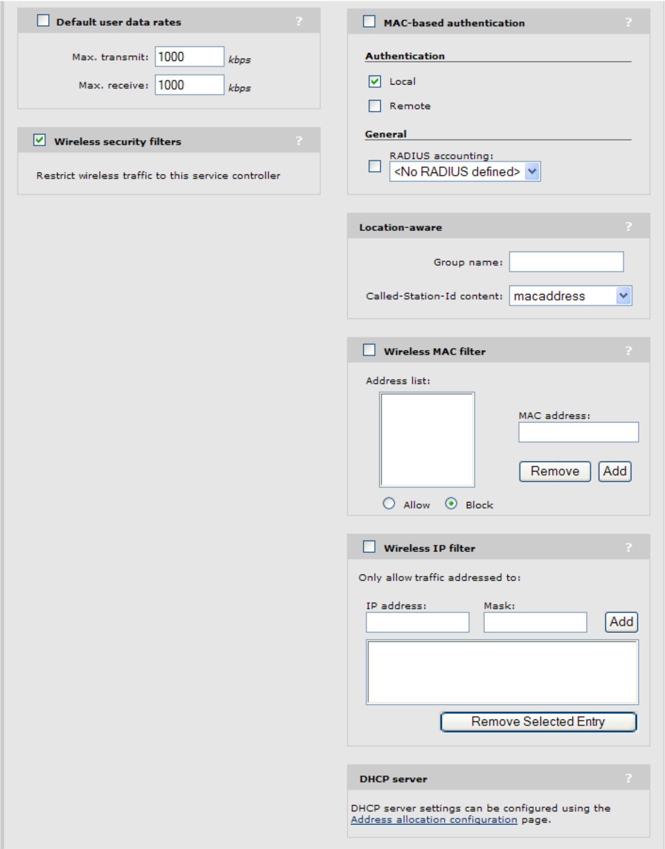
General
☐ RADIUS accounting: <No RADIUS defined>

☐ **VPN-based authentication**

Authentication
☑ Local
☐ Remote

General
☐ RADIUS accounting: <No RADIUS defined>

Continued from below left



☐ **Default user data rates**

Max. transmit: 1000 kbps
Max. receive: 1000 kbps

☑ **Wireless security filters**

Restrict wireless traffic to this service controller

☐ **MAC-based authentication**

Authentication
☑ Local
☐ Remote

General
☐ RADIUS accounting: <No RADIUS defined>

Location-aware

Group name:
Called-Station-Id content: macaddress

☐ **Wireless MAC filter**

Address list:
MAC address:
Remove Add
○ Allow ● Block

☐ **Wireless IP filter**

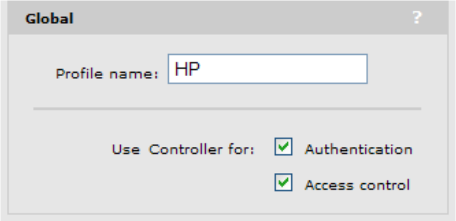
Only allow traffic addressed to:
IP address: Mask: Add
Remove Selected Entry

DHCP server

DHCP server settings can be configured using the Address allocation configuration page.

About access control and authentication

The availability of certain VSC features and their functionality is controlled by the settings of two important parameters in the **Global** box. These parameters determine how authentication and access control are handled by the VSC:



Global

Profile name: HP

Use Controller for: ☑ Authentication

☑ Access control

Use Controller for: Authentication

Determines if user authentication services (802.1X, WPA, WPA2, MAC-based) are provided by the controller. When enabled, APs forward user login requests to the controller. The controller resolves these requests using the local user accounts, or Active Directory, or acts as a RADIUS proxy for a third-party RADIUS server.

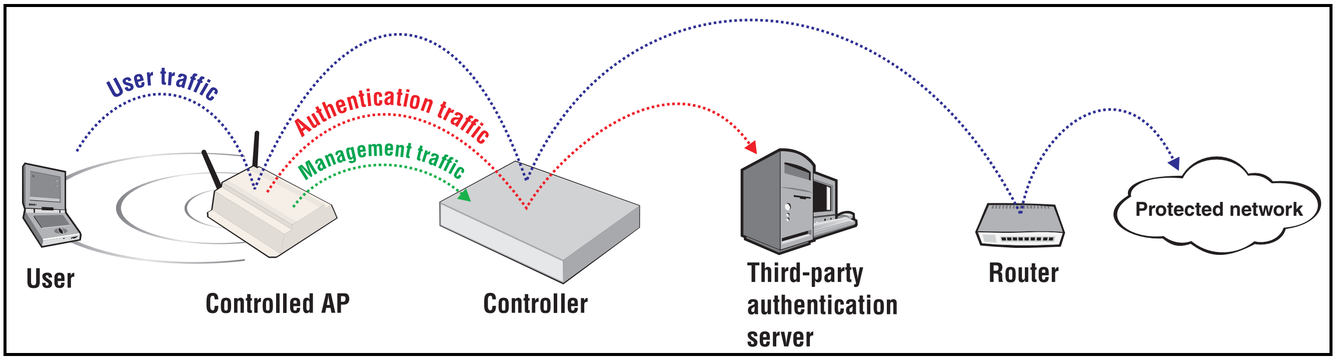
Use Controller for: Access control

This option can only be enabled if the **Authentication** option is enabled first. When enabled, this option creates an *access-controlled VSC*. This means that access to protected network resources via this VSC are restricted by the access control features on the controller. Access control features include the public/guest network access interface and access lists.

The following diagrams provide an overview of how user authentication and data traffic are handled depending on how these options are configured.

When both authentication and access control are enabled

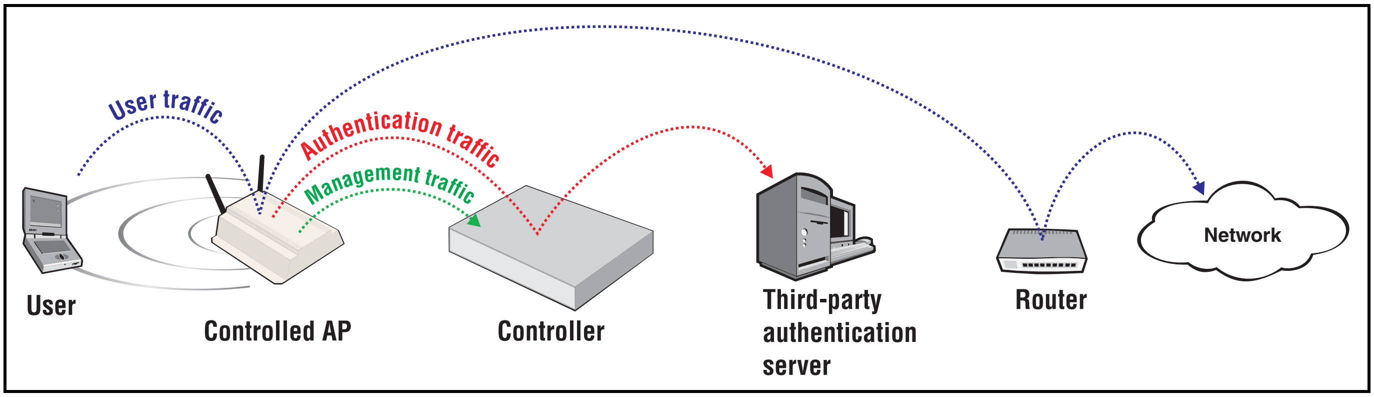
In this configuration, the controlled AP forwards authentication requests from users on the VSC to the controller. The controller resolves these requests using the local user list, or the services of a third-party authentication server (Active Directory or RADIUS server). The controller then manages access to the protected network using its access control features (public access, interface, access lists, etc.).



When only authentication is enabled

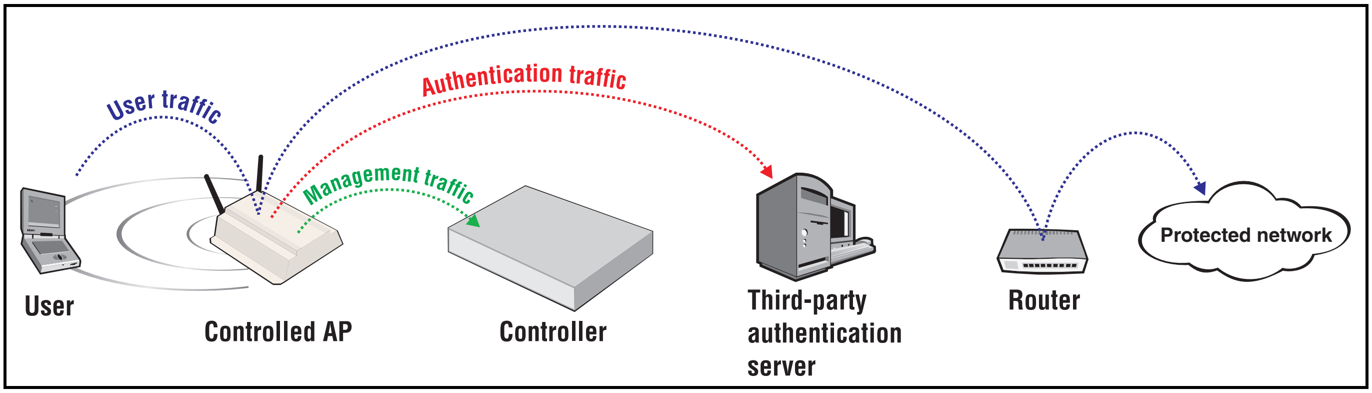
In this configuration, the controlled AP forwards authentication requests from users on the VSC to the controller. The controller resolves these requests using the local user list, or the services of a third-party authentication server (Active Directory or RADIUS server).

The controlled AP forwards all authenticated user traffic from users on the VSC to the protected network (or another device performing access control) according to settings defined on the controlled AP.



When neither option is enabled

In this configuration, the controlled AP can be configured to resolve authentication requests using a third-party RADIUS server and forward authenticated user traffic to the protected network (or another device performing access control). In this scenario, the controller is only used for management of the controlled AP.



Summary of VSC configuration options

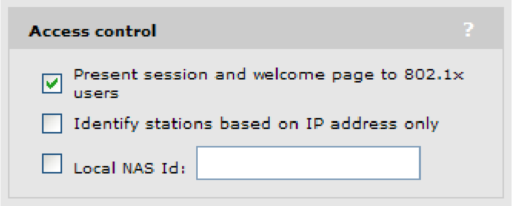
The following table lists the VSC configuration options that are available depending on how access control and authentication are configured.

	Use Controller for:		
VSC configuration option	**Authentication and Access control**	**Authentication only**	**Neither**
Access control	✔	✕	✕
Virtual AP	✔	✔	✔
VSC ingress mapping	✔	✔	✕
VSC egress mapping	✔	✕	✕
Default user data rates	✔	✕	✕
Wireless mobility	✕	✔	✔
Fast wireless roaming	✕	✔	✔
Wireless security filters	✔	✔	✔
Wireless protection	✔	✔	✔
802.1X authentication	✔	✔	✔
RADIUS authentication realms	✔	✔	✕
HTML-based user logins	✔	✕	✕
VPN-based authentication	✔	✕	✕
MAC-based authentication	✔	✔	✔
Location-aware	✔	✕	✕
Wireless MAC filter	✔	✔	✔
Wireless IP filter	✔	✔	✔
DHCP server	✔	✕	✕
DHCP relay	✔	✕	✕

The sections that follow provide an overview and use of each VSC option. For complete descriptions of individual parameters see the online help in the management tool.

Access control

The settings only apply to access-controlled VSCs.



Access control

☑ Present session and welcome page to 802.1x users

□ Identify stations based on IP address only

□ Local NAS Id:

Present session and welcome page to 802.1X users

Enable this option to have the public access interface present the Welcome, Transport, and Session pages to 802.1X users.

When disabled, these pages are not sent to 802.1X users.

Note Display of the Session page (and other pages that are part of the public access interface) may not work for all users. These pages will fail if the initial traffic from the user's computer is sent by an application other than the user's browser. For example: messaging software, automatic software update services, email applications.

Identify stations based on IP address only

This option only applies when the **HTML-based user logins** option is enabled.

This option controls how client stations are identified once they are logged in.

- **When enabled**, the controller identifies client stations by their IP address only. This setting provides support for network configurations where the MAC address of wireless stations is not visible to the controller, or for configurations where the MAC address changes when a client station roams.
- **When disabled** (default setting), the controller identifies client stations by both IP address and MAC address. Both addresses must remain the same after login for the client station to remain authenticated.

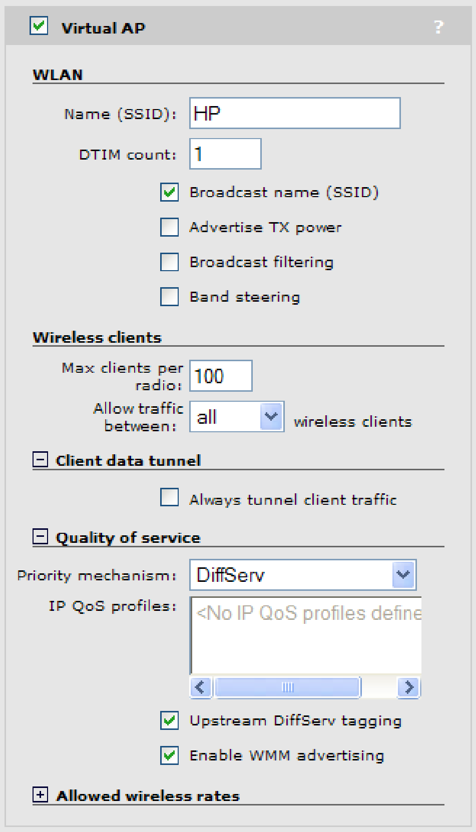
Local NAS ID

Defines a NAS ID for this profile. This ID is used only when RADIUS authentication is not configured for the profile.

Virtual AP

The virtual AP settings define the characteristics of the wireless network created by the VSC, including its name, the number of clients supported, and QoS settings.

Access control enabled



☑ Virtual AP ?

WLAN

Name (SSID): HP

DTIM count: 1

☑ Broadcast name (SSID)
☐ Advertise TX power
☐ Broadcast filtering
☐ Band steering

Wireless clients

Max clients per radio: 100

Allow traffic between: all wireless clients

⊟ Client data tunnel

☐ Always tunnel client traffic

⊟ Quality of service

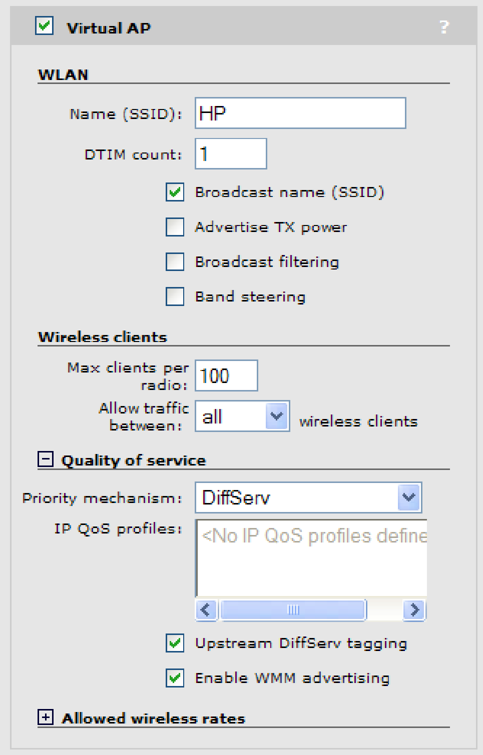
Priority mechanism: DiffServ

IP QoS profiles: <No IP QoS profiles define

☑ Upstream DiffServ tagging
☑ Enable WMM advertising

⊞ Allowed wireless rates

Access control disabled



☑ Virtual AP ?

WLAN

Name (SSID): HP

DTIM count: 1

☑ Broadcast name (SSID)
☐ Advertise TX power
☐ Broadcast filtering
☐ Band steering

Wireless clients

Max clients per radio: 100

Allow traffic between: all wireless clients

⊟ Quality of service

Priority mechanism: DiffServ

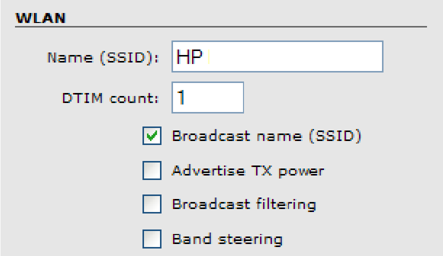
IP QoS profiles: <No IP QoS profiles define

☑ Upstream DiffServ tagging
☑ Enable WMM advertising

⊞ Allowed wireless rates

Select the **Virtual AP** checkbox to enable the wireless network defined by this VSC.

WLAN



WLAN

Name (SSID): HP

DTIM count: 1

☑ Broadcast name (SSID)
☐ Advertise TX power
☐ Broadcast filtering
☐ Band steering

Name (SSID)

Specify a name to uniquely identify the wireless network associated with this VSC. The wireless network is created by the controlled APs and managed by the controller.

Each wireless user that wants to connect to this VSC must use the WLAN name. The name is case-sensitive.

DTIM count

Specify the DTIM period in the wireless beacon sent by controlled APs. Client stations use the DTIM to wake up from low-power mode to receive multicast traffic.

APs transmit a beacon every 100 ms. The DTIM counts down with each beacon that is sent. Therefore if the DTIM is set to 5, then client stations in low-power mode will wake up every 500 ms (.5 second) to receive multicast traffic.

Broadcast name (SSID)

When this option is enabled, controlled APs will broadcast the wireless network name (SSID) to all client stations. Most wireless adapter cards have a setting that enables them to automatically discover APs that broadcast their names and connect to the one with the strongest signal.

If you disable this option, client stations will have to specify the network name you enter for **Name (SSID)** when they connect.

Advertise Tx power

When this option is enabled, controlled APs broadcast their current transmit power setting in the wireless beacon. It also enables support for 802.1h and 802.11d.

Broadcast filtering

Use this option to conserve wireless bandwidth by filtering out non-essential broadcast traffic. When broadcast filtering is enabled:

- DHCP broadcast requests are never forwarded on the wireless port.
- DHCP broadcast offers are never forwarded on the wireless port unless the target of the offer is an associated client on the wireless interface.
- ARP broadcast requests are never forwarded out the wireless port unless the target of the ARP request is an associated client on the wireless interface.

Broadcast filtering should be disabled in the following cases:

- An external DHCP server is connected to the wireless network.
- If a wireless client bridge is connected to the wireless network.

Band steering

Band steering is used to help solve dense client issues. When band steering is enabled, APs attempt to move wireless clients that are capable of 802.11a/n onto the 5 GHz band, thus reducing the load on the slower and more crowded 2.4 GHz band, leaving it for less capable legacy (802.11b/g) clients.

An AP uses the following methods to encourage a wireless client to associate at 5 GHz instead of 2.4 GHz.

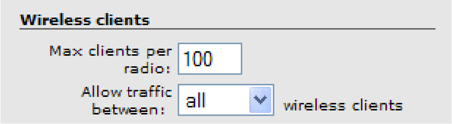
- The AP waits 200ms before responding to the first probe request sent by a client at 2.4 GHz.

- If the AP has learned that a client is capable of transmitting at 5 GHz, the AP refuses the first association request sent by the client at 2.4 GHz.
- Once a client is associated at 5 GHz, the AP will not respond to any 2.4 GHz probes from the client as long as the client's signal strength at 5 GHz is greater than -80 dBm (decibel milliwatt). If the client's signal strength falls below -80 dBm, then the AP will respond to 2.4 GHz probes from the client without delay.

Note

- To support band steering, the VSC must be bound to APs with two radios (MSM422, MSM430, MSM460, or MSM466). One radio must be configured for 2.4 GHz operation and the other for 5 GHz operation.
- Band steering is temporarily suspended on an AP when the radio configured for 5 GHz operation reaches its maximum number of supported clients.

Wireless clients


Wireless clients
Max clients per radio: 100
Allow traffic between: all wireless clients

Max clients per radio

Specify the maximum number of wireless client stations that can be associated with this SSID at the same time on each radio.

Allow traffic between *nn* wireless clients

Use this option to control how wireless clients that are connected to the same VSC can communicate with each other. The following settings are available:

- **No**: Blocks all inter-client communications.
- **802.1X**: Only authenticated 802.1X clients can communicate.
- **All**: All authenticated and unauthenticated clients can communicate. Default setting.
- **IPV6**: Only authenticated clients using IP version 6 can communicate.

Communicating between different VSCs

Communications between client stations connected to different VSCs can only occur if the clients are both assigned to the same VLAN. The easiest way to do this is to assign the same VLAN to both VSCs using the **Egress network** option in the VSC binding.

Another method, which only works with non-access-controlled VSCs, is to dynamically assign the same VLAN to two different users via RADIUS or the local user accounts. See *User-assigned VLANs on page 7-6*.

In addition, the following rules govern how traffic is exchanged:

- Unicast traffic exchanged between VSCs on the ***same*** radio is controlled by the setting of the receiver VSC.

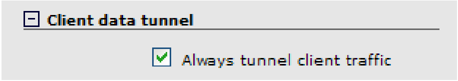
- Unicast traffic exchanged between VSCs on ***different*** radios is controlled by the setting of the sender's VSC.
- Multicast traffic exchanged between VSCs is always controlled by the setting of the sender's VSC.

Generally, most clients will be involved in the bidirectional exchange of unicast packets. In this case, the rules can be simplified by assuming that the most restrictive setting for this option takes precedence. For example:

- If VSC1 is set to **No** and VSC2 is set to **All**, no communication is permitted between clients on the two VSCs, or between clients on VSC1. However, all clients on VSC2 can communicate with each other.
- If VSC1 is set to **802.1X** and VSC2 set to **All**, only 802.1X clients can communicate between the two VSCs.

Client data tunnel

(Only available when **Access control** is enabled.)



☑ Always tunnel client traffic

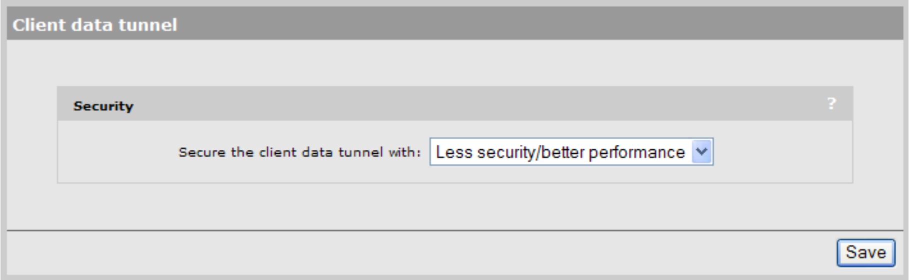
When a VSC is access-controlled, client traffic that is sent between the AP and controller can be carried in the client data tunnel. This provides the following benefits:

- User traffic is segregated from the backbone network and can only travel to the controller.
- Underlying network topology is abstracted enabling full support for L2-connected users across routed networks.

The client data tunnel is always used when the connection between a controlled AP and its controller traverses at least one router. The client data tunnel supports NAT traversal, so it can cross routers that implement NAT.

Optionally, the client data tunnel can also be used when a controlled AP and its controller are on the same subnet. To do this, enable the **Always tunnel client traffic** option.

Performance and security settings for the client data tunnel can be customized by selecting **Controller >> Controlled APs > Client data tunnel**.



Secure the client data tunnel with: Less security/better performance

- **Less security/better performance**: This option provides security using a secret key that is attached to each packet. The key is rotated every 200 seconds.

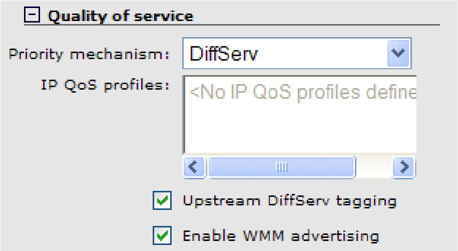
- **High security/less performance**: This option uses HMAC (Hash based message authentication code) to ensure the data integrity and authenticity of each packet. Performance is reduced due to the overhead needed to calculate HMAC.

Regardless of the security method used, the client tunnel **does not encrypt the data stream**. To protect client traffic with encryption requires that client stations use WPA or VPN software.

- Under **Wireless protection**, enable **WPA** with the **Terminate WPA at the controller.** This requires client stations that support WPA.
- Use **VPN-based authentication**. See *Securing wireless client sessions with VPNs on page 16-3*.

Quality of service

The quality of service (QoS) feature provides a number of different mechanisms to prioritize wireless traffic sent to wireless client stations. See *Quality of service (QoS) on page 5-37*.



⊟ Quality of service

Priority mechanism: DiffServ

IP QoS profiles: <No IP QoS profiles define

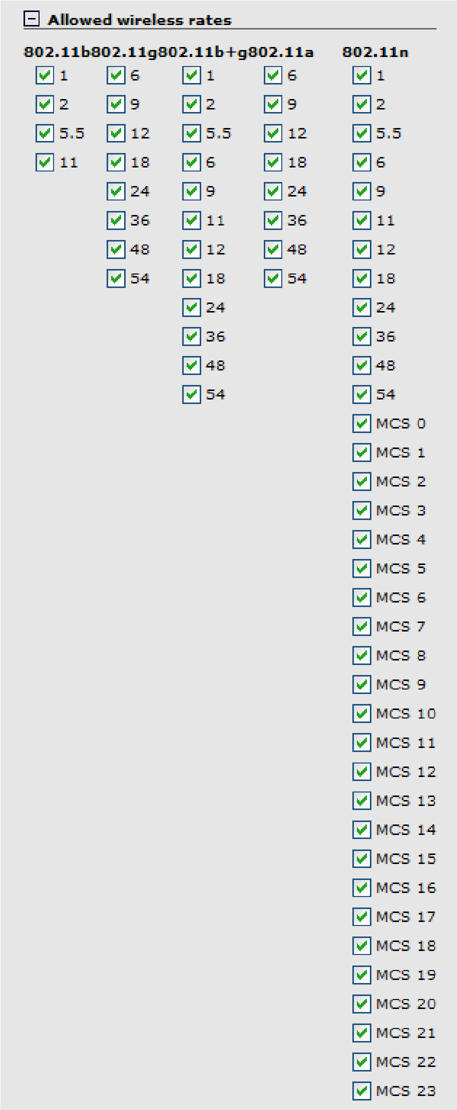
☑ Upstream DiffServ tagging

☑ Enable WMM advertising

Allowed wireless rates

Select the wireless transmission speeds (in Mbps) that this VSC will support for each wireless mode. Clients will only be able to connect at the rates that you select. If a client does not support the selected rate and mode, it will not be able to connect to this VSC.

Note that all APs do not support all wireless modes and rates. See *Wireless mode on page 4-20* for details.



⊟ **Allowed wireless rates**

802.11b	802.11g	802.11b+g	802.11a	802.11n
☑ 1	☑ 6	☑ 1	☑ 6	☑ 1
☑ 2	☑ 9	☑ 2	☑ 9	☑ 2
☑ 5.5	☑ 12	☑ 5.5	☑ 12	☑ 5.5
☑ 11	☑ 18	☑ 6	☑ 18	☑ 6
	☑ 24	☑ 9	☑ 24	☑ 9
	☑ 36	☑ 11	☑ 36	☑ 11
	☑ 48	☑ 12	☑ 48	☑ 12
	☑ 54	☑ 18	☑ 54	☑ 18
		☑ 24		☑ 24
		☑ 36		☑ 36
		☑ 48		☑ 48
		☑ 54		☑ 54
				☑ MCS 0
				☑ MCS 1
				☑ MCS 2
				☑ MCS 3
				☑ MCS 4
				☑ MCS 5
				☑ MCS 6
				☑ MCS 7
				☑ MCS 8
				☑ MCS 9
				☑ MCS 10
				☑ MCS 11
				☑ MCS 12
				☑ MCS 13
				☑ MCS 14
				☑ MCS 15
				☑ MCS 16
				☑ MCS 17
				☑ MCS 18
				☑ MCS 19
				☑ MCS 20
				☑ MCS 21
				☑ MCS 22
				☑ MCS 23

To ensure a high quality of service for voice applications, disable all rates below 5.5. Also, ensure that the radio is configured as follows:

- **Operating mode** is set to **Access point only**.
- **Channel** is set to a fixed channel, or **Automatic** with **interval** set to **Disabled**.
- **Automatic power control** is disabled under **Transmit power control**.
- On the **Wireless > Neighborhood** page, do not enable the **Repeat scan every nnn seconds** option.

Notes on 802.11n

802.11n supports legacy rates (1 to 54), as well as high-throughput (HT) rates MCS 0 to MSC 23.

- **MCS 0 to MCS 15** are supported by the MSM410, MSM422, E-MSM430, E-MSM460, and E-MSM466.
- **MCS 16 to MCS 23** are supported by the E-MSM460 and E-MSM466.
- You must always enable at least one legacy rate for 802.11n.

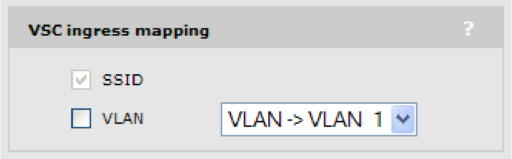
Notes regarding the E-MSM430, E-MSM460, and E-MSM466

On these products, the wireless rates shown for 802.11n apply to all wireless modes supported on both radios, which are 802.11a/b/g/n. If you remove a rate, it is removed for all wireless modes.

VSC ingress mapping

These settings apply to the controller only and define how ingress (incoming) user traffic is assigned to a VSC on the controller. The ingress lets you control what type of traffic the VSC will handle.

When access control is enabled, available options are:



VSC ingress mapping

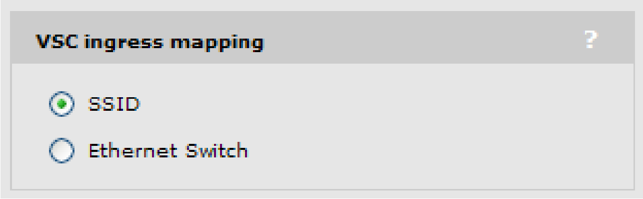
☑ SSID

☐ VLAN   VLAN -> VLAN 1

The **SSID** option cannot be disabled. When enabled, the VSC accepts incoming traffic that has its SSID set to the **WLAN name (SSID)** defined under **Virtual AP**.

If you enable the **VLAN** option, you can choose a single VLAN, or a VLAN range enabling the VSC to handle traffic from multiple sources. For example, if you define different Egress networks when binding VSCs to your APs, you could specify a range to have all traffic handled by one VSC. (Ingress VLANs are not supported when controller teaming is active.)

When access control is disabled, available options are:



VSC ingress mapping

● SSID

○ Ethernet Switch

When the **SSID** option is enabled, the VSC accepts incoming traffic that has its SSID set to the **WLAN name (SSID)** defined under **Virtual AP**.

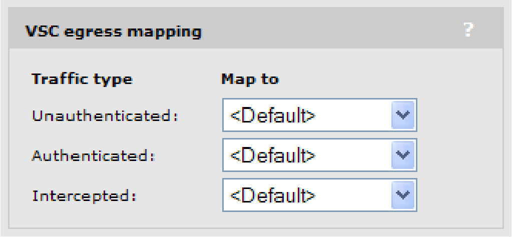
The **Ethernet Switch** option enables the VSC to be bound to the switch ports on an MSM317. See the *MSM317 Access Device Installation and Getting Started Guide*.

If a VSC is bound to the MSM317 Ethernet Switch, it cannot handle traffic from wireless clients on the MSM317 or other APs.

For more information, see *VSC data flow on page 5-32* and *Traffic flow for wireless users on page 7-6*.

VSC egress mapping

These options select the output interface on the controller on which an access-controlled VSC forwards user traffic. Different egress mappings can be defined depending on whether the user is unauthenticated, authenticated, or being intercepted. (To enable traffic interception for a specific user, you must specify the appropriate setting in the user's RADIUS account. See *Colubris-Intercept on page 15-25*.)



VSC egress mapping

Traffic type	Map to
Unauthenticated:	<Default>
Authenticated:	<Default>
Intercepted:	<Default>

Different types of traffic can be forwarded to different output interfaces, which include: the routing table, VLAN ID, or an IP GRE tunnel. Before you can map traffic to an output interface, the interface must already be defined. For VLANs to appear in the selection list they must be assigned an IP address. (Define VLANs on the **Controller >> Network > Ports** page.)

When the **Default** option is selected, the controller routing table is used for all egress traffic. Therefore, all traffic on this VSC is routed according to the routes defined on the **Controller >> Network > IP routes** page.

For more information, see *VSC data flow on page 5-32* and *Traffic flow for wireless users on page 7-6*.

Note

To set VSC egress options for controlled APs, see *Binding VSCs to groups on page 6-23*. On the MSM317, VSCs can also be bound directly to the switch ports. See the *MSM317 Access Device Installation and Getting Started Guide*.

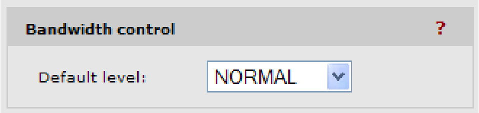
Bandwidth control

This option is only available if the **Internet port data rate limits** option is enabled on the **Controller >> Network > Bandwidth control** page. See *Bandwidth control on page 3-21*.

Select the bandwidth control level to regulate traffic flow for all user traffic handled by this VSC. Bandwidth levels are defined on the **Controller >> Network > Bandwidth control** page.

This default setting applies to all users that do not have a bandwidth level assigned in their account (local or RADIUS). Local accounts are defined on the Users menu.

For more information on setting the appropriate RADIUS attributes to accomplish this, refer to the Management and Configuration Guide for this product.

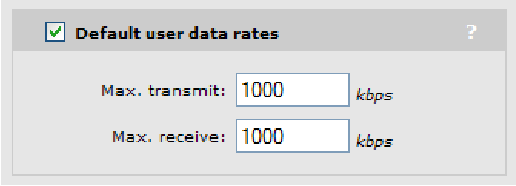


Bandwidth control ?

Default level: NORMAL

Default user data rates

These options enable you to set the default data rates for authenticated users that do not have a data rate set in their RADIUS accounts, and for unauthenticated users. For details on setting user data rates using RADIUS attributes, see *Chapter 14: Public/guest network access* and *Chapter 15: Working with RADIUS attributes*.



☑ **Default user data rates** ?

Max. transmit: 1000 *kbps*

Max. receive: 1000 *kbps*

Max transmit

Specify the maximum rate (in kbps) at which users can send data.

Max receive

Specify the maximum rate (in kbps) at which users can receive data.

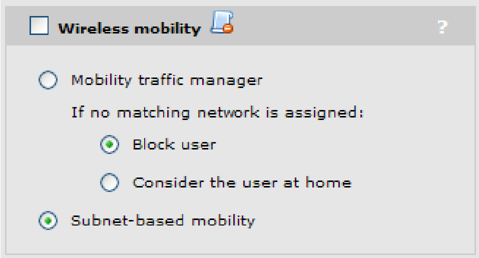
Note

The **Internet port data rate limits** defined on the **Controller >> Network > Bandwidth control** page always take precedence over user data rates set in the VSC. This means if you set a data rate which exceeds the configured bandwidth for the port, the rate will be capped.

Wireless mobility

The wireless mobility feature provides for seamless roaming of wireless users, while at the same time giving you complete control over how wireless user traffic is distributed onto the wired networking infrastructure. This enables you to implement a wireless networking solution that is perfectly tailored to meet the needs of you users and the topology of your network.

For detailed information on how to use and configure this feature, see *Chapter 9: Mobility traffic manager*.



☐ **Wireless mobility** ?

○ Mobility traffic manager

If no matching network is assigned:

● Block user

○ Consider the user at home

● Subnet-based mobility

To use wireless mobility, you must:

- Disable the **Access control** option under **Global**.
- Install a **Mobility** or **Premium** license on the controller.
- Bind the same VSC to all APs that will support roaming.
- Configure the **Wireless security filters** so that they do not interfere with roaming functionality. In most cases, these filters should be disabled. If you need to use them, note that:
  - The **Restrict wireless traffic to: Access point default gateway** option is not supported.
  - The **Restrict wireless traffic to: MAC** or **Custom** options can be used provided that they restrict traffic to destinations that are reachable from all subnets in the mobility domain.

Mobility traffic manager

Mobility Traffic Manager (MTM) enables you to take advantage of both distributed and centralized strategies when deploying a wireless networking solution. For a complete discussion of this feature and how to use it see, *Chapter 9: Mobility traffic manager on page 9-1*.

If you are using MTM to tunnel the traffic from wireless users to their home networks, set the following parameter to determine how MTM routes traffic if no home network is assigned to a user (via their RADIUS account or local user account), or if the user's home network is not found in the mobility domain.

If no matching network is assigned:

- **Block user:** User access is blocked.
- **Consider the user at home:** The user's home network is considered to be the subnet assigned to the AP.

Subnet-based mobility

This feature has been deprecated. *If you are creating a new installation, use Mobility Traffic Manager. If you are upgrading from a previous release, your subnet-based configuration will still work. However, for added benefits and greater flexibility you should migrate your setup to Mobility Traffic Manager.*

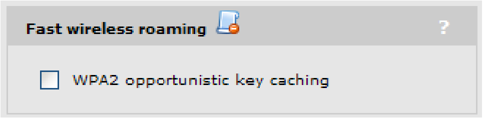
When Subnet-based mobility is enabled, a user's home subnet is determined based on the IPv4 address assigned to a user when they connect to the wireless network. If a user's IPv4 address is not within the scope of any of the local subnets assigned to the AP, the user is considered foreign to the network and their traffic is tunnelled via the controller to their home subnet. If the user's subnet does not match any subnets defined in the mobility domain, the user is blocked.

One issue with using this method to determine the home subnet is that a user's IPv4 address is typically retrieved through DHCP. If a user connects to an AP in a new location (rather than roaming to the AP), the IP address assigned through DHCP may identify the user as local to the network, and not roaming.

Fast wireless roaming

WPA2 opportunistic key caching eliminates the delays associated with reauthentication when client stations roam between APs installed on the same subnet.

The controller manages key distribution between the APs so that when wireless users roam between APs, reauthentication is not delayed by having to completely renegotiate key values.



Fast wireless roaming

□ WPA2 opportunistic key caching

To support fast wireless roaming:

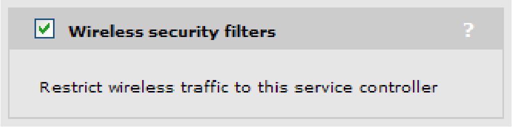
- Disable the **Access control** option under **Global**.
- Install a **Mobility** or **Premium** license on the controller.
- All APs must be on the same layer 2 network.
- All APs must have VSCs with the same name, SSID, and wireless protection settings.
- Wireless protection must be WPA, or 802.1X authentication must be enabled.

Note RADIUS accounting is not supported when this option is enabled.

Wireless security filters

APs feature an intelligent bridge that can apply security filters to safeguard the flow of wireless traffic. These filters limit both incoming and outgoing traffic as defined below and force the APs to exchange traffic with a specific upstream device.

When access control is enabled, available options are:



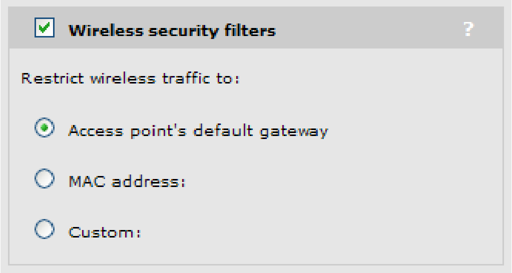
☑ Wireless security filters

Restrict wireless traffic to this service controller

The controlled AP will only allow user traffic that is addressed to the controller. All other traffic is blocked. Make sure that the controller is set as the default gateway for all users. If not, all user traffic will be blocked by the AP.

The default wireless security filters defined below are active.

When access control is disabled, available options are:



☑ Wireless security filters

Restrict wireless traffic to:

● Access point's default gateway

○ MAC address:

○ Custom:

Configure security filter settings using the available options as described in the following section.

Restrict wireless traffic to

This setting defines the upstream device to which the AP will forward wireless traffic. If you are using multiple VLANs, each with a different gateway, use the **MAC address** option.

- **Access point's default gateway:** This sends traffic to the default gateway assigned to the AP. The default wireless security filters are in effect for wireless traffic.
- **MAC address:** Specify the MAC address of the upstream device to which all traffic is to be forwarded. The default wireless security filters are in effect for wireless traffic.
- **Custom:** Use this option to define custom wireless security filters and a custom target address for the upstream device. Refer to the **Custom** section that follows for details.

Default wireless security filter definitions

The following filters are defined by default.

Incoming wireless traffic filters

Applies to traffic sent from wireless users to the AP.

Accepted

- Any IP traffic addressed to the controller.
- PPPoE traffic (The PPPoe server must be the upstream device.)
- IP broadcast packets, except NetBIOS
- Certain address management protocols (ARP, DHCP) regardless of their source address.
- Any traffic addressed to the AP, including 802.1X.

Blocked

- All traffic that is not accepted is blocked. This includes NetBIOS traffic regardless of its source/destination address. HTTPS traffic not addressed to the AP (or upstream device) is also blocked, which means wireless users cannot access the management tool on other HP ProCurve APs.

Outgoing wireless traffic filters

Applies to traffic sent from the AP to wireless users.

Accepted

- Any IP traffic coming from the upstream device, except NetBIOS packets.
- PPPoE traffic from the upstream device.
- IP broadcast packets, except NetBIOS
- ARP and DHCP Offer and ACK packets.
- Any traffic coming from the AP itself, including 802.1X.

Blocked

- All other traffic is blocked. This includes NetBIOS traffic regardless of its source/ destination address.

Custom wireless security filter definitions

Use this option to define your own security filters to control incoming and outgoing wireless traffic. To use the default filters as a starting point, select **Get Default Filters**.

Filters are specified using standard pcap syntax with the addition of a few HP ProCurve-specific placeholders. These placeholders can be used to refer to specific MAC addresses and are expanded by the AP when the filter is activated. Once expanded, the filter must respect the pcap syntax. The pcap syntax is documented in the tcpdump man page:

http://www.tcpdump.org/tcpdump_man.html

Placeholders

- MAC address of the controller.
- MAC address of the bridge.
- MAC address of the default gateway assigned to the AP.
- : MAC address of AP wireless port.

Wireless mobility considerations

If you enable the wireless mobility feature (to support roaming across different subnets), configuration of the wireless security filters must respect the following guidelines so as not to interfere with roaming functionality.

- The **Restrict wireless traffic to: Access point default gateway** option is not supported.
- The **Restrict wireless traffic to: MAC** or **Custom** options can be used provided that they restrict traffic to destinations that are reachable from all subnets in the mobile domain.

Wireless protection

Two types of wireless protection are offered. WPA and WEP.

On the MSM410 and MSM422
When using 802.11n, wireless protection settings are enforced as follows:

- WEP protection is never permitted. If selected, WPA or WPA2 protection is used instead.
- When using pure 802.11n in either the 2.4 or 5 GHz bands, WPA2 protection is used instead of WPA.

On the E-MSM430, E-MSM460, and E-MSM466
When using 802.11n, wireless protection settings are enforced as follows:

- WEP protection is permitted. If selected, all 802.11n features of the radio are disabled for this VSC. The VSC will only support legacy a/b/g traffic.
- WPA is not supported on these products.

WPA

This option enables support for users with WPA / WPA2 client software.

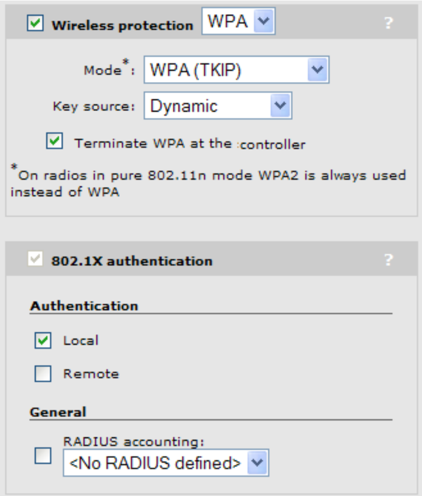
Mode
Support is provided for:

- **WPA (TKIP)**: WPA with TKIP encryption. (Not supported on the E-MSM430, E-MSM460, E-MSM466.)
- **WPA2 (AES/CCMP)**: WPA2 (802.11i) with AES/CCMP encryption.
- **WPA or WPA2**: Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time.

Key source
This option determines how the TKIP keys are generated.

- **Dynamic**: This is a dynamic key that changes each time the user logs in and is authenticated. The MPPE key is used to generate the TKIP keys that encrypt the wireless data stream. The key is generated via the configured **802.1X authentication** method. Therefore, when you enable this option, the **802.1X authentication** feature is automatically enabled.

Authentication can occur via the local user accounts and a remote authentication server (Active Directory, or third-party RADIUS server). If both options are enabled, the local accounts are checked first.



☑ **Wireless protection** WPA

Mode*: WPA (TKIP)

Key source: Dynamic

☑ Terminate WPA at the controller

*On radios in pure 802.11n mode WPA2 is always used instead of WPA

☑ **802.1X authentication**

Authentication

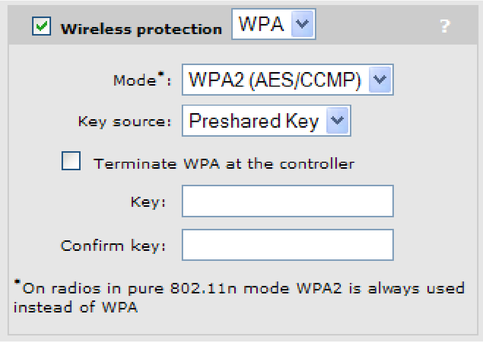
☑ Local

☐ Remote

General

☐ RADIUS accounting: <No RADIUS defined>

- **Preshared Key**: The controller uses the key you specify in the **Key** field to generate the TKIP keys that encrypt the wireless data stream. Since this is a static key, it is not as secure as the RADIUS option. Specify a key that is between 8 and 63 alphanumeric characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers. The double quote character (”) should not be used.



☑ **Wireless protection** WPA

Mode*: WPA2 (AES/CCMP)

Key source: Preshared Key

☐ Terminate WPA at the controller

Key:

Confirm key:

*On radios in pure 802.11n mode WPA2 is always used instead of WPA

Terminate WPA at the controller

This feature is intended for low throughput applications, such as supporting point of sale (POS) terminals.

- When enabled, the controller acts as the termination point for all WPA/WPA2 sessions. This enables the network to meet PCI (Payment Card Industry) compliance supporting the connection of point of sale (POS) terminals.

- When disabled, WPA/WPA2 sessions are terminated at the AP. This means that wireless communication between the client station and AP is secure, but traffic between the AP and controller is not. This is normally sufficient since outsiders do not have access to your wired network. However, in a public venue such as a hotel, if the public has access to your wired network, it may be necessary to provide end-to-end security for certain client stations, such as POS terminals.

Note This feature supports a maximum of 10 sessions on the MSM710, and 50 sessions on the MSM760 and MSM765.

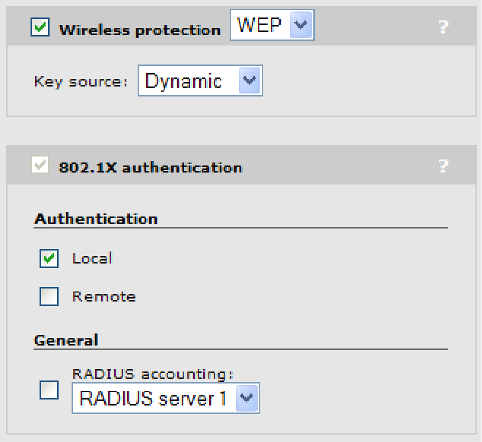
WEP

This option provides support for users using WEP encryption.

Key source

This option determines how the WEP keys are generated: dynamic or static key.

- **Dynamic**: This is a dynamic key that changes each time the user logs in and is authenticated.



☑ Wireless protection WEP

Key source: Dynamic

☑ 802.1X authentication

Authentication

☑ Local

□ Remote

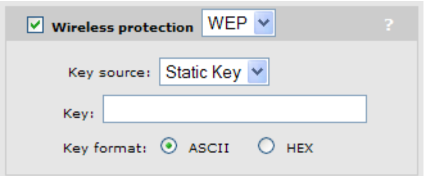
General

□ RADIUS accounting: RADIUS server 1

The key is generated via the configured **802.1X authentication** method. Therefore, when you enable this option, the **802.1X authentication** feature is automatically enabled.

Support static WEP: Enables support for users that are using the specified static WEP key. See the definitions below for information on how to define the key.

- **Static key**: This is a static key that you must define.



☑ Wireless protection WEP

Key source: Static Key

Key:

Key format: ● ASCII ○ HEX

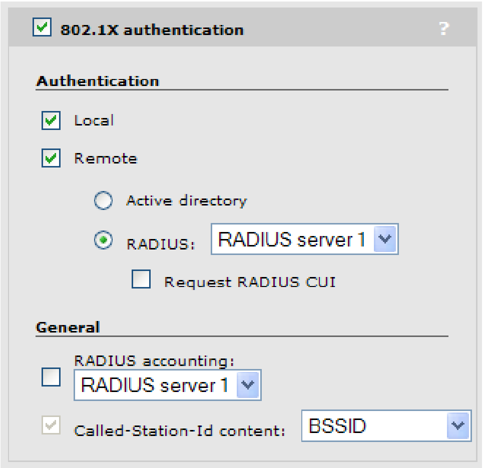
  - **Key:** The number of characters you specify for the key determines the level of encryption. For 40-bit encryption, specify 5 ASCII characters or 10 HEX digits. For 128-bit encryption, specify 13 ASCII characters or 26 HEX digits.

When encryption is enabled, wireless stations that do not support encryption cannot communicate with the AP. The definition for each encryption key must be the same on the AP and all client stations.

- **Key format:** Select the format used to specify the encryption key:
  - **ASCII:** ASCII keys are much weaker than carefully chosen HEX keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client stations support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.
  - **HEX:** Your keys should only include the following characters: 0-9, a-f, A-F

802.1X authentication

This option enables you to use 802.1X to authenticate wireless and wireless users. For configuration details, see *Configuring 802.1X support on a VSC on page 10-10*.



☑ 802.1X authentication ?

Authentication

☑ Local

☑ Remote

○ Active directory

● RADIUS: RADIUS server 1

□ Request RADIUS CUI

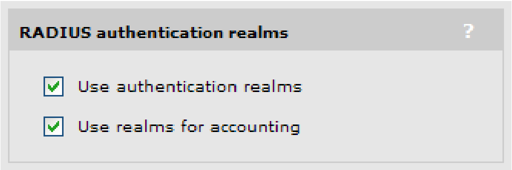
General

□ RADIUS accounting: RADIUS server 1

☑ Called-Station-Id content: BSSID

RADIUS authentication realms

When realms are enabled for accounting or authentication, selection of the RADIUS server to use is based on the realm name. If no match is found, then the configured RADIUS profile name is used. This applies to any VSC authentication or accounting setting that uses a RADIUS server.



RADIUS authentication realms ?

☑ Use authentication realms

☑ Use realms for accounting

Realm names are extracted from user names as follows: if the username is **person1@mydomain.com** then **mydomain.com** is the realm. The authentication request is sent to the RADIUS profile with the realm name **mydomain.com**. The username sent for authentication is still the complete **person1@mydomain.com**.

For added flexibility, regular expressions can be used in realm names, enabling a single realm name to match many users. For example, if a realm name is defined with the regular expression **^abc.*** then all usernames beginning with **abc** followed by any number of characters will match. The following usernames would all match:

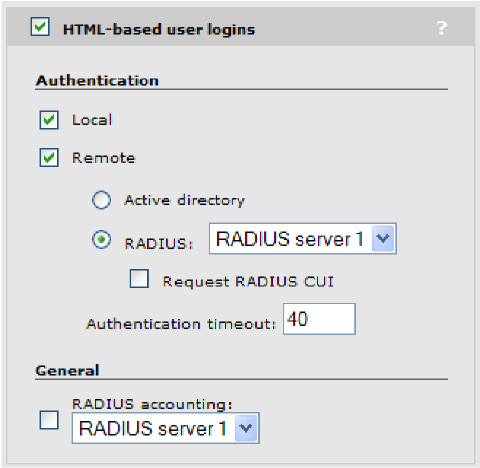
abc123.biz
abc321.lan
abc1

Important

- Realms are not case sensitive.
- Realms have a maximum length of 64 characters.
- A maximum of 200 realms can be defined across all profiles. However, there is no limit per profile.
- Each RADIUS profile can be associated with one or more realms. However, a realm cannot be associated with more than one profile.
- A realm overrides the authentication RADIUS server only; the server used for accounting is not affected.
- A realm overrides the authentication RADIUS server only. The server used for accounting is not affected.
- When the realm configuration is changed in any way, all authenticated users are logged out.

HTML-based user logins

This option defines settings for users who log in to the public access interface using a Web browser. If you disable this option, the public access interface Login page is not shown to these users. However, login is still possible via other methods such as MAC authentication and 802.1X.



☑ HTML-based user logins

Authentication

☑ Local

☑ Remote

○ Active directory

● RADIUS: RADIUS server 1

□ Request RADIUS CUI

Authentication timeout: 40

General

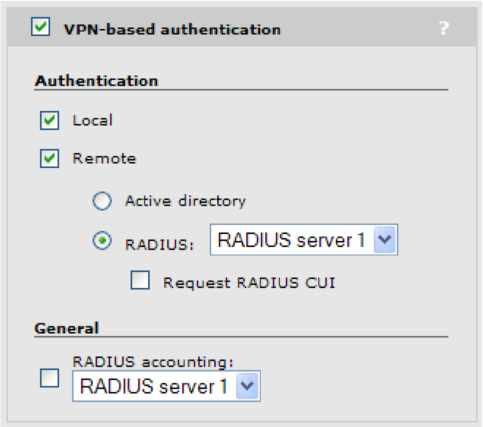
□ RADIUS accounting: RADIUS server 1

For configuration details, see *Configuring HTML-based authentication on a VSC on page 10-22*.

Note The global MAC-based authentication feature only applies on VSCs that have HTML-based user logins enabled. See *Configuring global MAC-based authentication on page 10-16*.

VPN-based authentication

VPN-based authentication can be used to provide secure access for client stations on VSCs that do not have encryption enabled.



☑ **VPN-based authentication** ?

Authentication

☑ Local

☑ Remote

○ Active directory

● RADIUS: RADIUS server 1

□ Request RADIUS CUI

General

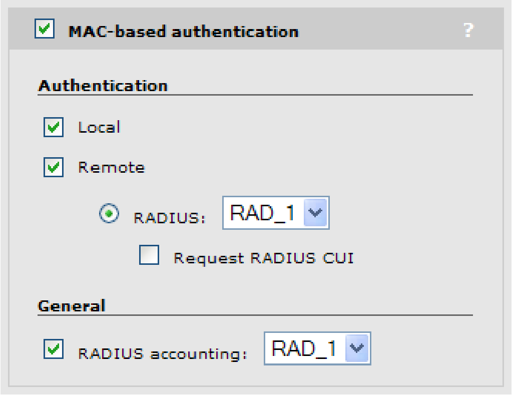
□ RADIUS accounting: RADIUS server 1

For configuration details, see *Configuring VPN-based authentication on a VSC on page 10-24*.

MAC-based authentication

This option can be used to authenticate both wireless and wired users, depending on how the VSC is configured. To configure this options, see *Configuring MAC-based authentication on a VSC on page 10-17*.

This option cannot be used at the same time as HTML-based authentication. If you want to use both MAC-based authentication and HTML-based authentication at the same time, use the global MAC-based authentication option See *MAC-based authentication on page 10-14*.



☑ **MAC-based authentication** ?

Authentication

☑ Local

☑ Remote

● RADIUS: RAD_1

□ Request RADIUS CUI

General

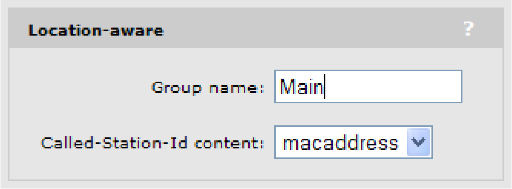
☑ RADIUS accounting: RAD_1

Location-aware

This option enables you to control logins to the public access network based on the AP, or group of APs, to which a user is connected. It is automatically enabled when a VSC is set to **Access control**.

Location-aware is always enabled when using the controller for authentication or access-control with a remote RADIUS server.

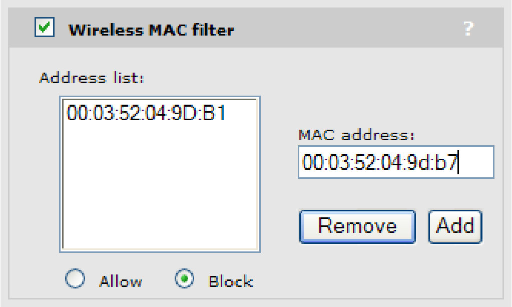
For each user login, location-aware sends the PHY Type, SSID, and VLAN to the remote RADIUS server. It also includes the specified **Called-Station-Id content**.



Group name: Main
Called-Station-Id content: macaddress

Wireless MAC filter

This option enables you to control access to the wireless network based on the MAC address of a device. You can either block access or allow access, depending on your requirements. To configure this option, see *Configuring MAC-based filters on a VSC on page 10-19*. Up to 64 MAC addresses can be defined per VSC.

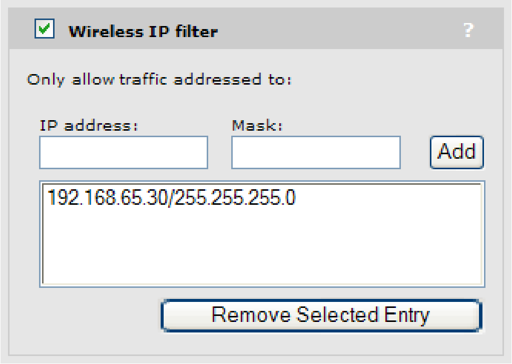

☑ Wireless MAC filter

Address list: 00:03:52:04:9D:B1
MAC address: 00:03:52:04:9d:b7
○ Allow ● Block

Wireless IP filter

When this option is enabled, the VSC only allows wireless traffic that is addressed to an IP address that is defined in the list. All other traffic is blocked, except for:

- DNS queries (i.e., TCP/UDP traffic on port 53)
- DHCP requests/responses



☑ Wireless IP filter

Only allow traffic addressed to:

IP address: Mask:

192.168.65.30/255.255.255.0

A maximum of two addresses can be defined. Each address can target a specific device or a range of addresses.

Examples
To only allow traffic addressed to a gateway at the address 192.168.130.1, define the filter as follows:

- Address = 192.168.130.1
- Mask = 255.255.255.255

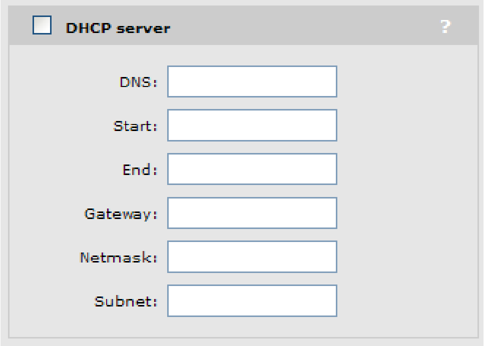
To only allow traffic addressed to the network 192.168.130.0, define the filter as follows:

- Address = 192.168.130.0
- Mask = 255.255.255.0

DHCP server

This option is only available if the controller is configured as a DHCP server on the **Controller >> Network > Address allocation** page. See *Address allocation on page 3-13*.

A separate DHCP server can be enabled on each VSC to provide custom addressing that is different from the base DHCP subnet that is determined by the LAN port IP address.



☐ **DHCP server** ?

DNS:

Start:

End:

Gateway:

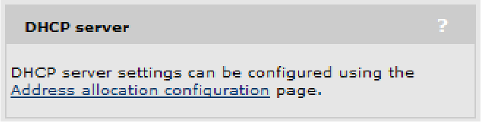
Netmask:

Subnet:

To receive traffic from users, the controller assigns the **Gateway** address you specify to its LAN port.

Note

These configuration options do not appear for the default VSC. The default VSC uses the same settings as defined on the **Controller >> Network > Address allocation** page.



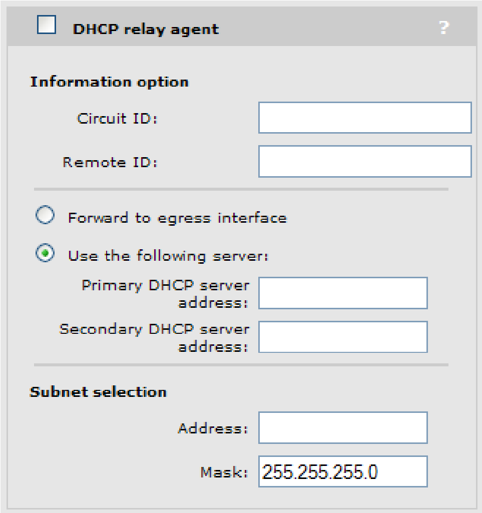
DHCP server ?

DHCP server settings can be configured using the Address allocation configuration page.

DHCP relay agent

This option is only available if the controller is currently configured as a DHCP relay agent on the **Controller >> Network > Address allocation** page. See *Address allocation on page 3-13*.

A separate DHCP relay agent can be enabled on each VSC to provide custom addressing to users.



☐ **DHCP relay agent** ?

Information option

Circuit ID:

Remote ID:

○ Forward to egress interface

● Use the following server:

Primary DHCP server address:

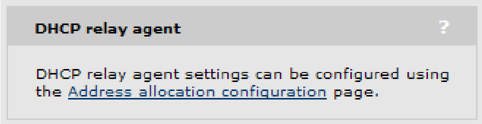
Secondary DHCP server address:

Subnet selection

Address:

Mask: 255.255.255.0

Note These DHCP relay agent options do not appear for the default VSC. The default VSC uses the same settings as defined on the **Controller >> Network > Address allocation** page.



DHCP relay agent

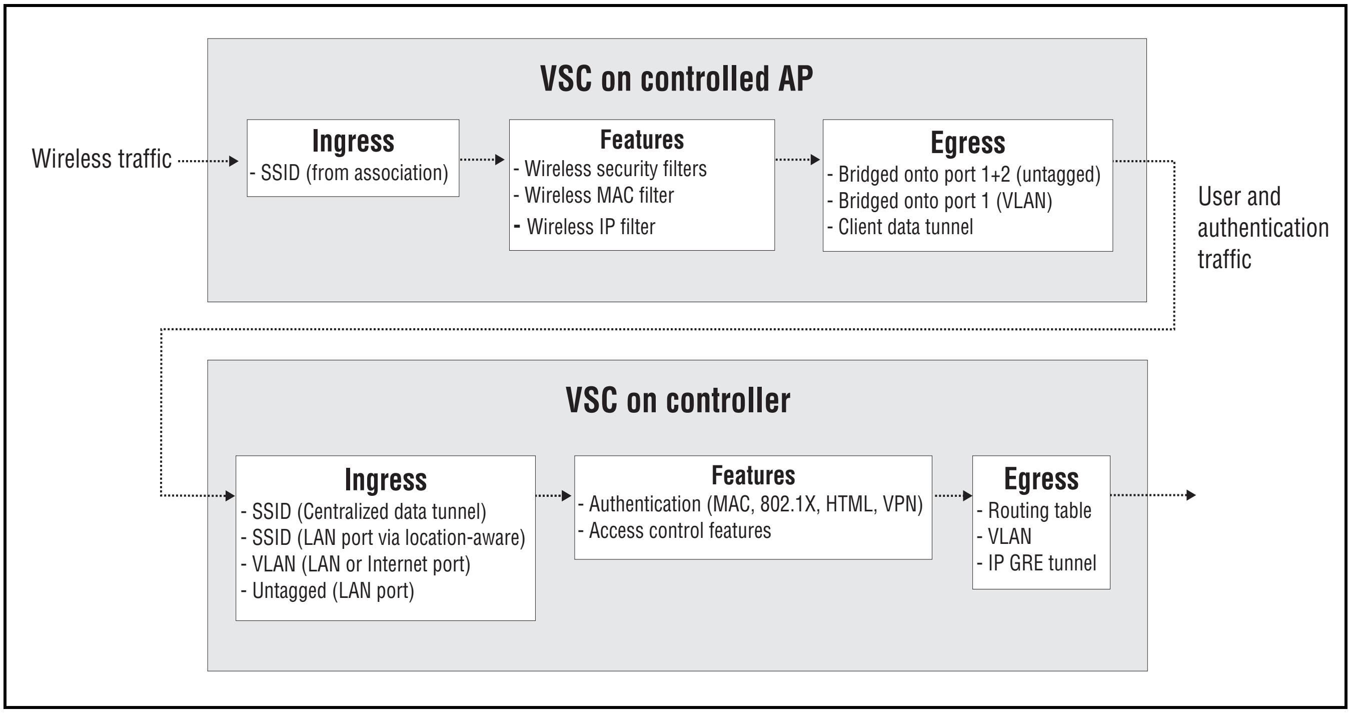
DHCP relay agent settings can be configured using the Address allocation configuration page.

VSC data flow

Each VSC provides a number of configurable options, some of which apply exclusively on controlled APs or the controller. The following diagrams illustrate how traffic from wireless users is handled by VSC definitions on a controlled AP and controller, and shows the options that apply on each device. For more on traffic flow, see *Traffic flow for wireless users on page 7-6*.

Access control enabled

This diagram shows traffic flow when an access-controlled VSC is bound to an AP.


VSC on controlled AP
Wireless traffic
Ingress
- SSID (from association)
Features
- Wireless security filters
- Wireless MAC filter
- Wireless IP filter
Egress
- Bridged onto port 1+2 (untagged)
- Bridged onto port 1 (VLAN)
- Client data tunnel
User and authentication traffic
VSC on controller
Ingress
- SSID (Centralized data tunnel)
- SSID (LAN port via location-aware)
- VLAN (LAN or Internet port)
- Untagged (LAN port)
Features
- Authentication (MAC, 802.1X, HTML, VPN)
- Access control features
Egress
- Routing table
- VLAN
- IP GRE tunnel

VSC on controlled AP

Ingress

The AP only handles traffic from wireless users, except for the MSM317 which can handle traffic from both wireless and wired users. The SSID is the name of the wireless network with which the user associates.

Features

- **Wireless security filters:** Enables the AP to block traffic unless it is addressed to a specific destination, such as the controller. See *Wireless security filters on page 5-20*.
- **Wireless MAC filter:** Enables the AP to allow or deny access to the wireless network based on for specific wireless user MAC addresses.
- **Wireless IP filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific destination IP addresses.

Egress

- **Bridged onto port 1+2 (untagged):** Untagged user and authentication traffic is bridged onto ports 1 and 2.
- **Bridged onto port 1 (VLAN):** VLAN tagged traffic is bridged onto port 1 only. VLAN tags can be assigned on a per-user basis via RADIUS attributes (see *Defining account profiles on page 10-32*), or for all traffic on a VSC (see *Assigning egress VLANs to a group on page 6-30*).
- **Client data tunnel:** When this option is enabled, the AP creates a data tunnel to the controller to carry all user traffic. See *Client data tunnel on page 5-13*.

For a more detailed explanation on how wireless traffic is routed between an AP and controller, see *Traffic flow for wireless users on page 7-6*.

VSC on controller

Ingress

- **SSID (Client data tunnel):** When a client data tunnel has been created between the AP and the controller, all user traffic comes in on it. See *Client data tunnel on page 5-13*. The tunnel is established using same interface on which the AP was discovered. (LAN or Internet port).
- **SSID:** SSID is retrieved using the location-aware function.
- **VLAN (LAN or Internet port):** Traffic with a VLAN ID is handled by the VSC with a matching VLAN definition. See *Using multiple VSCs on page 5-36*.
- **Untagged (LAN port):** Untagged traffic on the LAN port may originate from wired users, or MSM APs operating in autonomous mode.

Features

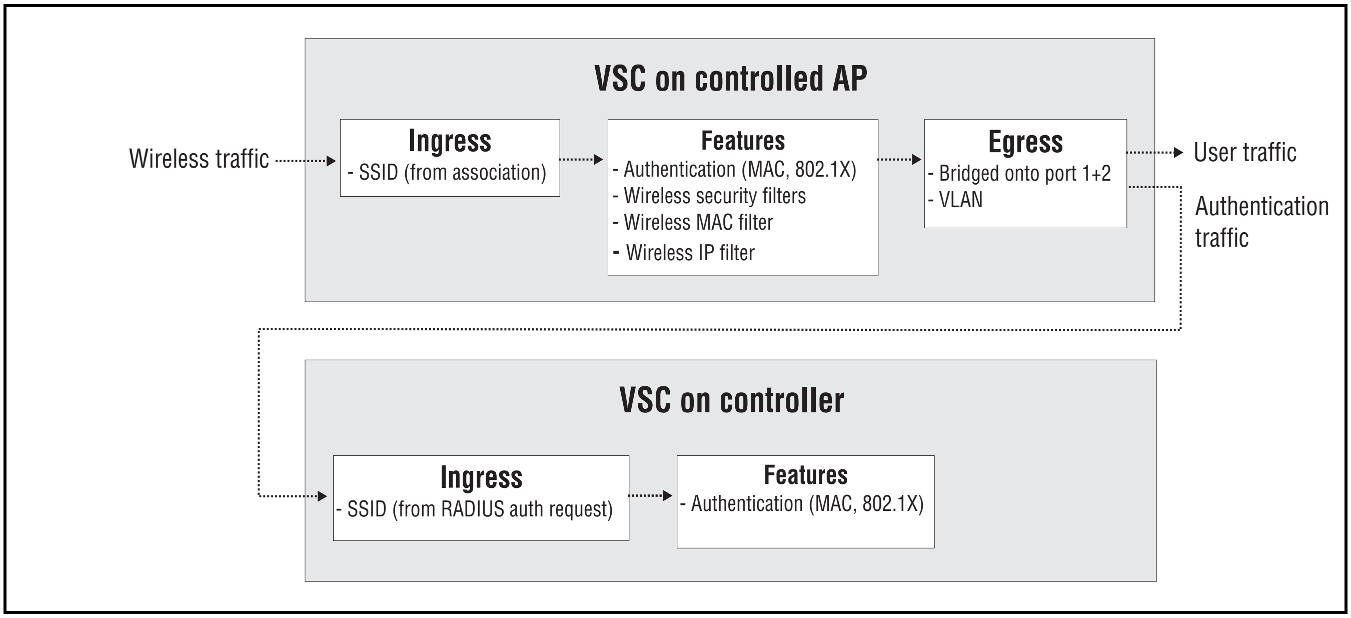
- **Authentication:** The controller supports 802.1X, MAC, or HTML authentication. To validate user login credentials the controller can use the local user accounts or make use of third-party authentication servers (Active Directory and/or RADIUS). See *Chapter 10: User authentication, accounts, and addressing*.
- **Access control features:** The controller provides a number of features that can be applied to user sessions. Features can be enabled globally or on a per-account basis. See *Account profiles on page 10-27*.

Egress

The controller enables user traffic to be forwarded to different output interfaces, which include the routing table, VLAN ID, or GRE tunnel. See *VSC egress mapping on page 5-17*.

Access control disabled

This diagram shows traffic flow when a non-access-controlled VSC is bound to an AP.



VSC on controlled AP

Ingress

The AP only handles traffic from wireless users, except for the MSM317 which can handle traffic from both wireless and wired users. The SSID is the name of the wireless network with which the user associates

Features

- **Authentication:** The AP supports 802.1X or MAC authentication. To validate user login credentials the AP makes use of a third-party authentication server (controller or third-party RADIUS server). See *Chapter 10: User authentication, accounts, and addressing*.

- **Wireless security filters:** Enables the AP to block traffic unless it is addressed to a specific destination (like the controller). See *Wireless security filters on page 5-20*.
- **Wireless MAC filter:** Enables the AP to allow or deny access to the wireless network based on specific wireless user MAC addresses.
- **Wireless IP filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific destination IP addresses.

Egress

- **Bridged onto port 1+2:** Unless a centralized mode tunnel has been established, user and authentication traffic is bridged onto ports 1 and 2.
- **VLAN:** VLAN tags can be assigned for all traffic on a VSC. See *Assigning egress VLANs to a group on page 6-30*.

VSC on controller

Ingress

- **SSID (from RADIUS auth request):** The controller determines the SSID from the RADIUS authentication request sent by the AP, and uses this SSID to determine the VSC to use for authentication.

Features

- **Authentication:** The controller supports 802.1X or MAC authentication. To validate user login credentials the controller can use the local user accounts or make use of third-party authentication servers (Active Directory and/or RADIUS). See *Chapter 10: User authentication, accounts, and addressing*.

Using multiple VSCs

When multiple VSCs are defined, it is important to know how user traffic is matched to a VSC definition. When VSCs have access control enabled, incoming traffic is handled on the controller as follows:

Incoming traffic properties	Port	If ...	Then ...
SSID and untagged	LAN	VSC with matching SSID exists.	Traffic is sent on the egress mapping defined on the matching VSC.
		No VSC with matching SSID exists.	Traffic is sent on the egress mapping defined on the default VSC.
SSID and VLAN or VLAN only	LAN or Internet	VSC with matching Ingress VLAN exists.	Traffic is sent on the egress mapping defined on the matching VSC.
		VLAN exists in VLAN table (but is not assigned to a VSC ingress.	Traffic is routed according to the global routing table.
		No VLAN exists.	Traffic is blocked.
Untagged	LAN		Traffic is sent on the egress mapping defined on the default VSC.

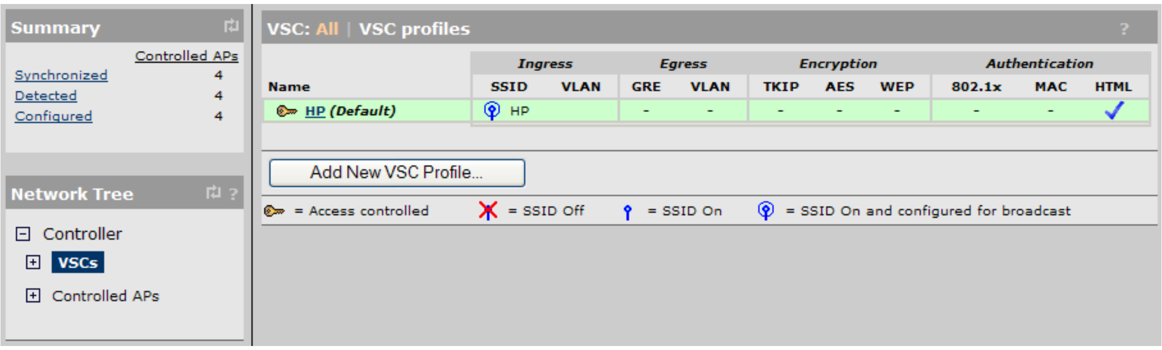
About the default VSC

The default VSC is automatically created by the controller. It is identified with the label ***(Default)*** in the VSC list. Initially, this VSC is named **HP** and has the following properties:

- Wireless network name: **HP**
- **Use Controller for Authentication** is enabled. (If you disable this option, the controller will not provide user authentication services for 802.1X, WPA, or WPA2.)
- **Use Controller for Access control** is enabled. (If you disable this option, you disable the public access interface and all users gain access to the protected network.)
- HTML-based authentication is enabled.

This means that when a user connects to the default VSC:

- Unauthenticated users cannot access the protected network, except for: procurve.com (for product registration) and windowsupdate.com (for IE, which tries to get to a windows update on a fresh start).
- Authenticated users *can access all* protected network resources.



Summary

	Controlled APs
Synchronized	4
Detected	4
Configured	4

Network Tree

⊟ Controller
⊞ VSCs
⊞ Controlled APs

VSC: All | VSC profiles

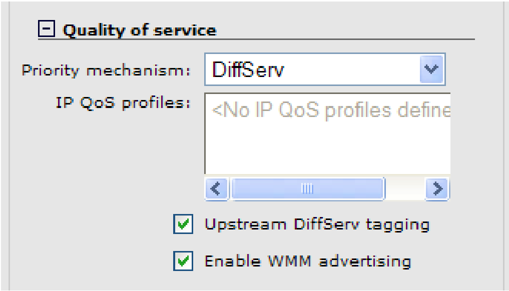
	Ingress		Egress		Encryption			Authentication		
Name	SSID	VLAN	GRE	VLAN	TKIP	AES	WEP	802.1x	MAC	HTML
HP (Default)	HP		-	-	-	-	-	-	-	✓

Traffic from wired users is always handled by the default VSC as follows:

- **When access control is disabled on the default VSC**, traffic from wired users connected to the controller LAN port is blocked.
- **When access control is enabled on the default VSC**, traffic from authenticated wired users connected to the controller LAN port is sent on the egress mapping defined on the default VSC. If HTML and 802.1X based authentication methods are disabled, traffic from all users is sent on the egress mapping without the need for authentication.

Quality of service (QoS)

The quality of service (QoS) feature (under Virtual AP) provides a number of different mechanisms to prioritize wireless traffic sent to wireless client stations. This is useful when the controller handles wireless traffic from multiple devices (or multiple applications on a single device), that have different data flow requirements.



⊟ **Quality of service**

Priority mechanism: DiffServ

IP QoS profiles: <No IP QoS profiles define

☑ Upstream DiffServ tagging

☑ Enable WMM advertising

The QoS feature defines four traffic queues based on the Wi-Fi Multimedia (WMM) access categories. In order of priority, these queues are:

Queue	WMM access category	Typically used for
1	AC_VO	Voice traffic
2	AC_VI	Video traffic
3	AC_BE	Best effort data traffic
4	AC_BK	Background data traffic

Outgoing wireless traffic on the VSC is assigned to a queue based on the selected priority mechanism. Traffic delivery is based on strict priority (per the WMM standard). Therefore, if excessive traffic is present on queues 1 or 2, it will reduce the flow of traffic on queue 3 and queue 4.

Regardless of the priority mechanism that is selected:

- Traffic that cannot be classified by a priority mechanism is assigned to queue 3.
- SVP (SpectraLink Voice Protocol) traffic is always assigned to queue 1, except if you select the VSC-based priority mechanism, in which case SVP traffic is assigned to the configured queue.

Priority mechanisms

Priority mechanisms are used to classify traffic on the VSC and assign it to the appropriate queue. The following mechanisms are available:

802.1p

This mechanism classifies traffic based on the value of the VLAN priority field present within the VLAN header.

Queue	802.1p (VLAN priority field value)
1	6, 7
2	4, 5
3	0, 3
4	1, 2

VSC-based priority

This mechanism is unique to HP. It enables you to assign a single priority level to all traffic on a VSC. If you enable the VSC-based priority mechanism, it takes precedence regardless of the priority mechanism supported by associated client stations. For example, if you set VSC-based low priority, then all devices that connect to the VSC have their traffic set at this priority, including SVP clients.

Queue	VSC-based priority value
1	VSC-based Very High
2	VSC-based High
3	VSC-based Normal
4	VSC-based Low

DiffServ (Differentiated Services)

This mechanism classifies traffic based on the value of the Differentiated Services (DS) codepoint field in IPv4 and IPv6 packet headers (as defined in RFC2474). The codepoint is composed of the six most significant bits of the DS field.

Queue	DiffServ (DS codepoint value)
1	111000 (Network control) 110000 (Internetwork control)
2	101000 (Critical) 100000 (Flash override)
3	011000 (Flash) 000100 (Routine)
4	010000 (Immediate) 001000 (Priority)

TOS

This mechanism classifies traffic based on value of the TOS (Type of Service) field in an IP packet header.

Queue	TOS (Type of Service field value)
1	0x30, 0xE0, 0x88, 0xB8
2	0x28, 0xA0
3	0x08, 0x20
4	All other TOS traffic

IP QoS

This option lets you assign traffic to the queues based on the criteria in one or more IP QoS profiles. Each profile lets you target traffic on specific ports or using specific protocols.

Disabled

When QoS traffic prioritization is disabled, all traffic is sent to queue 3.

IP QoS profiles

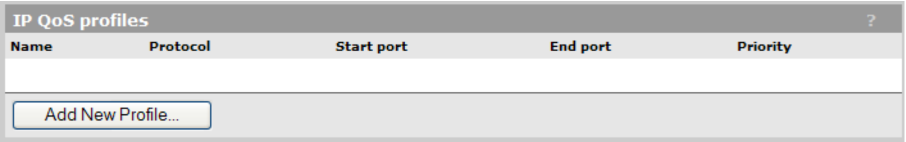
This option is only available if you set the **Priority mechanism** to **IP QoS**.

Select the IP QoS profiles to use for this profile. To add QoS profiles to the list, use the **Network > IP QoS** page.

Up to 10 profiles can be selected. To select more than one profile, hold down the CTRL key as you select profile names in the list.

To define an IP QoS profile

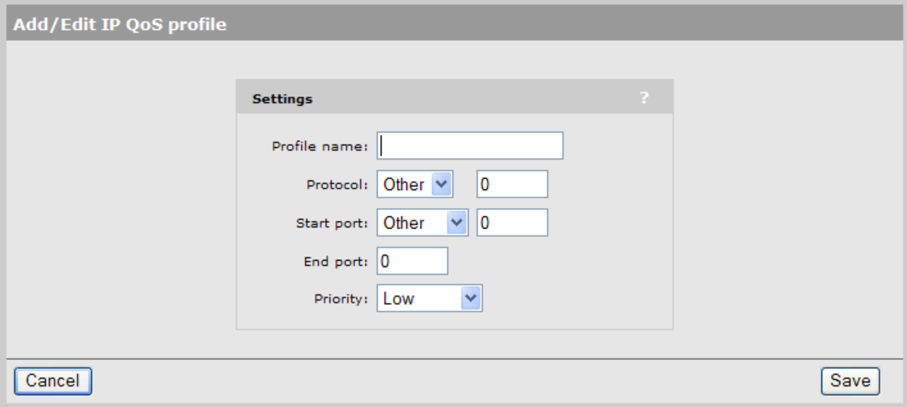
1. Select **Controller >> Network > IP QoS**. Initially, no profiles are defined.



IP QoS profiles

Name	Protocol	Start port	End port	Priority

2. Select **Add New Profile**.



Add/Edit IP QoS profile

Settings

Profile name:

Protocol: Other 0

Start port: Other 0

End port: 0

Priority: Low

3. Configure settings as follows:

Settings

Profile name
Specify a unique name to identify the profile.

Protocol
Specify an IP protocol to use to classify traffic by specifying its Internet Assigned Numbers Authority (IANA) protocol number. Protocol numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually. You can find IANA-assigned protocol numbers on the Internet.

Start port/ End port
Optionally specify the first and last port numbers in the range of ports to which this IP QoS profile applies. To specify a single port, specify the same port number for both **Start port** and **End port.** Port numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually.

Note To accept traffic on all ports for a specified protocol, set **Start port** to **Other** and **0**.

Priority
Select the priority level that will be assigned to traffic that meets the criteria specified in this IP QoS profile.

Note It is strongly recommended that you reserve **Very high** priority for voice applications.

Upstream DiffServ tagging

Enable this option to have the AP apply differentiated services marking to upstream traffic.

Layer 3 upstream marking ensures end-to-end quality of service in your network. Data originating on the wireless network can now be carried throughout the network (wireless *and* wired) with a consistent quality of service and priority. This feature is enabled by default.

When this feature is enabled, packets received on the wireless interface that include Wi-Fi Multimedia (WMM) QoS values are remarked using IP TOS/DiffServ values when transmitted to the wired network.

Upstream/downstream traffic marking

Depending on the priority mechanism that is active, upstream and downstream traffic is marked as described in this section.

Upstream traffic marking

This table describes the marking applied to wireless traffic sent by connected client stations to an AP and then forwarded onto the wired network by the AP.

		OUTGOING TRAFFIC Traffic sent by the AP to the network		
			L3 marking	
Mechanism	**INCOMING TRAFFIC** Wireless traffic sent from client stations to the AP	**L2 marking**	**Upstream DiffServ tagging is enabled**	**Upstream DiffServ tagging is disabled**
802.1p	WMM	802.1p (Requires an egress VLAN to be defined for the VSC.)	DiffServ	Pass-through (Original layer 3 marking, if any, is preserved.)
DiffServ	DiffServ	None		
TOS	TOS	None		
VSC-based	WMM Non-WMM	If an egress VLAN is defined for the VSC, then 802.1p and IP DSCP are set to reflect the VSC-based priority setting. If no egress VLAN is defined for the VSC, then the 802.1p header is not added, and only IP DSCP is set to reflect the VSC-based priority setting.		
IP QoS	WMM	None		

Downstream traffic marking

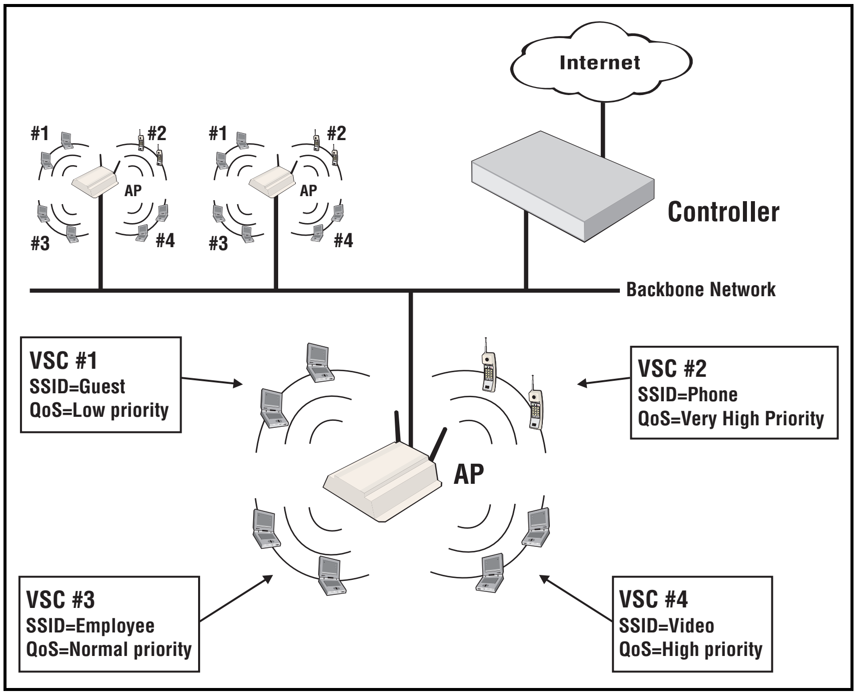
This table describes the marking applied to traffic received from the wired network by an AP and then sent to connected wireless client stations.

Mechanism	**INCOMING TRAFFIC** Traffic received from wired network	**OUTGOING TRAFFIC** Wireless traffic sent from the controller to client stations	
		WMM Client	**Non-WMM Client**
802.1p	802.1p	WMM + HPQ (WMM marking done according to the rules for the mechanism.)	HPQ (hardware priority queueing)
DiffServ	DiffServ		
TOS	TOS		
VSC-based	All traffic on the VSC.		
IP QoS	All traffic that matches the ports/protocols specified in the selected IP QoS profiles.		

Note Although the WMM specification refers to 802.1D and not 802.1p, this guide uses the term 802.1p because it is more widely recognized. (The updated IEEE 802.1D: ISO/IEC 15802-3 (MAC Bridges) standard covers all parts of the Traffic Class Expediting and Dynamic Multicast Filtering described in the IEEE 802.1p standard.)

QoS example

In this example, a single controller provides voice and data wireless support with different quality of service settings for guests and employees.



Creating a new VSC

To add a VSC, select **Controller > VSCs >>VSC Profiles > Add New VSC Profile**.

Define VSC parameters and select **Save**. Familiarize yourself with sections of interest in *VSC configuration options on page 5-5*. See the online help for parameter descriptions.

Assigning a VSC to a group

When working with controlled APs, VSC definitions must be bound to a group so that they will automatically be activated on the APs in the group. For information on how to bind (assign) a VSC to a group, see *Binding a VSC to a group on page 6-26*.

On the MSM317, VSCs can also be bound to a switch port. See the *MSM317 Access Device Installation and Getting Started Guide*.

Note

When working with autonomous APs, the VSC definition you create on the controller must be manually configured on each autonomous AP. See *Working with autonomous APs on page 19-1* and the *MSM3xx/MSM4xx Management and Configuration Guide*.

6

Working with controlled APs

Contents

Key concepts

The controller provides centralized management of APs operating in controlled mode. Controlled mode greatly simplifies the set up and maintenance of a Wi-Fi infrastructure by centralizing the configuration and management of distributed APs.

Note Starting with software version 5.x, APs operate in controlled mode by default. If you update an AP from an earlier release, the AP boots in autonomous mode. Subsequently resetting the AP to factory defaults switches it to controlled mode. For details on working with autonomous APs, see *Working with autonomous APs on page 19-1*, and *Resetting to factory defaults on page C-1*.

Plug and play installation

In most cases, initial configuration of an AP is not required. Simply power it up and plug it into a network that provides access to a controller. The AP will automatically discover and authenticate itself with the controller. The AP does not offer wireless services until it successfully connects and synchronizes with a controller. Layer 3 networks may require the APs first to be provisioned.

Automatic software updates

Once an AP establishes a management tunnel with a controller its software is automatically updated to match the version installed on the controller.

Centralized configuration management

All AP configuration settings are defined using the controller management tool and are automatically uploaded to all controlled APs with a single mouse select. For added flexibility, APs can be assigned to groups, enabling each group to have customized configuration settings. If needed, the individual settings for each AP in a group can also be customized.

Manual provisioning

By default, APs operating in controlled mode will automatically discover and connect with a controller on most network topologies. However, in certain cases it may be necessary to manually configure (provision) connectivity and discovery options. Manual provisioning can be done directly on the AP, or via the controller. When using the controller, provisioning can be applied to entire groups making it easy to customize many APs at once. When working with a controller team, APs must be provisioned to discover each team member to ensure that failover is supported. The APs must be able to migrate to a new team member if the current team member with which they are associated becomes unavailable.

Secure management tunnel

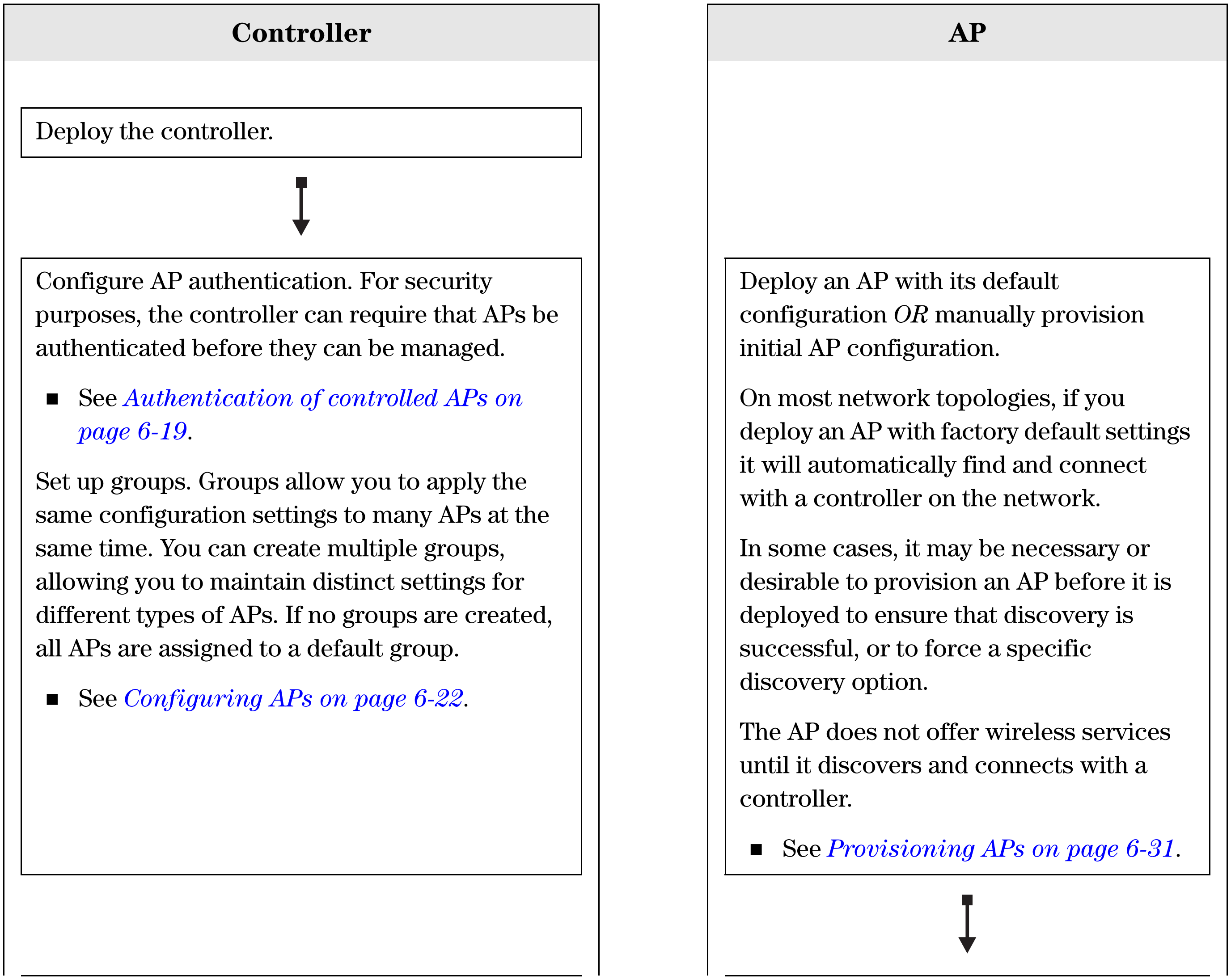
Once authenticated, a secure management tunnel is established between the AP and the controller to support the exchange of management traffic between the two devices.

AP authentication

The controller can be configured to authenticate APs by their MAC address before they are managed. The authentication can be defined locally on the controller, via a third-party RADIUS server, or using a remote text-based control file.

Key controlled-mode events

The following diagram provides an overview of key events that occur when working with APs in controlled mode.



Controller

Deploy the controller.

Configure AP authentication. For security purposes, the controller can require that APs be authenticated before they can be managed.

- See *Authentication of controlled APs on page 6-19*.

Set up groups. Groups allow you to apply the same configuration settings to many APs at the same time. You can create multiple groups, allowing you to maintain distinct settings for different types of APs. If no groups are created, all APs are assigned to a default group.

- See *Configuring APs on page 6-22*.

AP

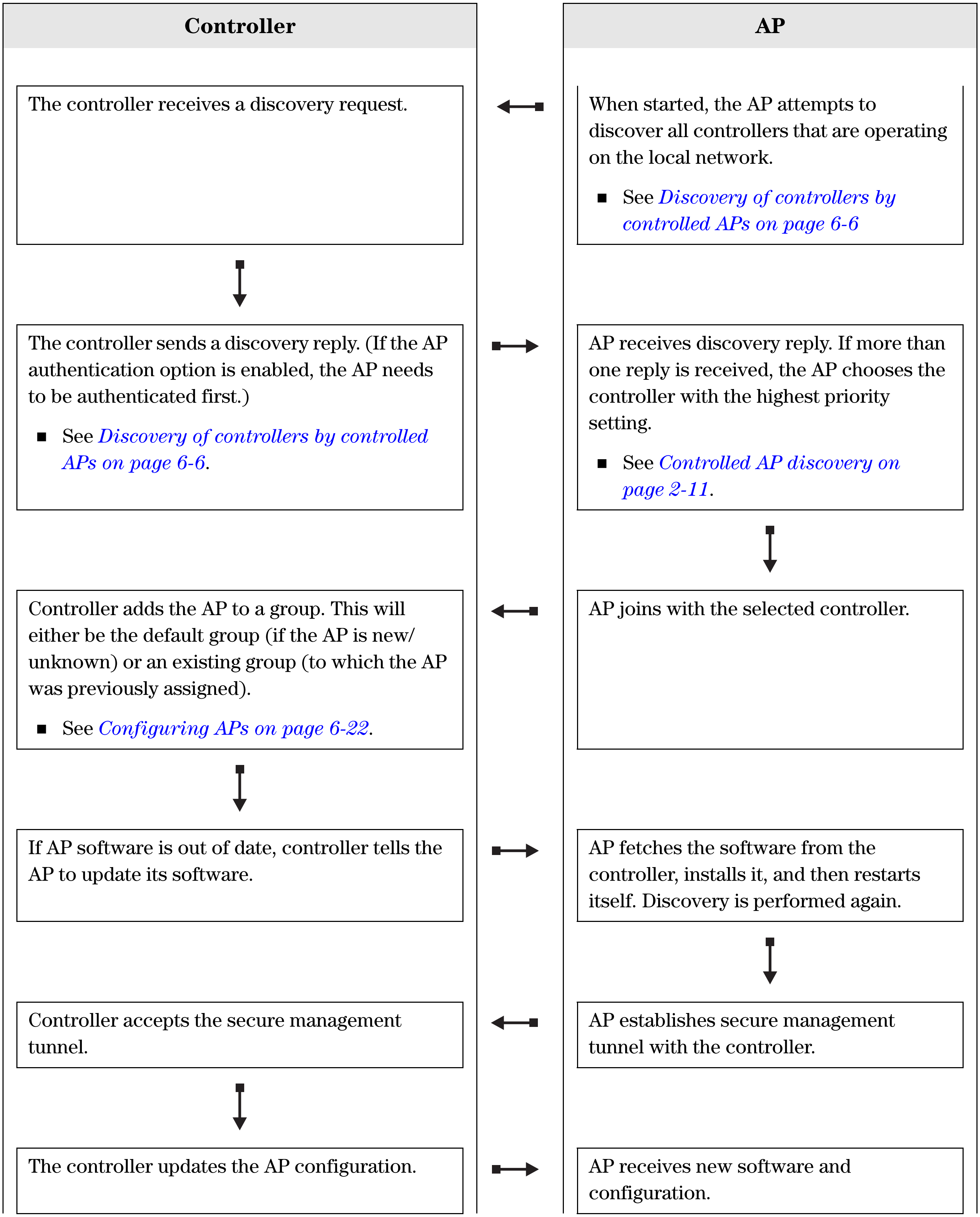
Deploy an AP with its default configuration *OR* manually provision initial AP configuration.

On most network topologies, if you deploy an AP with factory default settings it will automatically find and connect with a controller on the network.

In some cases, it may be necessary or desirable to provision an AP before it is deployed to ensure that discovery is successful, or to force a specific discovery option.

The AP does not offer wireless services until it discovers and connects with a controller.

- See *Provisioning APs on page 6-31*.



Controller

AP

When started, the AP attempts to discover all controllers that are operating on the local network.

- See *Discovery of controllers by controlled APs on page 6-6*

The controller receives a discovery request.

The controller sends a discovery reply. (If the AP authentication option is enabled, the AP needs to be authenticated first.)

- See *Discovery of controllers by controlled APs on page 6-6*.

AP receives discovery reply. If more than one reply is received, the AP chooses the controller with the highest priority setting.

- See *Controlled AP discovery on page 2-11*.

AP joins with the selected controller.

Controller adds the AP to a group. This will either be the default group (if the AP is new/ unknown) or an existing group (to which the AP was previously assigned).

- See *Configuring APs on page 6-22*.

If AP software is out of date, controller tells the AP to update its software.

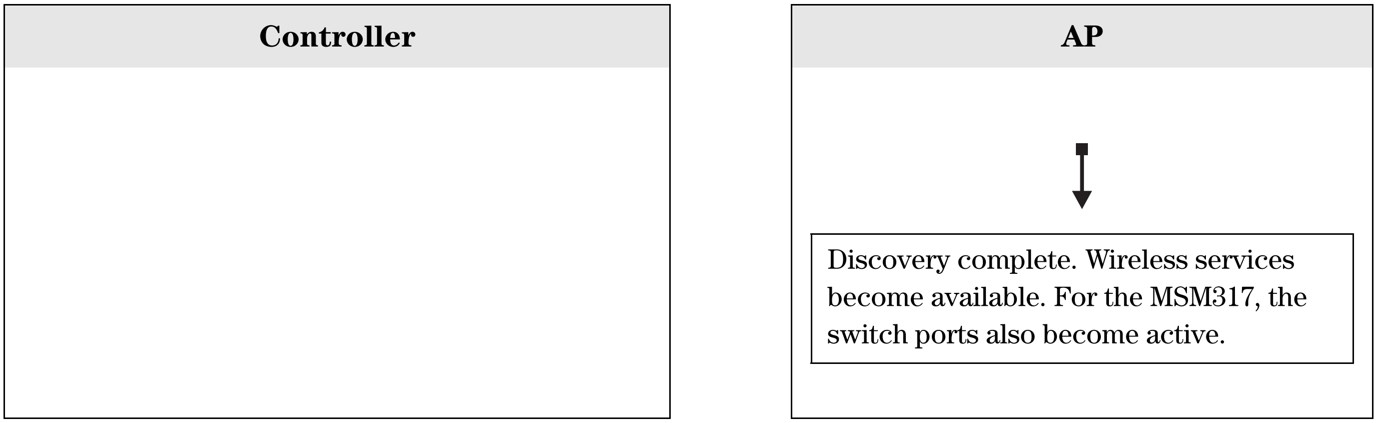
AP fetches the software from the controller, installs it, and then restarts itself. Discovery is performed again.

AP establishes secure management tunnel with the controller.

Controller accepts the secure management tunnel.

The controller updates the AP configuration.

AP receives new software and configuration.



Discovery complete. Wireless services become available. For the MSM317, the switch ports also become active.

Discovery of controllers by controlled APs

This section describes how the discovery process works and how it can be customized.

Discovery is the process by which a controlled AP finds a controller (or controller team) on a network and establishes a secure management tunnel with it. To see how the discovery process fits into overall controlled mode operations, see *Key controlled-mode events on page 6-4*.

In most cases, the factory default configuration of an AP will result in automatic discovery of a controller with no configuration required. However, for some network topologies it may be necessary to configure the discovery process as described in this section.

See *Discovery recommendations on page 6-10* for examples of topologies that can use automatic discovery and those that require discovery to be configured.

Note

- If you intend to manage controlled APs via local mesh, see *Local mesh on page 13-1*.
- Provisioning can limit the discovery of potential controllers. See *Provisioning APs on page 6-31*.

Discovery overview

Although the specifics of the discovery process vary depending on whether an AP is *unprovisioned* (in its factory default state) or *provisioned* (had its connectivity or discovery settings changed from their factory default settings), the discovery process can be summarized as follows:

1. The AP uses various methods to locate one or more controllers that are reachable on the network. The preferred way to monitor AP discovery is via the controller management tool (see *Monitoring the discovery process on page 6-13*). When in visual range of the APs, you can watch the status lights for an indication of discovery progress. See the status light information in the AP Quickstart (provided and available online).

2. Discovered controllers send a discovery reply to the AP. If the controller is configured to require AP authentication, the reply is only sent after the AP is authenticated by the controller.
3. The controller adds the AP to a group. This will either be the default group (if the AP is new/unknown) or an existing group (to which the AP was previously assigned).
4. The AP is now managed by the controller, and it can be configured and monitored using the controller management tool.

Note

- APs must be connected to the network via Port 1 (or the Uplink port on an MSM317) for discovery to work.
- Unprovisioned APs must obtain an IP address from a DHCP server before discovery can be initiated. When discovery occurs on a VLAN, the DHCP server must be active on the VLAN.

Discovery is performed whenever an AP:

- Is restarted (or reset to factory defaults)
- Loses connectivity with its controller
- Is removed and rediscovered using an action on the **Controlled APs >> Overview > Discovered APs** page.

Discovery methods

Four discovery methods are available. The following table summaries their features and recommended applications.

Method	Description	Supported by	Suggested use
UDP broadcast	AP issues UDP broadcasts to discover controllers on the same subnet.	Unprovisioned APs	Both the controller and AP reside on the same subnet.
DHCP	AP obtains controller address from a specially configured DHCP server.	Unprovisioned APs	The AP is on a different subnet than the controller.
DNS	AP obtains controller address from a DNS server using predefined host names.	Unprovisioned APs Provisioned APs	The AP is on a different subnet than the controller.
Specific IP addresses	AP connects to a specific controller using a pre-configured static IP address.	Provisioned APs	DHCP and DNS are not used and the AP is on a different subnet than the controller.

Note A controller listens for discovery requests on its LAN port and/or Internet port as configured on the **Controller >> Management > Device Discovery** page. (See *Device discovery on page 2-9*).

UDP broadcast discovery

The AP sends a UDP broadcast to discover all controllers that are on the same subnet as the AP.

DHCP discovery

When configured as DHCP client (which is the factory default setting for all APs), an AP can obtain the IP addresses of controllers on the network from any DHCP server configured to support the Colubris Vendor Class (DHCP option 43).

Vendor Class enables an administrator to define a list of up to five available controllers on the network to which APs can connect.

- If the controller is configured to operate as the DHCP server for the network, you can define the list of available controllers by selecting **Controller >> Network > Address allocation > DHCP server** and then configure the **Controller discovery** option. See *Controller discovery on page 3-16*.
- If an external DHCP server is used, it must have **Option 43** configured. For examples on how to configure some popular third-party DHCP servers, see *Appendix E: DHCP servers and Colubris vendor classes*.

DNS discovery

DNS discovery is attempted using UDP unicast discovery requests which are issued by the AP to the following default controller names:

- cnsrv1
- cnsrv2
- cnsrv3
- cnsrv4
- cnsrv5

This method enables discovery across various network configurations. It requires that at least one controller name is resolvable via a DNS server.

The AP appends the default domain name returned by a DHCP server (when it assigns an IP address to the AP) to the controller name. For example, if the DHCP server returns **mydomain.com**, then the AP will search for the following controllers in this order:

- cnsrv1.mydomain.com
- cnsrv2.mydomain.com
- cnsrv3.mydomain.com
- cnsrv4.mydomain.com
- cnsrv5.mydomain.com

Discovery using specific IP addresses

Provisioned APs can be configured to connect with a controller at a specific IP address. A list of addresses can be defined, allowing the AP to search for multiple controllers.

This can also be used to strengthen the security on a local network to make sure that the AP goes to a specific controller for management.

Discovery order

Discovery occurs differently for unprovisioned and provisioned APs.

Unprovisioned APs

Once an unprovisioned AP has received its IP address from a DHCP server, it attempts to discover a controller using the following methods, in order:

- UDP broadcast
- DHCP
- DNS

These discovery methods are applied on the following interfaces, in order:

- Last interface on which a controller was discovered. (Only applies to APs that have previously discovered a controller)
- Untagged on the Port 1
- All other detected VLANs (in sequence) on Port 1

Provisioned APs

If discovery settings are provisioned on the AP, then the AP uses only the provisioned settings (see *Provisioning discovery on page 6-37*). The following discovery settings are available on provisioned APs:

- DNS discovery: Enables custom controller names and domains to be used for discovery.
- Discovery using specific IP addresses: Enables the AP to find controllers operating at specific IP addresses.

Discovery recommendations

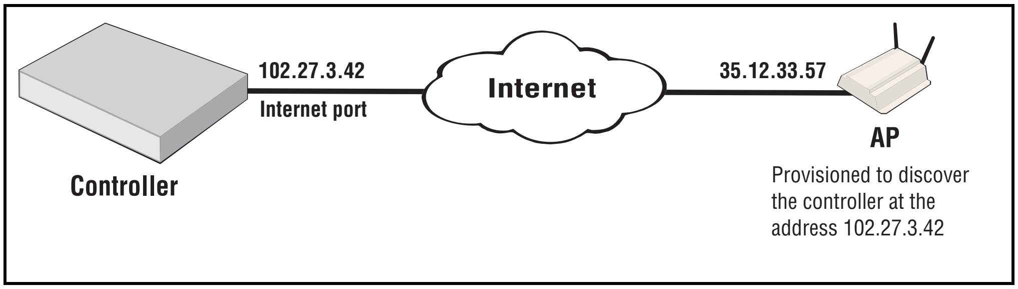
Note When controller teaming is active, controlled APs discover a team in the same way that they discover non-teaming controllers.

- **If the AP is on the same subnet as the controller**, then UDP discovery will work with no configuration required on either the AP or controller. This applies whether the controller is operating as the DHCP server for the network or if a third-party DHCP server is used.

  If VLANs are being used, then UDP discovery will also work with no configuration. However, to speed up the discovery process you can provision the AP with a specific VLAN ID. This will eliminate the need for the AP to find and attempt discovery on all available VLANs.

- **If the AP is on a different subnet than the controller,** UDP discovery will not work. Instead, DHCP or DNS discovery must be used, or direct IP address discovery must be provisioned.

  - **DHCP discovery:** If you have control of the DHCP server, enable support for the Colubris Vendor Class as explained in *DHCP discovery on page 6-8*.
  - **DNS discovery:** If you have control of the DNS server, you can configure it to resolve the default controller names that an AP will search for. To use custom names, you must provision discovery settings on the AP. For more information on using custom names, see *Provisioning discovery on page 6-37*.
  - **Specific IP discovery:** This method needs to be used when you do not have control over the DHCP and DNS servers and no domain is registered to the controller. For example, if the connection to the controller is routed over the public Internet.

    
    102.27.3.42
Internet port
Internet
35.12.33.57
Controller
AP
Provisioned to discover the controller at the address 102.27.3.42

    For discovery to succeed, the AP must be provisioned with the controller IP address. See *Provisioning discovery on page 6-37*.

- **When working with a controller team,** APs should be provisioned to discover all controllers that make up the team, not just the team manager. This is required for proper fail-over operation.

Discovery priority

Each controller or controller team that receives a discovery request sends the requesting AP a discovery reply. If the AP authentication option is enabled, the AP needs to be authenticated first. Requests from unauthenticated APs are ignored.

If an AP receives discovery replies from multiple controllers, the AP selects the controller that has the highest discovery priority setting. If that controller is already managing the maximum number of controlled APs, the AP will choose the controller with the next highest priority.

Non-teamed controllers are always higher priority than controller teams. Therefore, if your network contains both controller teams and non-teamed controllers, APs first attempt to establish a secure management tunnel with discovered non-teamed controllers in order of their discovery priority. Only if all non-teamed controllers are already managing the maximum number of controlled APs will the AP then consider controller teams in the order of their priority.

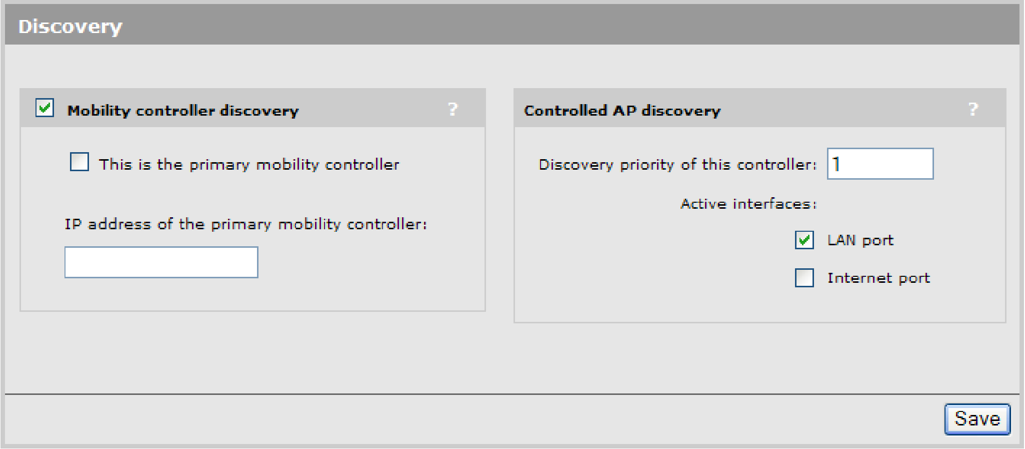
The following table shows how discovery would occur for several teamed and non-teamed controllers.

Controller or Team	Configured discovery priority setting	Actual order of discovery by APs
Controller 1	1	1
Controller 2	2	2
Controller 3	3	3
Team 1	1	4
Team 2	2	5
Team 3	3	6

If two controllers have the same priority setting, the AP will appear on the **Overview > Discovered APs** page of both controllers with a **Diagnostic** value of **Priority Conflict** (See *Viewing all discovered APs on page 6-14*). To resolve the conflict, change the priority setting of one of the controllers on its Discovery page.

Discovery priority is set on a controller using the **Discovery priority of this controller** option on the **Controller >> Management > Device Discovery** page.

On a non-teamed controller



Discovery

☑ Mobility controller discovery

□ This is the primary mobility controller

IP address of the primary mobility controller:

Controlled AP discovery

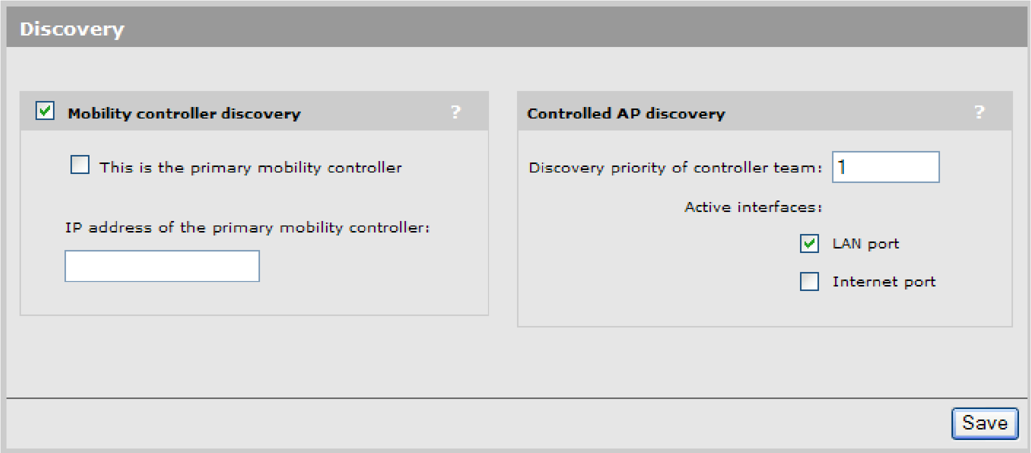
Discovery priority of this controller: 1

Active interfaces:

☑ LAN port

□ Internet port

On a controller team



Discovery

☑ Mobility controller discovery

□ This is the primary mobility controller

IP address of the primary mobility controller:

Controlled AP discovery

Discovery priority of controller team: 1

Active interfaces:

☑ LAN port

□ Internet port

If only connectivity settings are provisioned, then the AP attempts to discover a controller using the same methods as for unprovisioned APs, namely:

- UDP broadcast
- DHCP (the AP must be configured as a DHCP client for this to work)
- DNS

Tip For more information on provisioning APs, see *Provisioning APs on page 6-31*.

Discovery considerations

If controlled APs are behind a firewall or NAT device, refer to the following sections.

Firewall

If the network path between an AP and a controller traverses a firewall the following ports must be opened for management and discovery to work:

Protocol	Open these ports	Ports are used by
UDP	Source and destination = 38212 (9544 hex)	Discovery protocol the AP uses to find a controller.
UDP	Destination = 1194 (4AA hex)	Management tunnel that is established between an AP and a controller.
TCP	Source and destination = 1194 (4AA hex)	Software updates and certificate exchanges (for the management tunnel).
UDP	Source and destination = 3001 (BB9 hex)	Client data tunnel.

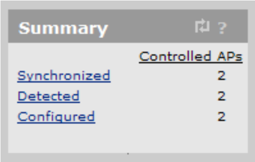
UDP	Source = 39064 (9898 hex)
	Destination = 1800 (708 hex), 1812 (714 hex), 1813 (715 hex), 30840 (7878 hex)
		Location aware. This is only necessary if autonomous APs are using the access-controlled (public access) interface.

NAT

If the network path between an AP and a controller implements NAT (network address translation), discovery will only work if NAT functions on outbound traffic sent from the AP to the controller. If NAT operates in the other direction, discovery will fail.

Monitoring the discovery process

This Summary menu lists the number of controlled APs discovered by the controller. APs are grouped according to their management state. For example: **Synchronized**, **Detected**, **Configured**, **Pending**.



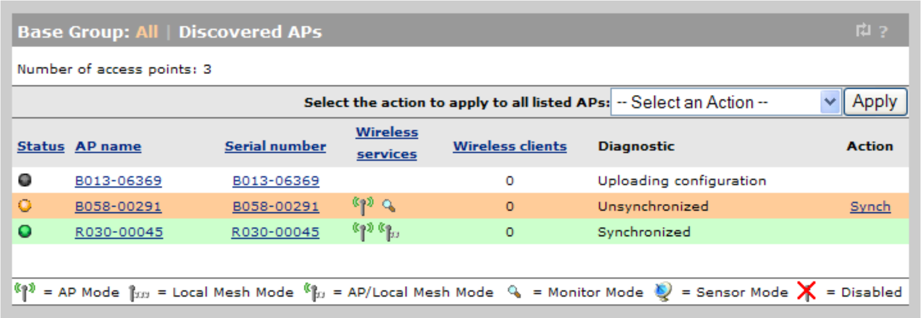
Summary

	Controlled APs
Synchronized	2
Detected	2
Configured	2

An AP may be active in more than one state at the same time. For example, an AP may be both **Detected** and **Synchronized**. Select the state name to display information about all APs in that state.

Viewing all discovered APs

To display information about APs discovered by the controller, select **Controlled APs >> Overview > Discovered APs**.



Base Group: All | Discovered APs

Number of access points: 3

Select the action to apply to all listed APs: -- Select an Action -- Apply

Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
●	B013-06369	B013-06369		0	Uploading configuration	
●	B058-00291	B058-00291		0	Unsynchronized	Synch
●	R030-00045	R030-00045		0	Synchronized	

= AP Mode = Local Mesh Mode = AP/Local Mesh Mode = Monitor Mode = Sensor Mode ✗ = Disabled

The **Discovered APs** page provides the following information:

- **Number of access points**: Indicates the number of APs that were discovered.
- **Select the action to apply to all listed APs**: Lets you apply the selected action to all APs in the list. Select an action and then **Apply**.
- **Status:**
  - Green: The AP is synchronized, meaning that the AP is connected, running, and has received its configuration from the controller.
  - Orange: The AP is unsynchronized, meaning that the AP is operational but does not have the same configuration as the controller, yet.
  - Red: The AP is not part of the controlled network and is not providing wireless services. See the **Diagnostic** column for details.
  - Grey blinking: An action is pending.
  - Grey: The AP is configured in a group, but has not been discovered on the network.
- **AP name**: Name assigned to the AP.
- **Serial number**: Unique serial number assigned to the AP at the factory. Cannot be changed.
- **Wireless services**: Indicates the status of wireless services on the AP. A separate icon appears for each radio on the AP. See the legend under the table for the meaning of each icon.
- **Wireless clients**: Indicates the number of wireless clients currently associated with the AP. Select the number to see more information.

- **Diagnostic**: Indicates the status of the AP with regards to management by the controller, as shown in the following table.

Diagnostic	Description
Detected	The AP was detected by the controller.
Enabling VSC services	The AP is enabling wireless services for all VSCs.
Establishing tunnel	A secure management connection is being established to the AP.
Firmware failure	New firmware failed to upload to the AP. The controller will retry soon.
Incompatible settings	Local mesh has been provisioned on the AP but: ■ The APs radio is disabled. ■ The AP radio operating mode does not support local mesh. ■ The APs radio wireless mode does not match the one provisioned. ■ The mesh ID is not uniquely assigned.
Installing firmware	New firmware has been successfully uploaded to the AP. Wait until the AP restarts to activate the new firmware.
Not authorized	The AP could not be authenticated by the controller. This may be due to invalid authentication credentials supplied by the AP. (Authentication settings used by the controller are defined on the **Controller >> Security > Controlled APs** page.) You should accept the AP unless it is an actual rogue.
Not responding	The AP has stopped sending management information to the controller. Rediscovery may re-establish the connection. If not the AP may have lost power or a network failure has occurred.
Priority conflict	More than one controller responded to the AP discovery request with the same priority. The AP is therefore unable to select a controller to function as its controller. The AP will retry its discovery request shortly. You must fix the priority conflict by changing the priority setting for one of the controllers (**Controller >> Management > Device discovery**).
Waiting for manager	When teaming is active, a newly discovered AP will temporarily be in this state while it waits for the team manager to add it to the network tree.

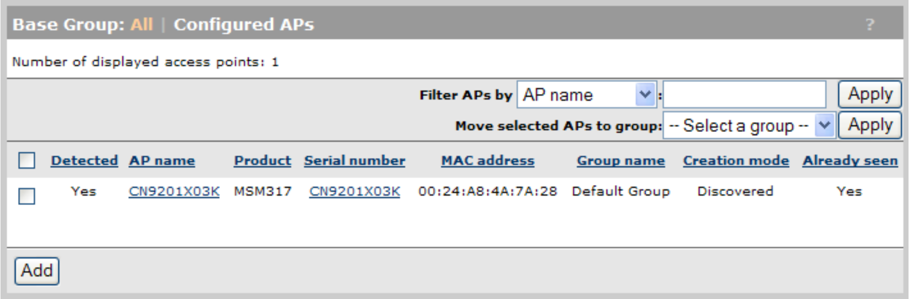
Diagnostic	Description
Rebooting	The AP is restarting.
Resetting configuration	The AP configuration is being reset to factory defaults. This is normal and will occur when the firmware version on the controller is changed or if the AP is not synchronized.
Restoring configuration	The AP is currently restoring its previous configuration settings.
Suspicious device	The AP unexpectedly requested new authentication certificates from the controller. Possible causes are as follows: ■ A previously synchronized AP was reset to factory defaults. ■ An unauthorized AP may be using the same MAC address. This is a possible security breach that should be investigated before authorizing the AP again.
Synchronized	The AP is up and running, offers wireless services, and had its firmware and configuration settings successfully updated by the controller.
Synchronized/License violation	Although the AP is synchronized it is non-functional (quarantined) due to a license violation. You must change the configuration to omit the affected licensed feature or acquire and install a valid license.
Unconfigurable	This AP cannot be added because the maximum number of configured APs has been reached. To add this AP you must first remove one or more currently configured APs.
Unsupported product	No suitable firmware is available for this AP on the controller. You should upgrade the controller firmware so that the newly-introduced product can be recognized.
Unsynchronized	The AP is up and running and offers wireless services. However, its configuration settings do not match the settings defined on the controller (at the group or AP level). You should Synchronize the AP.

Diagnostic	Description
Unsynchronized/License violation	The AP is not synchronized but can continue operation. However, if synchronized, it will become non-functional as described above for Synchronized/License violation. Before synchronizing, either change the configuration to omit the affected licensed feature or acquire and install a valid license.
Uploading configuration	Configuration settings are currently being sent to the AP.
Uploading firmware	The controller is uploading new firmware to the AP. Wait until the operation completes.
Validating configuration	The controller is waiting for the AP to send its configuration.
Validating firmware	The controller is waiting for the AP to send its firmware version number.
Waiting for acceptance	The AP has been authorized by the controller. However, the AP has not yet selected the controller to function as its controller. (If multiple controllers replied to the APs discovery request, the AP may choose to connect with another controller.)
Wrong product	The AP was created with a product type that does not match the detected product type. This can occur when an AP is manually added to a group with the wrong product type. You should verify and fix the product type.
Validating capabilities	The capabilities of the AP are being identified by the controller.

- **Action**: Indicates the recommended administrative action to be taken to resolve a diagnostic condition.

Viewing all configured APs

To display information about APs configured by the controller, select **Controlled APs >> Overview > Configured APs**.



Base Group: All | Configured APs ?

Number of displayed access points: 1

Filter APs by AP name : Apply

Move selected APs to group: -- Select a group -- Apply

□	Detected	AP name	Product	Serial number	MAC address	Group name	Creation mode	Already seen
□	Yes	CN9201X03K	MSM317	CN9201X03K	00:24:A8:4A:7A:28	Default Group	Discovered	Yes

Add

The **Configured APs** page provides the following information:

- **Number of displayed access points**: Number of configured APs that were discovered.
- **Filter APs by:** To narrow down the list of APs in the table, select a category and enter text on which to filter the AP list. Select **Apply** to activate the filter. To deactivate the filter, clear the filter text and then select **Apply**.
- **Move selected APs to group:** Select a group from the list and select apply to move all selected APs in the table to that group.

Table

Select the title of a column to sort the entries according to the values in the column.

- **Check boxes:** Use the check box to select an AP to move it to another group. Select the check box in the title bar to select all APs on this page.
- **Detected**:
  - **Yes:** The AP has been discovered and is listed on the AP overview page, where more information is provided on the AP.
  - **No:** The AP has not been discovered.
- **AP name**: Name assigned to the AP. Select the name to open its AP management page.
- **Serial number**: Serial number assigned to the AP. Select the serial number to open its AP management page.
- **Group Name**: Group that the AP is part of.
- **Product**: Product name of the MSM AP.

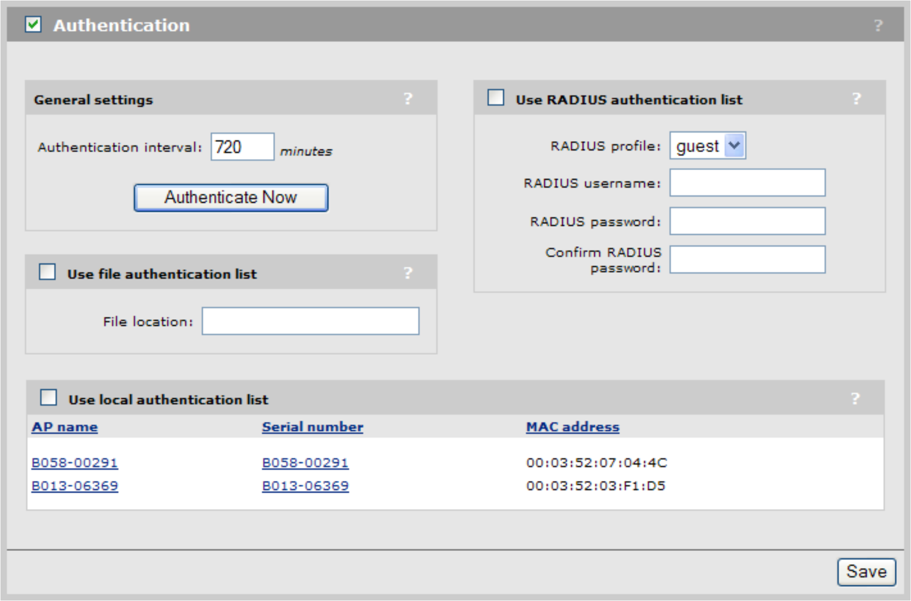
- **Creation mode**:
  - **Local**: AP was added manually, or was manually authenticated after being discovered.
  - **RADIUS**: AP was successfully authenticated via RADIUS and then created.
  - **External file**: AP was successfully authenticated using the external file option.
  - **Discovered**: Automatically detected by the controller based on discovery-time parameter exchange.
- **Already Seen**: The AP established a management tunnel to the controller at least once in the past.

Authentication of controlled APs

For security purposes, the controller can require that APs be authenticated before they are managed. Authentication is enabled by selecting **Controller >> Controlled APs > Authentication.**

Note

The AP authentication option is disabled by default, meaning that all discovered APs are authorized (no authentication is required).



☑ Authentication

General settings

Authentication interval: 720 *minutes*

□ Use RADIUS authentication list

RADIUS profile: guest

RADIUS username:

RADIUS password:

Confirm RADIUS password:

□ Use file authentication list

File location:

□ Use local authentication list

AP name	Serial number	MAC address
B058-00291	B058-00291	00:03:52:07:04:4C
B013-06369	B013-06369	00:03:52:03:F1:D5

The controller authenticates APs using their MAC addresses. When an AP sends a discovery request to the controller, it includes its Ethernet Base MAC address. The controller validates this address against its AP address authentication list. If the address appears in the list, the AP is authenticated and gains access to the controller's service control features.

If authentication fails (for example, this is a new AP), and the **Use the local authentication list** option is enabled, then the AP is added to the **Default Group** and flagged as requiring authentication. The AP must then be manually authenticated by a manager using the **Controlled APs >> Overview > Discovered APs** page. Once authenticated, the AP can be managed.

Note APs remain visible in this list as long as they have been detected and authorized at least once. If an AP is no longer part of the network then a manager must manually remove it.

Building the AP authentication list

The controller can retrieve authentication list entries from several sources: a RADIUS account, a file, or using the set of locally configured APs. All entries are merged to create a combined list.

The controller retrieves authentication list entries when:

- The **Authentication interval** expires
- **Authenticate Now** is selected
- **Save** is selected
- Each time the controller starts up.

Each time the authentication list entries are retrieved, all connected APs are checked against it. If an AP MAC address is no longer listed, its connection is terminated.

Note Although the same RADIUS account can be shared between this option and the **Public access > Attributes** page, it is recommended that a separate RADIUS account be created for each option.

General settings

Authentication interval

Specifies the interval at which the controller retrieves authentication list entries from the selected authentication sources. After the entries are retrieved all controlled APs are evaluated against the new list.

Authenticate Now

Causes the controller to retrieve authentication list entries from all selected sources.

Use file authentication list

When this option is selected, the controller retrieves authentication list entries from a file. This must be an ASCII file with one or more MAC addresses in it. Each address must be entered on a separate line. For example:

```
00:03:52:00:00:01
00:03:52:00:00:02
00:03:52:00:00:03
```

A label affixed to each AP indicates its Ethernet Base MAC Address. This is the address to specify in the authentication list.

File location

Specify the location of the file to use for authentication of APs using either HTTP or FTP. For example:

ftp://mydomain.com/auth_list
ftp://*username*:*password*@mydomain.com/auth_list
http://mydomain.com/auth_list

Use RADIUS authentication list

When this option is selected, the controller retrieves authentication list entries from a RADIUS server. List entries must be defined in the RADIUS account for the controller using the following Colubris-AVPair value string:

`managed-ap=`*MAC_address*

Where *MAC_address* is the Ethernet Base port MAC address of the controlled AP (which is printed on a sticker affixed to the AP case). Use colons to separate characters in the address.

For example: `00:20:E0:6B:4B:44`.

To define multiple addresses, specify additional entries as needed.

This attribute conforms to RADIUS RFC 2865. You may need to define this attribute on your RADIUS server if it is not already present as follows:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 0
- Attribute type = string

RADIUS profile

When the **Authentication** source is **RADIUS**, this option specifies the name of the RADIUS profile to use. There is no default. To configure RADIUS profiles, select **Controller >> Authentication > RADIUS profiles**.

RADIUS username

When the **Authentication** source is **RADIUS**, specifies the RADIUS username assigned to the controller.

RADIUS password / Confirm RADIUS password

Specifies the password that corresponds with **RADIUS username**.

Use the local authentication list

When this option is selected, the controller creates authentication list entries based on the set of APs that are currently defined on the controller. For reference purposes, the table shows the **AP name**, **Serial number** and **MAC address** of all APs that are defined and will be included in the authentication list.

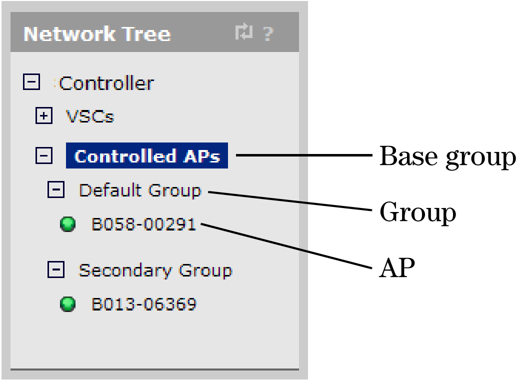
Note When the local authentication list is enabled, the first time an AP tries to connect to the controller, a manager must manually accept the AP on the **Controlled APs >> Overview > Discovered APs** page by selecting the **Authorize** in the **Action** column for the AP. Otherwise, the AP will not be able to connect to the controller.

Configuring APs

This section explains how to configure APs using the Controlled APs menu in the Network Tree.

Overview

To make the configuration of multiple APs easier to manage, parameters settings are managed using a hierarchal structure, where the configuration settings at lower levels are inherited from those at higher levels. There are three levels to the hierarchy: base group, group, and AP. For example:



- Select the **+** symbol next to **Controlled APs** to expand the tree to see all groups.
- Select the **+** symbol next to each group to see its APs.

The levels are defined as follows:

- **Base group:** The base group is called **Controlled APs**. This name cannot be changed and you cannot create an additional base group. Settings made to the base group are inherited by groups and APs.

- **Group:** Group-level configuration enables you to define settings that are shared by APs with similar characteristics. For example, if you have several APs at a location that are all providing the same service, putting them in the same group makes them easier to manage. The **Default Group** is always present. All newly-discovered APs are initially placed into this group. You can create multiple groups.
- **APs:** AP-level configuration enables you to specify configuration settings for a particular AP that overrides corresponding group-level settings.

Note

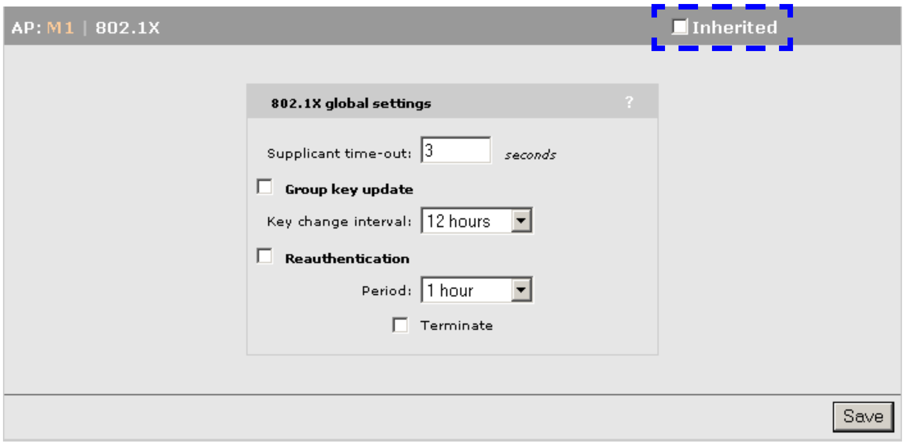
Assignment of VSCs can only be done at the group level. This means that all APs in a group always have the same VSC settings. The only exception to this is the MSM317 which allows VSCs to be bound to individual ports on its integrated switch. See the *MSM317 Access Device Installation and Getting Started Guide*.

Inheritance

Configuration settings are inherited as follows:

- Settings made at the **Controlled APs** level are inherited by all groups.
- Settings made at the **Group** level are inherited by all the APs in a group.

To change inherited configuration settings you must first clear the **Inherited** checkbox. For example, the following image shows the **802.1X** page with the **Inherited** checkbox cleared, allowing all settings on this page to be customized.



AP: M1 | 802.1X

☐ Inherited

802.1X global settings

Supplicant time-out: 3 seconds

☐ Group key update

Key change interval: 12 hours

☐ Reauthentication

Period: 1 hour

☐ Terminate

Binding VSCs to groups

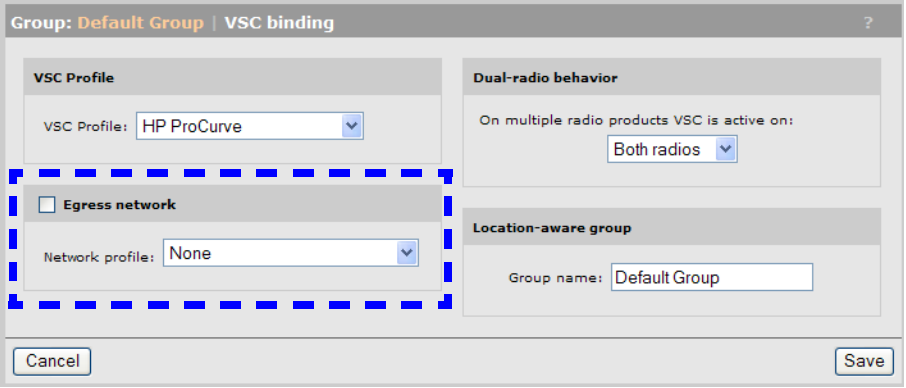
The controller defines a global pool of VSCs (see *Working with VSCs on page 5-1*) that represents all services that are available. From this pool, specific VSCs can be *bound* to one or more groups, to define the features that will be offered to users throughout the wireless network.

Note

VSCs cannot be bound to individual APs or to the base group. VSC can only be bound to a group.

Any changes to a bound VSC affect all groups (and APs) to which the VSC is bound, making it easy to manage configuration changes network-wide.

A key setting when binding a VSC to a group is the **Egress network**. If you enable this option, it can alter where the APs send user traffic. See *Traffic flow for wireless users on page 7-6* for detailed information on how the Egress network in a VSC binding can be affected by different configuration settings.



Group: Default Group | VSC binding

VSC Profile

VSC Profile: HP ProCurve

☐ Egress network

Network profile: None

Dual-radio behavior

On multiple radio products VSC is active on: Both radios

Location-aware group

Group name: Default Group

Note

On the MSM317, VSCs can also be bound directly to the switch ports. See the *MSM317 Access Device Installation and Getting Started Guide.*

Synchronizing APs

After making configuration changes to an AP or a group, you must update all affected controlled APs with the new settings by synchronizing them. See *Synchronizing APs on page 6-29*.

Configuration strategy

There are two ways to approach AP configuration:

Discover APs and then configure groups

This strategy works as follows:

1. Deploy the APs in their default configuration on the network.
2. Allow the discovery process to find the APs and place them in the default group.
3. Create group definitions and then move the APs to the appropriate group.

Tip

Configure the default group to disable all radios. In this way, the default group becomes a staging area to hold newly added APs. Once discovered, the new AP can be moved to its appropriate group where its radio is activated.

Configure groups and then discover APs

This strategy works as follows:

1. Create group definitions.

2. Manually define each AP in the appropriate group.

3. Deploy the APs in their default configuration on the network.

4. Allow the discovery process to find the APs and place them in the pre-configured groups.

Working with groups

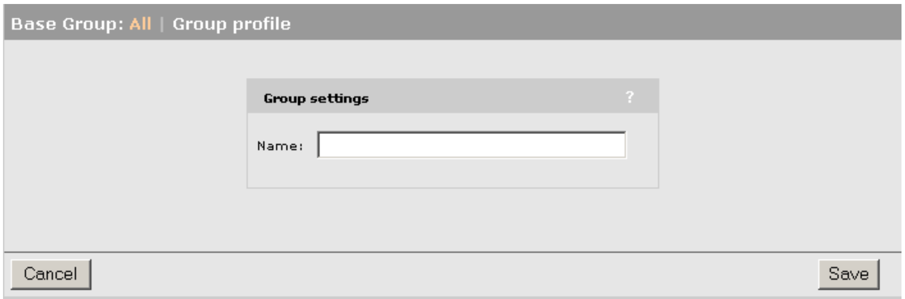
Adding a new group

To create a new group, do the following:

1. Select **Controlled APs >> Group management**.

2. Select **Add New Group**.

3. Specify the name of the new group and select **Save**.



Deleting a group

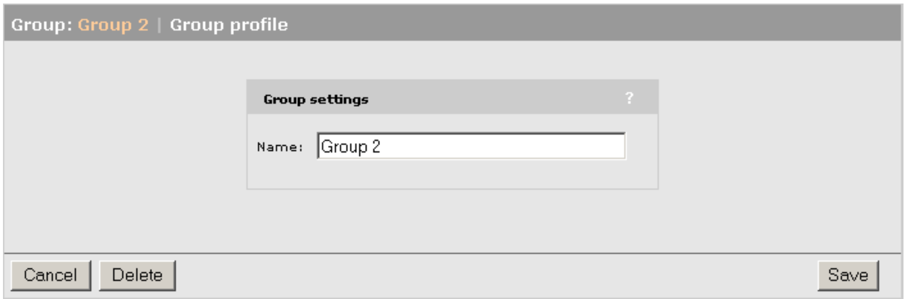
Note You must remove all APs from a group before you delete it.

To delete a group, do the following:

1. Select **Controlled APs >> Group management**.

2. Select the name of the group you want to delete.

3. Select **Delete**.

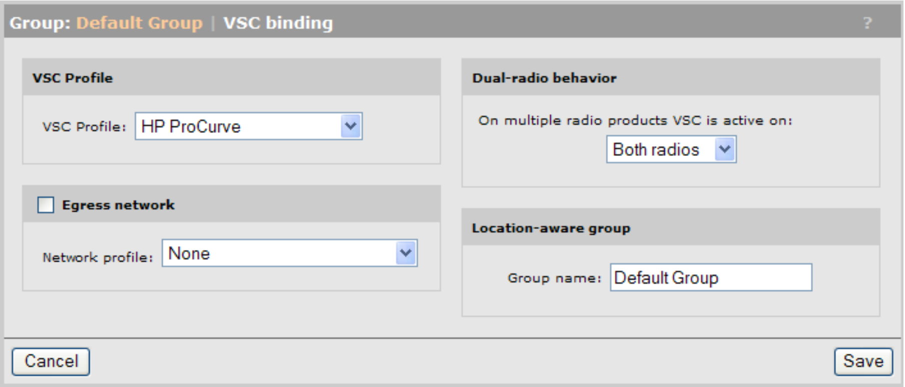


Name: Group 2

Binding a VSC to a group

To bind a VSC to a group, do the following:

1. Select the target group under **Controlled APs**.
2. In the right pane, select **VSC bindings**, then select **Add New Binding**.



VSC Profile: HP ProCurve

☐ Egress network

Network profile: None

On multiple radio products VSC is active on: Both radios

Group name: Default Group

3. Select the **VSC profile** to which the group will be bound.
4. If you want to assign an egress mapping to the binding, select **Egress network** and select the required **Network profile**. The Egress network can be used to assign all traffic on the group to a specific VLAN. Other uses are also possible depending on the type of VSC to which the group is being bound. For more information, see *Traffic flow for wireless users on page 7-6*.
5. Select **Save**.

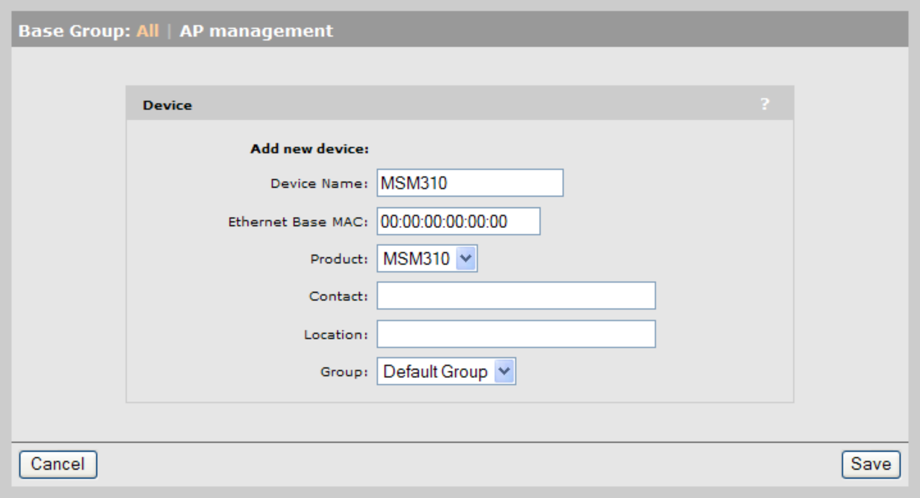
Working with APs

Manually adding a new AP

You can manually add APs to the controller before connecting the APs to the network. This is useful, for example, when you want to pre-designate the group into which an AP will be placed.

1. Select **Controlled APs >> Overview > Configured APs**.
2. Select **Add**.

3. In the **Device** box, identify the new AP, specifying at a minimum, **Device Name**, **Ethernet BASE MAC** (printed on the label affixed to each AP), and **Group**.



Base Group: All | AP management

Device

Add new device:

Device Name: MSM310

Ethernet Base MAC: 00:00:00:00:00:00

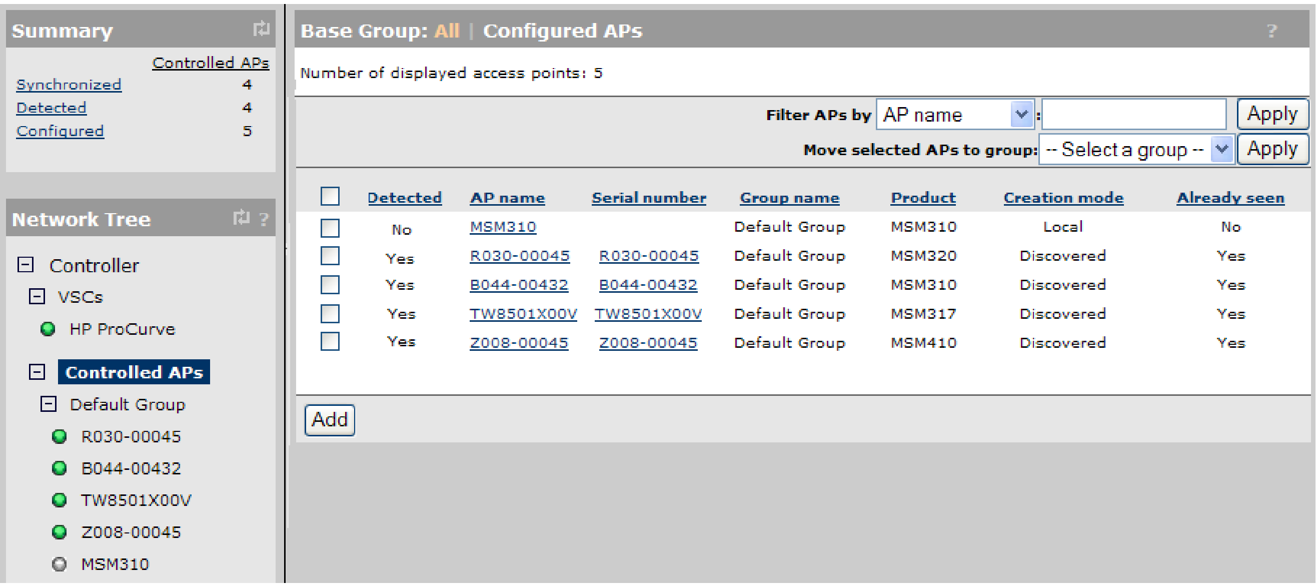
Product: MSM310

Contact:

Location:

Group: Default Group

Select **Save**. The AP is added to the selected group in the Network tree and will also be shown in the Configured APs list.



Summary

	Controlled APs
Synchronized	4
Detected	4
Configured	5

Network Tree

- Controller
  - VSCs
    - HP ProCurve
  - Controlled APs
    - Default Group
      - R030-00045
      - B044-00432
      - TW8501X00V
      - Z008-00045
      - MSM310

Base Group: All | Configured APs

Number of displayed access points: 5

Filter APs by: AP name

Move selected APs to group: -- Select a group --

□	Detected	AP name	Serial number	Group name	Product	Creation mode	Already seen
□	No	MSM310		Default Group	MSM310	Local	No
□	Yes	R030-00045	R030-00045	Default Group	MSM320	Discovered	Yes
□	Yes	B044-00432	B044-00432	Default Group	MSM310	Discovered	Yes
□	Yes	TW8501X00V	TW8501X00V	Default Group	MSM317	Discovered	Yes
□	Yes	Z008-00045	Z008-00045	Default Group	MSM410	Discovered	Yes

Note

- When the AP is physically connected to the network, it will discover the controller and automatically be accepted into the selected group. Make sure you configure the correct MAC address, otherwise the AP will just be discovered as a new AP and will not be placed into the selected group.
- If an AP is created with the wrong product type it will go into the **Wrong product** state when discovered. (For example, if you specify MSM310 for an AP that is an MSM320.) To remedy this, select **Overview > Discovered APs** and select the **Accept Products** link in the **Action** column. (This action will override the pre-configured product setting by the information discovered from the actual physical AP.)

Deleting an AP

Note When the AP authentication feature is disabled, a deleted AP may automatically rediscover the controller if the AP is left connected to the network. Therefore, before deleting, disconnect the AP unless you want it to rediscover the controller.

1. To delete an AP, select the AP in the **Network tree**, and then in the **Configured APs** list, select the AP name in the **Link** column.
2. On the **AP management** page, select **Delete**. The AP is deleted.

Moving an AP to a different group

Note Moving an AP to a different group causes it to be restarted.

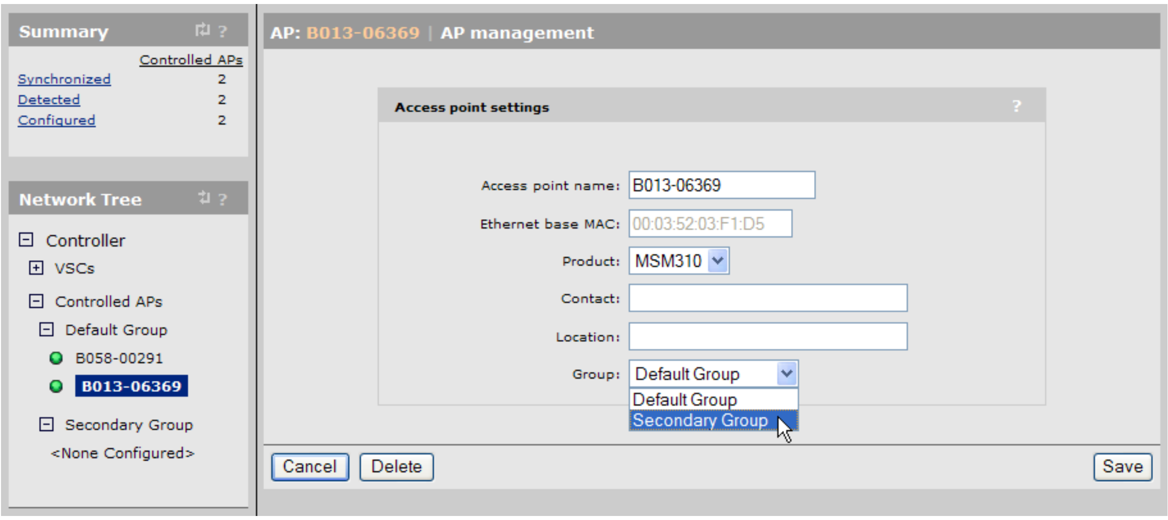
Using drag-and-drop

The easiest way to move an AP to a different group is to drag-and-drop it from the old group to the new group. Both groups must be visible in the Network tree for this to work.

The move to the different group does not actually occur until the AP is synchronized as described in the next section, *Synchronizing APs on page 6-29*.

Using menus

1. In the **Network tree** select the AP and then on the main menu, select **Device Management > AP management**.
2. Under Access point settings, select the desired **Group** and select **Save**.



	Controlled APs
Synchronized	2
Detected	2
Configured	2

AP: B013-06369 | AP management

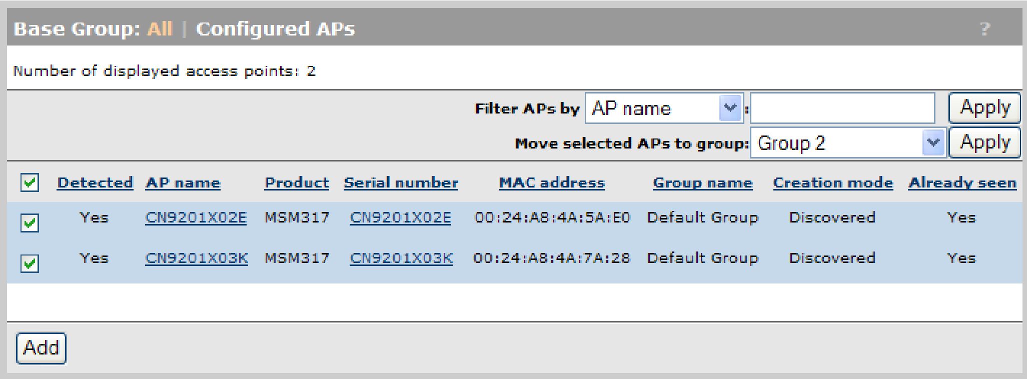
Access point name: B013-06369
Ethernet base MAC: 00:03:52:03:F1:D5
Product: MSM310
Contact:
Location:
Group: Default Group

This puts the AP into the unsynchronized state (it will be displayed in orange). The move does not occur until the AP is synchronized as described in the next section.

Moving multiple APs between groups

To move one or more APs between groups, do the following:

1. Use the check boxes in the table to select one or more APs. Select the check box in the table header to select all the APs in the table.



Base Group: All | Configured APs ?

Number of displayed access points: 2

Filter APs by AP name : Apply

Move selected APs to group: Group 2 Apply

☑	Detected	AP name	Product	Serial number	MAC address	Group name	Creation mode	Already seen
☑	Yes	CN9201X02E	MSM317	CN9201X02E	00:24:A8:4A:5A:E0	Default Group	Discovered	Yes
☑	Yes	CN9201X03K	MSM317	CN9201X03K	00:24:A8:4A:7A:28	Default Group	Discovered	Yes

Add

2. Select the group into which to move the APs from the list next to **Move selected APs to group**.

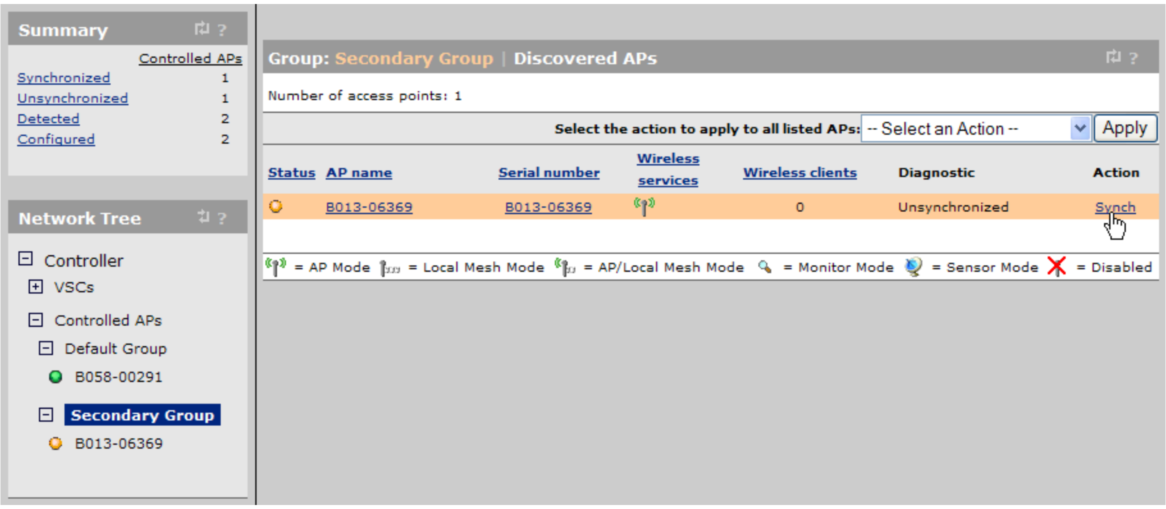
3. Select **Apply**.

Synchronizing APs

Depending on the type of configuration changes that are being synchronized, wireless users may be forced to reassociate or log in again.

After making configuration changes, you must synchronize the APs with the updated configuration as follows:

1. In the **Network tree**, select the group that contains the APs, and then in the right pane, select **Discovered APs**. For example, **Secondary Group**.



Summary ?

	Controlled APs
Synchronized	1
Unsynchronized	1
Detected	2
Configured	2

Network Tree ?

- Controller
  - VSCs
  - Controlled APs
    - Default Group
      - ● B058-00291
    - **Secondary Group**
      - ○ B013-06369

Group: Secondary Group | Discovered APs ?

Number of access points: 1

Select the action to apply to all listed APs: -- Select an Action -- Apply

Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
○	B013-06369	B013-06369		0	Unsynchronized	Synch

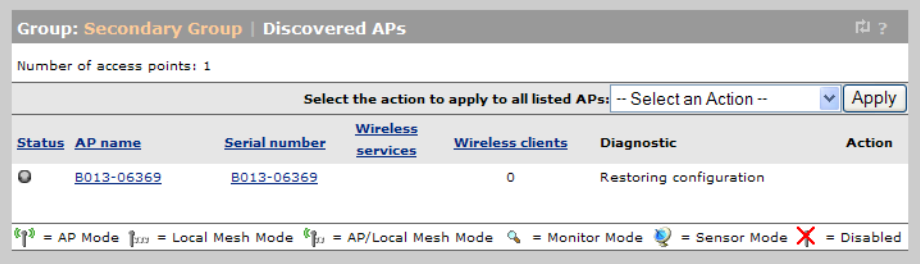
= AP Mode = Local Mesh Mode = AP/Local Mesh Mode = Monitor Mode = Sensor Mode ✗ = Disabled

APs requiring synchronization are displayed with an orange background and show **Unsynchronized** in the **Diagnostic** column.

2. Select a **Synch** link in the **Action** column to synchronize a single AP.

   Or, to synchronize all unsynchronized APs in the group, select **Synchronize Configuration** in the **Select the action to apply to all listed APs** list, and select **Apply**.

3. Monitor synchronization progress by watching the **Diagnostic** column. Messages such as **Resetting configuration** and **Restoring configuration** will appear during the synchronization process.



Group: Secondary Group | Discovered APs

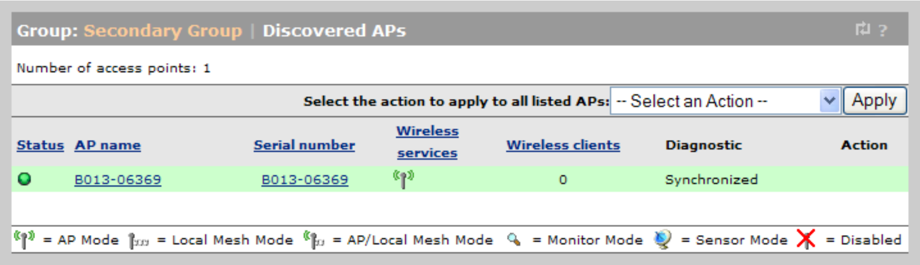
Number of access points: 1

Select the action to apply to all listed APs: -- Select an Action -- Apply

Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
●	B013-06369	B013-06369		0	Restoring configuration	

= AP Mode = Local Mesh Mode = AP/Local Mesh Mode = Monitor Mode = Sensor Mode ✗ = Disabled

4. As each synchronization completes, the **Status** light icon and background color of the synchronized AP changes to green. The status light icon next to the AP name under the pertinent group name in the Network tree also changes to green. This indicates that the AP is fully operational and using its new configuration.



Group: Secondary Group | Discovered APs

Number of access points: 1

Select the action to apply to all listed APs: -- Select an Action -- Apply

Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
●	B013-06369	B013-06369		0	Synchronized	

= AP Mode = Local Mesh Mode = AP/Local Mesh Mode = Monitor Mode = Sensor Mode ✗ = Disabled

Assigning egress VLANs to a group

When you bind an AP to a VSC, you are able to assign an egress network to the binding. The egress network can be used to assign all the traffic on the group to a specific VLAN. Other uses are also possible depending on the type of VSC to which the group is being bound. For more information, see *Traffic flow for wireless users on page 7-6*.

Assigning country settings to a group

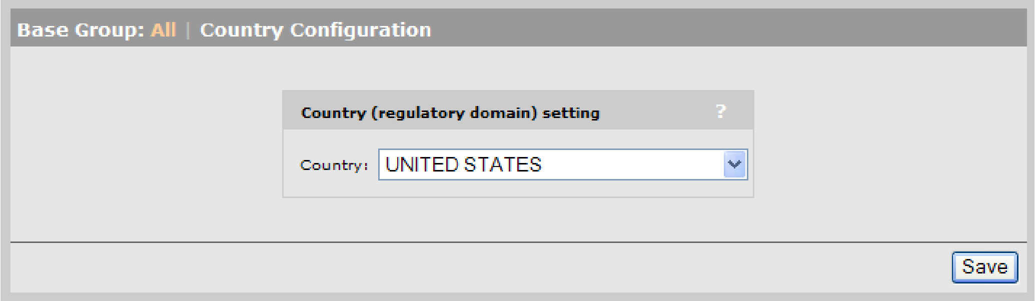
The country of operation, also known as the regulatory domain, determines the availability of certain wireless settings on an AP. The country of operation is configured at the group level.

To configure country settings, select either:

Controlled APs >> Configuration > Country

Controlled APs > [*group*] >> Configuration > Country

The country configuration for the Base group looks like this:


Base Group: All | Country Configuration
Country (regulatory domain) setting
?
Save

Country: UNITED STATES

After changing the country setting, APs must be synchronized.

Note

In some regions, APs are delivered with a fixed country setting. If you place an AP with a fixed country setting into a group that has a different country configuration, the AP will fail to be synchronized. (The error **Incompatible settings** will be displayed on the **Controlled APs >> Overview > Discovered APs** page).

Caution

Incorrectly setting the country may result in illegal operation and may cause harmful interference to other systems. Please consult with a professional installer who is trained in RF installation and knowledgeable about local regulations to ensure that the AP is operating in accordance with channel, power, indoor/outdoor restrictions and license requirements for the intended country. If you fail to heed this caution, you may be held liable for violating the local regulatory compliance

Provisioning APs

Provisioning is the means by which you can change the factory default IP addressing method and controller discovery settings on controlled APs.

Provisioning is generally not required when deploying controlled APs in simple network topologies. However, it is required as when:

- Controlled APs do not have layer 2 connectivity to a controller and where it is not possible to control the DNS or DHCP server configuration. See *Discovery recommendations on page 6-10*.
- Controlled APs need to be deployed with static IP addresses.
- Controlled APs use a local mesh to connect to the controller. See *Provisioning local mesh links on page 13-12*. This feature is not supported on the MSM317.
- To accelerate the discovery process on networks with a large number of VLANs, or when many VLANs are connected to many controllers.
- When multiple controllers are available to an AP and you want to make sure an AP always connects to the same controller.

Provisioning methods

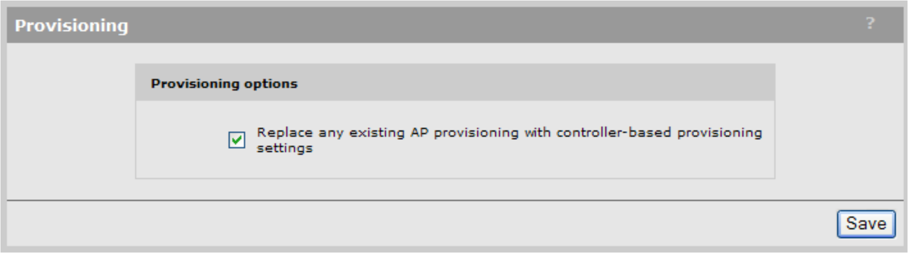
Provisioning can be done in two ways: provision settings using the controller or provision settings directly on APs.

Using the controller to provision APs

On the controller, provisioning can be done at the group or AP level for added flexibility. Provisioning via the controller enables you to quickly provision many APs at once.

In certain scenarios it may be practical to use one controller to provision APs, and then have the APs associate with another controller after being deployed. For example, provisioning could occur at the network operations center by connecting APs to the same subnet as a controller. Once provisioned, the APs can then be deployed in the field where they will discover a controller already in operation.

To enable a controller to send provisioned settings to controlled APs, you must first activate the **Enable provisioning of controlled APs** option on the **Controller >> Controlled APs > Provisioning** page.



☑ Replace any existing AP provisioning with controller-based provisioning settings

Define provisioning settings as described in *Displaying the provisioning pages on page 6-33*.

Note

- Until this option is enabled, provisioned settings defined on the controller are not sent to any controlled APs.
- After an AP has been updated with provisioned settings, these settings do not become active ***until the AP is restarted***, or a **Remove and rediscover** action is executed on the **Controlled APs >> Configured APs** page.

Directly provisioning an AP using its management tool

In its factory default state, the AP provides a provisioning menu with the same options that are available on the controller. Use this method when there is no local controller on which to perform the provisioning. See *Displaying the provisioning pages on page 6-33*.

Note

Once an AP has established the secure management tunnel with a controller, the provisioning menu on the AP is no longer accessible.

In both cases, the configuration settings that you have access to are the same. They are described in the following sections.

Displaying the provisioning pages

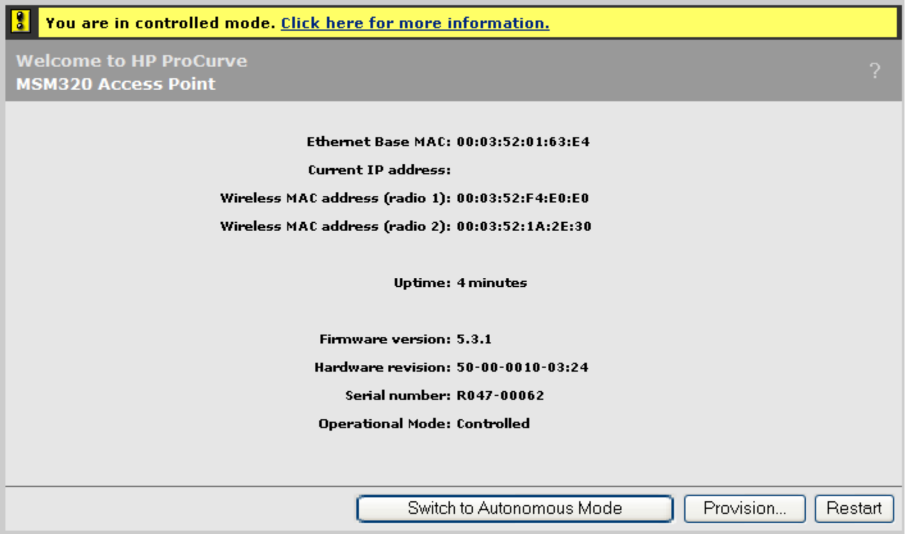
To display the provisioning pages, do the following:

On a controller

1. Select one of the following in the Network tree:
   - Controlled APs
   - A group
   - An AP
2. In the right pane, select **Provisioning > Connectivity**.
3. Configure provisioning settings as described in the sections that follow.

On an AP in its factory-default state

1. Log in to its management tool.
2. Select **Provision** at the bottom of the home page.



You are in controlled mode. Click here for more information.

Welcome to HP ProCurve
MSM320 Access Point

Ethernet Base MAC: 00:03:52:01:63:E4
Current IP address:
Wireless MAC address (radio 1): 00:03:52:F4:E0:E0
Wireless MAC address (radio 2): 00:03:52:1A:2E:30

Uptime: 4 minutes

Firmware version: 5.3.1
Hardware revision: 50-00-0010-03:24
Serial number: R047-00062
Operational Mode: Controlled

Note

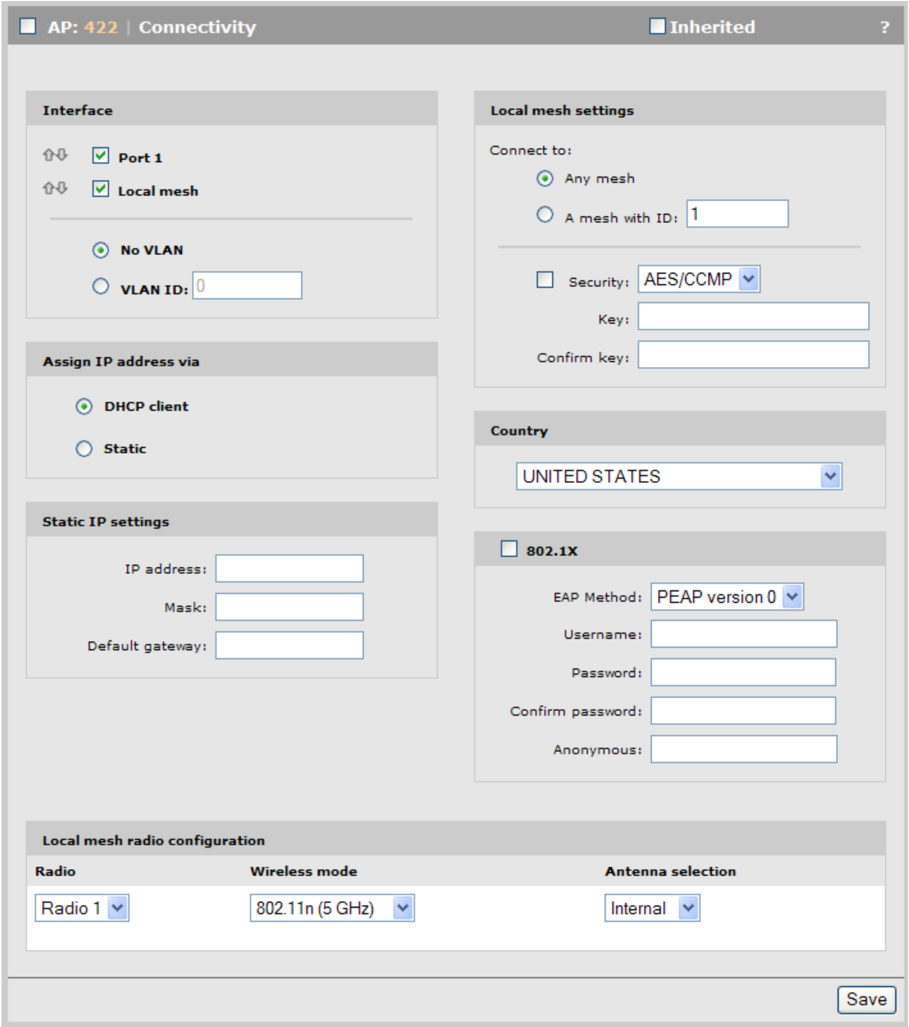
The **Provision** button is only available if the AP is in its factory-default state, meaning it has not yet been provisioned and that the AP has never discovered a controller (since last factory default). To force an AP into its factory-default state, press and hold its reset button until the status lights blink three times.

3. Configure provisioning settings as described in the sections that follow.

Provisioning connectivity

Use the **Provisioning > Connectivity** page to provision connectivity settings for a controlled AP. The following page will appear on all APs except for the MSM317.

Enable provisioning here:



□ AP: 422 | Connectivity □ Inherited ?

Interface

☑ Port 1
☑ Local mesh

● No VLAN
○ VLAN ID: 0

Assign IP address via

● DHCP client
○ Static

Static IP settings

IP address:
Mask:
Default gateway:

Local mesh settings

Connect to:
● Any mesh
○ A mesh with ID: 1

□ Security: AES/CCMP
Key:
Confirm key:

Country

UNITED STATES

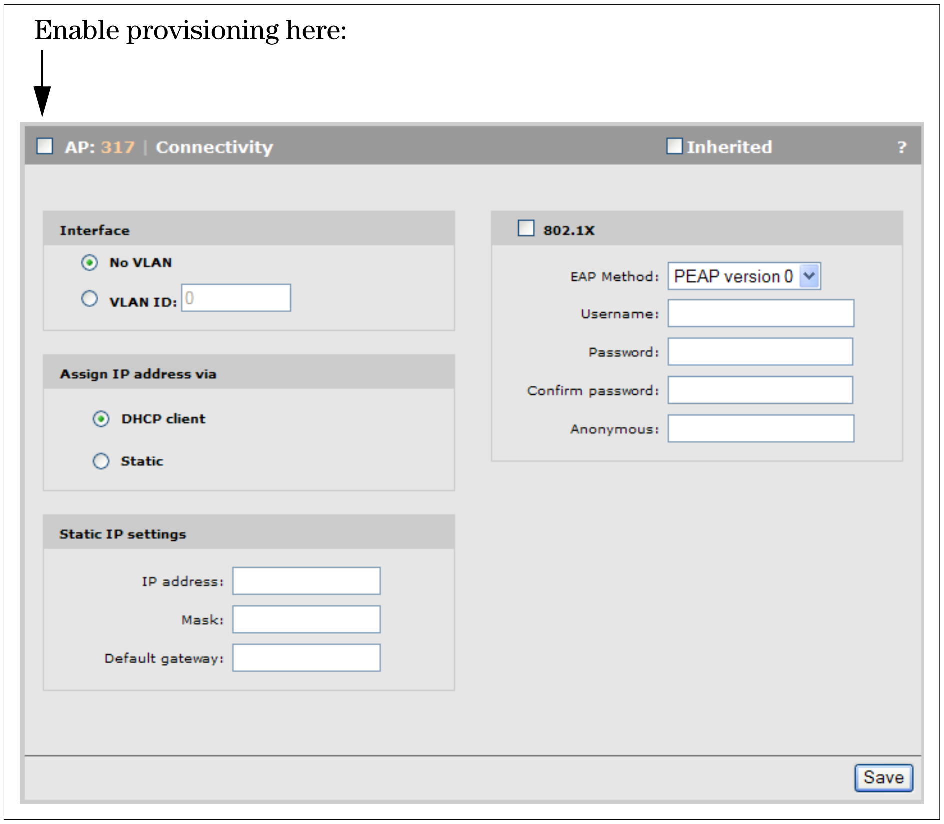
□ **802.1X**

EAP Method: PEAP version 0
Username:
Password:
Confirm password:
Anonymous:

Local mesh radio configuration

Radio	Wireless mode	Antenna selection
Radio 1	802.11n (5 GHz)	Internal

The following page will appear on the MSM317.



Enable provisioning here:

☐ AP: 317 | Connectivity ☐ Inherited ?

Interface

● No VLAN

○ VLAN ID: 0

Assign IP address via

● DHCP client

○ Static

Static IP settings

IP address:

Mask:

Default gateway:

☐ **802.1X**

EAP Method: PEAP version 0

Username:

Password:

Confirm password:

Anonymous:

Save

Interface

Select the interface you want to configure and then define its settings using the other options on this page. Set **VLAN ID** if applicable.

Assign IP address via

- **DHCP client:** Address is assigned using a DHCP server. Enable this option to have the interface act as a DHCP client. The AP sends DHCP requests on the specified VLAN. If no VLAN is specified, the request is sent untagged.
- **Static:** Select this option to manually assign an IP address to the interface.

Static IP settings

When you select **Static** for **Assign IP address via**, configure settings in this box.

- **IP address:** Specify the IP address you want to assign to the interface.
- **Address mask:** Specify the appropriate subnet mask for the IP address you specified.
- **Default gateway:** Specify the IP address of the default gateway.

Local mesh settings

For information on provisioning these settings, see *Local mesh on page 13-1*.

Country

Select the country in which the AP is operating.

Caution

- Selecting the wrong country may result in illegal operation and may cause harmful interference to other systems. Please consult with a professional installer who is trained in RF installation and knowledgeable about local regulations to ensure that the service controller is operating in accordance with channel, power, indoor/outdoor restrictions and license requirements for the intended country.
- The Country option is not available on APs delivered with a fixed country setting.

802.1X

Enable this option when the AP is connected to a secured switch port that requires 802.1X authentication. Once the AP is authenticated, controller discovery proceeds as usual.

Note

- If this option is enabled and the AP is connected to a unsecured switch port, 802.1X is ignored and discovery proceeds as usual.
- The switch port is expected to be multi-homed, so that once authentication is successful, tagged and untagged traffic for any MAC addresses (including wireless clients) will be accepted by the switch.

In this type of environment. deployment can be a challenge, since the AP must already be configured with the correct 802.1X username and password before it is connected to the secured switch port. There are three solutions to this problem:

- During AP deployment, 802.1X is deactivated on the switch ports. The APs are connected and provisioned with the correct 802.1X settings by the controller. Once all APs are synchronized, 802.1X authentication can be enabled on the switch ports.
- Before being deployed, the APs are first connected to a controller via a non-secure switch. The APs are provisioned and synchronized with the correct 802.1X settings by the controller. Next, the APs are deployed to their final location.
- For small deployments, the administrator could connect each AP in turn to a computer and configure the appropriate 802.1X settings using the AP provisioning interface. This solution is time consuming and is not a realistic option for a large deployments.

EAP method

Select the extensible authentication protocol method to use:

- **PEAP version 0:** Authentication occurs using MS-CHAP V2.
- **PEAP version 1**: Authentication occurs using EAP-GTC.
    - **TTLS:** The Tunneled Transport Layer Security protocol requires that the switch first authenticate itself to the AP by sending a PKI certificate. The AP authenticates itself to the switch by supplying a username and password over the secure tunnel.

Username

Username that the AP will use inside the TLS tunnel.

Password / Confirm password

Password assigned to the AP.

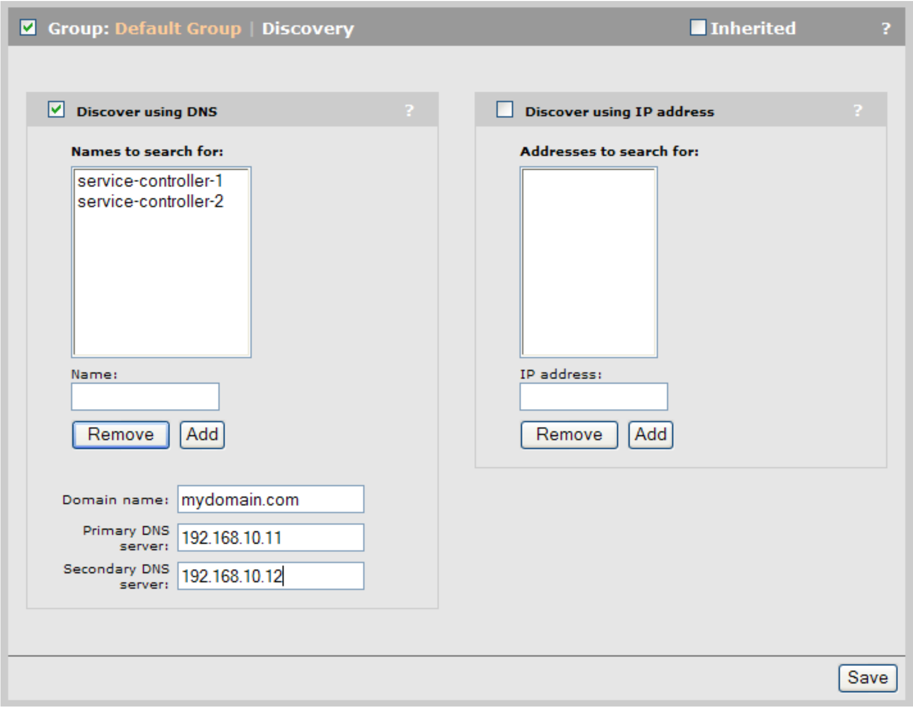
Anonymous

Name used outside the TLS tunnel by all three EAP methods. If this field is blank, then the value specified for **Username** is used instead.

Provisioning discovery

Use the **Provisioning > Discovery** page to provision the method a controlled AP uses to discover a controller. Two options can be provisioned: DNS discovery or discovery via IP address. The following page shows Discovery using DNS provisioned.

Enable provisioning here:



☑ Group: Default Group | Discovery ☐ Inherited

☑ Discover using DNS

Names to search for:

service-controller-1
service-controller-2

Domain name: mydomain.com

Primary DNS server: 192.168.10.11

Secondary DNS server: 192.168.10.12

☐ Discover using IP address

Addresses to search for:

Discover using DNS

The AP attempts to connect with a controller using the names in the order that they appear in this list.

To discover the controller on the network, the AP appends each name with the specified **Domain name**.

In the above example, the AP will search for controllers with the names:

- service-controller-1.mydomain.com
- service-controller-2.mydomain.com

If you define a name that contains a dot, then the domain name is not appended . For example, if the name is **controller.yourdomain.com**, no domain name is appended.

If the AP is operating as a DHCP client, the DHCP server will generally return a domain name when it assigns an IP address to the AP. If you leave the **Domain name** field on this page blank, then the DHCP domain name is appended to the specified names instead.

Discover using IP address

The AP attempts to connect with a controller using the IP addresses in the order that they appear in this list.

Provisioning summary

The following table defines the potential outcome for all provisioning scenarios.

Connectivity provisioned	Discovery provisioned	Result
No	No	Default behavior is used for connectivity and discovery. See *Discovery of controllers by controlled APs on page 6-6*.
No	Yes	Discovery occurs using the provisioned methods on the following interfaces: ■ Last interface on which a controller was discovered. (Only applies to APs that have previously discovered a controller.) ■ Untagged on port 1 (Uplink port on the MSM317). ■ All detected VLANs (in sequence) on port 1 (Uplink port on the MSM317).
Yes	No	Discovery methods are used according to the provisioned connectivity settings. See *Discovery of controllers by controlled APs on page 6-6*. Note: DHCP discovery is not executed if a static IP address is provisioned.
Yes	Yes	Discovery occurs using the provisioned methods over the provisioned connectivity. The provisioned discovery method is retried indefinitely if it fails, however other discovery methods are not attempted.

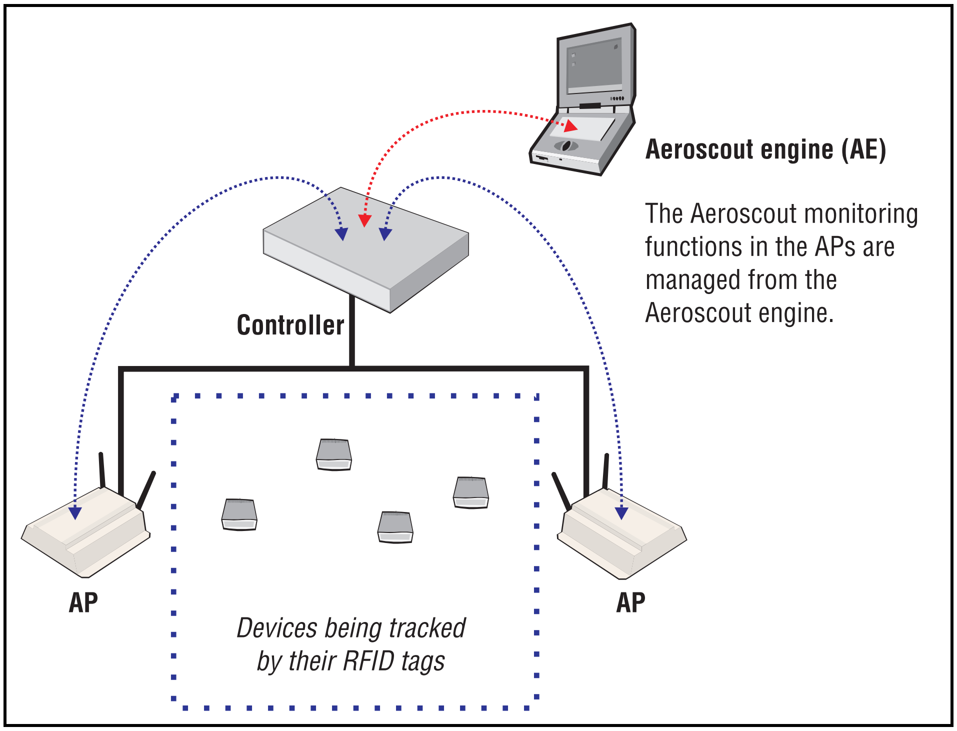
Provisioning example

The following example shows how to use the default group as a staging area, where APs are discovered and then provisioned before being moved into their actual production group.

1. Select **Controller >> Controlled APs > Provisioning**.
2. Select the **Enable provisioning of controlled APs** option.
3. Select **Save**.
4. Select **Controller > Controlled APs > Default group >> Configuration > Radios.**
5. Select each product in the table in turn, and disable its radio(s).
6. Select **Controller > Controlled APs > Default group >> VSC bindings.**
7. Disable any active VSC bindings.
8. Connect all APs that need to be provisioned. Wait until they are discovered and assigned to the default group.
9. Select **Controller > Controlled APs > Default group >> Provisioning > Connectivity**. Configure provisioning settings as required. For details, see ***Provisioning connectivity on page 6-34*****.**
10. Select **Controller > Controlled APs > Default group >> Provisioning > Discovery**. Configure provisioning settings as required. For details, see ***Provisioning discovery on page 6-37*****.**
11. If required, select individual APs and define provisioning settings accordingly.
12. Synchronize the APs. For details, see ***Synchronizing APs on page 6-29*****. The provisioned settings are not active at this point.**
13. Move the APs from the default group to their actual production group. For details, see ***Moving an AP to a different group on page 6-28*****.** This will force a restart of the APs and initiate the provisioned settings.

AeroScout RTLS

Controllers and their controlled APs can be used to provide the Wi-Fi infrastructure for an AeroScout Real-Time Location Tracking (RTLS) system. APs, AeroScout Wi-Fi RFID tags, and the AeroScout MobileView software work together for the purpose of wirelessly tracking the location of valuable assets in real time. The controller forwards AeroScout tag information from controlled APs to a computer running the AeroScout Engine and MobileView software.


Aeroscout engine (AE)
The Aeroscout monitoring functions in the APs are managed from the Aeroscout engine.
Controller
AP
AP
Devices being tracked by their RFID tags

Note

- HP does not sell or promote AeroScout products. Contact AeroScout for information on obtaining its MobileView software, Wi-Fi RFID tags, and associated hardware. Consult the AeroScout documentation for deployment information.
- To work with MSM APs, the Wi-Fi RFID tags must be configured to send data in the WDS format (4 addresses). Channel allocation on the AP and tag must match as well.
- AeroScout MobileView should be configured with the team IP address of the team that is managing the controlled AP.

To enable AeroScout support

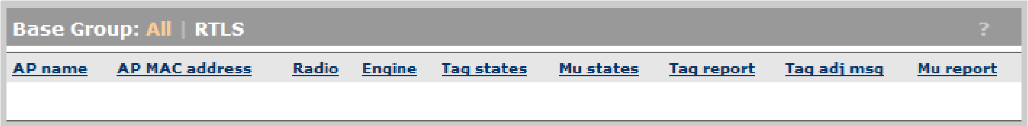
AeroScout support is only available for controlled APs, with radios configured as **Access point only** or **Access point and Local mesh**, and operating in the 2.4 GHz band.

To configure the controller (and all its controlled APs) to work with AeroScout:

1. Select **Controller >> Controlled APs > RTLS.**
2. Select **Enable support for AeroScout tags and MU**.
3. Select **Save**.

Viewing status information

Basic AP and AeroScout tag status information is available by selecting **Controller > Controlled APs >> Overview > RTLS**. For example:



All AeroScout management and monitoring is performed in the AeroScout software itself. Aeroscout documentation and AeroScout software must be used to operate and monitor the tags.

AP name

Name of the AP on which HP RTLS is enabled.

AP MAC address

MAC address of the AP.

Radio

Radio on the AP to which the AeroScout tag is connected.

Engine

IP address and port to which the controller sends the tag and Mu reports generated by the AP.

Tag states

Shows two values: admin state / operational state

- Admin state: Indicates if the AeroScout engine requested that the AP process frames generated by AeroScout tags.
- Oper state: Indicates if the radio is actually listening for frames generated by AeroScout tags.

Mu states

Shows two values: admin state / operational state

- Admin state: Indicates if the AeroScout engine requested that the AP process Mu (mobile unit) information.
- Oper state: Indicates if the radio is actually listening for Mu (mobile unit) information.

Tag report

Number of tag reports sent to the Aeroscout engine.

Tag adj msg

Number of tag messages that were dropped because they were received on the wrong channel.

Mu report

Number of Mu reports sent to the Aeroscout engine.

Software retrieval/update

Software management of controlled APs is automatically performed by the controller after the AP is discovered (see *Key controlled-mode events on page 6-4*).

If the software version on the AP does not match the version installed on the controller, new software is installed on the AP by the controller.

For information on how to update the controller software see *Software updates on page 20-4*.

Monitoring

The controller provides a series of pages that present monitoring and status information for controlled APs. You can view these pages for all controlled APs, for all APs in a group, or for just a specific AP. All options appear on the **Overview** menu, which can be reached by selecting:

- **Controlled APs >> Overview**.
- **Controlled APs > [*group*] >> Overview**.
- **Controlled APs > [*group*] > [*AP*] >> Overview**.

See the online help for details about the information provided on these status pages.

7

Working with VLANs

Contents

Key concepts

The controller provides a robust and flexible virtual local area network (VLAN) implementation that supports a wide variety of scenarios.

Up to 80 VLAN definitions can be created on the controller. VLAN ranges are supported, enabling a single definition to span a range of VLAN IDs.

The following controller features are supported on a VLAN:

- Network address translation (*However, static NAT mappings are not supported.)*
- Management tool access
- SNMP access
- SOAP access
- VPN traffic
- L3 mobility

VLAN usage

VLANs can be used in a number of different ways to affect traffic routing on a controller and its APs. The following is a list of the most common VLAN uses:

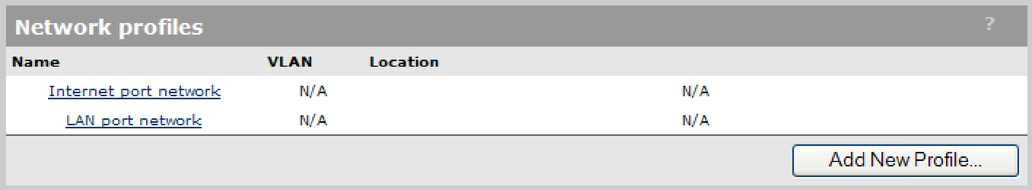
- **Controller VSC ingress:** VLANs can be used to determine how incoming traffic is mapped to a VSC on a controller. Assigning a VLAN range enables a single VSC to handle incoming traffic on multiple VLANs.
- **Controller VSC egress:** VLANs can be used to control how traffic is forwarded onto the wired network by a VSC on the controller. Traffic can be sent to the LAN port or Internet port, either untagged (no VLAN), tagged with a specific VLAN ID, or distributed across a range of VLAN IDs (using a round-robin mechanism).
- **VSC binding:** When an AP group is bound to a VSC, an egress VLAN can be specified. This egress is used in several different ways to route traffic depending on the features that are active on the VSC. For example, when Mobility traffic manager is active, this VLAN becomes the user's home network. See *Traffic flow for wireless users on page 7-6*.
- **Switch port VLANs:** The switch ports on the MSM317 can be bound to a specific VLAN. See the *MSM317 Installation and Getting Started Guide*.
- **User account profile VLAN:** A VLAN can be assigned in a user account profile, enabling you to configure VLAN usage for groups of users.
- **VLAN assignment via RADIUS attributes:** A VLAN can be assigned in a user's RADIUS account, enabling you to customize VLANs on a per-user basis. For example, when Mobility traffic manager support is enabled on a VSC, RADIUS VLAN attributes can be used to define a user's home network.
- **Discovery VLAN:** APs can be provisioned to discover controllers on a specific VLAN. See *Provisioning APs on page 6-31*.

Defining a VLAN

To create a new VLAN definition, first you must define a network profile with the required VLAN ID. Next, you use the profile to define a VLAN on a port, VSC interface, or user account.

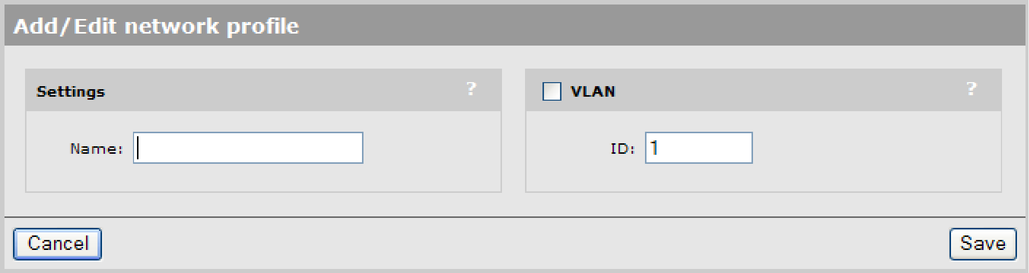
Creating a network profile

1. Select **Controller >> Network > Network profiles.** By default the list contains two definitions: **Internet port network** and **LAN port network**.



Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A

2. Select **Add New Profile**.



Settings

Name:

☐ VLAN

ID: 1

3. Under **Settings**, specify a **Name** to identify the profile.
4. Select **VLAN**, and then set **ID** to the VLAN ID you want to assign. You can also define a range of VLANs in the form *X-Y*, where *X* and *Y* can be 1 to 4094. For example: 50-60.

   This enables a single VLAN definition to accept traffic for one or more VLAN IDs, making it easy to manage a large number of contiguously assigned VLANs. You can define more than one VLAN range, but each range must be distinct and contiguous. VLANS with ranges cannot be assigned an IP address.
5. Select **Save**. The definition is added to the Network profiles page.

Defining a VLAN

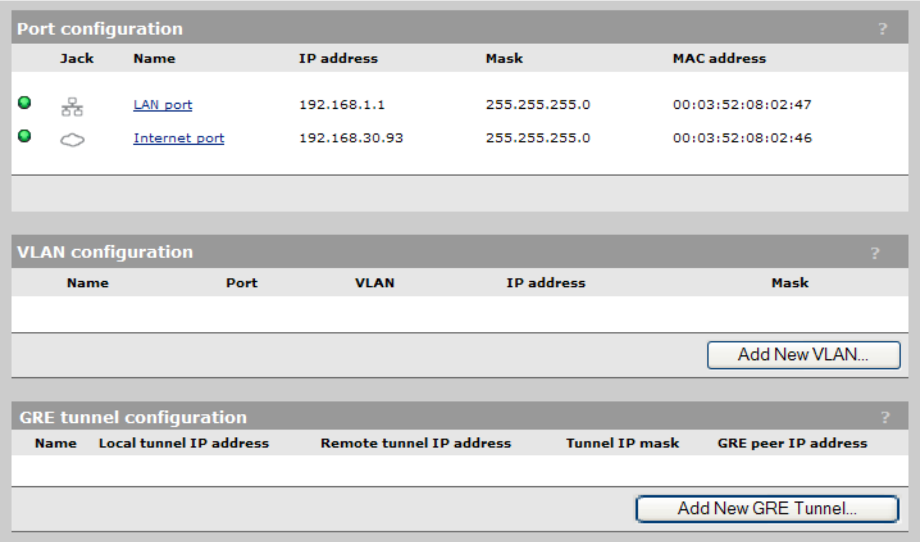
Once you have created a network profile with a VLAN ID, you can use the profile to define a VLAN on the controller and APs. Some of the more frequently defined VLANs are listed in the following table.

To define a VLAN on ...	See ...
A controller port	*Defining a VLAN on a controller port on page 7-4*
The ingress mapping in a VSC profile	*VSC ingress mapping on page 5-16*
The egress mapping in a VSC profile	*VSC egress mapping on page 5-17*
The egress network in a VSC binding	*Binding VSCs to groups on page 6-23*

Defining a VLAN on a controller port

Define a VLAN on a controller port as follows:

1. Select **Controller >> Network > Ports**. By default, no VLANs are defined.



Port configuration

	Jack	Name	IP address	Mask	MAC address
●		LAN port	192.168.1.1	255.255.255.0	00:03:52:08:02:47
●		Internet port	192.168.30.93	255.255.255.0	00:03:52:08:02:46

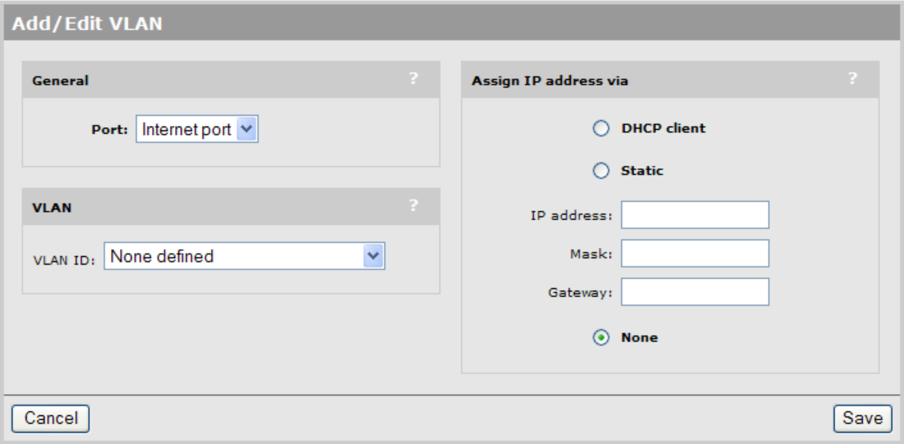
VLAN configuration

Name	Port	VLAN	IP address	Mask

GRE tunnel configuration

Name	Local tunnel IP address	Remote tunnel IP address	Tunnel IP mask	GRE peer IP address

2. Select **Add New VLAN.** The **Add/Edit VLAN** page opens.



Port: Internet port

VLAN ID: None defined

○ DHCP client

○ Static

IP address:

Mask:

Gateway:

● None

3. Under **General**, select the port to which the VLAN will be bound. Once a VLAN has been defined on a port, the port assignment cannot be changed. To assign the VLAN to a different port, delete the VLAN definition and create a new one on the required port**.**

4. Under **VLAN**, select the VLAN ID to assign. The list contains all network profiles that are defined with a VLAN ID or range.

5. Specify how the VLAN obtains an IP address.

   An IP address cannot be assigned to a VLAN range.

   - **DHCP client**: The VLAN obtains its IP address from a DHCP server on the same VLAN. Note: There is no support for obtaining a default gateway from the DHCP server.

   - **Static**: Enables you to manually assign an IP address to the VLAN. If you select this option, you must specify a static **IP address, Mask,** and **Gateway.**

   - **None**: Specifies that this VLAN has no IP address, so that you can use the VLAN for a VSC ingress mapping.

6. Enable NAT support if required. (Available only if addressing is **DHCP client** or **Static.)** By default NAT is disabled**.** See *Network address translation (NAT) on page 3-30*.

7. Select **Save**.

User-assigned VLANs

VLANs can be assigned on a per-user basis using attributes defined in a user's RADIUS account, or via VLAN definitions in a local user account profile. These user-assigned VLANs are also called dynamic VLANs because they are applied dynamically after a user is authenticated and override the static definitions on VSCs or VSC bindings.

For a complete description on how VLANs affect traffic flow, see *Traffic flow for wireless users on page 7-6*.

VLAN assignment via RADIUS

To define a VLAN in a user's RADIUS account, you need to set the RADIUS attributes Tunnel-Medium-Type, Tunnel-Private-Group-ID, and Tunnel-Type. The Tunnel-Private-Group-ID attribute should be set to the name of the VLAN. A VLAN number can also be specified, but this not recommended.

See the *Access Accept* section under *User attribute definitions on page 15-20* for more information on these attributes.

VLAN assignment via the local user accounts

VLANs can be assigned on a per-user basis by configuring a user account profile with the appropriate VLAN number. See *Defining a user account on page 10-30* and *Defining account profiles on page 10-32*.

Traffic flow for wireless users

Due to the large number of features that can make use of VLANs, and the way in which these features interact, VLAN settings at different points in the configuration can affect traffic flow for wireless users in different ways. The following tables provide an overview of all possible configuration settings and how they affect data flow. The tables are organized according to the type of VSC that is being bound to an AP.

Binding to a VSC that has *Wireless mobility* disabled

				User-assigned VLAN is assigned via RADIUS or local user accounts		
					User-assigned VLAN does not exist on AP or controller	
VSC type	**Egress network in VSC binding**	**Client data tunnel**	**User-assigned VLAN is not assigned via RADIUS or local user accounts**	**User-assigned VLAN exists on AP or controller**	**VLAN ID**	**VLAN name**
Access-controlled	Defined	Active	The Egress network setting in the VSC binding is ignored. Traffic is sent to the controller in the client data tunnel. It exits the controller on the egress mapping defined on the appropriate VSC.	The Egress network setting in the VSC binding is ignored. Traffic is sent to the controller in the client data tunnel. It exits the controller on the user-assigned VLAN, which overrides any egress mapping defined on the controller's VSC.	User traffic will never reach its destination because the user-assigned VLAN does not match any VLAN IDs defined on the AP or controller.	The Egress network setting in the VSC binding is ignored. Traffic is sent to the controller in the client data tunnel. It exits the controller on the egress mapping defined on the appropriate VSC.
		Disabled	Traffic is sent on the AP Ethernet port tagged with the VLAN specified by the Egress network in the VSC binding. The Egress network VLAN must match the ingress VLAN on the bound VSC (or be altered by a switch between the AP and the controller to do so) otherwise traffic from the AP will not reach the controller. Traffic exits the controller on the egress mapping defined on the appropriate VSC.	Traffic is sent on the AP Ethernet port tagged with the VLAN specified by the Egress network in the VSC binding. The Egress network VLAN must match the ingress VLAN on the bound VSC (or be altered by a switch between the AP and the controller to do so) otherwise traffic from the AP will not reach the controller. Traffic exits the controller on the user-assigned VLAN, which overrides any egress mapping defined on the controller's VSC.		Traffic is sent on the AP Ethernet port tagged with the VLAN specified by the Egress network in the VSC binding. The Egress network VLAN must match the ingress VLAN on the bound VSC (or be altered by a switch between the AP and the controller to do so) otherwise traffic from the AP will not reach the controller. Traffic exits the controller on the egress mapping defined on the appropriate VSC.
	Not defined	Active	Traffic is sent to the controller in the client data tunnel and is mapped to a VSC on the controller by SSID. It exits the controller on the egress mapping defined on the appropriate VSC.	Traffic is sent to the controller in the client data tunnel and is mapped to a VSC on the controller by SSID. It exits the controller on the user-assigned VLAN, which overrides any egress mapping defined on the controller's VSC.		Traffic is sent to the controller in the client data tunnel and is mapped to a VSC on the controller by SSID. It exits the controller on the egress mapping defined on the appropriate VSC.
		Disabled	Traffic is sent to the controller untagged via the AP Ethernet port and is mapped to a VSC on the controller by SSID. It exits the controller on the egress mapping defined on the appropriate VSC.	Traffic is sent to the controller untagged via the AP Ethernet port and is mapped to a VSC on the controller by SSID. It exits the controller on the user-assigned VLAN, which overrides any egress mapping defined on the controller's VSC.		Traffic is sent to the controller untagged via the AP Ethernet port and is mapped to a VSC on the controller by SSID. It exits the controller on the egress mapping defined on the appropriate VSC.

<table>
<tr><th rowspan="3">VSC type</th><th rowspan="3">Egress network in VSC binding</th><th rowspan="3">Client data tunnel</th><th rowspan="3">User-assigned VLAN is not assigned via RADIUS or local user accounts</th><th colspan="3">User-assigned VLAN is assigned via RADIUS or local user accounts</th></tr>
<tr><th rowspan="2">User-assigned VLAN exists on AP or controller</th><th colspan="2">User-assigned VLAN does not exist on AP or controller</th></tr>
<tr><th>VLAN ID</th><th>VLAN name</th></tr>
<tr><td rowspan="2">Non-access-controlled</td><td>Defined</td><td>Does not apply.</td><td>Traffic is sent on the AP Ethernet port tagged with the VLAN specified by the Egress network in the VSC binding.</td><td colspan="2">The Egress network setting in the VSC binding is ignored.
Traffic is sent on the AP Ethernet port tagged with the user-assigned VLAN.</td><td rowspan="2">The user is disconnected.</td></tr>
<tr><td>Not defined</td><td>Does not apply.</td><td>Traffic is sent on the AP Ethernet port untagged.</td><td colspan="2">Traffic is sent on the AP Ethernet port tagged with the user-assigned VLAN.</td></tr>
</table>

Binding to a VSC that has *Wireless mobility* and *Mobility traffic manager* enabled

<table>
<tr><th rowspan="3">Egress network in VSC binding</th><th rowspan="3">User-assigned VLAN is not assigned via RADIUS or local user accounts</th><th colspan="4">User-assigned VLAN is assigned via RADIUS or local user account</th></tr>
<tr><th colspan="2">User-assigned VLAN exists in the mobility domain</th><th colspan="2">User-assigned VLAN does not exist in the mobility domain</th></tr>
<tr><th>VLAN ID</th><th>VLAN name</th><th>VLAN ID</th><th>VLAN name</th></tr>
<tr><td>Defined</td><td>Assign the Egress network defined in the VSC binding as the user’s home network.</td><td>The Egress network setting in the VSC binding is ignored.
The first network that is found with the same VLAN ID specified in the user-assigned VLAN is assigned as the user’s home network.</td><td>The Egress network setting in the VSC binding is ignored.
The VLAN name contained in the user-assigned VLAN is assigned as the user’s home network.</td><td rowspan="2">Use the fallback setting defined by the VSC option <b>If no matching network is assigned</b> (either block user or consider the user at home).</td><td rowspan="2">The AP blocks the user from accessing the network.</td></tr>
<tr><td>Not defined</td><td>Use the fallback setting defined by the VSC option <b>If no matching network is assigned</b> (either block user or consider the user at home).</td><td>The first network that is found with the same VLAN ID specified in the user-assigned VLAN, is assigned as the user’s home network.</td><td>The VLAN name contained in the user-assigned VLAN is assigned as the user’s home network.</td></tr>
</table>

Binding to a VSC that has *Wireless mobility* and *Subnet-based mobility* enabled

Egress network in VSC binding	User-assigned VLAN is not assigned via RADIUS or local user accounts	User-assigned VLAN is assigned via RADIUS or local user account		
		User-assigned VLAN exists in the mobility domain	User-assigned VLAN does not exist in the mobility domain	
			VLAN ID	VLAN name
Defined.	The IP address of the user is compared against the list of home subnets defined for the AP to determine if the user is at home or roaming. If the user is at home, traffic is sent on the AP Ethernet port tagged with the VLAN specified by the Egress network in the VSC binding. If the user is roaming, traffic is tunneled to the users home subnet within the mobility domain, where it egresses tagged with the VLAN specified by the Egress network in the VSC binding.	The IP address of the user and the VLAN ID are compared against the list of home subnets defined for the AP to determine if the user is at home or roaming. (Both the IP and VLAN must match the home subnet.) If the user is at home, traffic is sent on the AP Ethernet port tagged with the user-assigned VLAN. The Egress network in the VSC binding is ignored. If the user is roaming, traffic is tunneled to the users home network within the mobility domain, where it will egress tagged with the user-assigned VLAN.	The Egress network setting in the VSC binding is is ignored. User is considered to be at home and traffic is sent on the AP's Ethernet port tagged with the user-assigned VLAN.	The user is disconnected.
Not defined.	The IP address of the user is compared to the IP address of the AP's Ethernet port to determine if the user is at home or roaming. If the user is at home, traffic is sent on the AP Ethernet port untagged. If the user is roaming, traffic is tunneled to the users home network within the mobility domain, where it will egress untagged.	The IP address of the user and the VLAN ID are compared against the list of home subnets defined for the AP to determine if the user is at home or roaming. (Both the IP and VLAN must match the home subnet.) If the user is at home, traffic is sent on the AP Ethernet port tagged with the user-assigned VLAN. If the user is roaming, traffic is tunneled to the users home network within the mobility domain, where it will egress tagged with the user-assigned VLAN.	User is considered to be at home and traffic is sent on the AP's ethernet port tagged with the user-assigned VLAN.	

Terms used in the tables

- **Egress network in VSC binding:** This column refers to the Egress network option that can be configured when an AP group is bound to a VSC. The egress network can be used to assign a specific VLAN. How this VLAN is applied to the routing of traffic is illustrated by the tables.
- **Client data tunnel:** The client data tunnel can be used by an AP to transport wireless user traffic to the controller. The client data tunnel is automatically used if the network path between an AP and the controller traverses a router. In the case where the AP is on the same layer 2 subnet as the controller, the client data tunnel is not automatically used, but can be manually activated by enabling the **Always tunnel client traffic option** on the VSC configuration page. Available on access-controlled VSCs only.
- **User-assigned VLAN is not assigned via RADIUS or local user accounts:** This column indicates what happens when a user-assigned VLAN attribute is not assigned via RADIUS or via a local user account or account profile.
- **User-assigned VLAN exists in the mobility domain:** This column indicates what happens when a user-assigned VLAN attribute is assigned via RADIUS or via a local user account or account profile, and if that VLAN (or network) is defined within the mobility domain. In some cases the behavior is different if the VLAN attribute specifies a network profile name or an actual VLAN ID (number).
- **User-assigned VLAN does not exist in the mobility domain:** This column indicates what happens when a user-assigned VLAN attribute is assigned via RADIUS or via a local user account or account profile, and if that VLAN (or network) is not defined within the mobility domain. In some cases the behavior is different if the VLAN attribute specifies a network profile name or an actual VLAN ID (number).

Traffic flow examples

The following examples illustrate some typical VLAN scenarios using the information from the tables in section *Traffic flow for wireless users on page 7-6*.

To help cross-reference with the tables, all configuration settings are shown using the headings and descriptions from the tables.

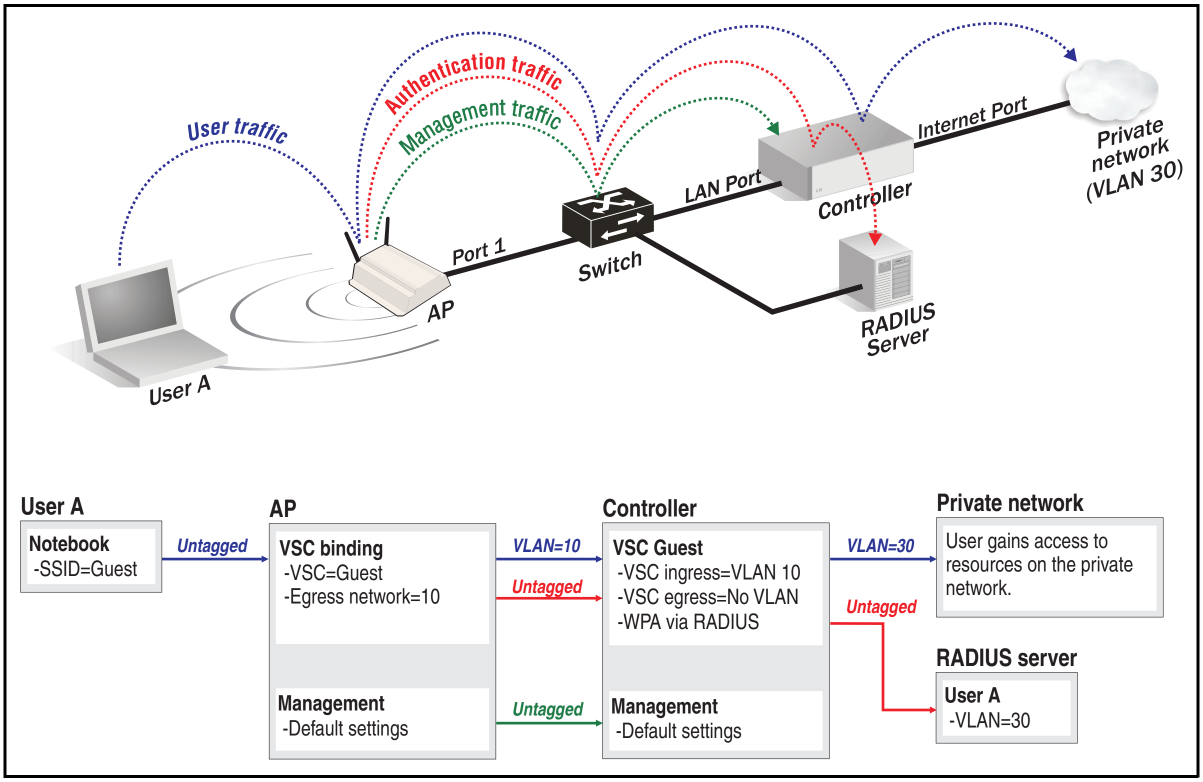
Example 1: Overriding the VSC egress on a controller with a user-assigned VLAN

This example illustrates how a user-assigned VLAN can override a VSC egress setting on the controller.

Configuration summary

- **APs are bound to a VSC that has Wireless mobility disabled**
- **VSC type:** Access controlled

- **Egress network in VSC binding:** Defined VLAN = 10
- **Client data tunnel:** Disabled
- **User-assigned VLAN is assigned via RADIUS or local user accounts:** Assigned VLAN = 30
- **User-assigned VLAN exists on AP or controller:** VLAN 30 is defined on the controller's Internet port
- **Result:** Traffic is sent on the APs Ethernet port tagged with the VLAN specified by the Egress network in the VSC binding. The Egress network VLAN must match the ingress VLAN on the bound VSC (or be altered by a switch between the AP and the controller to do so) otherwise traffic from the AP will not reach the controller. Because the is a non-access controlled VSC, the user-assigned VLAN applies only on the controller. Therefore, user traffic exits the controller on the user-assigned VLAN, which overrides the VSC egress mapping (no VLAN) defined for the VSC Guest.



In this example, the egress network in the AP's VSC binding is set to 10. The AP sends user wireless traffic to the controller on VLAN 10. This traffic is picked up by the controller's VSC with ingress set to 10.

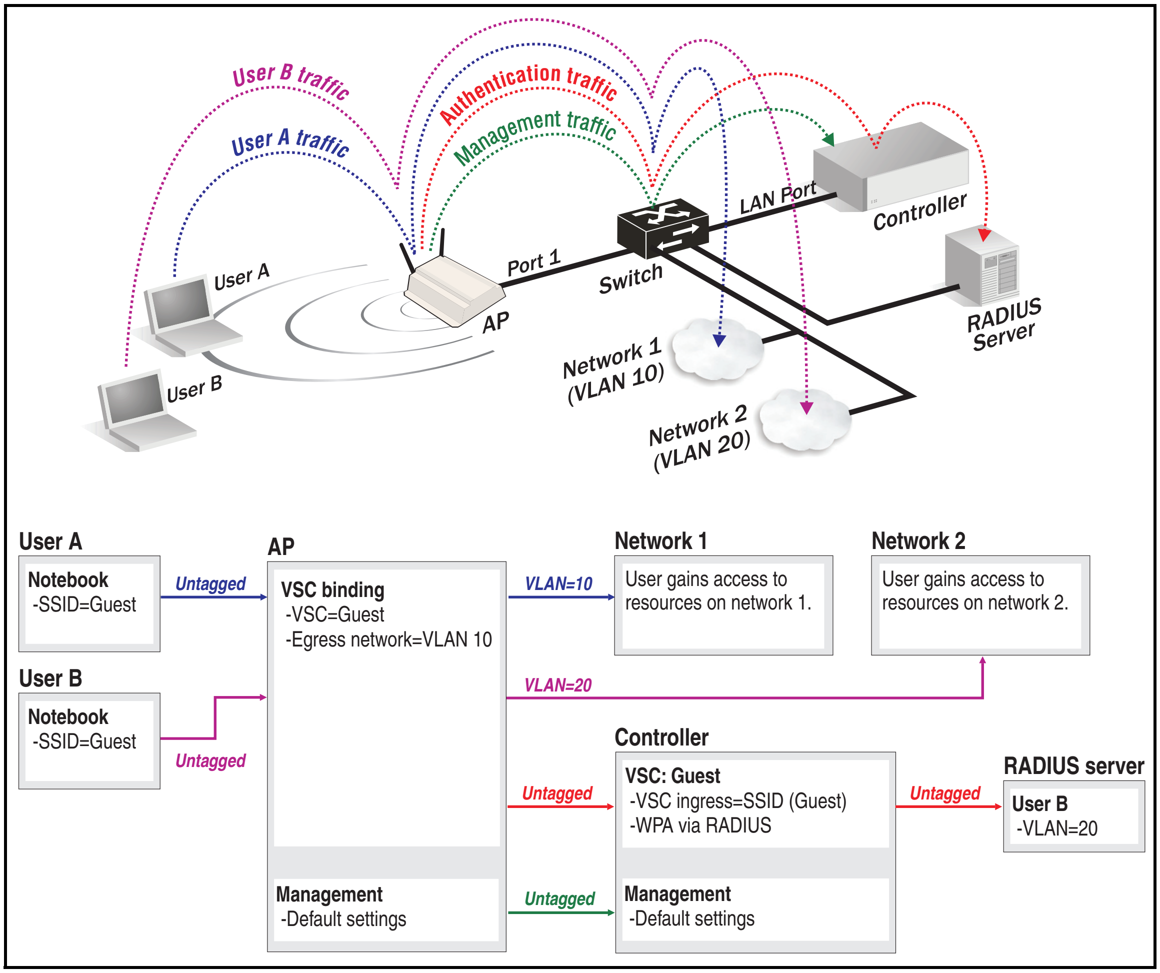
A VLAN of 30 is assigned to the user via their RADIUS account, which overrides the egress setting for the VSC on the controller. As a result, the user's traffic exits the controller on VLAN 30, which is mapped to the controller's Internet port.

Example 2: Overriding the egress network in a VSC binding with a user-assigned VLAN

In this scenario, a non-access-controller VSC is used to illustrate how a user-assigned VLAN can override the egress network defined for a VSC binding.

Configuration summary

- **APs are bound to a VSC that has Wireless mobility disabled**
- **VSC type:** Non-access-controlled
- **Egress network in VSC binding:** Defined VLAN = 10
- **Client data tunnel:** Disabled
- **User-assigned VLAN is assigned via RADIUS or local user accounts:** No VLAN is assigned to User A. A VLAN of 20 is assign to User B.
- **User-assigned VLAN exists on AP or controller:** Not applicable
- **Result:**
  - User A: The Egress network setting in the VSC binding is used. Traffic is sent on the APs Ethernet port tagged with VLAN 10.
  - User B: The Egress network setting in the VSC binding is ignored. Traffic is sent on the APs Ethernet port tagged with the user-assigned VLAN (20).



In this example, the AP is bound to an non-access-controlled VSC. User A illustrates default behavior. User B illustrates how to override the default behavior with an user-assigned VLAN.

- **User A** does not have a VLAN assigned via RADIUS, so traffic from this user exits the AP's Ethernet port on the egress network (VLAN 10) defined in the VSC binding, allowing it to reach the network 1.
- **User B** has a VLAN of 20 assigned via their RADIUS account, which **overrides** the egress network defined in the VSC binding. As a result, traffic from User B is sent on the AP's Ethernet port tagged with VLAN 30, allowing it to reach the network 2.

8

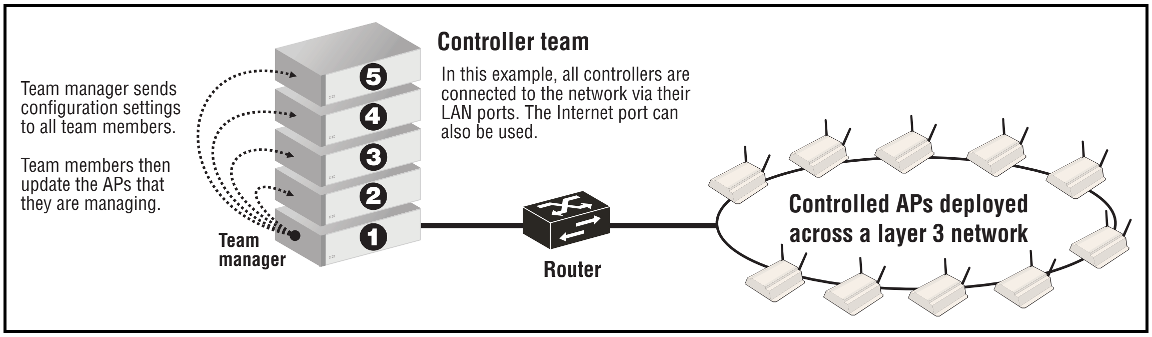
Controller teaming

Contents

Key concepts

Controller teaming enables you to easily configure and monitor multiple controllers and their access points, providing the following key benefits: centralized management and monitoring, service scalability, and redundancy in case of controller failure.

Up to five controllers can be combined into a team enabling support for up to 800 APs (four controllers x 200 APs per controller plus one additional controller for backup/redundancy). For example:


Team manager sends configuration settings to all team members.
Team members then update the APs that they are managing.
5
4
3
2
1
Team manager
Controller team
In this example, all controllers are connected to the network via their LAN ports. The Internet port can also be used.
Router
Controlled APs deployed across a layer 3 network

Centralized configuration management

Each controller that is part of a team is called a *team member*. To centralize management and control of the team, one controller is designated as the *team manager*. Configuration and monitoring of team members and their APs is performed on the team manager using its management tool. For more information, see *Team configuration on page 8-17*.

Team IP address

To simplify access to the management tool on the team manager, an IP address is assigned to the team. This is called the *team IP address*. This address is independent of the address assigned to the manager's LAN or Internet ports, and can therefore be transferred to another controller if the manager is unavailable and another team member must take over as manager.

Firmware updates

The team manager is responsible for enforcing and updating the firmware of team members. An update to the team manager firmware triggers an update of all members and their controlled APs, ensuring that the entire network is running the same firmware. The synchronization of firmware between controllers and APs alleviates any potential issue regarding compatibility.

Centralized monitoring and operation

The team manager is responsible for handling the addition and deletion of controlled APs, including newly discovered APs. It also displays status information for all team members and their APs, as well as APs directly connected to the manager. For more information, see *Viewing all team members on page 8-16*.

Redundancy and failover support

The team provides for service redundancy in case of failure. If one of the controllers in a team becomes inoperative (due to network problems, hardware failure, etc.), its APs will automatically migrate to another controller in the team allowing for continuation of services. For this to work, sufficient capacity must be available on the remaining controllers in the team to support the APs from the inoperative controller. For more information see, *Failover on page 8-22*.

Important When a controller becomes inoperative and failover occurs, all services provided by the controller are temporarily interrupted. Once failover is complete and services return, users that were connected to an access-controlled VSC must login again.

Scalability

Controller teaming enables you to scale up your wireless network as your needs increase. Simply add additional APs, controllers, and licenses to meet the required demand. Up to 800 APs are supported per team in its maximum configuration (four controllers x 200 APs per controller plus one additional controller for backup/redundancy).

Deployment considerations

Controllers/APs

- Teaming is only supported on the MSM760 and MSM765 controllers.
- A controller can only be a member of one team at a time.
- Controllers must be the same model type as the team manager.
- Up to five controllers can be combined into a team supporting up to 800 APs (four controllers x 200 APs per controller + one controller reserved for backup purposes).

Licensing

- MSM760 Controllers must have the Premium license installed to support teaming. (Licenses must be installed individually on each controller that is part of the team.) MSM765 Controllers come with this license preinstalled.
- You must install enough AP licenses to support all the APs you intend to manage with the team. When teaming is enabled, AP licenses are pooled across all controllers. See *Failover on page 8-22* for more information on how AP licenses are managed.

Networking

- The LAN and Internet ports on all team members must be configured with the same networking options (subnet, VLAN, etc.). For example, if you configure the LAN port on the manager to be on the 192.168.1.0 subnet, then all other team members must have their LAN ports on the same subnet. The LAN port and Internet port cannot be on the same subnet.

IMPORTANT: All team members must have an IP address assigned to their LAN port. *This must be done even if the LAN port is not connected or not used in your setup.*

- The DHCP server feature is not supported when controller teaming is active, therefore an external DHCP server needs to be installed to support dynamic addresses assignment to controlled APs and their users.
- APs do not have to be located on the same subnet as the team, but can be connected to the team via an L3 network. However, all APs must reach the team on the same interface (port, VLAN, etc.).
- If the APs are provisioned for controller discovery, than the APs must be provisioned to discover all controllers in the team, not just the team manager, otherwise failover is not supported.
- Multiple teams can be installed on the same subnet.
- To successfully support controller teaming, the network that connects the controllers must not block TCP port 4999 and UDP ports 4999, 38215, 51936.
- The networking settings on each controller must match. If a VLAN is configured on the Internet port of one controller, it is automatically configured on the Internet port of every other team member. The switch ports to which controllers are connected must be configured identically.

Public access

- Customization of the public access interface web content should be done via attributes retrieved from a third-party RADIUS server. If RADIUS is not available, you must manually configure each controller in the team with matching settings.
- Payment services are not supported.

Users

- Wired users are only supported via the MSM317 switch ports. Wired users cannot connect directly to a team via the LAN or Internet ports.
- The local user accounts do not support subscription plans when teaming is enabled.
- Accounting persistence is not supported.

Firmware

- When a controller becomes a member of a team, its firmware and configuration will be updated by the team manager. This means that almost all configuration settings on the controller will be lost, including any VSC definitions. You can keep a record of the settings on the controller by backing up its configuration before enabling teaming.

Limitations

The following features are not supported when teaming is enabled:

- DHCP server
- L2TP server
- PPTP server
- PPTP client
- Subscription plans
- Payment services
- Accounting persistence
- Billing records
- Ingress VLAN on a VSC and untagged traffic on the LAN port (All APs use the client data tunnel to send traffic to the team.)
- Wired client connected to the LAN port on a controller
- sFlow
- LLDP dynamic naming

Creating a team

The following list is an overview of the key steps you need to execute when creating a controller team. The *Configuration example on page 8-6* shows how to apply these steps to actually create a team.

- **Configure connectivity:** Configure each controller that will be part of the team with a static IP address on the same subnet. Make sure to define a DNS server and default gateway on each controller.
- **Configure DHCP services:** Configure a third-party DHCP server to handle address assignment for APs and wireless users. (The DHCP server feature on all team members is automatically disabled when the teaming is enabled.) In addition, you may need to enable DHCP relay on the team, depending on your network topology, to forward DHCP requests to the third-party DHCP server
- **Install licenses:** Install the Premium licenses on each controller and the required number of AP licenses. (MSM765 controllers come with the Premium license preinstalled.) AP licenses are pooled when controllers are teamed. For more information, see *Failover on page 8-22*.
- **Configure the team:** Enable teaming on each controller by selecting **Controller >> Management > Teaming**. On the controller that will act as the team manager, set the **Team name** and **Team IP address**.
- **Authorize discovered controllers:** The first time that a controller is discovered by the team manager, it must be manually authorized by an administrator (unless the controller was manually added to the team). To authorize a discovered controller, select **Controllers >> Overview > Discovered controllers** and select **Authorize** in the **Action** column.

- **Install APs:** Connect all APs. The APs will automatically discover the team (if on the same subnet) and be synchronized with the firmware and configuration settings on the manager. If APs are installed on a different subnet than the controller, their discovery settings may need to be provisioned for them to successfully discovery the team.

About the team IP address

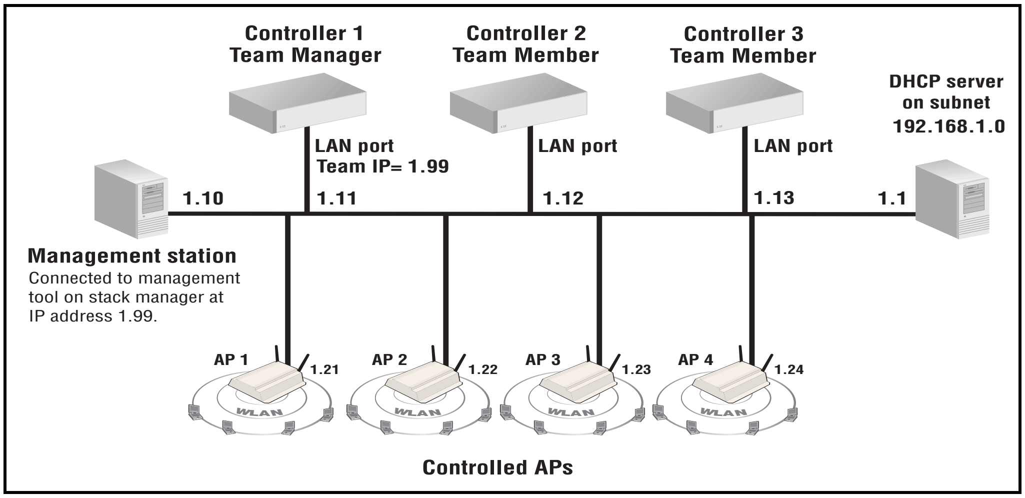
Once a team is operational, you should always use the team IP address to reach the management tool on the team manager, and not the physical address assigned to the manager. In case of failover, the team IP address will be assigned to the interim manager. This way, you will always be able to configure the team.

Important notes about the team IP address.

- The team IP address cannot be used when provisioning AP for discovery. AP must be provisioned with the actual IP addresses assigned to each team member.
- When configuring RTLS, the team IP address should be used. See *AeroScout RTLS on page 6-40*.
- When mobility discovery is configured, the team IP address should be used to identify the controller team. See *Mobility support on page 8-26*.

Configuration example

The following example illustrates the team creation process in detail using a simple topology featuring three teamed controllers and four APs. The topology for this example looks like this:



The controllers are connected to the network (192.168.1.0) via their LAN ports. Static addressing is used on each port.

The APs are also connected to the 192.168.1.0 network. Address assignment for the APs and all wireless users is provided by the DHCP server at 192.168.1.1.

Configure connectivity and licenses on each controller

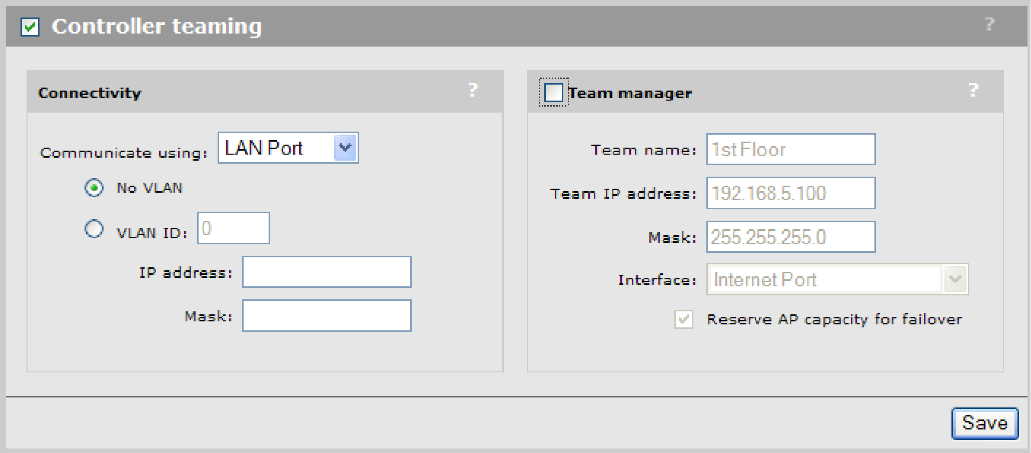
Use the management station to connect to each controller in turn and do the following:

1. Select **Controller >> Maintenance > Licenses.** Install the Premium license and any required AP licenses. For information on how to install licenses, see *Licenses on page 20-6*.
2. Select **Controller >> Network > Ports.**
3. Select **LAN port**. Set the static IP address as shown in the diagram.

Configure the team

On controller 2 and controller 3, do the following:

1. Select **Controller >> Management > Teaming.**
2. Select the **Controller teaming** checkbox.



☑ Controller teaming

Connectivity

Communicate using: LAN Port

● No VLAN

○ VLAN ID: 0

IP address:

Mask:

□ Team manager

Team name: 1st Floor

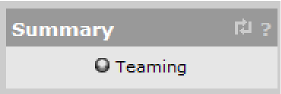
Team IP address: 192.168.5.100

Mask: 255.255.255.0

Interface: Internet Port

☑ Reserve AP capacity for failover

3. Under **Connectivity,** set **Communicate using** to **LAN port**.
4. Select **Save**.
5. The Network Tree will no longer be visible. The Summary box will show **Teaming** with a blinking gray status light. This indicates that the controller is searching for a team.



Summary

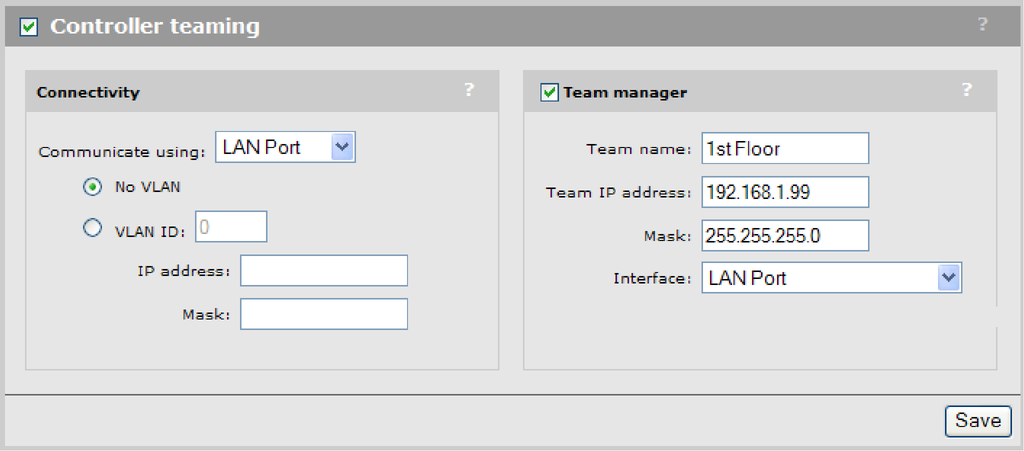
● Teaming

Once the controller successfully joins a team, the status light turns green.

On controller 1, do the following:

1. Select **Controller >> Management > Teaming.**

2. Select the **Controller teaming** checkbox.



☑ Controller teaming

Connectivity

Communicate using: LAN Port

● No VLAN

○ VLAN ID: 0

IP address:

Mask:

☑ Team manager

Team name: 1st Floor

Team IP address: 192.168.1.99

Mask: 255.255.255.0

Interface: LAN Port

3. Under **Connectivity,** set **Communicate using** to **LAN port**.

4. Select the **Team manager** checkbox, and configure the following settings under it:

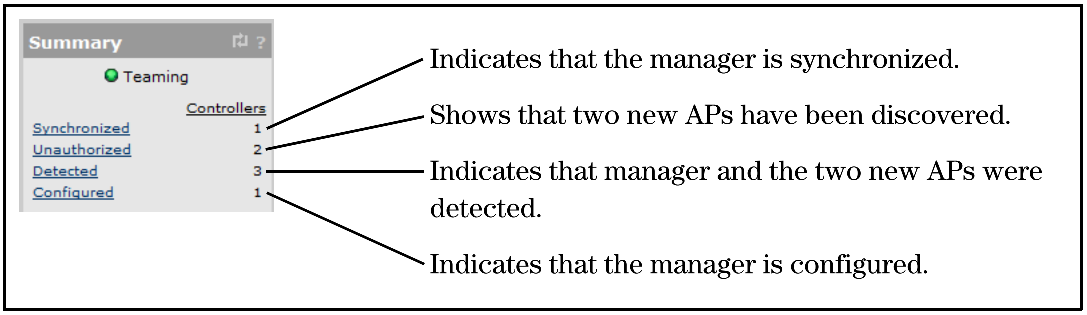
   - Set **Team name** to a name that identifies the team. This example uses **1st Floor**. The team name provides a convenient way to identify a team.
   - Set **Team IP address** to the virtual IP address that will be used to provide access to the team manager. This example uses the address **192.168.1.99.**
   - Set **Mask** to **255.255.255.0.**

     Note: If the **Team IP address** is on the same subnet as the physical address assigned to the selected **Interface**, then you must set **Mask** to match the IP mask set on the physical interface. This applies even if the physical interface is set to act as a DHCP client.

   - Set **Interface** to **LAN port.** This makes the **Team IP address** available on the LAN port.

5. Select **Save**.

6. Controller 2 and 3 will now attempt to discover the manager. Monitor the **Summary** box until you see two **Unauthorized** controllers in the list.



Summary

● Teaming

Controllers

Synchronized 1

Unauthorized 2

Detected 3

Configured 1

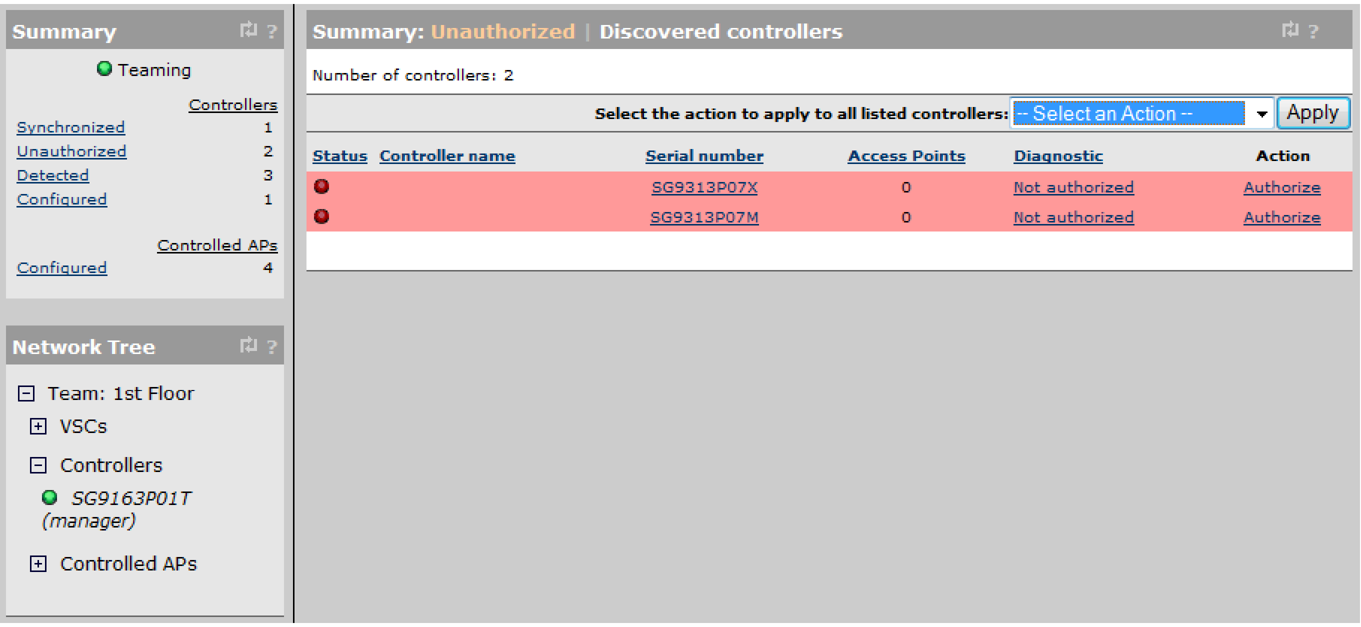
Indicates that the manager is synchronized.

Shows that two new APs have been discovered.

Indicates that manager and the two new APs were detected.

Indicates that the manager is configured.

7. Under **Network Tree**, select **Controllers** to view more detailed information about the discovery process. The two new controllers should be listed in red. Select **Authorize** in the **Action** column for each controller.



Summary

● Teaming

	Controllers
Synchronized	1
Unauthorized	2
Detected	3
Configured	1

	Controlled APs
Configured	4

Network Tree

- ⊟ Team: 1st Floor
  - ⊞ VSCs
  - ⊟ Controllers
    - ● *SG9163P01T (manager)*
  - ⊞ Controlled APs

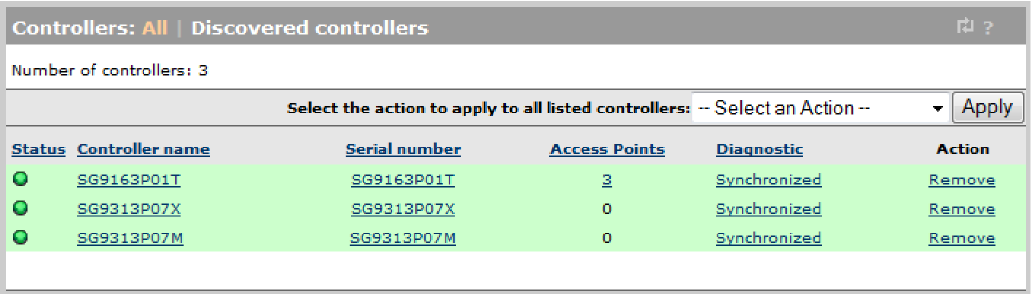
Summary: Unauthorized | Discovered controllers

Number of controllers: 2

Select the action to apply to all listed controllers: -- Select an Action -- Apply

Status	Controller name	Serial number	Access Points	Diagnostic	Action
●		SG9313P07X	0	Not authorized	Authorize
●		SG9313P07M	0	Not authorized	Authorize

8. The manager will now attempt to authorize and synchronize controllers 2 and 3. Once synchronized, their status will change to green.

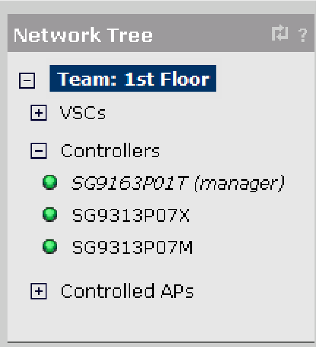


Controllers: All | Discovered controllers

Number of controllers: 3

Select the action to apply to all listed controllers: -- Select an Action -- Apply

Status	Controller name	Serial number	Access Points	Diagnostic	Action
●	SG9163P01T	SG9163P01T	3	Synchronized	Remove
●	SG9313P07X	SG9313P07X	0	Synchronized	Remove
●	SG9313P07M	SG9313P07M	0	Synchronized	Remove



Network Tree

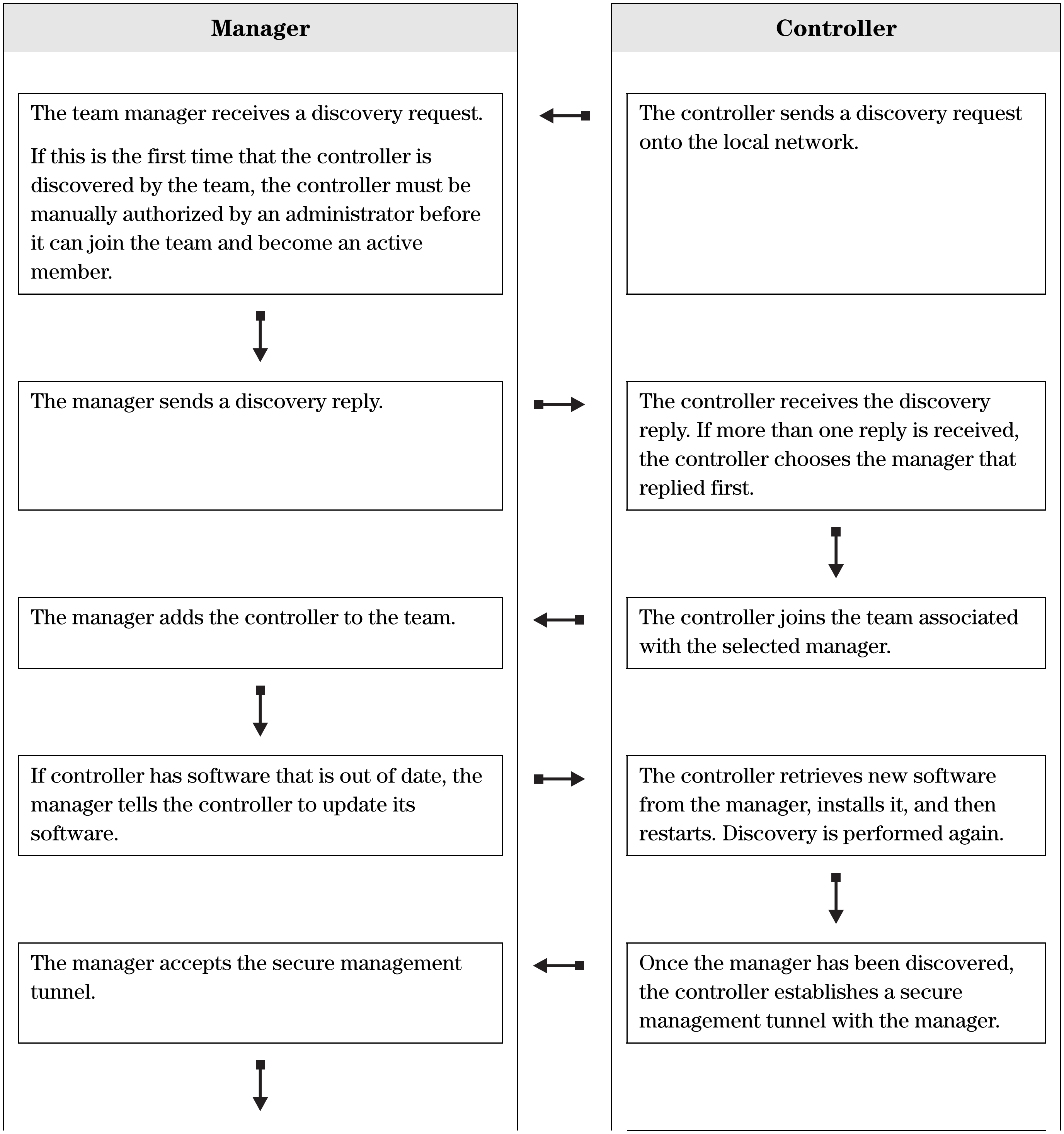
- ⊟ **Team: 1st Floor**
  - ⊞ VSCs
  - ⊟ Controllers
    - ● *SG9163P01T (manager)*
    - ● SG9313P07X
    - ● SG9313P07M
  - ⊞ Controlled APs

For more information on summary states and the network tree, see *Monitoring the discovery process on page 8-11*.

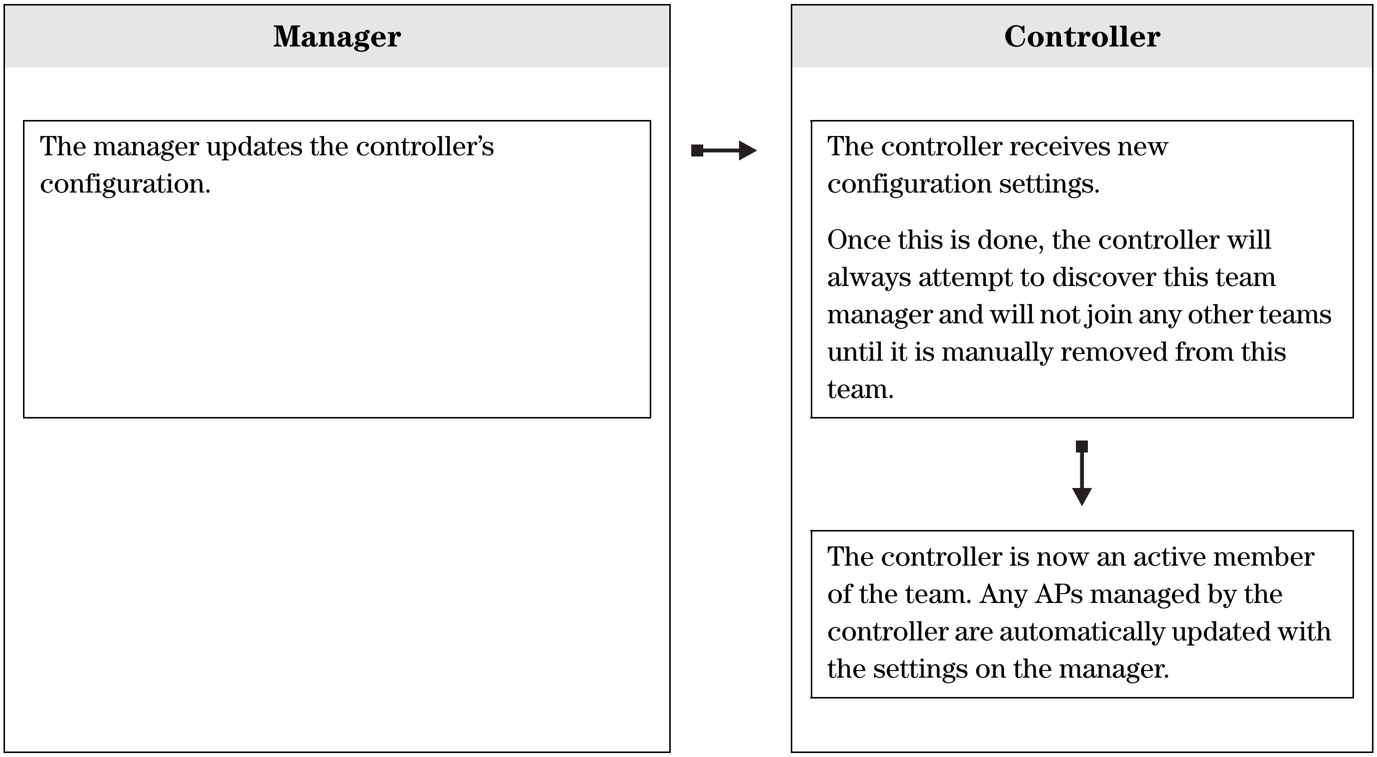
Once all members are synchronized, the team is ready for further configuration. See *Team configuration on page 8-17* for details.

Controller discovery

The following is an overview of key events that occur when a controller attempts to discover and join a team for the first time.



Manager		Controller
The team manager receives a discovery request. If this is the first time that the controller is discovered by the team, the controller must be manually authorized by an administrator before it can join the team and become an active member.	←	The controller sends a discovery request onto the local network.
The manager sends a discovery reply.	→	The controller receives the discovery reply. If more than one reply is received, the controller chooses the manager that replied first.
The manager adds the controller to the team.	←	The controller joins the team associated with the selected manager.
If controller has software that is out of date, the manager tells the controller to update its software.	→	The controller retrieves new software from the manager, installs it, and then restarts. Discovery is performed again.
The manager accepts the secure management tunnel.	←	Once the manager has been discovered, the controller establishes a secure management tunnel with the manager.



Manager

The manager updates the controller's configuration.

Controller

The controller receives new configuration settings.

Once this is done, the controller will always attempt to discover this team manager and will not join any other teams until it is manually removed from this team.

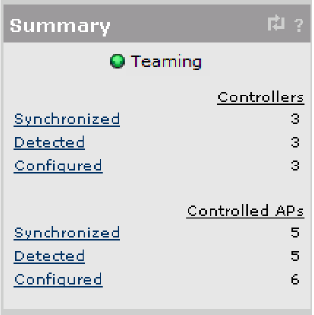
The controller is now an active member of the team. Any APs managed by the controller are automatically updated with the settings on the manager.

Monitoring the discovery process

The **Summary** box and **Network Tree** on the team manager provide an overview of the discovery process.

Summary box

The summary box provides an overview of the status of controllers and controlled APs.



Summary

● Teaming

	Controllers
Synchronized	3
Detected	3
Configured	3

	Controlled APs
Synchronized	5
Detected	5
Configured	6

Teaming light

This light indicates how the team is being managed.

- **Green:** This controller is the primary team manager.
- **Yellow:** The primary team manager has become inoperative and an interim team manager has taken over. For details, see *Failover on page 8-22*

Controllers

This section shows the number of controllers that are active in each management state. A controller may be active in more than one state at the same time. For example, a controller may be both **Detected** and **Synchronized**. Select the state name to display information about all controllers in that state.

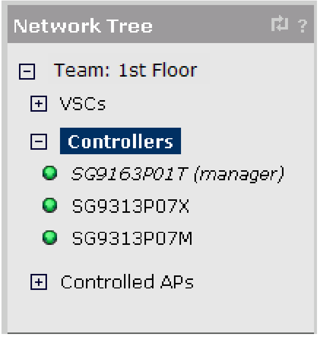
- **Configured:** These controllers are configured as part of the team.
- **Synchronized**: These controllers had their software and configuration settings successfully updated by the team manager and are fully operational.
- **Unsynchronized**: This can occur if the primary manager becomes non-functional during the synchronization process leaving one or more team members with partially updated configurations. When the interim manager takes over, it cannot update these controllers. Therefore, the solution is to promote the interim manager to become the primary manager. It can fully synchronize the configuration settings on all controllers.
- **Pending**: An action is in progress. For example, firmware or configuration may be uploading to the controller or the controller is restarting.
- **Unresponding**: These controllers have stopped sending management information to the manager. Rediscovery may re-establish the connection. If not, a network failure may have occurred or the controllers may be inoperative.
- **Unauthorized**: These controllers have not yet been authorized to join the team. Authorization must be performed manually by an administrator by selecting **Controllers >> Overview > Discovered controllers** and then selecting **Authorize** in the **Action** column.
- **Unconfigurable:** These controllers cannot be added because the team already has the maximum number of supported members. To add these controllers you must first remove one or more team members by selecting **Controllers >> Overview > Team members,** then selecting the name of the controller you want to delete and then selecting **Delete**.
- **Detected**: These controllers have sent a discovery request to the team manager and the team manager has replied.
- **Configured**: These controllers are members of the team. They may have been automatically discovered or manually added.

Controlled APs

This section lists the number of controlled APs discovered by the team. APs are grouped according to their management state. For a complete description of all management states, see *Monitoring the discovery process on page 6-13*.

Network Tree

The network tree provides access to configuration options for the team. And shows a status light for each controller.



Team: *team name*

Select **Team: [*name*]** to access configuration items that apply to all members of the team and their controlled APs. Configure these options using the main menu in the right pane.

VSC

Select the **VSCs** node to manage the virtual service communities that are defined on the team. Once you define a VSC it is automatically synchronized on all member controllers, and can be assigned (bound) to one or more controlled APs.

Status lights

A status is light is displayed for each VSC.

- **Green**: Indicates that the VSC is properly configured.
- **Red**: Indicates that the VSC has a configuration problem.

Once you define a VSC it is automatically active on the controller.

Controllers

This section lists all controllers that are members of the team. Team members are controllers that fall into one of the following categories:

- The controller was discovered on the network, authorized by an administrator, and successfully joined the team at least once.

  or

- The controller was manually added to the team by selecting **Add New Controller** on the **Overview > Configured controllers** page.

Each controller is identified by a name (which is initially set to the controller's serial number for discovered controllers). Select a controller's name to access configuration items that are specific to the controller. These configuration items are presented in the main menu in the right pane.

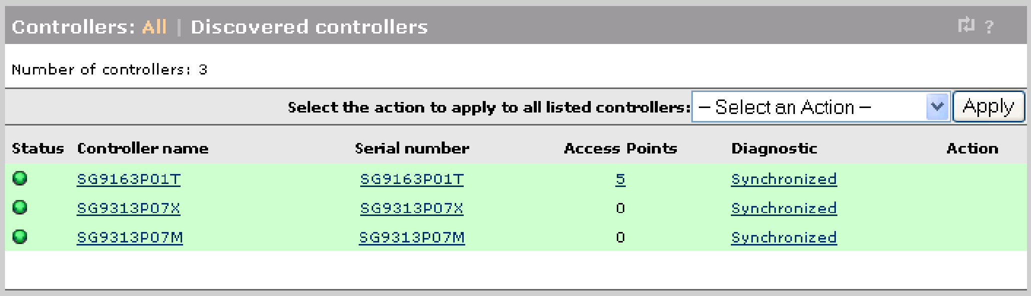
Status lights

Controllers that are part of the team are listed under Controllers in the Network Tree. The status lights provide an indication of their state as follows:

- **Green**: The controller has joined the team and its configuration is synchronized with the settings defined on the team manager. It is fully operational.
- **Red**: The controller is not functioning normally. Select **Overview > Discovered controllers** and refer to the **Diagnostic** column for details.
- **Grey flashing**: An action is pending. Select **Overview > Discovered controllers** and refer to the **Action** column for details.
- **Grey solid**: The controller is configured as a member of the team, but is currently not active.

Viewing all discovered controllers

To display information about controllers discovered by the manager, select **Controllers >> Overview > Discovered controllers**.



Controllers: All | Discovered controllers

Number of controllers: 3

Select the action to apply to all listed controllers: – Select an Action – Apply

Status	Controller name	Serial number	Access Points	Diagnostic	Action
●	SG9163P01T	SG9163P01T	5	Synchronized	
●	SG9313P07X	SG9313P07X	0	Synchronized	
●	SG9313P07M	SG9313P07M	0	Synchronized	

The **Discovered controllers** page provides the following:

- **Select the action to apply to all listed controllers**: Lets you apply the selected action to all controllers in the list. Select an action and then **Apply**.
- **Status lights**

  A status light is displayed for each controller as follows:

  - **Green**: The controller has joined the team and its configuration is synchronized with the settings defined on the team manager. It is fully operational.
  - **Red**: The controller is not functioning normally. Select **Overview > Discovered controllers** and refer to the **Diagnostic** column for details.
  - **Grey flashing**: An action is pending. Select **Overview > Discovered controllers** and refer to the **Action** column for details.
  - **Grey solid**: The controller is configured as a member of the team, but is currently not active.
- **Controller name**: Name assigned to the controller. By default, this is the controller serial number.

- **Serial number**: Unique serial number assigned to the controller at the factory. Cannot be changed.
- **Access points**: Indicates number of APs connected to the controller.
- **Diagnostic**: Indicates the status of the controller as shown in the following table.

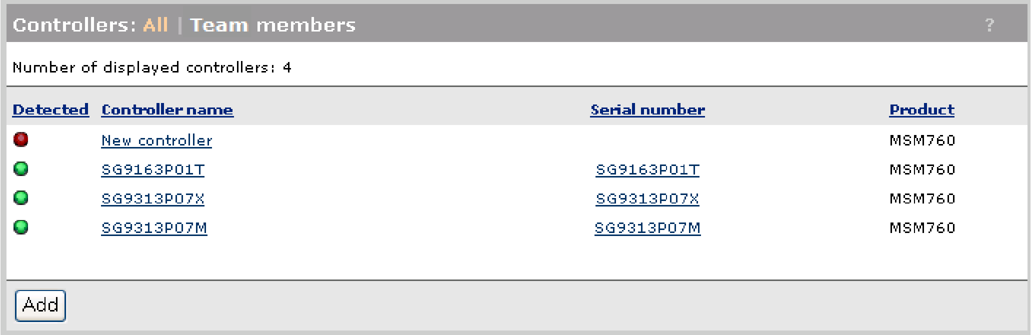
Diagnostic	Description
Detected	The controller sent a discovery request to the team manager and the team manager has replied.
Establishing tunnel	A secure management connection is being established between the team manager and the controller.
Firmware failure	New software failed to upload to the controller. The manager will retry soon.
Installing firmware	New software has been successfully uploaded to the controller. The controller will restart to activate the new software.
Not authorized	The controller has not yet been authorized to join the team. Authorization must be performed manually by an administrator by selecting **Authorize** in the **Action** column.
Not responding	The controller has stopped sending management information to the team manager. Rediscovery may re-establish the connection. If not, a network failure may have occurred or the controller may be inoperative.
Resetting configuration	The controller configuration is being reset to factory defaults. This is normal and will occur when the software version on the manager is changed or if the controller is not synchronized.
Restoring configuration	The controller is currently restoring its previous configuration settings.
Synchronized	The controller had its software and configuration settings successfully updated by the team manager and is fully operational.
Unconfigurable	The controller cannot be added because the team already has the maximum number of supported members. To add the controller you must first remove one or more team members.
Unsupported product	The product type of the controller is not supported on this team. All controllers must have the same product type as the team manager.

Diagnostic	Description
Uploading configuration	Configuration settings are currently being sent to the controller.
Uploading firmware	The team manager is uploading new software to the controller. Wait until the operation completes.
Validating capabilities	The capabilities of the controller are being identified by the team manager.
Validating configuration	The team manager is waiting for the controller to send its configuration.
Validating firmware	The team manager is waiting for the controller to send its software version number.
Waiting for acceptance	The controller has been authorized by the team manager. However, the controller has not yet decided to join this team. (If multiple managers replied to the controller discovery request, the controller may choose to connect with another team.)

- **Action**: Indicates the recommended administrative action to be taken to resolve a diagnostic condition.

Viewing all team members

To display information about controllers that are members of the team, select **Controllers >> Overview > Team members**.



Number of displayed controllers: 4

Detected	Controller name	Serial number	Product
🟥	New controller		MSM760
🟩	SG9163P01T	SG9163P01T	MSM760
🟩	SG9313P07X	SG9313P07X	MSM760
🟩	SG9313P07M	SG9313P07M	MSM760

Team members are controllers that fall into one of the following categories:

- The controller was discovered on the network, authorized by an administrator, and successfully joined the team at least once.
- The controller was manually added to the team by selecting **Add New Controller** on the **Overview > Configured controllers** page.

Select the title of a column to sort the table according to the values in the column.

The **Team members** page provides the following information:

- **Number of controllers**: Number of controllers that are configured as members of the team.
- **Detected**: Status light icon indicating if the controller has been discovered on the network.
  - **Green:** The controller has been discovered on the network and is listed on the **Overview > Discovered controllers** page, where more information is provided about the controller.
  - **Red:** The controller was manually added to the team, but it has never been discovered and successfully joined the team.
- **Controller name**: Name assigned to the controller. Select the name to configure controller settings.
- **Serial number**: Serial number assigned to the controller. Select the name to configure controller settings.
- **Product**: Product name of the controller.

Team configuration

Once a team is operational, configuration and management of VSCs and controlled APs occurs via the team manager, using the **VSC** and **Controlled APs** options in the Network Tree. Configuration of these elements is the same as during non-teamed operation. Refer to *Chapter 5: Working with VSCs* and *Chapter 6: Working with controlled APs* for more information.

Configuration settings for the team members however, can occur at three different levels:

- **Team:** These are global configuration settings that are defined using the management tool on the team manager and are synchronized on all team members. Most team configuration settings fall into this category.
- **Controller:** The team manager provides a separate configuration menu for each controller in a team, including the team manager. This allows individual settings specific to a controller to be defined.
- **Local:** The management tool on each controller can also be accessed directly to define any options that are not directly configurable using the team manager. For example, some connectivity settings must be defined locally on each controller.

Accessing the team manager

To reach the management tool on the team manager, you should always point your browser to the team IP address, and not the physical address assigned to the manager. In case of failover, the team IP address will be assigned to the interim manager. This way, you will always be able to configure the team.

Team configuration options

This section describes the configuration options available on the team manager.

When you select **Team** in the Network Tree, the menu in the right pane presents all configuration options that are common to all team members. Any settings that you make using this menu are synchronized on all team members.

The available options on this menu are identical to what you would see on a non-teamed controller, except for a few options that are not supported in teaming mode, or if supported, must be defined individually on each controller. On the team manager, these settings can be defined by selecting the manager under **Controller**. Settings for team members must be defined by directly accessing their management tools.

The following table lists the configuration options that are affected when teaming is active.

Configuration option	Notes
Network > Ports page	The **Port configuration** option is not available at the team level. VLAN and GRE configuration options are available.
Network > Address allocation	The **DHCP server** option is not supported when teaming is enabled. The **VPN address pool** option is not supported when teaming is enabled.
Security > Certificate stores	Not available at the team level.
Security > Certificate usage	Not available at the team level.
VPN > IPSec	Not available at the team level.
VPN > L2TP server	Not supported when teaming is enabled.
VPN > PPTP server	Not supported when teaming is enabled.
VPN > PPTP client	Not supported when teaming is enabled.
Authentication > Active Directory	The **General** and **Join** options are not available at the team level.

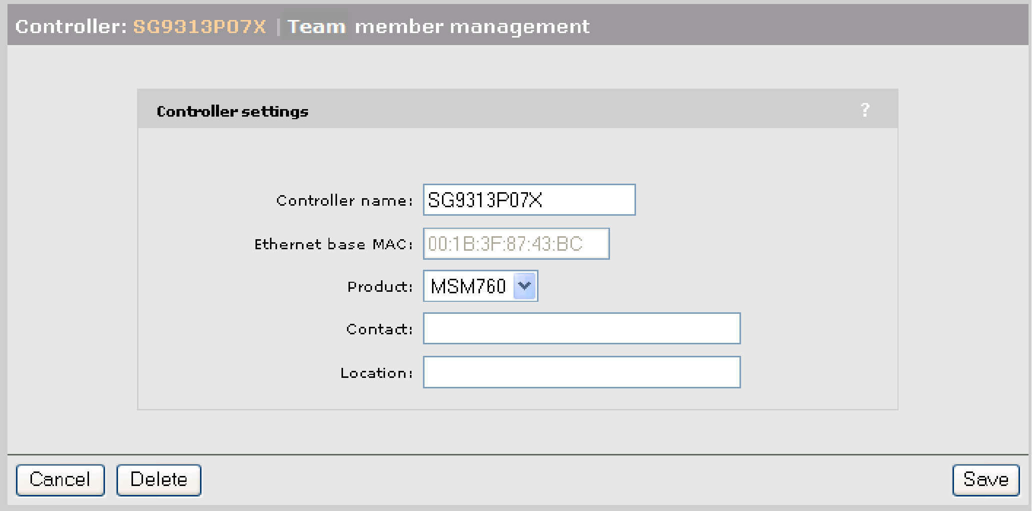
Configuration option	Notes
Public Access > Web content	The **Site file archive**, **FTP server**, and **Current site files** options are not available at the team level.
Public Access > Attributes	New attributes cannot be added to the **Configured attributes** table at the team level.
Users > Subscription plans	Feature not supported when teaming is enabled.
Users > Accounting persistence	Feature not supported when teaming is enabled.
Management > Teaming	Not available at the team level.
Status	Not available at the team level.
Tools > IPSec	Not available at the team level.
Tools > System tools	Not available at the team level.
Tools > Network trace	Not available at the team level.
Tools > sFlow	Not supported when teaming is enabled.
Maintenance > Registration	Not available at the team level.
Maintenance > Licenses	Not available at the team level.

Removing a controller from a team

To remove a controller from a team, do the following:

Remove the controller from the team

1. Under **Controllers**, select a team member.
2. In the right pane, select **Device management.**



Controller: SG9313P07X | Team member management

Controller settings

Controller name: SG9313P07X

Ethernet base MAC: 00:1B:3F:87:43:BC

Product: MSM760

Contact:

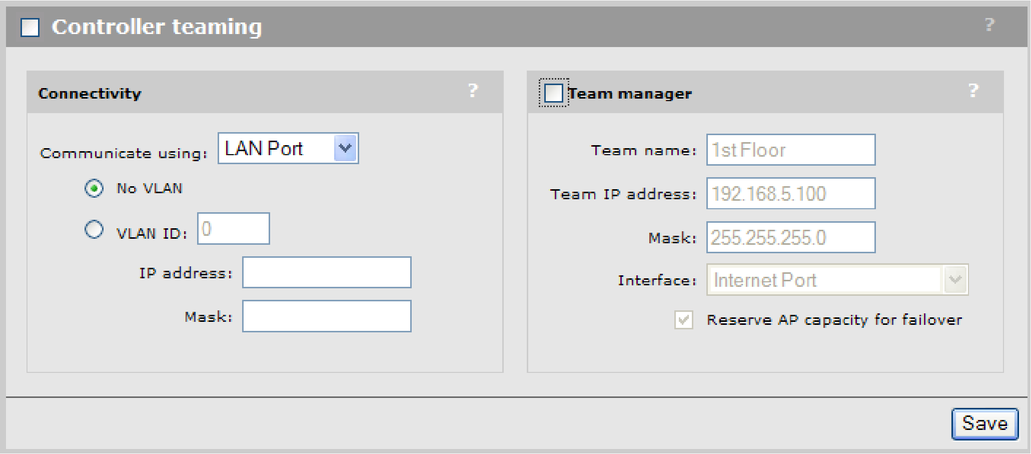
Location:

3. Select **Delete**.

4. Select **Save**.

Disable teaming on the controller

1. Open the management tool directly on the controller.
2. Select **Management > Teaming**.



□ Controller teaming

Connectivity

Communicate using: LAN Port

● No VLAN

○ VLAN ID: 0

IP address:

Mask:

□ Team manager

Team name: 1st Floor

Team IP address: 192.168.5.100

Mask: 255.255.255.0

Interface: Internet Port

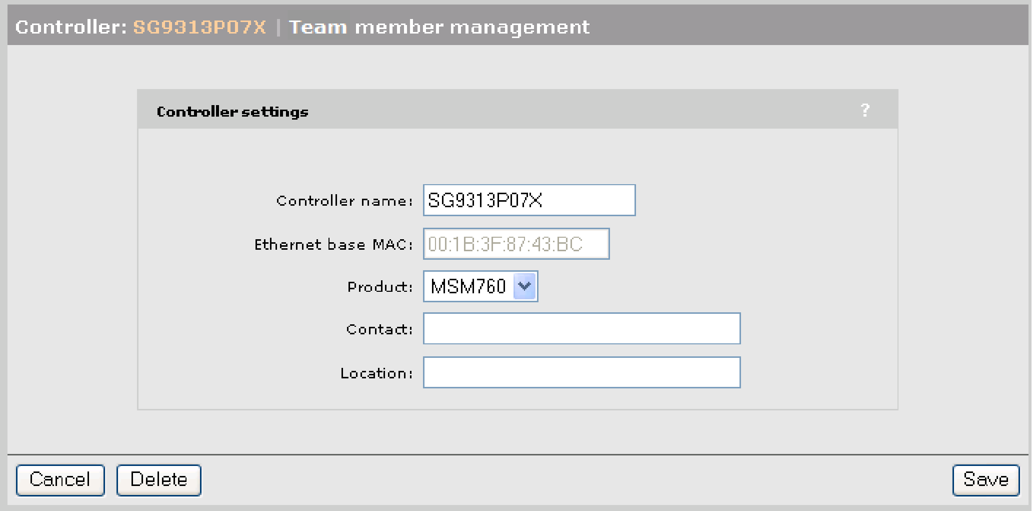
☑ Reserve AP capacity for failover

3. Disable the **Controller teaming** option.
4. Select **Save**.

Editing team member settings

To change settings for a team member:

1. Under **Controllers**, select a team member.
2. In the right pane, select **Device management.**



Controller: SG9313P07X | Team member management

Controller settings

Controller name: SG9313P07X

Ethernet base MAC: 00:1B:3F:87:43:BC

Product: MSM760

Contact:

Location:

3. Change settings as required. Note that the **Ethernet base MAC** address cannot be changed. To change the MAC address you must delete the controller and then add it again.

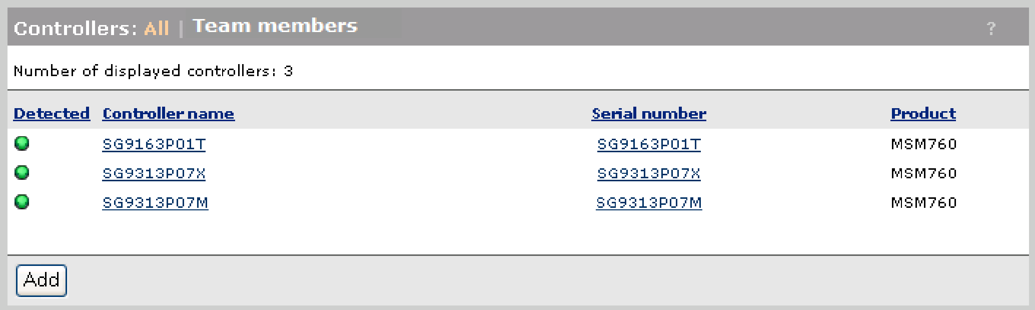
4. Select **Save**.

Manually adding a controller to a team

Instead of using the automatic discovery to find controllers and add controllers to the team, you can manually preconfigure one or more controllers as team members. The main advantages of doing this is that manually added controllers do not have to be manually authorized the first time they are discovered. Instead, they automatically become active team members.

To manually add a controller:

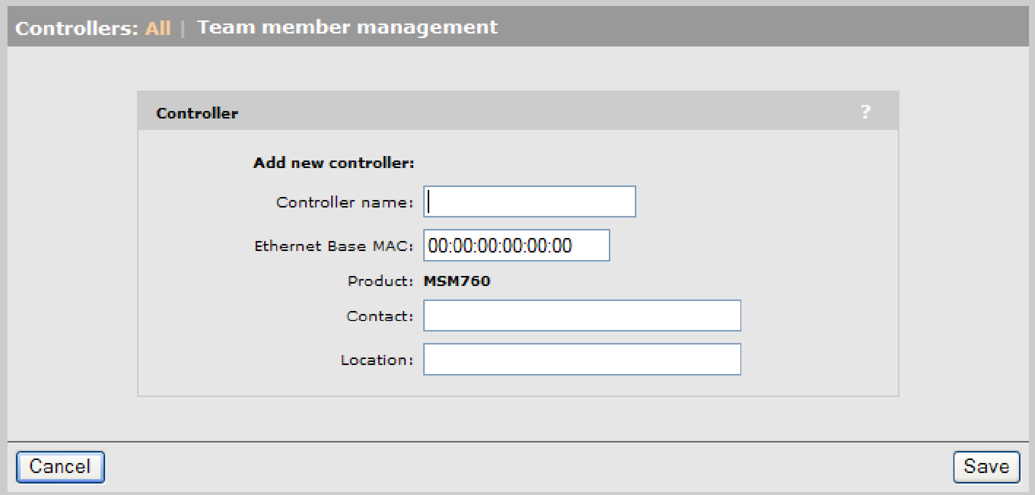
1. Select **Controllers >> Overview > Team members**.



Number of displayed controllers: 3

Detected	Controller name	Serial number	Product
●	SG9163P01T	SG9163P01T	MSM760
●	SG9313P07X	SG9313P07X	MSM760
●	SG9313P07M	SG9313P07M	MSM760

2. Select **Add.**



Add new controller:

Controller name:

Ethernet Base MAC: 00:00:00:00:00:00

Product: MSM760

Contact:

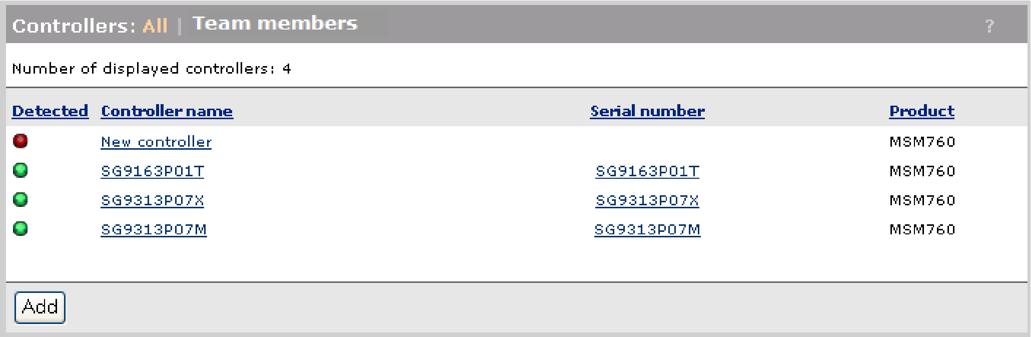
Location:

3. Define settings as follows:

- **Controller name:** Specify a name to identify the controller.
- **Ethernet base MAC:** Displays the MAC address of the controller. This value cannot be changed once the controller information is saved.
- **Product:** Select the product type of the controller.
- **Contact:** Specify contact information for the controller.
- **Location:** Specify the location where the controller is installed.

4. Select **Save**.

5. The new controller will appear in the team members list with a red status light until it is discovered on the network.



Controllers: All | Team members ?

Number of displayed controllers: 4

Detected	Controller name	Serial number	Product
🔴	New controller		MSM760
🟢	SG9163P01T	SG9163P01T	MSM760
🟢	SG9313P07X	SG9313P07X	MSM760
🟢	SG9313P07M	SG9313P07M	MSM760

Discovery of a controller team by controlled APs

For a complete discussion of controller discovery, see *Discovery of controllers by controlled APs*.

Failover

During normal operation, the team manager and team members are in continuous contact to ensure the integrity of the team. This allows for quick detection of an inoperative or unreachable team member, and implementation of failover procedures to ensure continuity of network services.

Note When a team member becomes inoperative and failover occurs, all services provided by the failed controller are temporarily interrupted. Once failover is complete and services return, users that were connected to an access-controlled VSC on this controller must login again.

Supporting N + N redundancy

A controller team can be configured to provide different levels of redundancy, from N + 1 up to N + 3. Use the following formula to calculate the number of team members you will need based on the number of APs that you want to deploy and the required level of redundancy.

Required team members = (*APs* / 200) + *Redundancy_level*

(If there is a remainder after performing the division, round up.)

Where:

- *APs* is the total number of APs you want to deploy. You must buy one license for each controlled AP. Although licenses are installed on individual team members, licenses are pooled across the entire team and are automatically re-allocated when a team member becomes inoperative.
- *Redundancy_level*: This is the number of redundant controllers that you want to support: 1, 2, or 3.

For example:

Number of APs you want to deploy	**APs / 200**	**Number of team members required to support redundancy**		
		N + 1	**N + 2**	**N + 3**
120	.6	2	3	4
200	1	2	3	4
400	2	3	4	5
440	2.2	4	5	-
520	2.6	4	5	-
600	3	4	5	-
800	4	5	-	-

Another way to look at it is as follows:

Number of team members	**Maximum AP licences that can be installed**	**Maximum APs you can deploy to ensure redundancy**		
		N + 1	**N + 2**	**N +3**
2	400	200	-	-
3	600	400	200	-
4	800	600	400	200
5	800	800	600	400

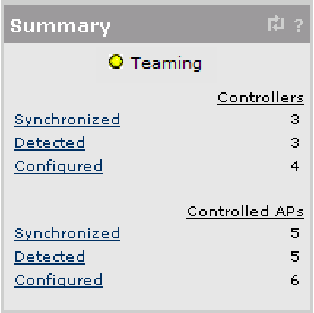
Note A team supports a maximum of 800 APs and 5 team members.

Primary team manager failure

The controller that is designated as the team manager on the **Controllers > [*team-manager*] >> Management > Teaming page** is called the primary team manager.

If the primary team manager becomes inoperative, an interim team manager is automatically selected by the existing team members. The interim manager assumes the team IP address and all management functions until the primary team manager returns, with the following limitation: the interim manager cannot modify the configuration or update the firmware for members. This is done to avoid the situation where configuration changes made by interim manager are undone by the primary manager when it comes back online.

When an interim manager is active, the **Teaming** status light in the **Summary** box will be yellow.



Summary

● Teaming

	Controllers
Synchronized	3
Detected	3
Configured	4

	Controlled APs
Synchronized	5
Detected	5
Configured	6

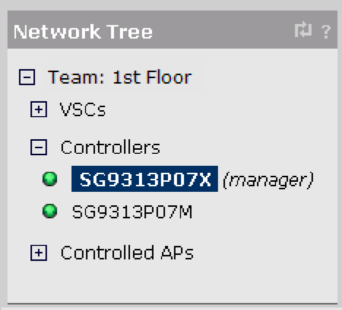
All configurable settings on the menus in the right pane will be grayed out. Status information however, will be visible.

Replacing the team manager

If the primary team manager has failed and will not be returning, you can promote the interim manager to primary so that configuration options will be available.

Important Once you promote the interim manager to primary manager, you **cannot** return the old team manager to the team without changing its configuration so that it becomes a team member. Only one manager is supported per team.

1. Under **Controllers**, select the team manager (which is now the interim manager).

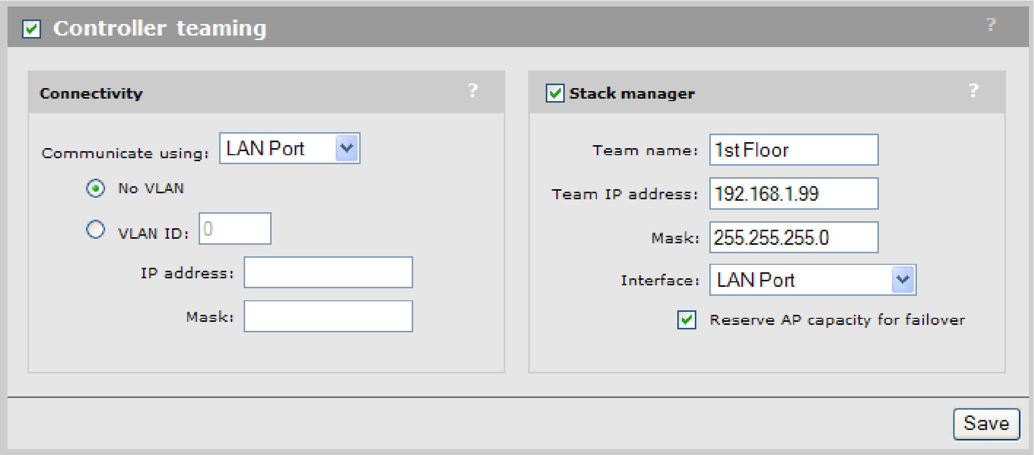


Network Tree

⊟ Team: 1st Floor
⊞ VSCs
⊟ Controllers
● SG9313P07X *(manager)*
● SG9313P07M
⊞ Controlled APs

2. In the right pane, select **Management > Teaming.**

3. Enable the **Team manager** option. The settings for this option should already be defined with the values that were set on the primary team manager.



☑ Controller teaming

Connectivity

Communicate using: LAN Port

● No VLAN

○ VLAN ID: 0

IP address:

Mask:

☑ Stack manager

Team name: 1st Floor

Team IP address: 192.168.1.99

Mask: 255.255.255.0

Interface: LAN Port

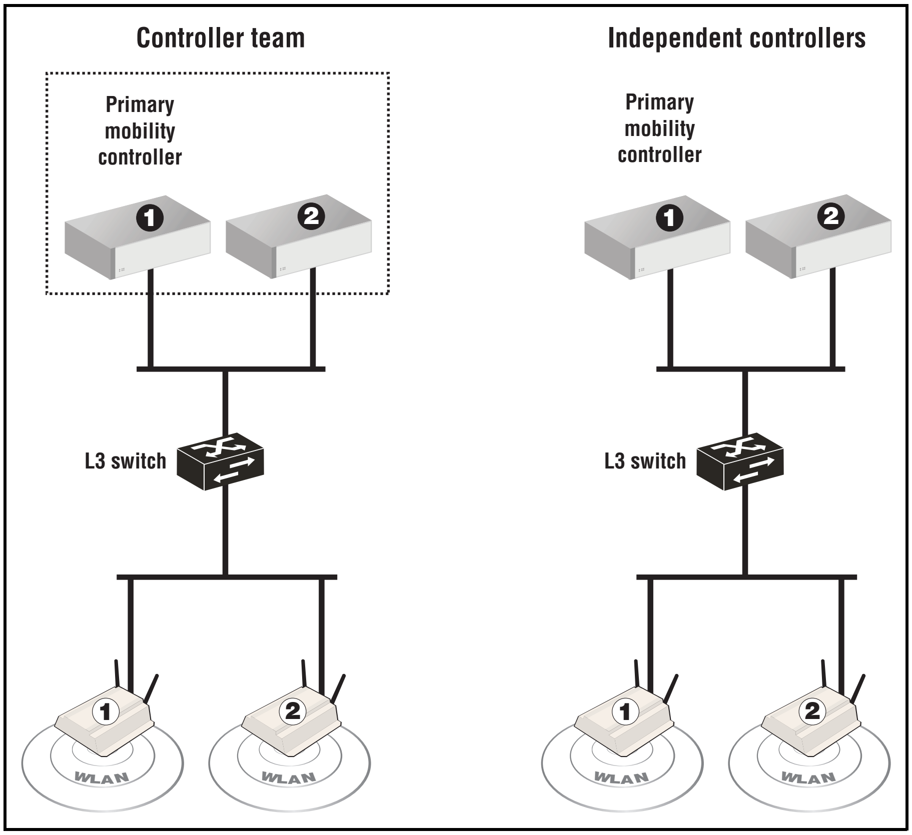
☑ Reserve AP capacity for failover

4. Select **Save**.

Mobility support

Mobility support when controller teaming is active is very similar to mobility support on non-teamed controllers. This section discusses the differences and configuration issues involved. For an explanation of mobility concepts used in this section, see *Chapter 9: Mobility traffic manager on page 9-1*.

The key benefit of using a team to provide a mobility solution is support for failover if the primary mobility controller becomes inoperative. The following diagram shows two identical setups, except that one is a team and the other is independent controllers.



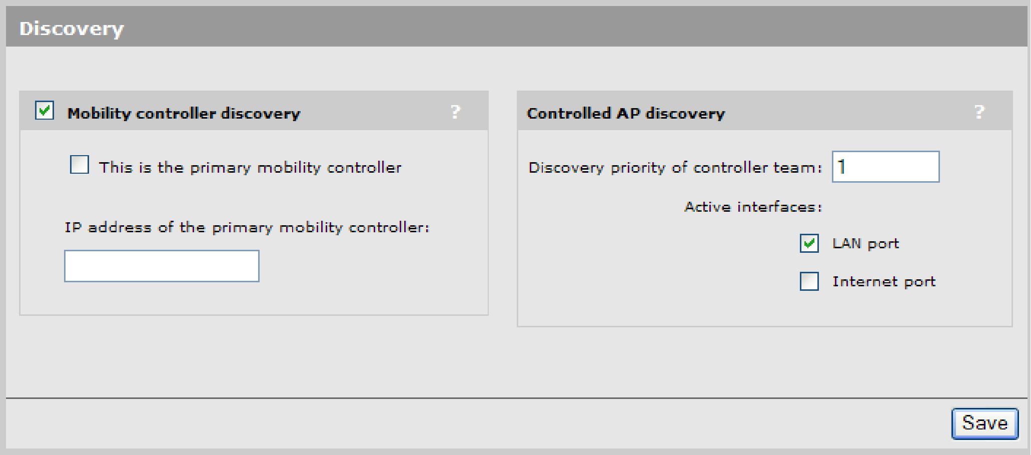
In the controller team, the primary mobility controller is also the team manager. If the team manager becomes inoperable, then controller 2 is automatically promoted to become the interim manager and assumes the role of primary mobility controller as well.

If the primary mobility controller fails in the independent controllers setup, mobility services are interrupted until you manually reconfigure controller 2 as the primary mobility controller.

Single controller team operating alone

If you have a single controller team, the mobility domain is automatically created when you do the following:

1. Start the management tool on the team manager by pointing your browser to the team IP address.
2. Select **Team: [*name*] >> Management > Device discovery**.
3. Select **Mobility controller discovery**.
4. Select **This is the primary mobility controller.**



☑ Mobility controller discovery

□ This is the primary mobility controller

IP address of the primary mobility controller:

Controlled AP discovery

Discovery priority of controller team: 1

Active interfaces:

☑ LAN port

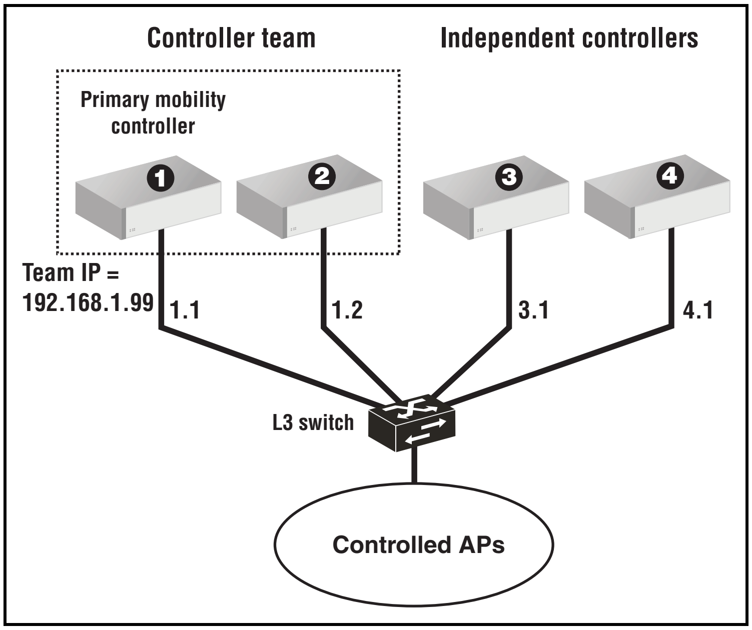
□ Internet port

5. Select **Save.**

You can now configure mobility options, such as home networks, as explained in *Chapter 9: Mobility traffic manager*.

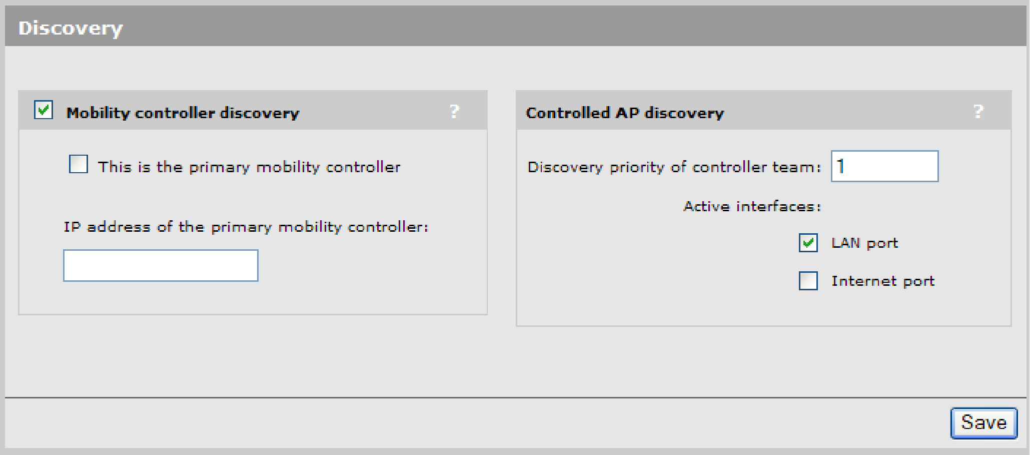
Single controller team operating with non-teamed controllers

In this type of setup, the team is configured as the primary mobility controller and the non-teamed controllers set the **IP address of primary controller** parameter to the team IP address. (In this scenario, the team IP address is defined on the LAN port of the team manager.)



Configure the team

1. Start the management tool on the team manager by pointing your browser to the team IP address.
2. Select **Team: [*name*] >> Management > Device discovery**.
3. Select **Mobility controller discovery**.
4. Select **This is the primary mobility controller**.



Discovery

☑ Mobility controller discovery

□ This is the primary mobility controller

IP address of the primary mobility controller:

Controlled AP discovery

Discovery priority of controller team: 1

Active interfaces:

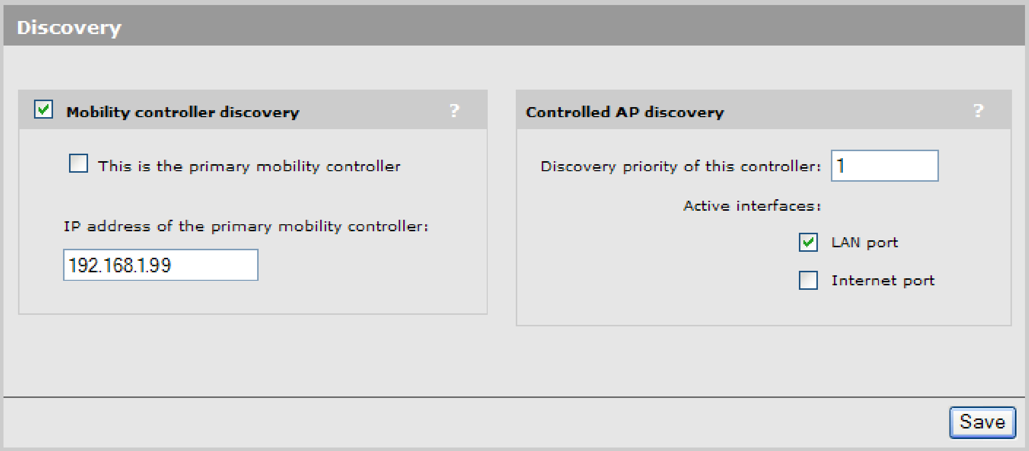
☑ LAN port

□ Internet port

5. Select **Save.**

Configure controller #3 and #4

1. Start the management tool each independent controller by pointing your browser to appropriate IP address.
2. Select **Management > Device discovery**.
3. Select **Mobility controller discovery**.
4. Set **IP address of the primary mobility controller** to **192.168.1.99**.



Discovery

☑ Mobility controller discovery

□ This is the primary mobility controller

IP address of the primary mobility controller: 192.168.1.99

Controlled AP discovery

Discovery priority of this controller: 1

Active interfaces:

☑ LAN port

□ Internet port

5. Select **Save.**

You can now configure wireless mobility options, as explained in *Chapter 9: Mobility traffic manager*.

Multiple teamed and non-teamed controllers

If you have multiple teams with or without multiple non-teamed controllers, mobility support is configured as follows: Choose one team as the primary mobility controller. On all other teams/non-teamed controllers set the **IP address of primary mobility controller** parameter to the team IP address of the primary mobility controller.

9

Mobility traffic manager

Contents

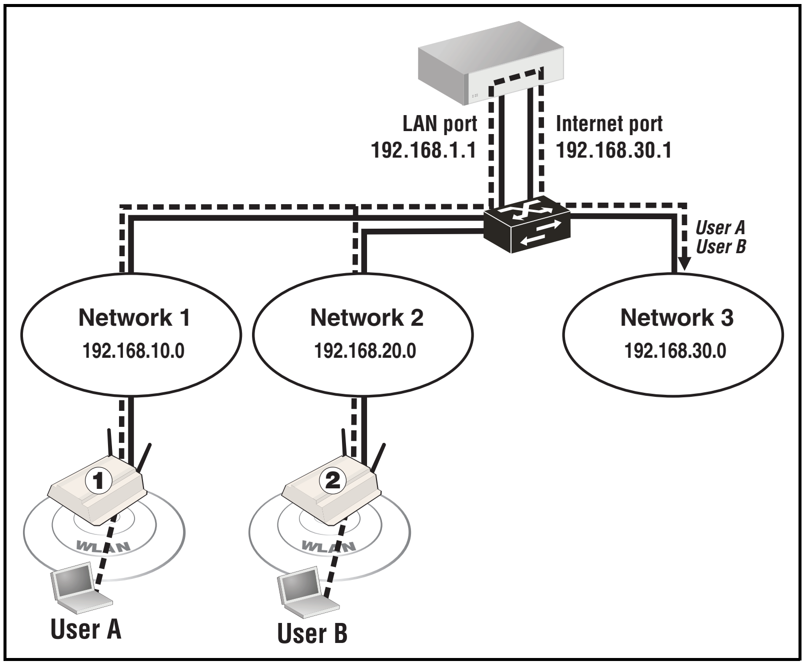
Key concepts

Note This chapter discusses how to use and configure Mobility traffic manager (MTM) with non-teamed controllers. If you are working with a controller team, most of the same information applies. Essentially, a controller team is treated the same way as a single non-teamed controller. For more information, see *Mobility support on page 8-26*.

MTM provides for seamless roaming of wireless users, while at the same time giving you complete control over how wireless user traffic is distributed onto the wired networking infrastructure. MTM enables you to implement a wireless networking solution using both centralized and distributed strategies, allowing you to create a wireless network that is perfectly tailored to meet the needs of your users and the requirements of your network. Some of the deployment strategies that you can use with MTM include:

- **Centralized wireless traffic:** All traffic from wireless users is tunneled back to a central controller where it is egressed onto the wired infrastructure. Wireless users can be connected to any AP within the layer 3 network serviced by MTM.

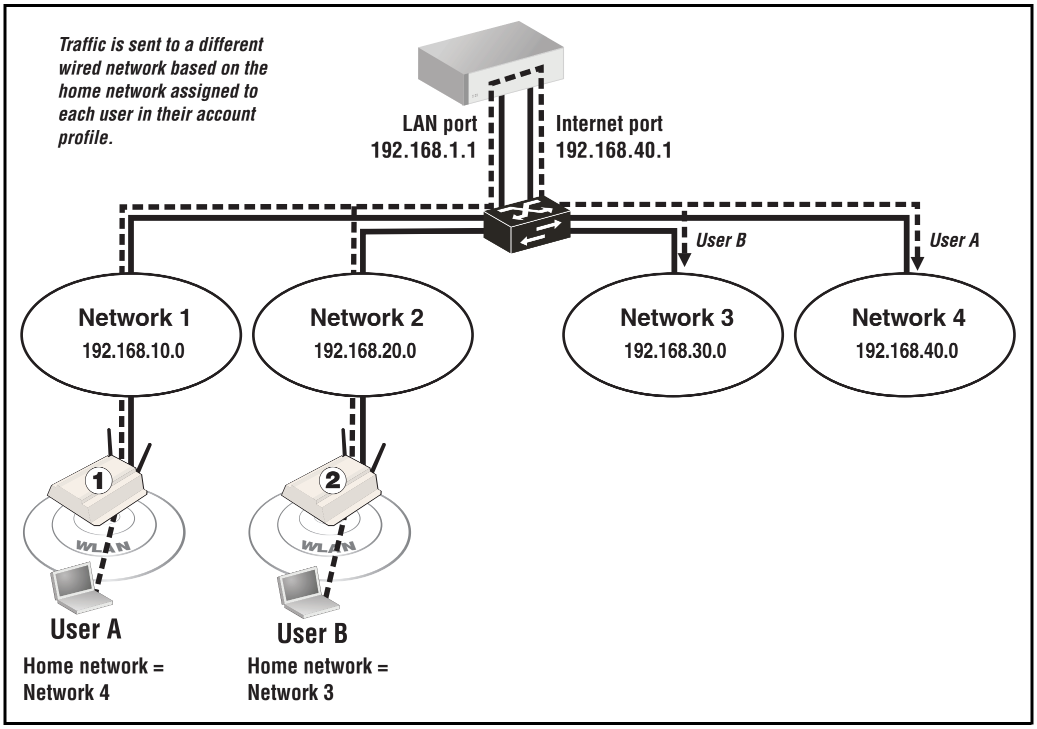
  The following diagram shows a deployment where all wireless traffic is egressed onto a specific network segment (192.168.30.0).



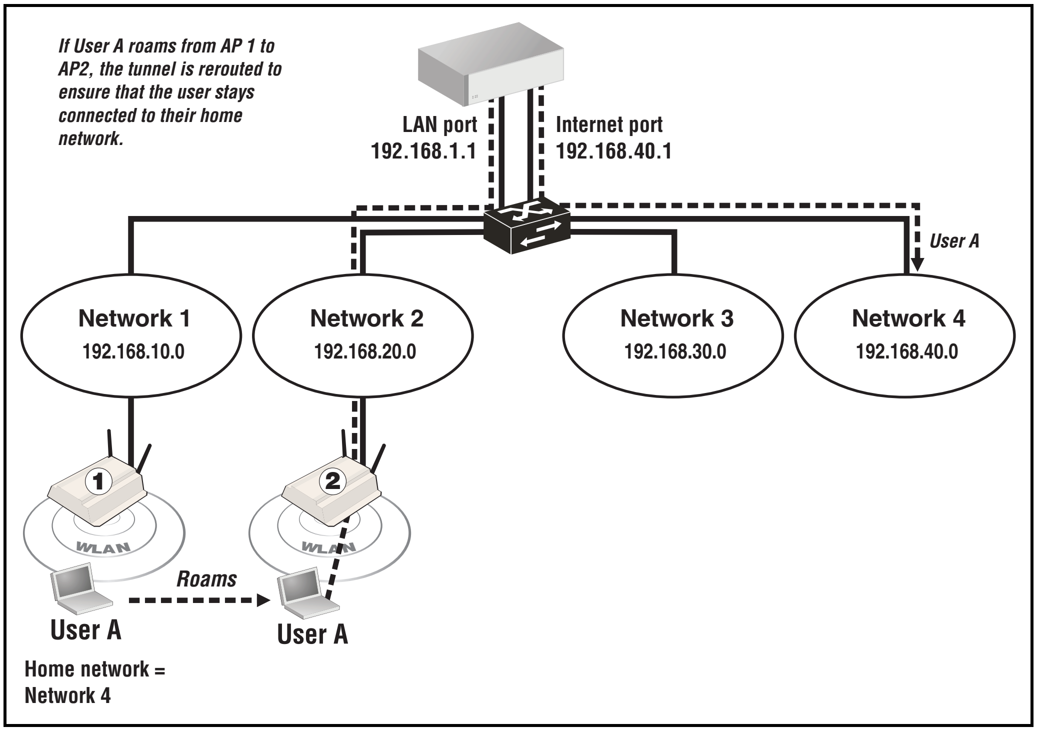
  MTM can also be used to send traffic to different networks or VLANs based on criteria such as username, network location, VSC, or AP group.

- **Traffic distribution using home networks:** A home network can be assigned to each wireless user (via RADIUS, local user accounts, or through a VSC egress). MTM can then be used to tunnel the user’s traffic to their home network, regardless of the AP to which a user connects within the mobility domain.

The following diagram shows a deployment where the wireless traffic for each user is egressed onto a specific network segment by assigning a home network to each user.



If a user roams between APs, MTM adjusts the tunnel to maintain the user's connection to their home network.



- **Automatic traffic distribution:** VLAN ranges can be used to automatically spread wireless user traffic across multiple VLANs on the wired infrastructure. See *Scenario 6: Distributing traffic using VLAN ranges*.

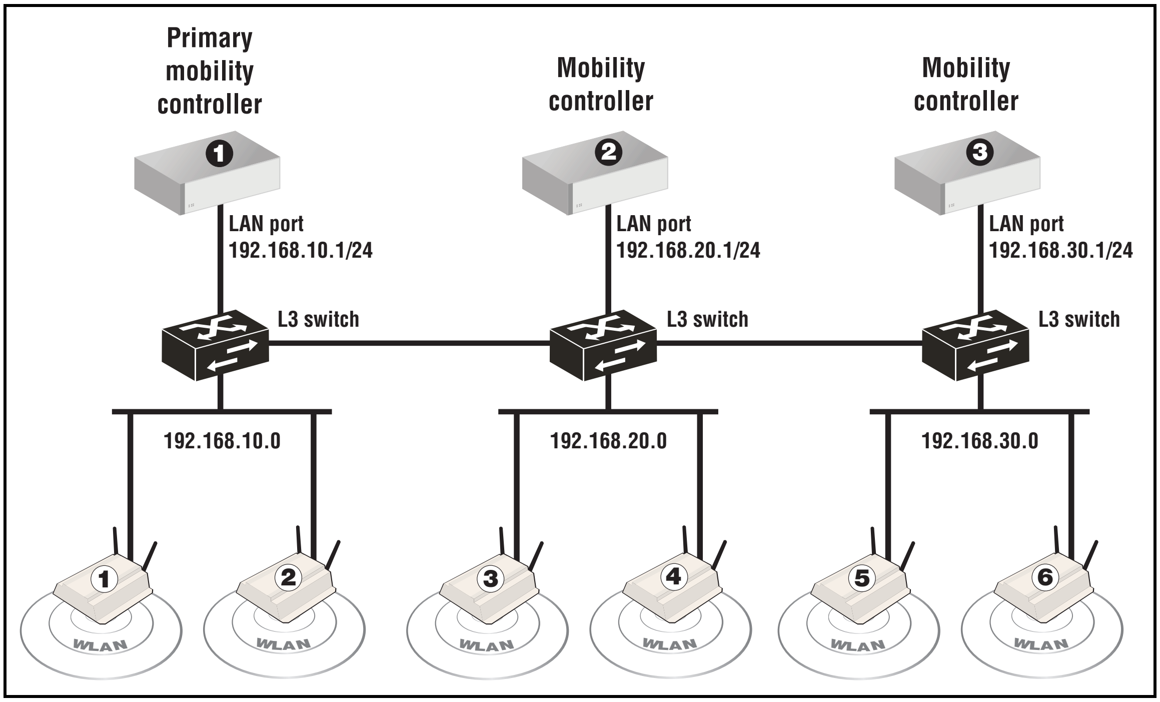
Important

- **MTM is only available on non-access-controlled VSCs.**
- **The same VSCs must be defined on all controllers in the mobility domain, even on controllers that are not managing any APs.**

The mobility domain

The mobility domain is an interconnection between controllers allowing for the exchange of information about wireless users and the home/local networks managed by controllers. The mobility domain can span multiple controllers and controller teams, whether they are installed on the same subnet or on different subnets, and includes all controlled APs managed by the controllers.

In the following example the mobility domain spans three controllers and their APs operating on three different subnets.



MTM makes use of the mobility domain to locate the home network for roaming users, or the target network when tunneling traffic to a specific network on the wired infrastructure.

For each mobility domain, one controller is defined as the *primary mobility controller.* This controller acts as the central site for the distribution of mobility information to all other controllers. (When controller teaming is active, an entire team is defined as the primary mobility controller. See *Mobility support on page 8-26*.)

Note

- All controllers in the mobility domain must be running the same software version. This means that the first two numbers in the software revision must be the same. For example: All controllers running 5.4.x, or all controllers running 5.5.x.
- Discovery automatically takes place on both the LAN port and Internet port. **VLANs are not supported.**

Network requirements

The network that interconnects the controllers and APs that make up a mobility domain must not block any of the following ports/protocols:

- UDP port 1194
- UDP port 12141
- UDP port 3000
- UDP port 3001
- UDP port 3518
- TCP port 5432
- Internet protocol number 47 (GRE)

Home networks

A home network is the root network for a user within a mobility domain. The home network specifies the network on which a user's wireless traffic is sent onto the wired infrastructure. A user's connection is always local to their home network, regardless of where their wireless connection is made within the mobility domain. For example, if a user roams between an AP that is directly connected to their home network, to an AP on a different subnet, MTM creates a tunnel that connects the user back to their home network.

When a user first connects to an AP, MTM must determine whether the user is *at home* (i.e., connected to the user's home network) or *roaming* (connected to an AP on a different network). MTM does this by comparing the home network assigned to the user with the list of local networks associated with the AP.

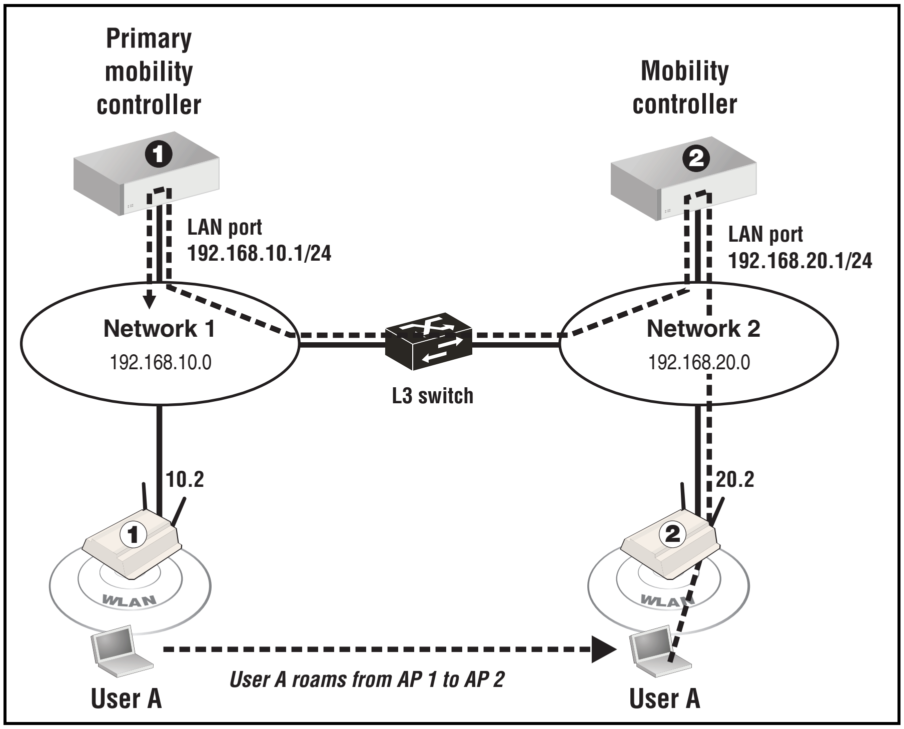
- If a match is found, the user is considered to be at home and the user's traffic is sent onto the wired network via the AP's Ethernet port.
- If **no** match is found, MTM then tries to locate the user's network within the mobility domain. If found, MTM creates a tunnel between the AP and the controller to carry the user's traffic. If the network is not defined on any controller within the mobility domain, the user is blocked (or assigned to the network on which the AP discovered the controller, depending on how MTM support is configured on the VSC).

Note

Certain configuration settings on the controller may override the specific configuration settings that you define on a VSC to assign user traffic to a home network. For details, see *Traffic flow for wireless users on page 7-6*.

Example

In following example, User A roams between AP # 1 and AP #2. When connected to AP #2, User A is identified as roaming and traffic is tunneled back to subnet 10.0 via controller 1 and controller 2.



Local networks

In order for a wireless user’s traffic to be sent to the appropriate destination within the mobility network, local networks must be defined on controllers, and optionally APs.

When a user is roaming, the path to the user’s home network cannot end at an AP. This means that each home network that is assigned to a user **must** be defined as the local network on at least one controller in the mobility domain.

- When an AP is directly connected to a user’s home network, the user’s data will **only** reach the wired network through the AP’s Ethernet port when the user is directly connected to the AP.
- When roaming, the user’s traffic is always tunneled to the controller that provides the data path to the user’s home network.

In the previous example, when User A is directly connected to AP 1, traffic reaches Network 1 via the APs Ethernet port. When User A roams to AP 2, traffic reaches Network 1 via the LAN port on controller 1.

Configuring Mobility Traffic Manager

MTM configuration can be separated into the following tasks:

- Define the mobility domain.
- Define network profiles.
- Assign home networks to users.
- Define local networks on controllers and APs.
- Configure mobility settings for each VSC. (*The same VSCs must be defined on all controllers in the mobility domain, even on controllers that are not managing any APs.*)
- Bind VSCs to the APs.

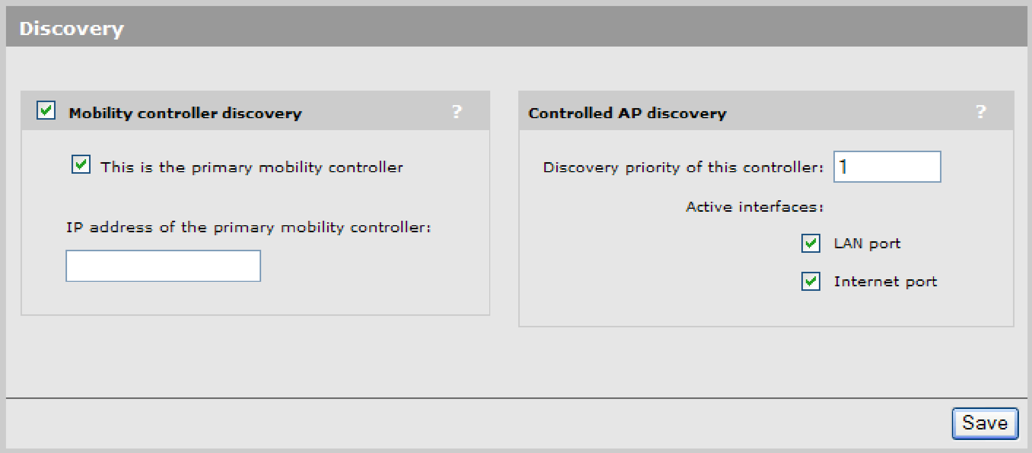
Each task is described in more detail in the sections that follow.

Defining the mobility domain

When MTM will be used on more than one controller, or with a controller team, you must define a mobility domain. The following instructions apply to non-teamed controllers. If you are working with a controller team, see *Mobility support on page 8-26*.

Connect to the management tool on the controller that will be the primary mobility controller, and do the following:

1. Select **Controller >> Management > Device discovery**.
   - Select **Mobility controller discovery**.
   - Select **This is the primary mobility controller.**



Discovery

☑ Mobility controller discovery

☑ This is the primary mobility controller

IP address of the primary mobility controller:

Controlled AP discovery

Discovery priority of this controller: 1

Active interfaces:

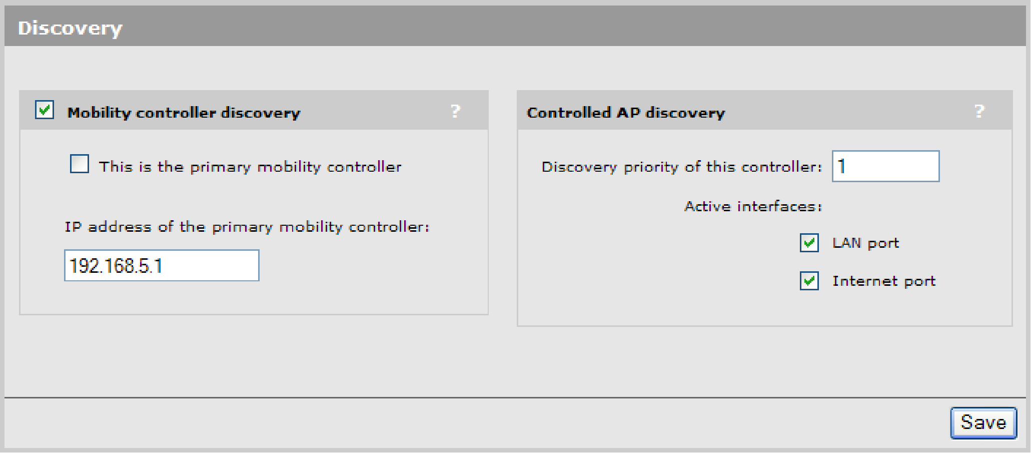
☑ LAN port

☑ Internet port

2. Select **Save**.

Connect to the management tool on all other controllers, that will be part of the mobility domain and do the following:

1. Select **Controller >> Management > Device discovery**.
2. Select **Mobility controller discovery**.
3. Specify the **IP address of the primary mobility controller**. This can be the address of its Internet port or LAN port as long as the port is reachable. For example, if the primary is at 192.168.5.1, you would configure the other controllers as follows:



Discovery

☑ Mobility controller discovery

□ This is the primary mobility controller

IP address of the primary mobility controller: 192.168.5.1

Controlled AP discovery

Discovery priority of this controller: 1

Active interfaces:

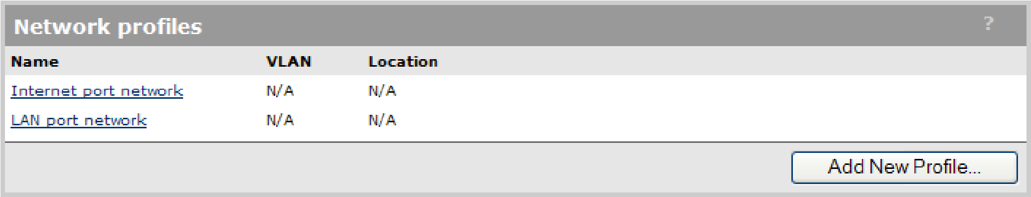
☑ LAN port

☑ Internet port

4. Select **Save**.

Defining network profiles

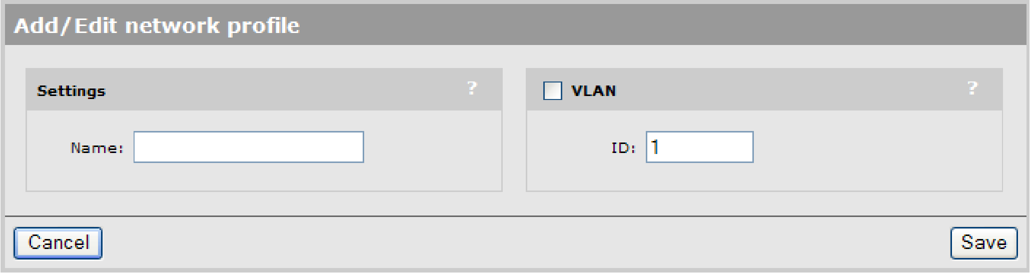
Global definitions for all home networks and local networks are created using the network profiles feature which is found on the **Controller >> Network > Network profiles** page. Initially, two profiles are defined as shown.



Network profiles

Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A

To create a new profile, select **Add New Profile**.



Add/Edit network profile

Settings

Name:

□ VLAN

ID: 1

For each network profile you can define a VLAN ID or just a name.

About the default profiles

Two network profiles are created by default: **LAN port network** and **Internet port network**. These profiles are associated with the two physical Ethernet ports on the controller. You can rename these profiles, but you cannot assign a VLAN to them or delete them. You can use these profiles to send untagged traffic to a specific port on the controller.

Both ports are considered to be local networks on the controller, which means that they automatically map the network that is assigned to each physical port as a local network on the controller. However, the LAN and Internet port network profiles can also be assigned as a local network on an AP (for example, using the **Controlled APs >> Configuration > Local networks** page). When this is done, both profiles refer to the untagged Ethernet port on the AP.

Assigning a home network to a user

When you activate MTM support for a VSC, a user's home network is defined in one of the following ways:

- It can be configured in the user's account on a third-party RADIUS server by setting the attributes Tunnel-Medium-Type, Tunnel-Private-Group-ID, and Tunnel-Type. For details on how to set these attributes, see *User attributes on page 15-13*.

  The Tunnel-Private-Group-ID attribute should be set to the name of the network profile that identifies the user's home network (A VLAN number can also be specified, but is not recommended since two profiles could exist with the same VLAN ID but bound to different physical ports or VLAN ports.)

- Configured in a locally defined user account or user account profile. (User accounts are defined by selecting **Controller >> Users**.) Currently this method only supports VLAN ID. To specify a network profile name, Use the Custom attributes option in a network profile to specify the attributes Tunnel-Medium-Type, Tunnel-Private-Group-ID, and Tunnel-Type.

- Configured by setting the **Egress network** option when binding the VSC to an AP group. This lets you assign the same home network to a group of APs. Any user connected to one of these APs then gets the specified home network. Note that if both the Egress network and a RADIUS attribute are assigned, the Egress network is overwritten by the RADIUS attribute.

A number of configuration settings on the controller can affect how user traffic is routed. Some of these settings may override the choices you make to assign user traffic to a home network. See *Traffic flow for wireless users on page 7-6*.

Note

At least one controller must be assigned to each home network defined in the mobility domain. See *Local networks on page 9-8*.

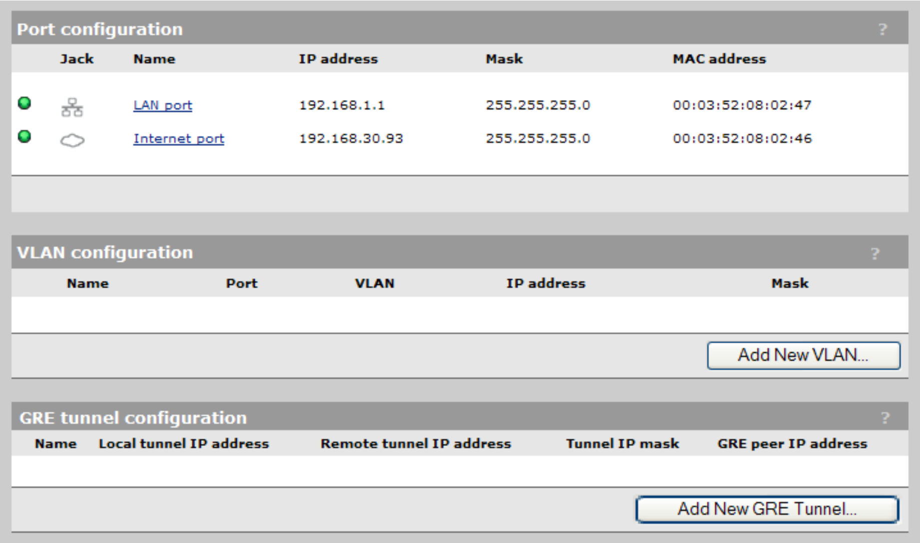
Defining local networks on a controller

Local networks on a controller are composed of the following interfaces:

- The network connected to the LAN port. Identified by the network profile **LAN port network**.
- The network connected to the Internet port. Identified by the network profile **Internet port network**.
- Any VLAN definition created on the **Controller >> Network > Ports** page.

To add additional VLANs on a controller, do the following:

1. Select **Controller > Network > Ports**.



Port configuration

	Jack	Name	IP address	Mask	MAC address
●		LAN port	192.168.1.1	255.255.255.0	00:03:52:08:02:47
●		Internet port	192.168.30.93	255.255.255.0	00:03:52:08:02:46

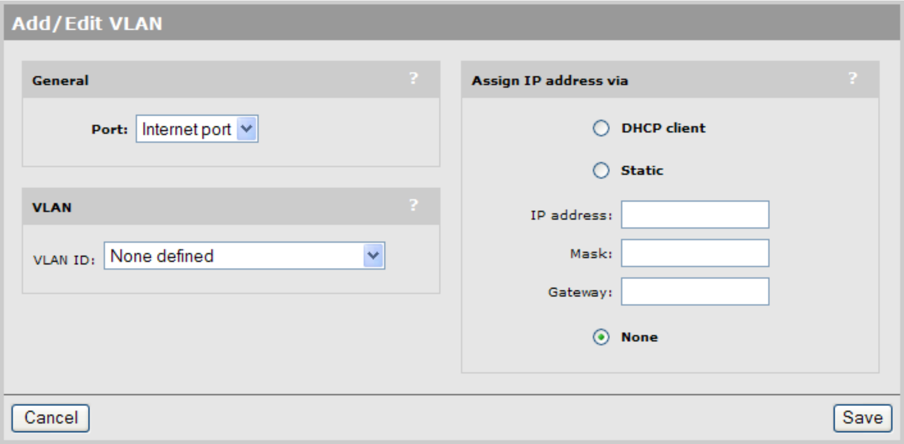
VLAN configuration

Name	Port	VLAN	IP address	Mask

GRE tunnel configuration

Name	Local tunnel IP address	Remote tunnel IP address	Tunnel IP mask	GRE peer IP address

2. Select **Add New VLAN**.



Add/Edit VLAN

General

Port: Internet port

VLAN

VLAN ID: None defined

Assign IP address via

○ DHCP client

○ Static

IP address:

Mask:

Gateway:

● None

3. Under **General**, set **Port** to **LAN port** or **Internet port**.
4. Under **VLAN**, set **VLAN ID** to the appropriate network profile.
5. Under **Assign IP address via**, select an addressing method.

6. Select **Save**.

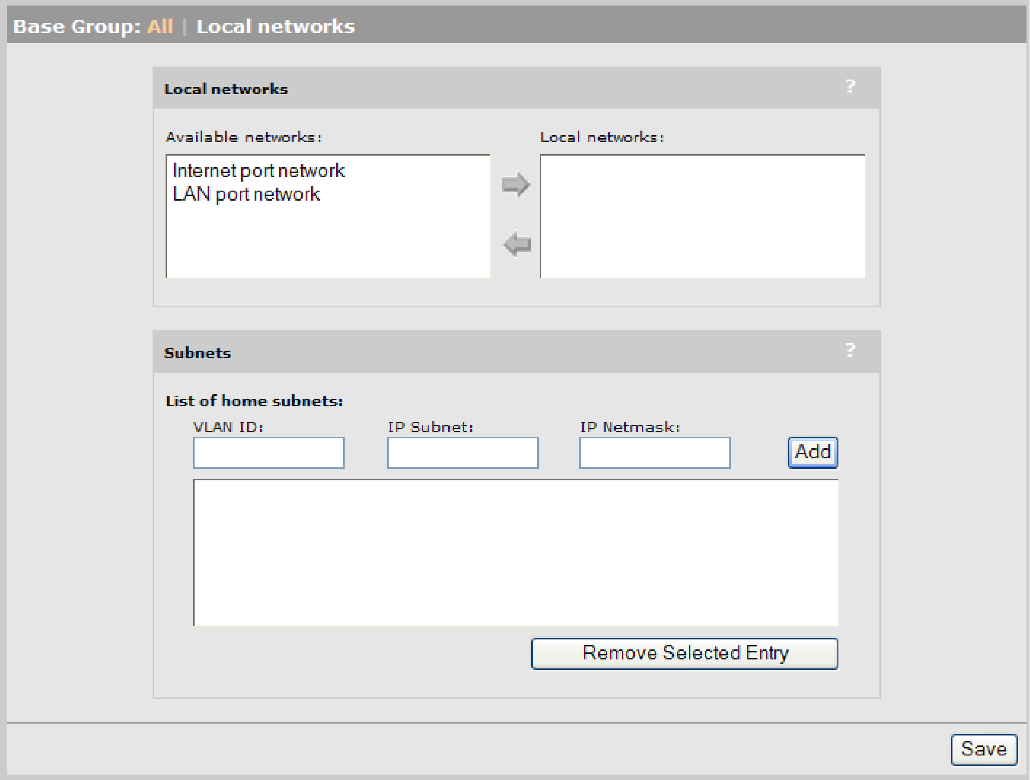
Assigning local networks to an AP

Each AP can be configured to support one (or more) local networks. By comparing the home network assigned to a user with the list of local networks associated with an AP, MTM can determine if the user is at home or roaming.

Local networks can be assigned by selecting one of the following (depending on whether you want to define local networks for all APs, a group of APs, or a single AP):

- **Controller > Controlled APs >> Configuration > Local networks**
- **Controller > Controlled APs > [*group*] >> Configuration > Local networks**
- **Controller > Controlled APs > [*AP*] >> Configuration > Local networks**

In all cases you will see the Home networks configuration page.



Local networks

Select the local networks that are connected to the Ethernet port(s) on the AP.

- **Available networks:** This box lists all network profiles defined on the controller. Select a network profile and then select the right arrow to assign it as a local network on the AP.
- **Local networks:** This box lists all the networks that are local to the AP. These networks are used to determine if a user is roaming or at home when they connect to the AP.

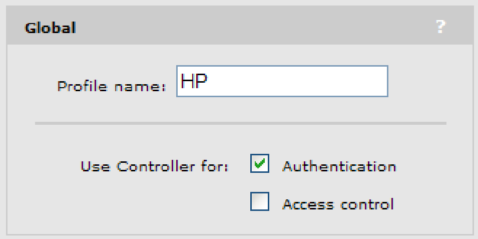
- If a user's home network matches a local network on the AP, the user is considered to be at home, and their traffic is bridged onto the wired network via the Ethernet port on the AP.
- If a user's home network does not match a local network on the AP, the user is considered to be roaming, and their traffic is tunneled to appropriate home network via the controllers that make up the mobility domain.

Note This Subnets feature has been deprecated. See *Subnet-based mobility* for more information.

Configuring the mobility settings for a VSC

Once all home and local networks have been assigned, you can configure VSC definitions to support MTM.

1. Select the **Controller > VSCs > [*VSC-name*]**.
2. Disable the **Access control** option under **General**.

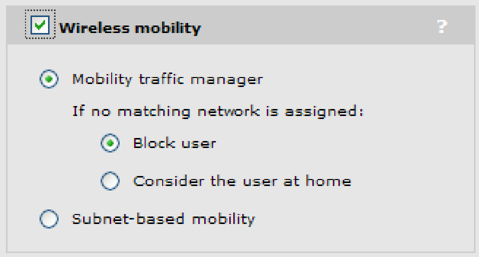


Global

Profile name: HP

Use Controller for: ☑ Authentication
□ Access control

3. Select **Wireless mobility**, and under it, select **Mobility traffic manager.**



☑ Wireless mobility

● Mobility traffic manager
If no matching network is assigned:
● Block user
○ Consider the user at home
○ Subnet-based mobility

If you are using MTM to tunnel the traffic from wireless users to their home networks, set the following parameter to determine how MTM routes traffic if no home network is assigned to a user (via their RADIUS account or local user account), or if the user's home network is not found in the mobility domain.

If no matching network is assigned

- **Block user:** User access is blocked.
- **Consider the user at home:** The user's home network is considered to be the network assigned to the AP's Ethernet port and traffic is bridged locally by the AP.

4. Select **Save**.

5. Configure the **Wireless security filters** so that they do not interfere with roaming functionality. In most cases, these filters should be disabled. If you need to use them, note that:

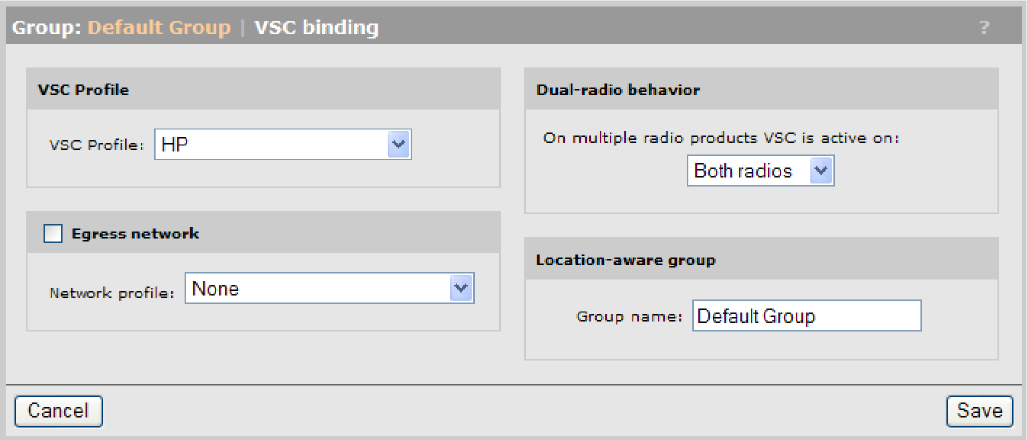
   - The **Restrict wireless traffic to: Custom** option can be used provided that it restricts traffic to destinations that are reachable from all subnets in the mobility domain.

   - Neither the **Restrict wireless traffic to: Access point's default gateway** nor **Restrict wireless traffic to: MAC address** options can be used.

Binding a VSC to an AP

After you have defined a VSC, you need to bind it to all the APs in the mobility domain.

1. Select **Controller > Controlled APs > [*group*] >> VSC bindings** and then the VSC configured for mobility. The VSC binding page opens.



Group: Default Group | VSC binding

VSC Profile

VSC Profile: HP

□ Egress network

Network profile: None

Dual-radio behavior

On multiple radio products VSC is active on: Both radios

Location-aware group

Group name: Default Group

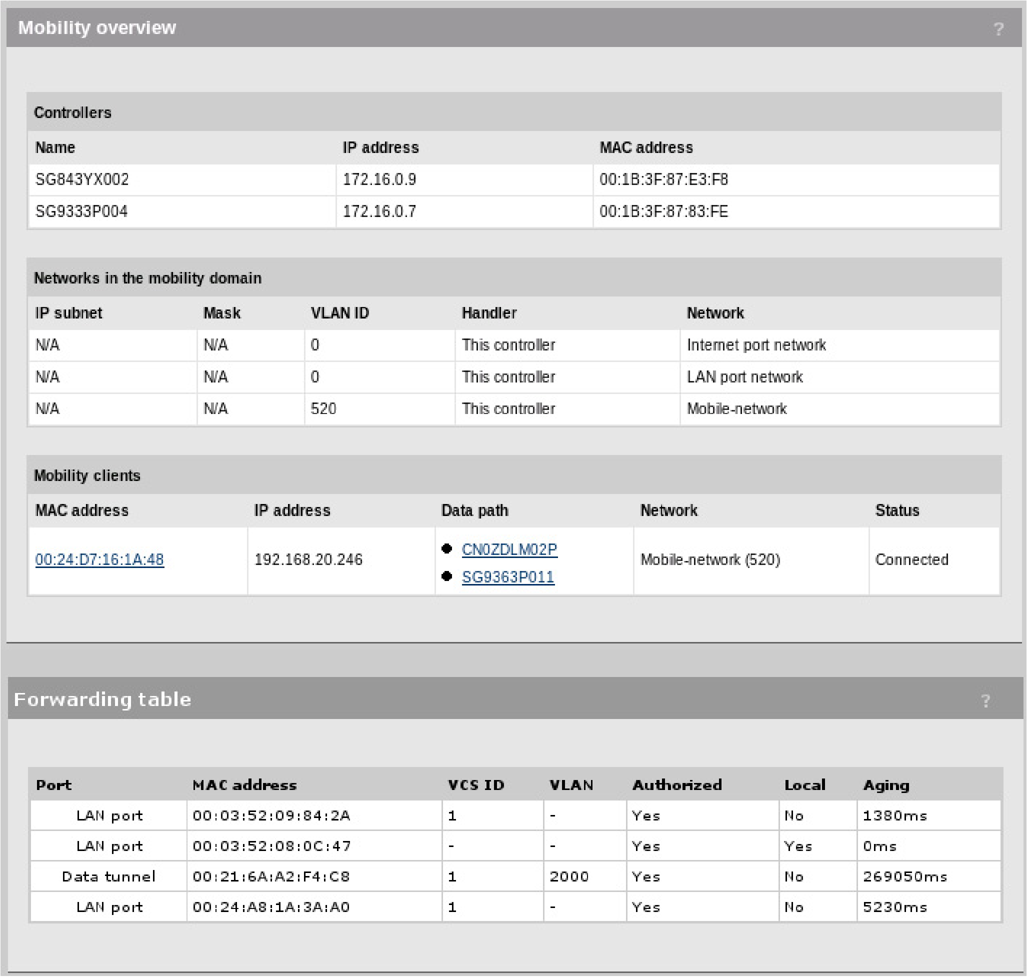
For **VSC profile**, select the VSC that you just configured for mobility.

You have the option of assigning an **Egress network** to the binding. When mobility is active on the VSC, the **Egress network** is assigned as the user's home network (unless a dynamic VLAN is assigned to the user). You also have the option of selecting any untagged interfaces, such as the default profiles for the LAN port and Internet port.

A number of configuration settings on the controller can affect how user traffic is routed. Some of these settings may override the choices you make to assign user traffic to a home network. See *Traffic flow for wireless users on page 7-6*.

Monitoring the mobility domain

The mobility overview page displays status information for the mobility domain. For example:



Mobility overview

Controllers

Name	IP address	MAC address
SG843YX002	172.16.0.9	00:1B:3F:87:E3:F8
SG9333P004	172.16.0.7	00:1B:3F:87:83:FE

Networks in the mobility domain

IP subnet	Mask	VLAN ID	Handler	Network
N/A	N/A	0	This controller	Internet port network
N/A	N/A	0	This controller	LAN port network
N/A	N/A	520	This controller	Mobile-network

Mobility clients

MAC address	IP address	Data path	Network	Status
00:24:D7:16:1A:48	192.168.20.246	● CN0ZDLM02P ● SG9363P011	Mobile-network (520)	Connected

Forwarding table

Port	MAC address	VCS ID	VLAN	Authorized	Local	Aging
LAN port	00:03:52:09:84:2A	1	-	Yes	No	1380ms
LAN port	00:03:52:08:0C:47	-	-	Yes	Yes	0ms
Data tunnel	00:21:6A:A2:F4:C8	1	2000	Yes	No	269050ms
LAN port	00:24:A8:1A:3A:A0	1	-	Yes	No	5230ms

To view this page:

- On a non-teamed controller, select **Controller >> Status > Mobility**.
- On a controller team, select **Team:[*Team-name*] > Controllers [*Team-manager*] >> Status > Mobility**.

Controllers

This table lists all controllers that are part of the mobility domain.

- **Name:** Name assigned to the controller.
- **IP address:** IP address of the controller.
- **MAC address:** Medium access control address of the associated controller.

Networks in the mobility domain

This table lists all networks that are defined in the mobility domain and indicates the address of the **Handler** (AP or controller) that provides the data path to each network.

This list should be identical on all controllers that are part of the mobility domain. The handler will differ on each controller, depending on whether the network is supported locally or not.

IP subnet

(*This field does not apply when using Mobility Traffic Manager.*)

IP subnet assigned to the network, if applicable. For example, if the network is a VLAN, then no IP subnet/mask information is shown.

Mask

Network mask associated with the IP subnet, if applicable.

VLAN ID

VLAN ID associated with the network.

Handler

A handler is the AP or controller that provides the data path to a network.

- If the network is handled by an AP managed by this controller, then this column shows the names of controlled APs supporting the network. Up to five APs can be displayed (the first five APs registered by the controller for the specific network).
- If the network is local to this controller, then this column shows **This controller**.
- If the network is directly connected to another controller, then this column shows the name of the other controller.

Network

Name of the network.

Mobility clients

This table provides information on all roaming clients that are active in the mobility domain.

MAC address

Media access control (hardware) address of the client. Select the address to see a log of mobility-related events for the client. For details, see *Mobility client event log on page 9-19*.

IP address

IP address of the client.

Data path

Lists all the APs and controllers that are in the data path between a user and their home network.

Network

The name of the user's home network.

Status

Possible values are:

- **Connected:** The client is connected to their home network.
- **Blocked:** Client data transfer is blocked because the home network could not be found.

Forwarding table

Port

Identifies the logical or physical port on which traffic is being forwarded.

MAC address

Identifies the MAC address to be matched. Traffic addressed to this address is forwarded on the corresponding port.

VSC ID

Identifies the VSC that a wireless client is connected to.

VLAN

Identifies the VLAN that the MAC address is associated with.

Authorized

Indicates if the wireless client is authorized to send traffic on the bridge.

Local

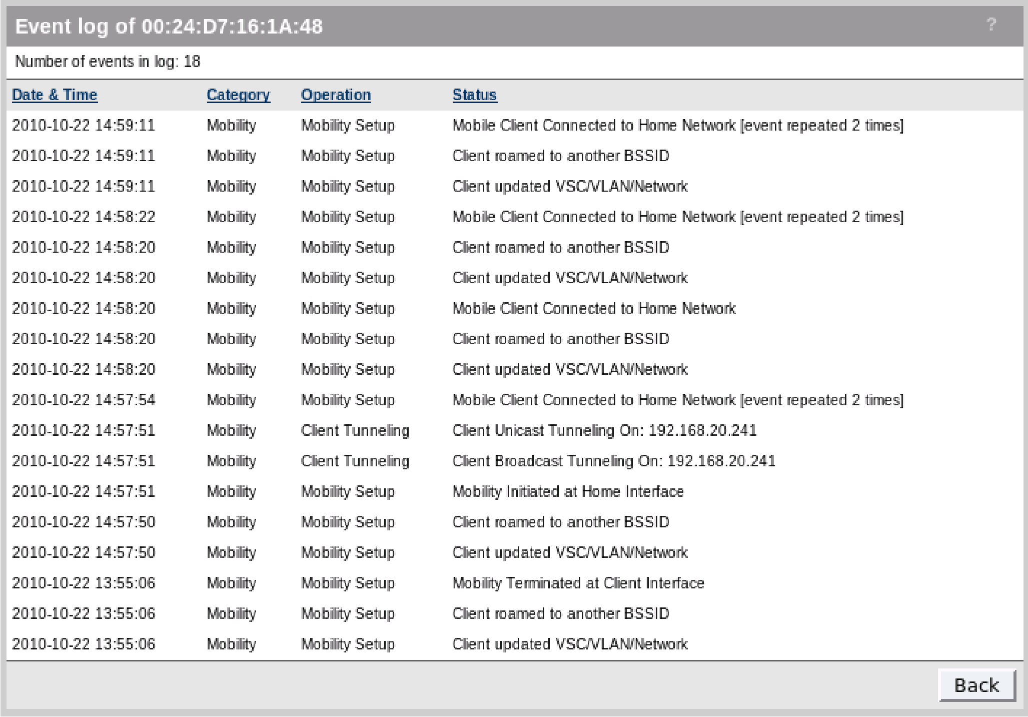
- Yes: Indicates that the MAC address identifies an interface on the service controller.
- No: Indicates that the MAC address is learned (not on the service controller).

Aging

Indicates how long (in seconds) until the entry is deleted from the table. Once deleted the entry must be relearned.

Mobility client event log

This page lists all events for a roaming client.



Event log of 00:24:D7:16:1A:48

Number of events in log: 18

Date & Time	Category	Operation	Status
2010-10-22 14:59:11	Mobility	Mobility Setup	Mobile Client Connected to Home Network [event repeated 2 times]
2010-10-22 14:59:11	Mobility	Mobility Setup	Client roamed to another BSSID
2010-10-22 14:59:11	Mobility	Mobility Setup	Client updated VSC/VLAN/Network
2010-10-22 14:58:22	Mobility	Mobility Setup	Mobile Client Connected to Home Network [event repeated 2 times]
2010-10-22 14:58:20	Mobility	Mobility Setup	Client roamed to another BSSID
2010-10-22 14:58:20	Mobility	Mobility Setup	Client updated VSC/VLAN/Network
2010-10-22 14:58:20	Mobility	Mobility Setup	Mobile Client Connected to Home Network
2010-10-22 14:58:20	Mobility	Mobility Setup	Client roamed to another BSSID
2010-10-22 14:58:20	Mobility	Mobility Setup	Client updated VSC/VLAN/Network
2010-10-22 14:57:54	Mobility	Mobility Setup	Mobile Client Connected to Home Network [event repeated 2 times]
2010-10-22 14:57:51	Mobility	Client Tunneling	Client Unicast Tunneling On: 192.168.20.241
2010-10-22 14:57:51	Mobility	Client Tunneling	Client Broadcast Tunneling On: 192.168.20.241
2010-10-22 14:57:51	Mobility	Mobility Setup	Mobility Initiated at Home Interface
2010-10-22 14:57:50	Mobility	Mobility Setup	Client roamed to another BSSID
2010-10-22 14:57:50	Mobility	Mobility Setup	Client updated VSC/VLAN/Network
2010-10-22 13:55:06	Mobility	Mobility Setup	Mobility Terminated at Client Interface
2010-10-22 13:55:06	Mobility	Mobility Setup	Client roamed to another BSSID
2010-10-22 13:55:06	Mobility	Mobility Setup	Client updated VSC/VLAN/Network

Date and time

Date and time that the even occurred.

Category

Always set to **Mobility**.

Operation

Possible values are:

- **Client tunneling:** Client tunneling events indicate activities related to establishing the data tunnel to a remote controller or AP for the purposes of transporting client data to its home network.
- **Mobility setup:** Mobility setup events indicate activities related to the detection and status of mobile clients, such as association, de-association, and state changes.

Status

Possible values are:

- **Client Unicast Tunneling On:** The unicast tunneling path to the indicated device (AP or another controller) has been established.
- **Client Broadcast Tunneling On:** The multicast/broadcast tunneling path to the indicated device (either AP or another controller) has been established.

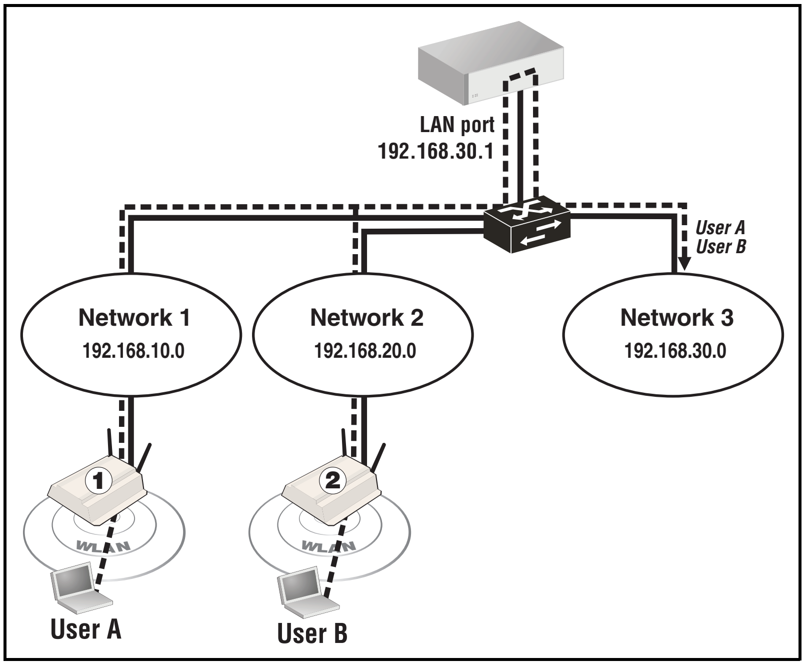
- **Client Unicast Tunneling Off:** The unicast tunneling path to the indicated device (either AP or another controller) has been removed. This is normally done only when the client has disassociated or its home network has changed.
- **Client Broadcast Tunneling Off:** The multicast/broadcast tunneling path to the indicated device (either AP or another controller) has been removed. This is normally done only when the client has disassociated or its home network has changed.
- **Mobile Client Connected from Local Network:** The tunneling path for data sent from the wireless client has been established.
- **Mobile Client Connected to Home Network:** The tunneling path at the client's home network egress point has been established.
- **Mobility Initiated at Home Interface:** A request to setup a client connection at its home network has been received.
- **Mobile Terminated at Home Interface:** A client connection at its home network has been terminated. This normally happens only when the client has disconnected or the network path to its connection point has been disrupted.
- **Mobility Initiated at Client Interface:** A request to setup a client connection at its connection point (the AP where the client is associated) has been received.
- **Mobility Terminated at Client Interface:** A client connection at its connection point has been terminated. This normally happens only when the client has disconnected or the network path to its home network has been disrupted.
- **Client roamed to another BSSID:** A client for which a tunneling path has been established has roamed to another AP. In this case, the tunneling path from its previous AP to its home network is disconnected, and a tunneling path from its new AP to its home network is established.
- **Client updated VSC/VLAN/Network:** A client for which a tunneling path has been established has re-connected to a network and as a result has a new home network assignment. In this case, the tunneling path to its previous home network is disconnected, and a tunneling path to its new home network is established.
- **No AP available to terminate client traffic:** A home network terminated by an AP is not currently available to egress the client traffic. In this case, data from the client will be blocked until the home network (i.e., the AP) becomes available.

Scenario 1: Centralizing traffic on a controller

This scenario illustrates how to centralize the traffic from a VSC that is deployed on several APs on different subnets.

How it works

In this scenario, a single controller manages several APs deployed on different subnets. The default VSC (named HP) is assigned to each AP and is used to provide wireless services for users. All traffic on this VSC is tunneled to the controller by MTM, where it is egressed onto the wired network. To accomplish this, the egress network in the VSC binding is set to the network profile that is assigned to the controller's LAN port.



Configuration overview

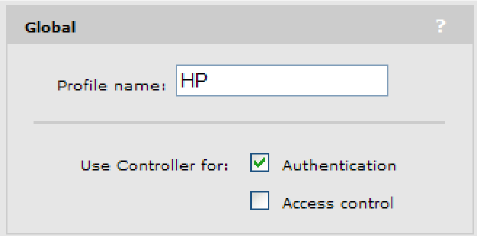
The following sections provide a summary of the configuration settings needed to enable MTM support only. It is assumed that installation and configuration of all controllers and APs so that they are fully operational on the network was performed as explained in the other chapters in this guide.

VSC configuration

Enable MTM support on the VSC.

1. Select **Controller > VSCs > HP**.

   - Under **Global**, clear **Access control**.



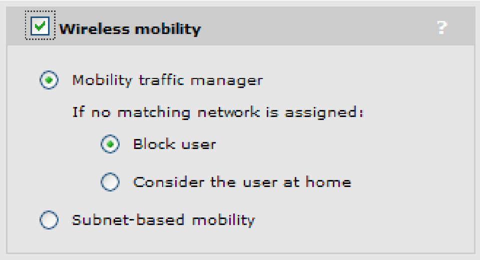
Global

Profile name: HP

Use Controller for: ☑ Authentication
☐ Access control

(For complete screenshot see *VSC configuration options on page 5-5*.)

   - Select **Wireless mobility**, then under it:
   - Select **Mobility traffic manager**.
   - Select **Block user.**



☑ **Wireless mobility**

● Mobility traffic manager
If no matching network is assigned:
● Block user
○ Consider the user at home
○ Subnet-based mobility

(For complete screenshot see *VSC configuration options on page 5-5*.)

2. Either disable **Wireless security filters** or set it to **Custom**.

3. Select **Save**.

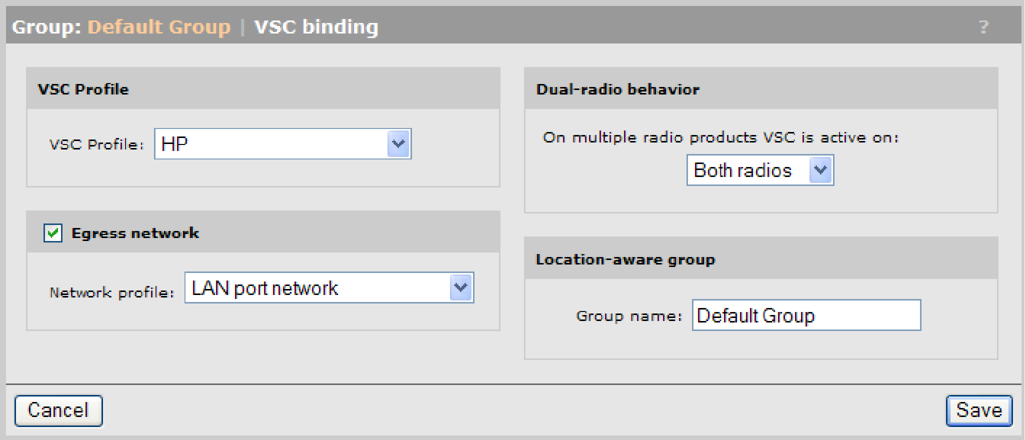
Network profiles

This scenario uses the default network profiles, so no configuration is necessary.

VSC binding

This scenario assumes that all APs are part of the **Default Group**. Set the egress for the group to the Internet port on the controller.

1. Select **Controller > Controlled APs > Default Group >> VSC bindings** and then select **HP**. The **VSC binding** page appears.



Group: Default Group | VSC binding

VSC Profile

VSC Profile: HP

☑ Egress network

Network profile: LAN port network

Dual-radio behavior

On multiple radio products VSC is active on: Both radios

Location-aware group

Group name: Default Group

- Under **VSC Profile**, set **VSC profile** to **HP**.
- Select **Egress network**, and under it, set **Network profile** to **LAN port network**.

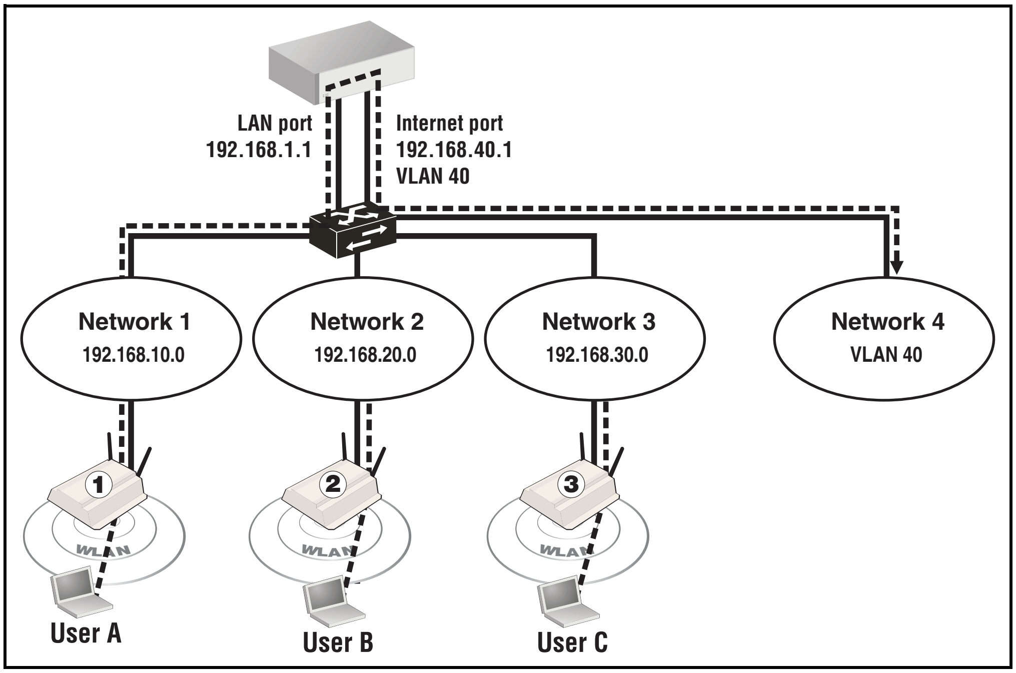
2. Select **Save**.

Scenario 2: Centralized traffic on a controller with VLAN egress

This scenario illustrates how to centralize the traffic from a VSC that is deployed on several APs on different subnets and send it to one or more VLANs via the controller.

How it works

In this scenario, a single controller manages several APs deployed on different subnets. The default VSC (named HP) is assigned to each AP and is used to provide wireless services for users. All traffic on this VSC is tunneled to the controller by MTM, where it is egressed onto the wired network on VLAN 40. To accomplish this, the egress network in the VSC binding is set to a network profile that defines a VLAN on the controller's Internet port.



Configuration overview

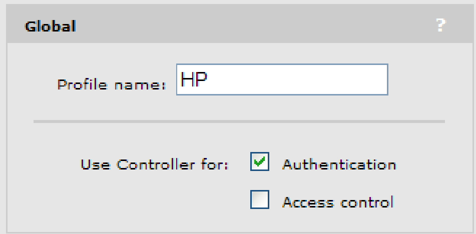
The following sections provide a summary of the configuration settings needed to enable MTM support only. It is assumed that installation and configuration of all controllers and APs so that they are fully operational on the network was performed as explained in the other chapters in this guide.

VSC configuration

Enable MTM support on the VSC.

1. Select **Controller > VSCs > HP**.

   - Under **Global**, clear **Access control**.



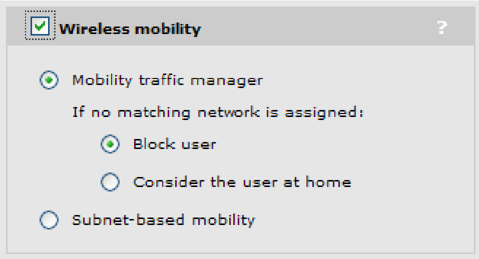
Global

Profile name: HP

Use Controller for: ☑ Authentication
□ Access control

(For complete screenshot see *VSC configuration options on page 5-5*.)

   - Select **Wireless mobility**, then under it:
   - Select **Mobility traffic manager**.
   - Select **Block user.**



☑ Wireless mobility

● Mobility traffic manager

If no matching network is assigned:

● Block user

○ Consider the user at home

○ Subnet-based mobility

(For complete screenshot see *VSC configuration options on page 5-5*.)

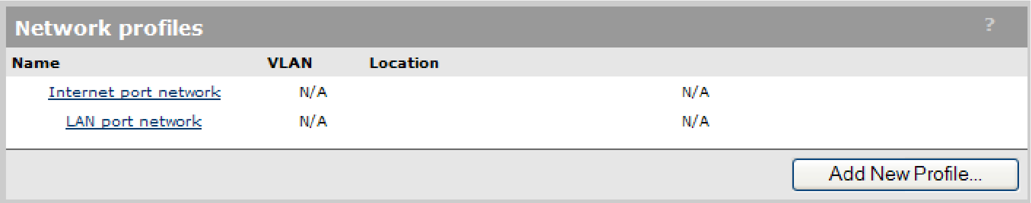
2. Either disable **Wireless security filters** or set it to **Custom**.

3. Select **Save**.

Network profiles

Define a network profile that maps VLAN 40 to the Internet port on the controller.

1. Select **Controller > Network > Network profiles**.



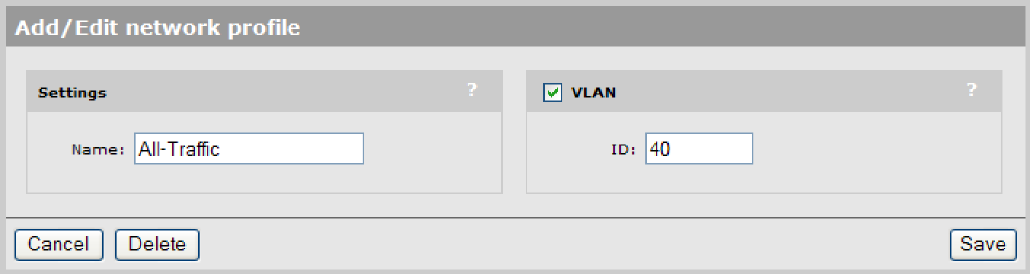
Network profiles

Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A

2. Select **Add New Profile**.

3. Under **Settings**, set **Name** to **All-Traffic**.

4. Select **VLAN**, and under it, set **ID** to **40**.



Add/Edit network profile

Settings

Name: All-Traffic

☑ VLAN

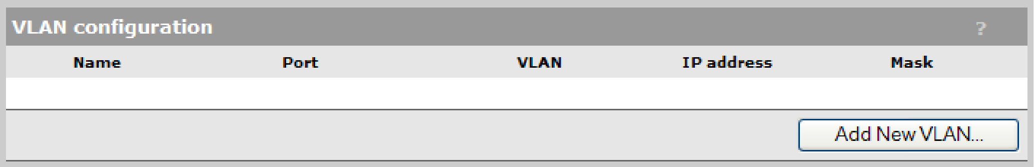
ID: 40

5. Select **Save**.

Create the VLAN

Create a VLAN on the Internet port using the network profile you just defined.

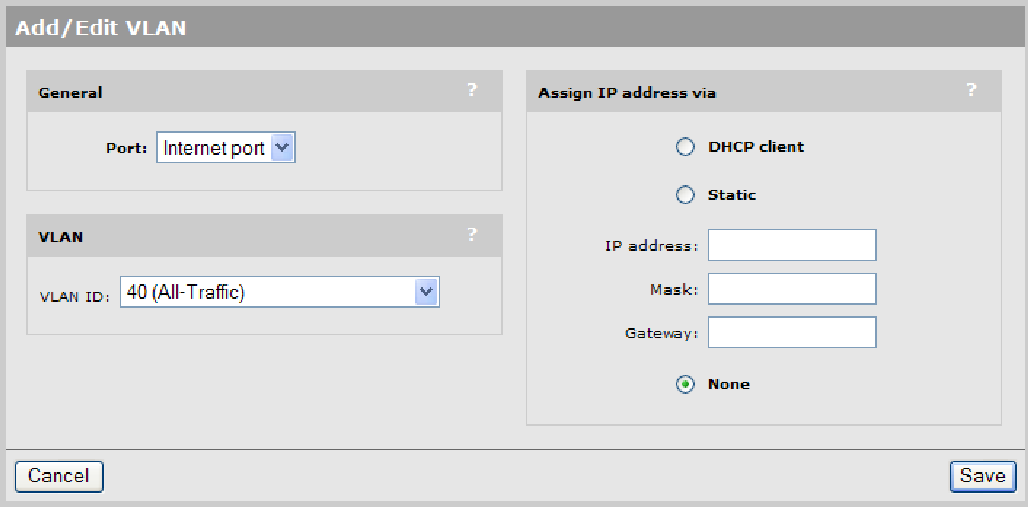
1. Select **Controller > Network > Ports**. Initially, the VLAN configuration list will be empty.



VLAN configuration

Name	Port	VLAN	IP address	Mask

2. Select **Add New VLAN**.



Add/Edit VLAN

General

Port: Internet port

VLAN

VLAN ID: 40 (All-Traffic)

Assign IP address via

○ DHCP client

○ Static

IP address:

Mask:

Gateway:

● None

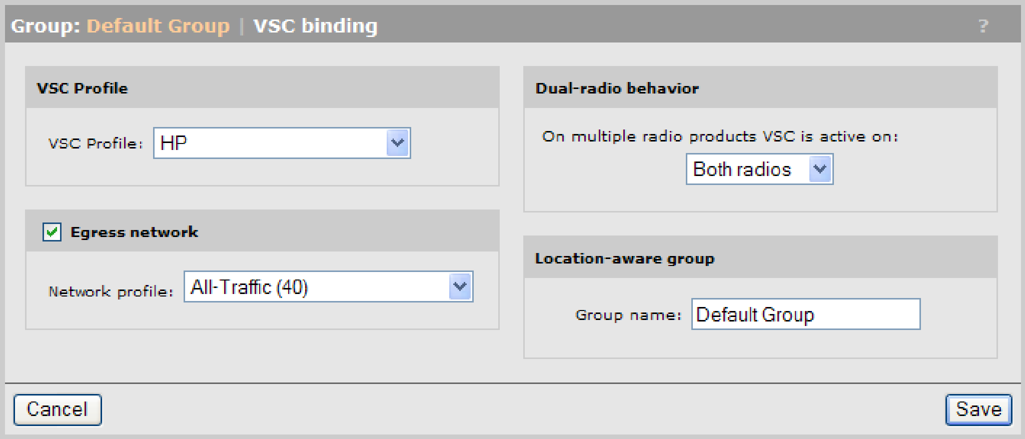
- Under **General**, set **Port** to **Internet port**.
- Under **VLAN**, set **VLAN ID** to **40 (All-Traffic)**.
- Under **Assign IP address** via, let the setting **None**. An address is not needed.

3. Select **Save**.

VSC binding

This scenario assumes that all APs are part of the **Default Group**.

1. Select **Controller > Controlled APs > Default Group >> VSC bindings** and then select **HP**. The **VSC binding** page appears.



Group: Default Group | VSC binding

VSC Profile

VSC Profile: HP

☑ Egress network

Network profile: All-Traffic (40)

Dual-radio behavior

On multiple radio products VSC is active on: Both radios

Location-aware group

Group name: Default Group

   - Under **VSC Profile**, set **VSC profile** to **HP**.
   - Select **Egress network**, and under it set **Network profile** to **Internet port network**.

2. Select **Save**.

Scenario 3: Centralized traffic on a controller with per-user traffic routing

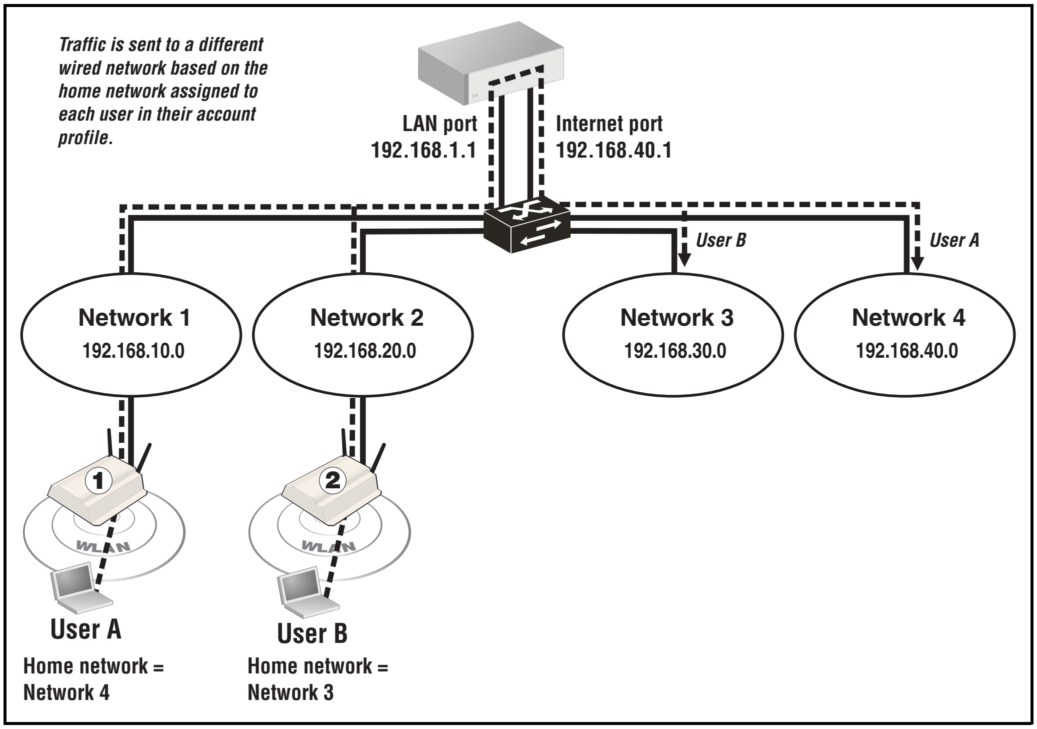
This scenario illustrates how to centralize the traffic from a VSC that is deployed on several APs on different subnets and send it to different VLANs for different groups of users.

How it works

In this scenario, a single controller manages several APs deployed on different subnets. The default VSC (named HP) is assigned to each AP and is used to provide wireless services for users. All traffic on this VSC is tunneled to the controller by MTM, where it is egressed onto different VLANs for different user groups.

An account profile is created for each user that define the egress VLAN for their traffic. This profile is then associated with the user's account.

WPA is enabled on the VSC to control user authentication. When the user logs in, the VLAN is retrieved from the account profile and is used by MTM to route the user's traffic to the appropriate network via the Internet port.



Configuration overview

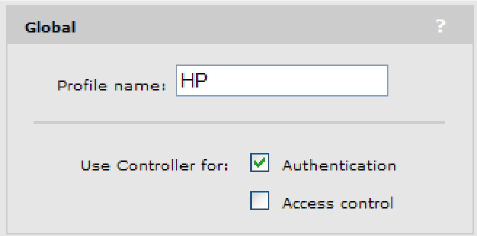
The following sections provide a summary of the configuration settings needed to enable mobility support only. It is assumed that installation and configuration of all controllers and APs so that they are fully operational on the network was performed as explained in the other chapters in this guide.

VSC configuration

Enable MTM support on the VSC.

1. Select **Controller > VSCs > HP**.

   - Under **Global**, clear **Access control**.



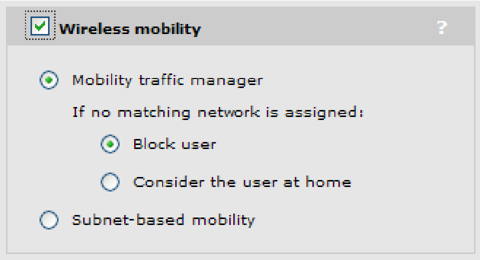
Global ?

Profile name: HP

Use Controller for: ☑ Authentication
☐ Access control

(For complete screenshot see *VSC configuration options on page 5-5*.)

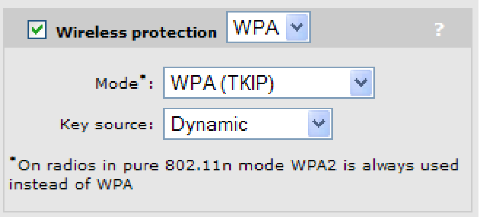
   - Select **Wireless mobility**, then under it:
   - Select **Mobility traffic manager**.
   - Select **Block user.**



☑ Wireless mobility ?

● Mobility traffic manager
If no matching network is assigned:
● Block user
○ Consider the user at home
○ Subnet-based mobility

   - Select **Wireless protection**, and then select **WPA**. Under it, do the following:
   - Set **Mode** to **WPA (TKIP)**.
   - Set **Key source** to **Dynamic**.

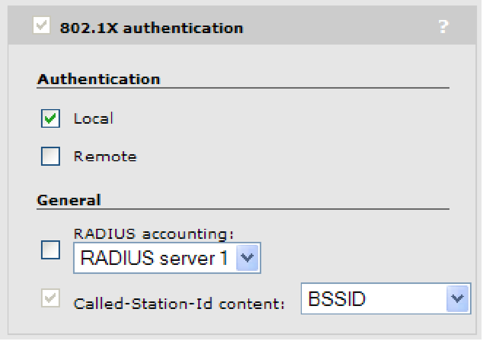


☑ Wireless protection WPA ?

Mode*: WPA (TKIP)
Key source: Dynamic

*On radios in pure 802.11n mode WPA2 is always used instead of WPA

This will automatically enable the **802.1X authentication** option and set it to use the local user accounts.



☑ 802.1X authentication

Authentication

☑ Local

□ Remote

General

□ RADIUS accounting: RADIUS server 1

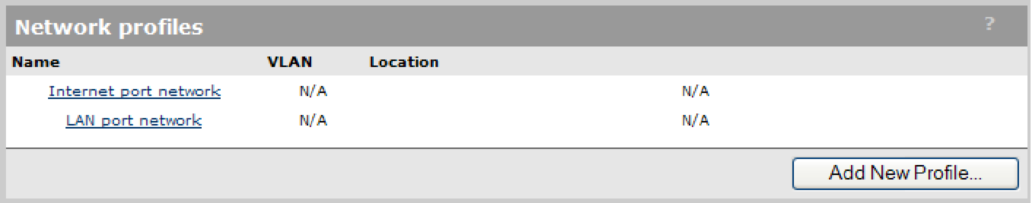
☑ Called-Station-Id content: BSSID

2. Either disable **Wireless security filters** or set it to **Custom**.
3. Select **Save**.

Network profiles

Define network profiles that map VLAN 30 and 40 to the Internet port on the controller.

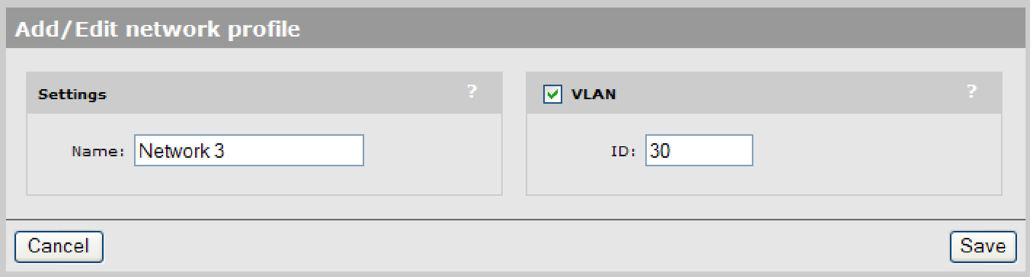
1. Select **Controller > Network > Network profiles**.



Network profiles

Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A

2. Select **Add New Profile**.
3. Under **Settings**, set **Name** to **Network 3**.
4. Select **VLAN**, and under it, set **ID** to **30**.



Add/Edit network profile

Settings

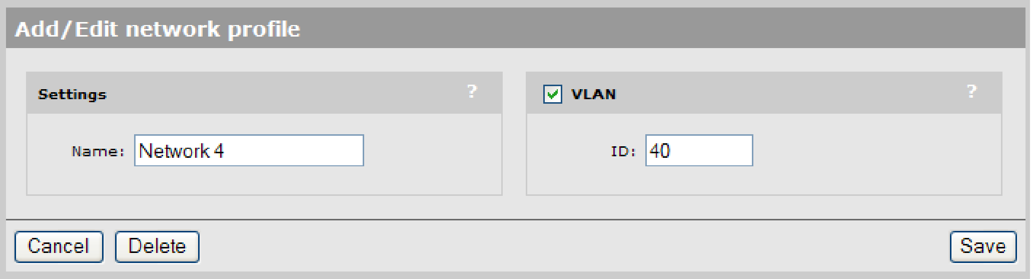
Name: Network 3

☑ VLAN

ID: 30

5. Select **Save**.
6. Select **Add New Profile**.
7. Under **Settings**, set **Name** to **Network 4**.

8. Select **VLAN**, and under it, set **ID** to **40**.



Add/Edit network profile

Settings

Name: Network 4

☑ **VLAN**

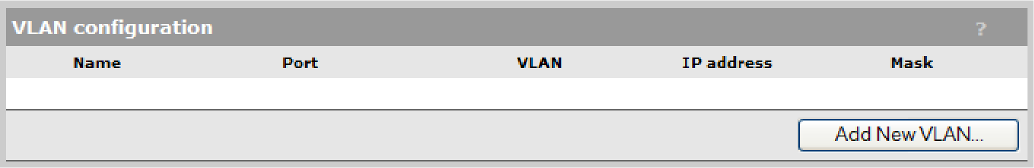
ID: 40

9. Select **Save**.

Create the VLANs

Create VLANs on the Internet port using the network profiles you just defined.

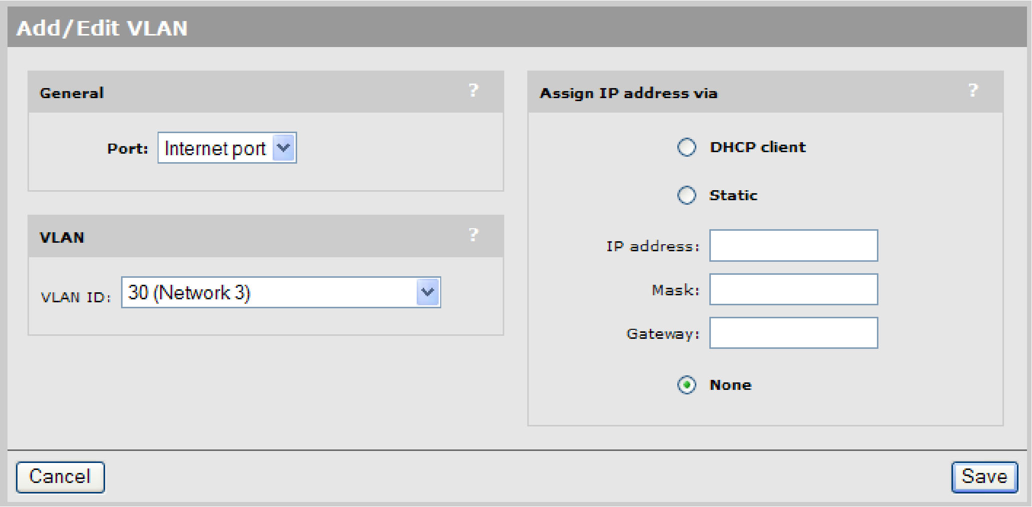
1. Select **Controller > Network > Ports**. Initially, the VLAN configuration list will be empty.



VLAN configuration

Name	Port	VLAN	IP address	Mask

2. Select **Add New VLAN**.



Add/Edit VLAN

General

Port: Internet port

VLAN

VLAN ID: 30 (Network 3)

Assign IP address via

○ DHCP client

○ Static

IP address:

Mask:

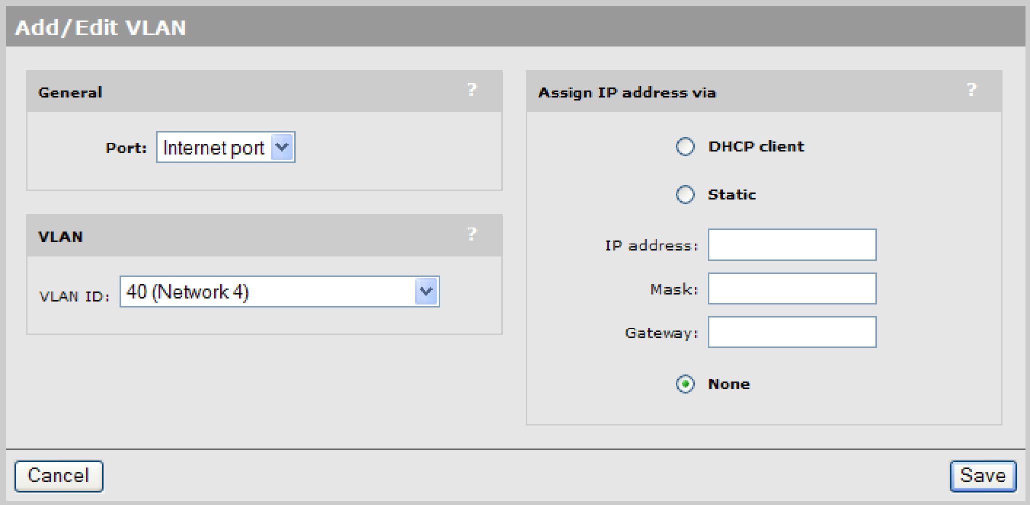
Gateway:

● None

- Under **General**, set **Port** to **Internet port**.
- Under **VLAN**, set **VLAN ID** to **30 (Network 3)**.
- Under **Assign IP address** via, let the setting **None**. An address is not needed.

3. Select **Save**.

4. Select **Add New VLAN**.



Add/Edit VLAN

General

Port: Internet port

VLAN

VLAN ID: 40 (Network 4)

Assign IP address via

○ **DHCP client**

○ **Static**

IP address:

Mask:

Gateway:

● **None**

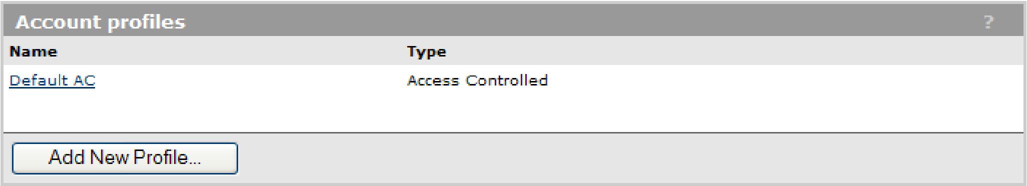
- Under **General**, set **Port** to **Internet port**.
- Under **VLAN**, set **VLAN ID** to **40 (Network 4)**.
- Under **Assign IP address** via, let the setting **None**. An address is not needed.

5. Select **Save**.

User accounts

Next you need to define user accounts and account profiles.

1. Select **Controller >> Users > Account profiles**.



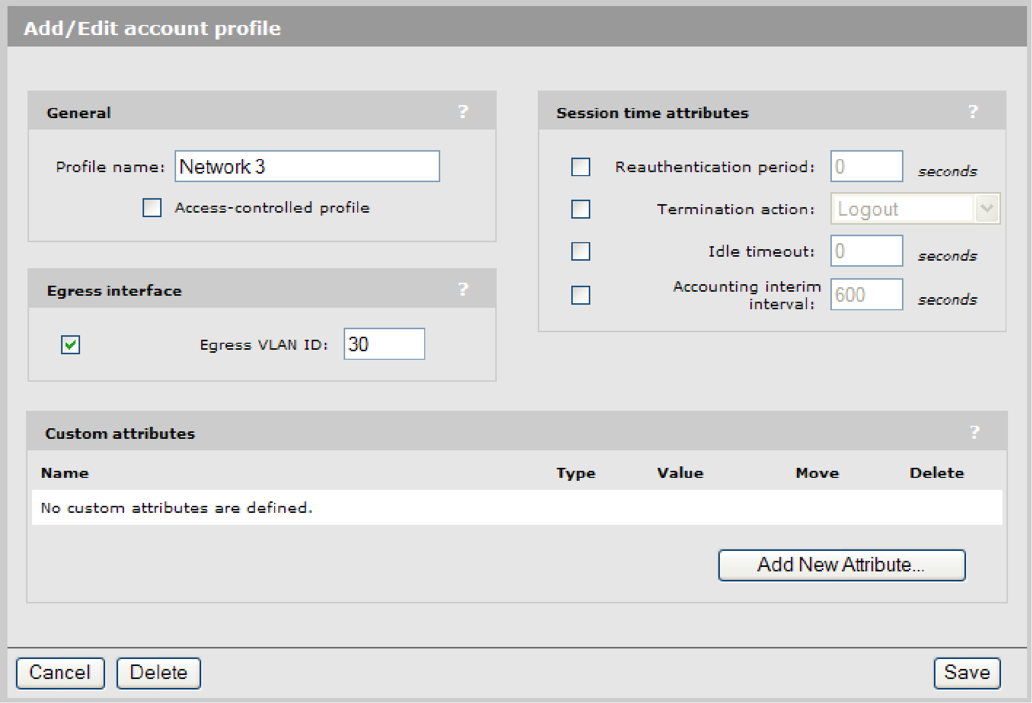
Account profiles

Name	Type
Default AC	Access Controlled

2. Select **Add New Profile**.

3. Under **General,** set **Profile name** to **Network 3** and disable **Access-controlled profile**.

4. Select **Egress interface**, and under it select **Egress VLAN ID** and set it to **30**.



Add/Edit account profile

General

Profile name: Network 3

□ Access-controlled profile

Egress interface

☑ Egress VLAN ID: 30

Session time attributes

□ Reauthentication period: 0 seconds

□ Termination action: Logout

□ Idle timeout: 0 seconds

□ Accounting interim interval: 600 seconds

Custom attributes

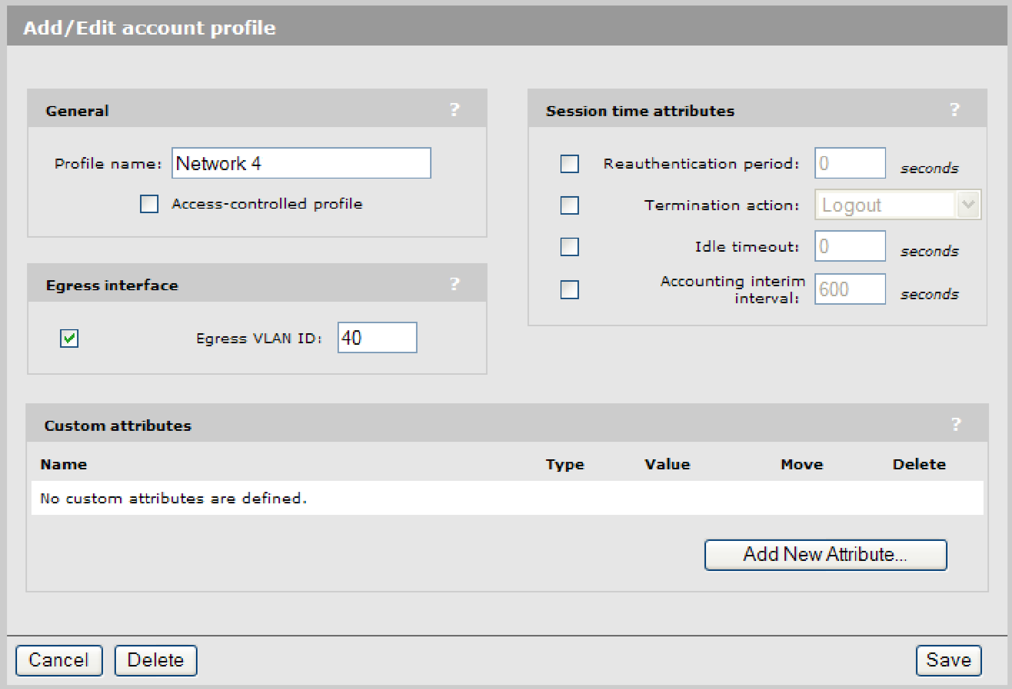
Name	Type	Value	Move	Delete
No custom attributes are defined.				

5. Select **Save**.

6. Select **Add New Profile**.

7. Under **General,** set **Profile name** to **Network 4** and disable **Access-controlled profile**.

8. Select **Egress interface**, and under it select **Egress VLAN ID** and set it to **40**.



Add/Edit account profile

General

Profile name: Network 4

□ Access-controlled profile

Egress interface

☑ Egress VLAN ID: 40

Session time attributes

□ Reauthentication period: 0 seconds

□ Termination action: Logout

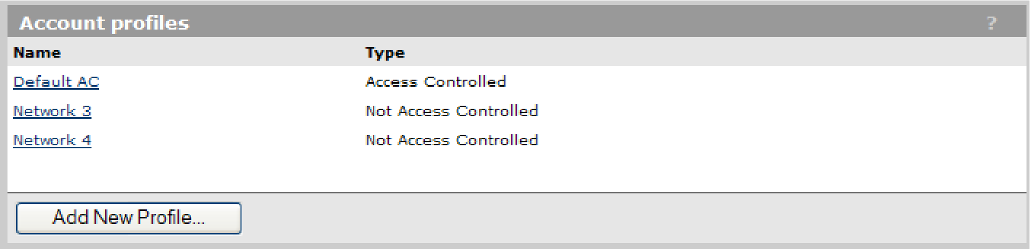
□ Idle timeout: 0 seconds

□ Accounting interim interval: 600 seconds

Custom attributes

Name	Type	Value	Move	Delete
No custom attributes are defined.				

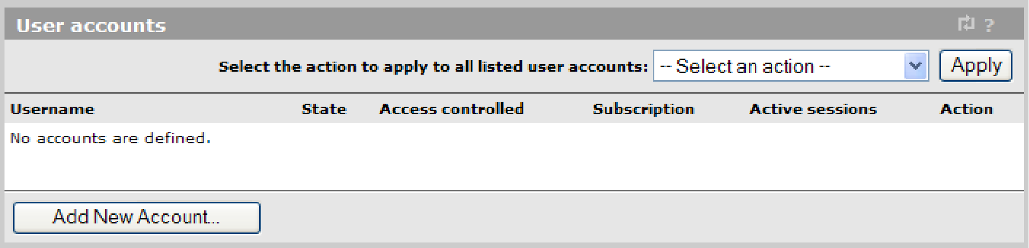
9. Select **Save**. The profiles list should now look like this:



Account profiles

Name	Type
Default AC	Access Controlled
Network 3	Not Access Controlled
Network 4	Not Access Controlled

10. Select **Controller >> Users > User accounts**. Initially, no accounts are defined.

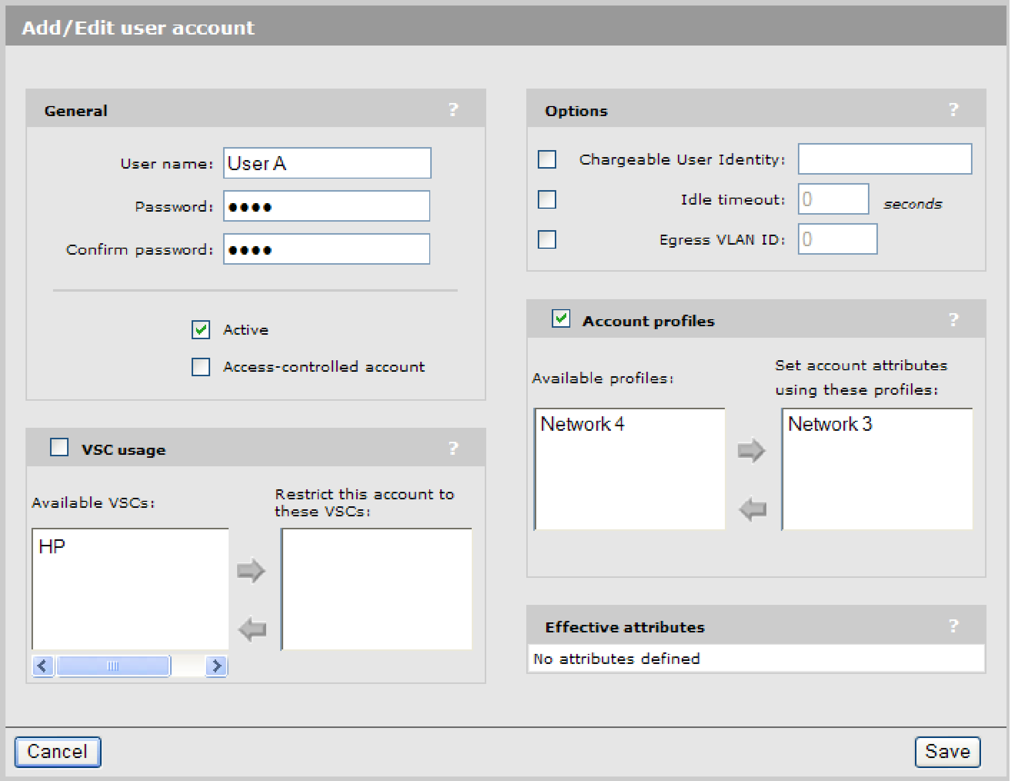


User accounts

Select the action to apply to all listed user accounts: -- Select an action --

Username	State	Access controlled	Subscription	Active sessions	Action
No accounts are defined.					

11. Select **Add New Account**.



Add/Edit user account

General

User name: User A

Password: ●●●●

Confirm password: ●●●●

☑ Active

☐ Access-controlled account

☐ VSC usage

Available VSCs: HP

Restrict this account to these VSCs:

Options

☐ Chargeable User Identity:

☐ Idle timeout: 0 seconds

☐ Egress VLAN ID: 0

☑ Account profiles

Available profiles: Network 4

Set account attributes using these profiles: Network 3

Effective attributes

No attributes defined

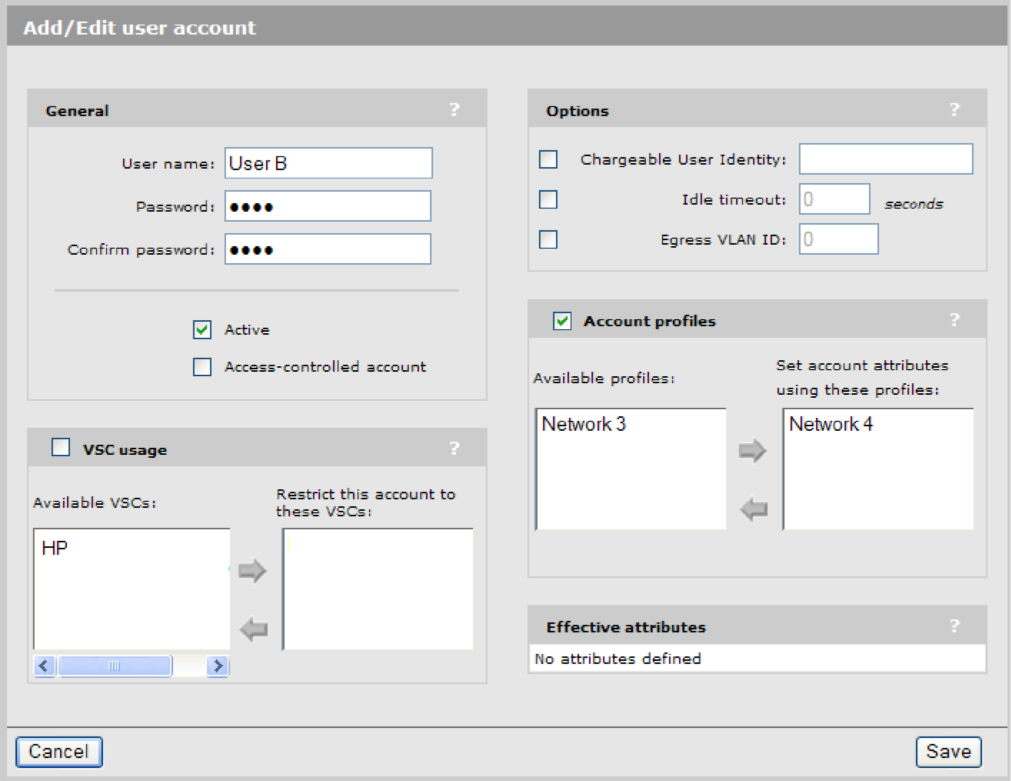
12. Under **General:**

- Set **User name** to **User A**.
- Set **Password** to a secure password.
- Clear **Access-controlled account**.

13. Select **Account profiles**, and under it move **Network 3** to the box titled **Set account attributes using these profiles**.

14. Select **Save**.

15. Select **Add New Account**.



Add/Edit user account

General

User name: User B

Password: ●●●●

Confirm password: ●●●●

☑ Active

□ Access-controlled account

□ VSC usage

Available VSCs: HP

Restrict this account to these VSCs:

Options

□ Chargeable User Identity:

□ Idle timeout: 0 seconds

□ Egress VLAN ID: 0

☑ Account profiles

Available profiles: Network 3

Set account attributes using these profiles: Network 4

Effective attributes

No attributes defined

16. Under **General:**

- Set **User name** to **User B**.
- Set **Password** to a secure password.
- Clear **Access-controlled account**.

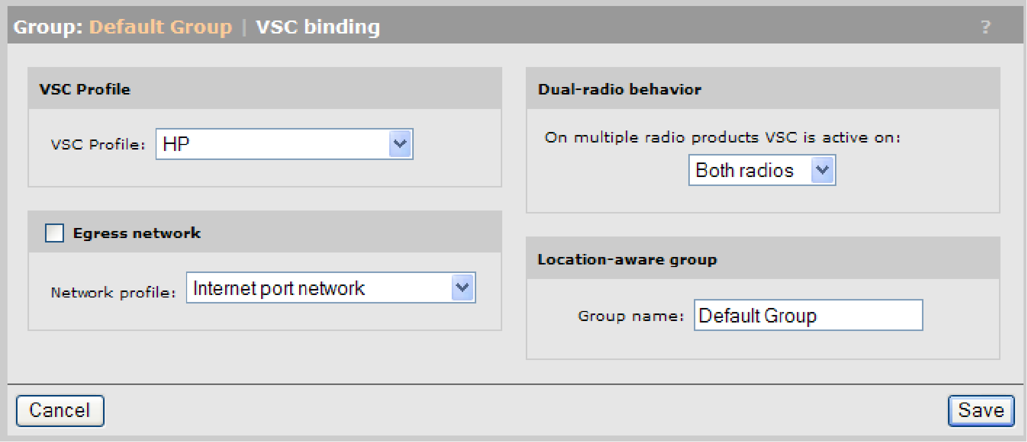
17. Select **Account profiles**, and under it move **Network 4** to the box titled **Set account attributes using these profiles**.

18. Select **Save**.

VSC binding

This scenario assumes that all APs are part of the **Default Group**.

1. Select **Controller > Controlled APs > Default Group >> VSC bindings** and then select **HP**. The **VSC binding** page appears.



Group: Default Group | VSC binding

VSC Profile

VSC Profile: HP

□ Egress network

Network profile: Internet port network

Dual-radio behavior

On multiple radio products VSC is active on: Both radios

Location-aware group

Group name: Default Group

   - Under **VSC Profile**, set **VSC profile** to **HP**.

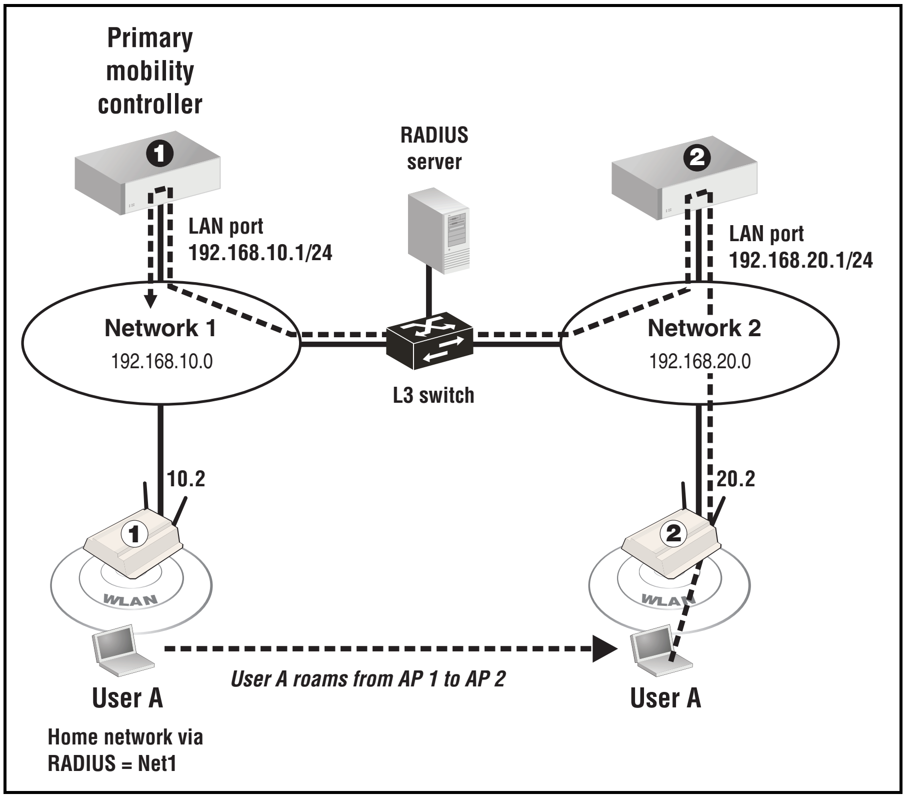
2. Select **Save**.

Scenario 4: Assigning home networks on a per-user basis

This scenario illustrates how to assign home networks on a per-user basis using RADIUS attributes.

How it works

In this scenario, wireless services have been added to two wired networks. A single controller and multiple APs are installed on each network. The two networks are connected with an L3 switch. The following diagram provides an overview of the setup. (A single AP is shown on each network for clarity).



Wireless clients receive their DHCP address from the controller on their network, or use a static IP addressing scheme.

A single VSC is used in this scenario. It is configured with the **Wireless mobility, Mobility traffic manager** option enabled. Home network assignment for users is done by setting RADIUS VLAN attributes which map users to one of two network profiles:

Network profile name	Assigned to
Net1	- Controller 1 LAN port - All APs attached to network 10.0 use this as their home network
Net2	- Controller 2 LAN port - All APs attached to network 20.0 use this as their home network

Each profile must be assigned to an AP as well as a controller. This is done to ensure that when a user logs in on an AP installed on the same subnet as the home network, traffic is not routed through the controller, but is sent directly onto the network via the Ethernet port not the AP. For example:

- When User A logs onto AP 1, RADIUS returns the VLAN ID **Net1**. Since Net1 is defined as a home network on AP 1, traffic is sent directly onto network 1 via the Ethernet port on the AP.
- When User A roams to (or logs into) AP 2, RADIUS returns the VLAN ID **Net1**. Since Net1 is not defined as a home network on AP 2, MTM tunnels the user’s traffic back to network 1.

A RADIUS account is defined for each user with attributes set as follows to identify the home network using a network profile name:

RADIUS attribute	Network 1 users	Network 2 users
Tunnel-Medium-Type	802	802
Tunnel-Private-Group-ID	Net1	Net2
Tunnel-Type	VLAN	VLAN

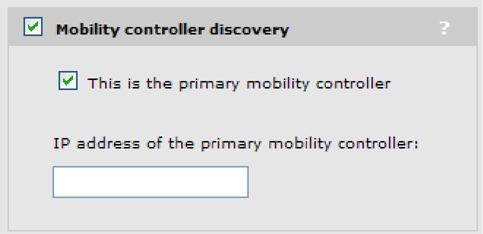
Configuration overview

The following sections provide a summary of the configuration settings needed to enable mobility support only. It is assumed that installation and configuration of all controllers and APs so that they are fully operational on the network was performed as explained in the other chapters in this guide.

Controller 1 configuration

Mobility domain

1. Select **Controller >> Management > Device discovery**.
   - Select **Mobility controller discovery**.
   - Select **This is the primary mobility controller.**



☑ Mobility controller discovery ?

☑ This is the primary mobility controller

IP address of the primary mobility controller:

(For complete screenshot see *Defining the mobility domain on page 9-9*.)

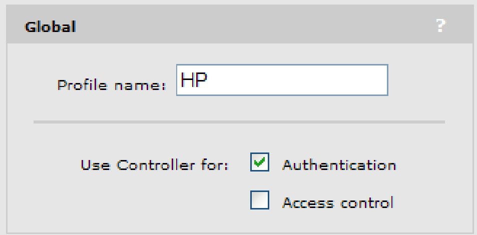
2. Select **Save**.

VSC

1. Select **Controller > VSCs > HP**.

Under Global

- Clear **Access control**.



Global ?

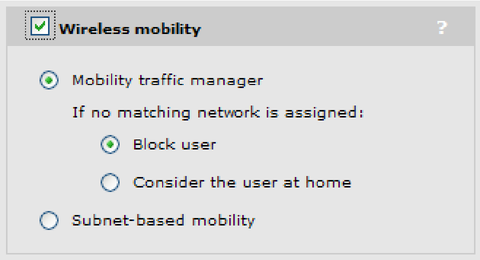
Profile name: HP

Use Controller for: ☑ Authentication

□ Access control

(For complete screenshot see *VSC configuration options on page 5-5*.)

- Select **Wireless mobility**, then under it:
- Select **Mobility traffic manager**.
- Select **Block user.**



☑ Wireless mobility ?

● Mobility traffic manager

If no matching network is assigned:

● Block user

○ Consider the user at home

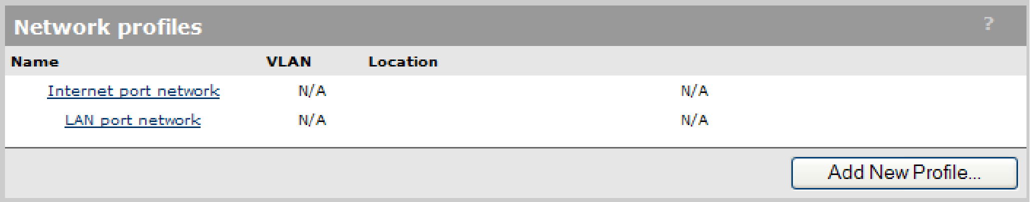
○ Subnet-based mobility

(For complete screenshot see *VSC configuration options on page 5-5*.)

2. Either disable **Wireless security filters** or set it to **Custom**.
3. Select **Save**.

Network profiles

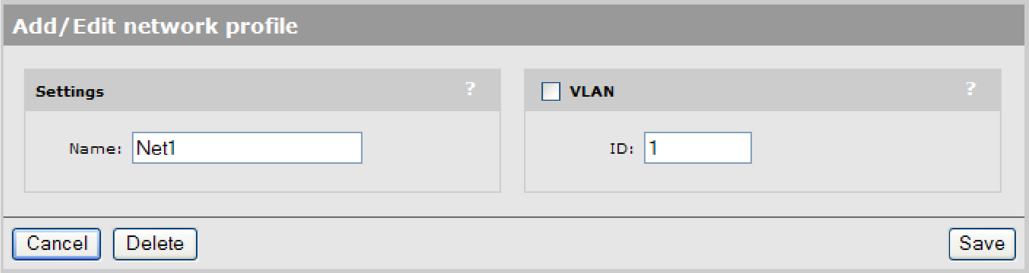
1. Select **Controller > Network > Network profiles**.



Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A

2. Select **LAN port network**.

3. Under **Settings**, change **Name** to **Net1**.



Settings

Name: Net1

□ VLAN

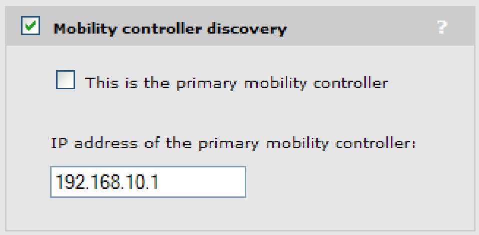
ID: 1

4. Select **Save**.

Controller 2 configuration

Mobility domain

1. Select **Controller >> Management > Device discovery**.



☑ Mobility controller discovery

□ This is the primary mobility controller

IP address of the primary mobility controller:

192.168.10.1

(For complete screenshot see *Defining the mobility domain on page 9-9*.)

- Select **Mobility controller discovery**.
- Clear **This is the primary mobility controller.**
- Specify the **IP address of the primary mobility controller**. In this example: **192.168.10.1**.

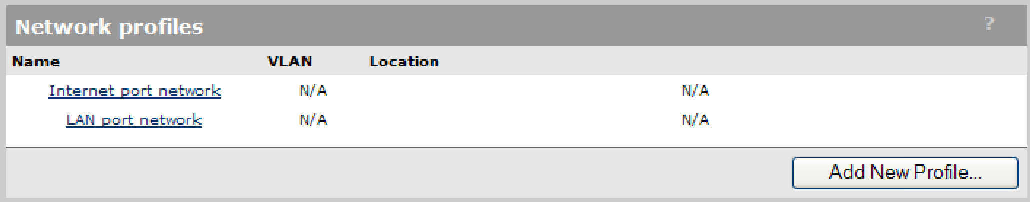
2. Select **Save**.

VSC

VSC configuration is the same as for controller 1.

Network profiles

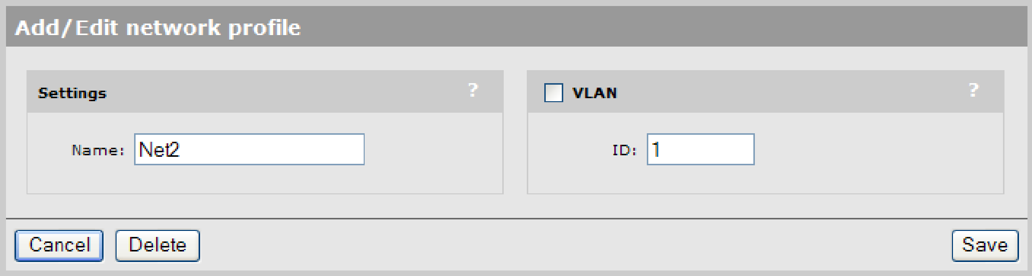
1. Select **Controller >> Network > Network profiles**.



Network profiles

Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A

2. Select **LAN port network**.
3. Under **Settings**, change **Name** to **Net2**.



Add/Edit network profile

Settings

Name: Net2

☐ VLAN

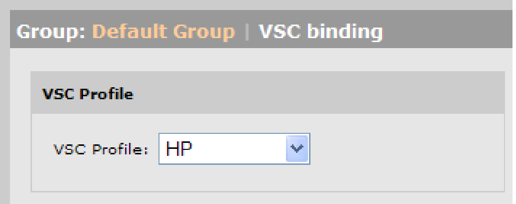
ID: 1

4. Select **Save**.

AP configuration

VSC binding

1. Select **Controller > Controlled APs > Default Group >> VSC bindings** and then select **HP**. The **VSC binding** page appears.



Group: Default Group | VSC binding

VSC Profile

VSC Profile: HP

(For complete screenshot see *VSC configuration options on page 5-5*.)

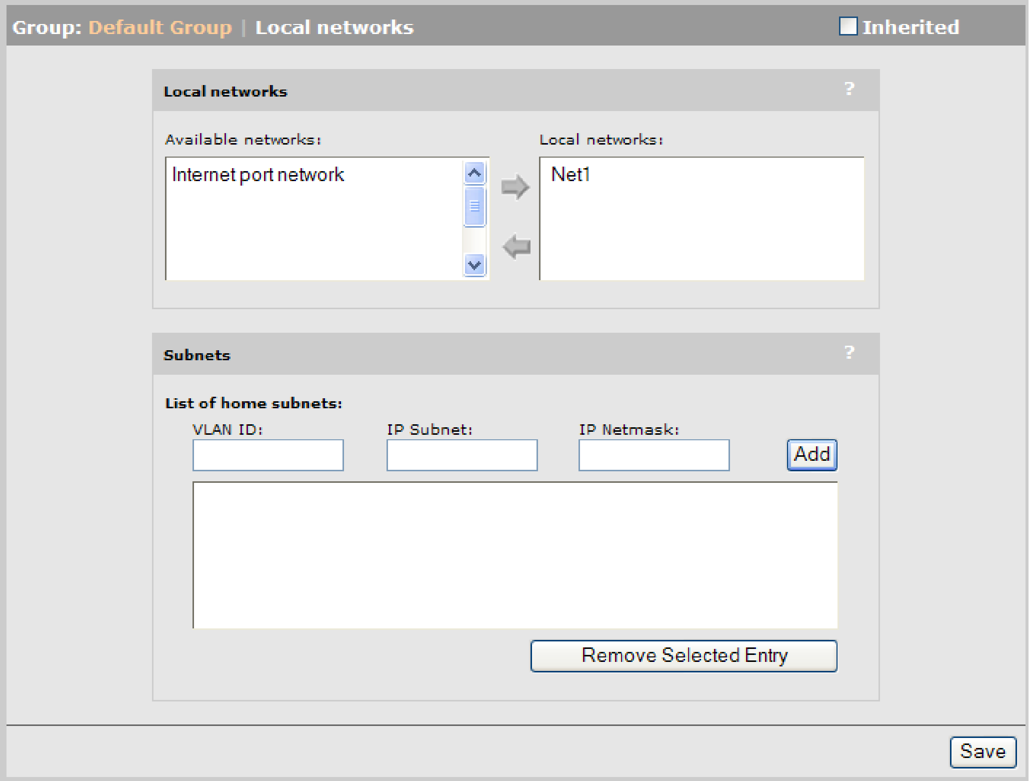
- Set **VSC profile** to **HP**.

2. Select **Save**.

Local network assignment

1. Select **Controller > Controlled APs > Default group >> Configuration > Home networks**.

   - For each AP on network 1, double-click **Net1** to add it to the **Local networks** list.
   - For each AP on network 2, double-click **Net2** to add it to the **Local networks** list.



2. Select **Save**.

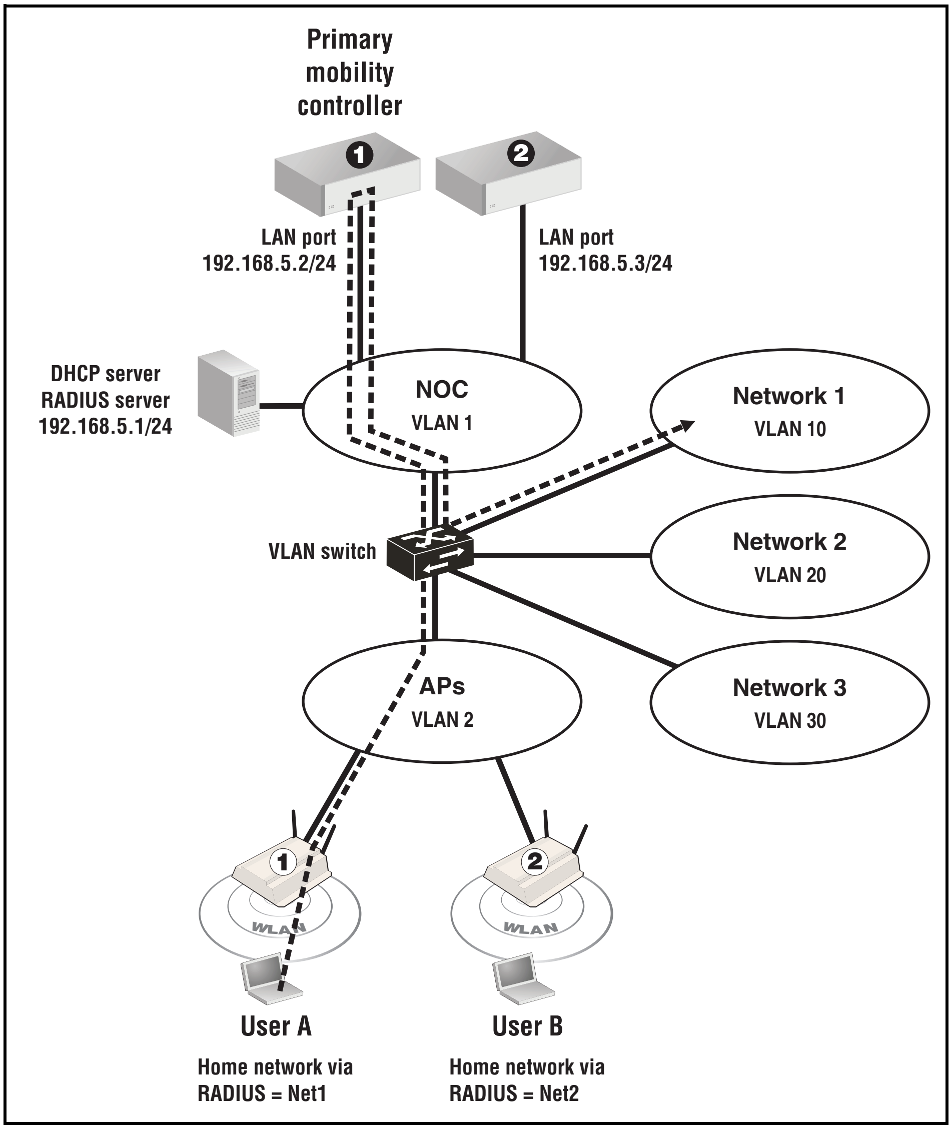
Scenario 5: Traffic routing using VLANs

This scenario explains how to route the traffic from users onto specific VLANs on the wired network.

How it works

In this scenario, traffic on a corporate network is routed using VLANs, creating several logical networks to isolate the network resources for each workgroup. A number of wireless APs are distributed throughout the company and are connected using VLAN 2. Network administrators use VLAN 1 for all equipment installed on the network and in the network operations center (NOC).

The following diagram provides a logical overview of the setup. (Only two APs are shown for clarity).



Wireless clients receive their DHCP address from the DHCP server on the network.

A single VSC is used. It is configured with the **Mobility traffic manager** option enabled. Home networks for users are determined by setting RADIUS VLAN attributes, which map users to the following network profiles:

Network profile name	Assigned to LAN port on	Assigned to VLAN ID
Net1	Controller 1	10
Net2	Controller 2	20
Net3	Controller 2	30
NOC	Controller 1	1

Since all traffic is routed to the VLANs through the LAN port on either controller 1 or 2, no home networks are assigned on the APs.

By assigning different VLANs to different controller ports, traffic can be split between controllers. To reduce the amount of traffic that needs to be tunneled between controllers, APs are assigned to controllers based on their expected use:

- AP 1 is physically located in an area where most of the users as assigned to network 1, therefore it is managed by controller 1.
- AP 2 is physically located in an area where most of the users as assigned to network 2, therefore it is managed by controller 2.

A RADIUS account is defined for each user with attributes set to identify their home network using one of the network profile names:

RADIUS attribute	Network 1 users	Network 2 users	Network 3 users	Network administrators
Tunnel-Medium-Type	802	802	802	802
Tunnel-Private-Group-ID	Net1	Net2	Net3	NOC
Tunnel-Type	VLAN	VLAN	VLAN	VLAN

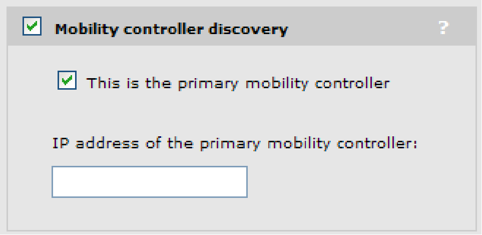
Configuration overview

The following sections provide a summary of the configuration settings needed to enable mobility support only. It is assumed that installation and configuration of all controllers and APs so that they are fully operational on the network was performed as explained in the other chapters in this guide.

Controller 1 configuration

Mobility domain

1. Select **Controller >> Management > Device discovery**.
    - Select **Mobility controller discovery**.
    - Select **This is the primary mobility controller.**



☑ Mobility controller discovery

☑ This is the primary mobility controller

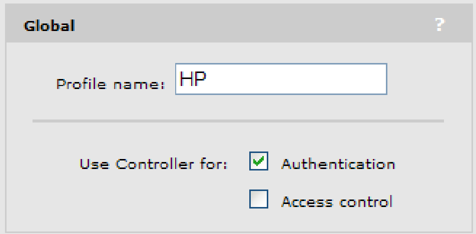
IP address of the primary mobility controller:

(For complete screenshot see *Defining the mobility domain on page 9-9*.)

2. Select **Save**.

VSC

1. Select **Controller >> VSCs > HP**.
    - Under **Global,** disable **Access control**.



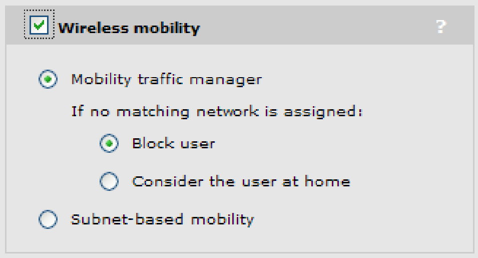
Global

Profile name: HP

Use Controller for: ☑ Authentication
□ Access control

(For complete screenshot see *VSC configuration options on page 5-5*.)

- Select **Wireless mobility**, then under it:
- Select **Mobility traffic manager**.
- Select **Block user.**



☑ Wireless mobility

● Mobility traffic manager

If no matching network is assigned:

● Block user

○ Consider the user at home

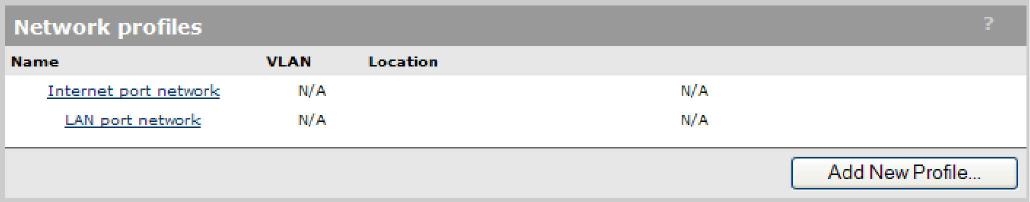
○ Subnet-based mobility

(For complete screenshot see *VSC configuration options on page 5-5*.)

2. Either disable **Wireless security filters** or set it to **Custom**.
3. Select **Save**.

Network profiles

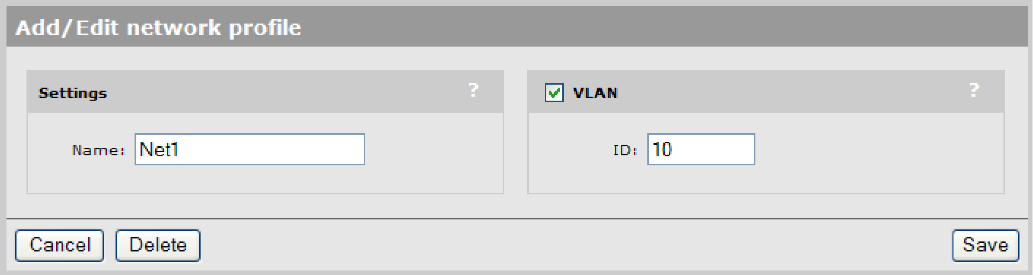
1. Select **Controller >> Network > Network profiles**.



Network profiles

Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A

2. Select **Add New Profile**.



Add/Edit network profile

Settings

Name: Net1

☑ VLAN

ID: 10

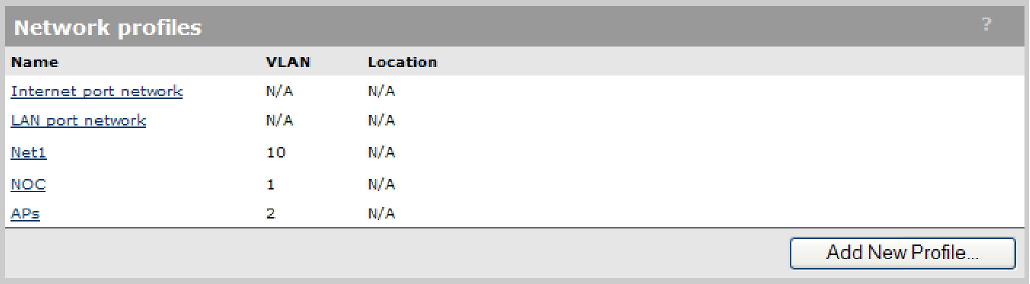
- Under **Settings**, set **Name** to **Net1**.
- Select **VLAN**.
- Under **VLAN**, set **ID** to **10**.

3. Select **Save**.

4. Repeat steps 2 and 3 to define the following profiles:

- Profile name = Net1, VLAN ID = 10
- Profile name = NOC, VLAN ID = 1
- Profile name = APs, VLAN ID = 2

5. When done, the list of network profiles should look like this:

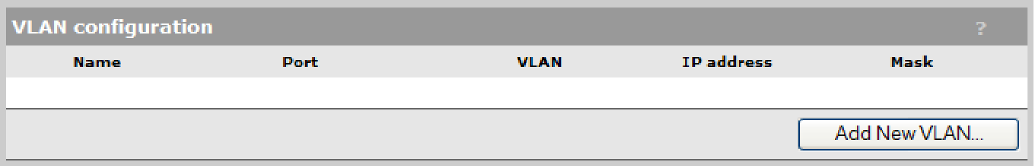


Network profiles

Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A
Net1	10	N/A
NOC	1	N/A
APs	2	N/A

VLANs

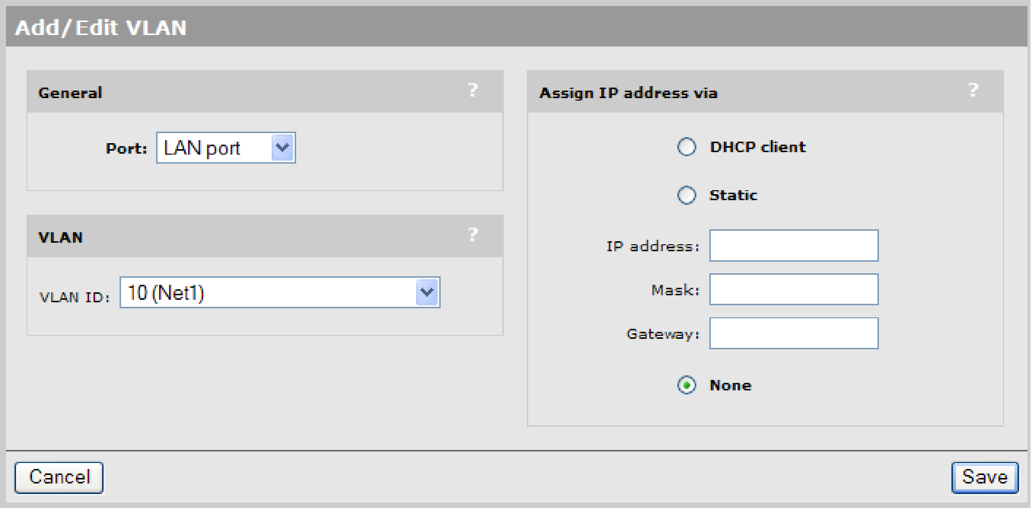
1. Select **Controller > Network > Ports**. Initially, the VLAN configuration list will be empty.



VLAN configuration

Name	Port	VLAN	IP address	Mask

2. Select **Add New VLAN**.



Add/Edit VLAN

General

Port: LAN port

VLAN

VLAN ID: 10 (Net1)

Assign IP address via

○ DHCP client

○ Static

IP address:

Mask:

Gateway:

● None

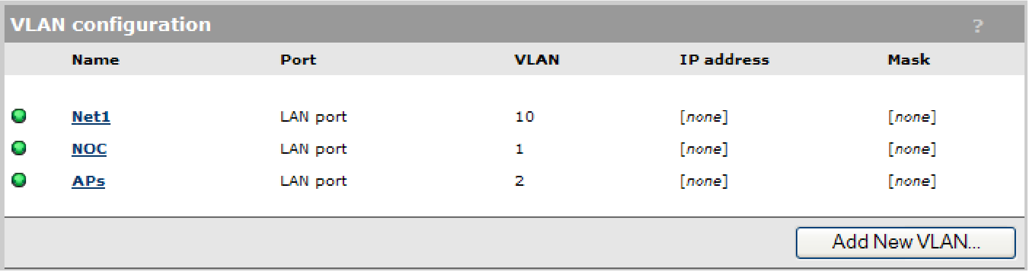
- Under **General**, set **Port** to **LAN port**.
- Under **VLAN**, set **VLAN ID** to **10 (Net1)**.

3. Select **Save**.

4. Repeat steps 2 and 3 to define the following VLANs:

- Port = LAN port, VLAN ID = 1 (NOC)
- Port = LAN port, VLAN ID = 2 (APs)

5. When done, the list of VLANs should look like this:



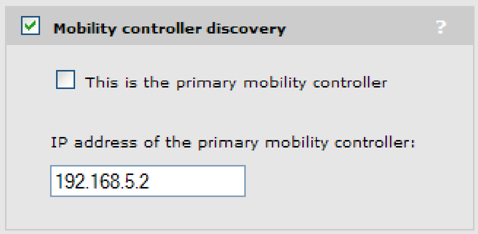
VLAN configuration

	Name	Port	VLAN	IP address	Mask
●	Net1	LAN port	10	[none]	[none]
●	NOC	LAN port	1	[none]	[none]
●	APs	LAN port	2	[none]	[none]

Controller 2 configuration

Mobility domain

1. Select **Controller >> Management > Device discovery**.



☑ Mobility controller discovery

□ This is the primary mobility controller

IP address of the primary mobility controller: 192.168.5.2

(For complete screenshot see *Defining the mobility domain on page 9-9*.)

- Select **Mobility controller discovery**.
- Clear **This is the primary mobility controller.**
- Set the **IP address of the primary mobility controller** to **192.168.5.2**.

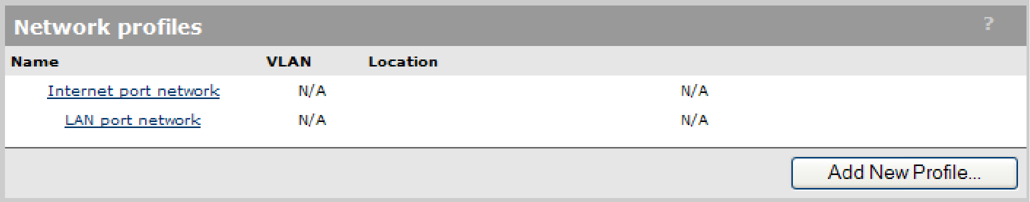
2. Select **Save**.

VSC

Configuration is the same as for controller 1.

Network profiles

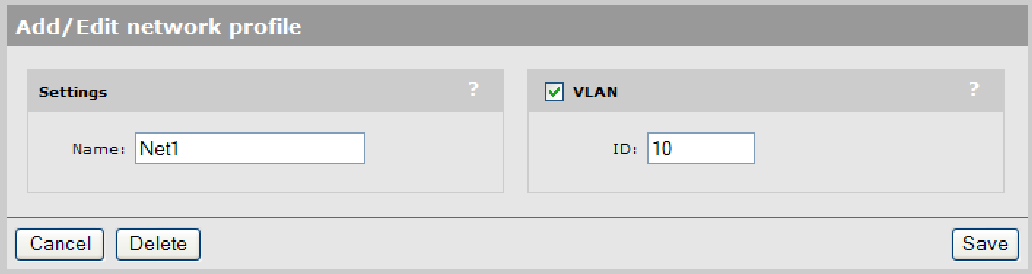
1. Select **Controller >> Network > Network profiles**.



Network profiles

Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A

2. Select **Add New Profile**.



Add/Edit network profile

Settings

Name: Net1

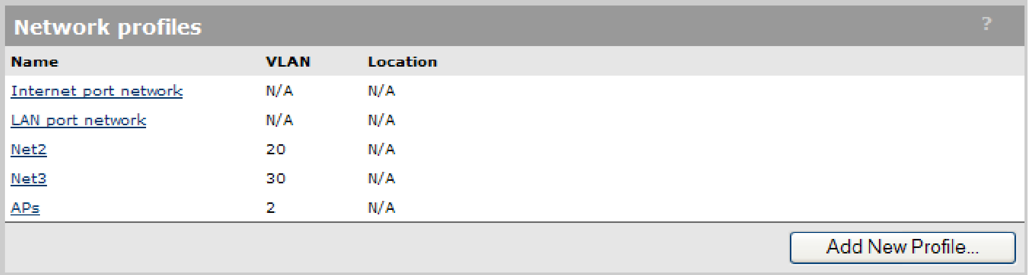
☑ VLAN

ID: 10

- Under **Settings**, set **Name** to **Net1**.
- Select **VLAN**.
- Under **VLAN**, set **ID** to **10**.

3. Select **Save**.

4. Repeat steps 2 and 3 to define the following profiles:
   - Profile name = Net2, VLAN ID = 20
   - Profile name = Net3, VLAN ID = 30
   - Profile name = APs, VLAN ID = 2
5. When done, the list of network profiles should look like this:

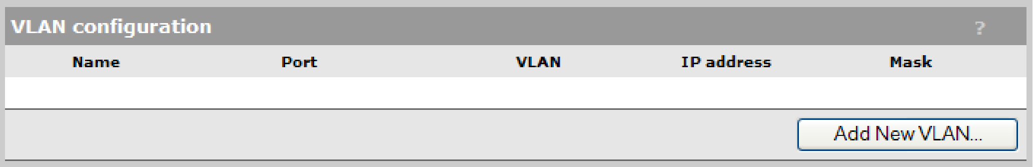


Network profiles

Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A
Net2	20	N/A
Net3	30	N/A
APs	2	N/A

VLANs

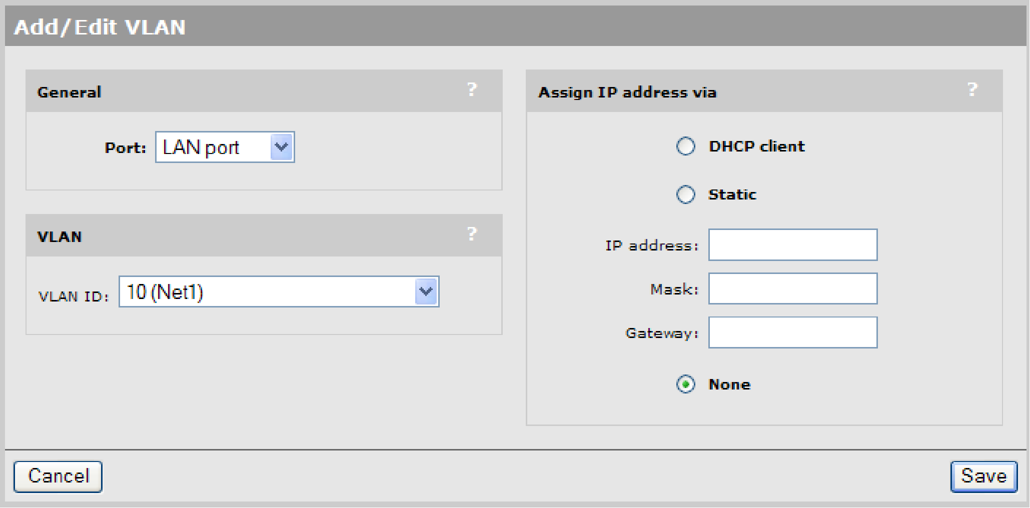
1. Select **Controller > Network > Ports**. Initially, the VLAN configuration list will be empty.



VLAN configuration

Name	Port	VLAN	IP address	Mask

2. Select **Add New VLAN**.



Add/Edit VLAN

General

Port: LAN port

VLAN

VLAN ID: 10 (Net1)

Assign IP address via

○ DHCP client

○ Static

IP address:

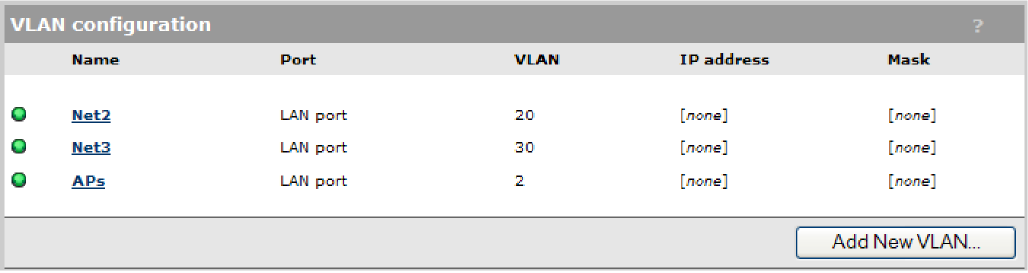
Mask:

Gateway:

● None

   - Under **General**, set **Port** to **LAN port**.
   - Under **VLAN**, set **VLAN ID** to **10 (Net1)**.
3. Select **Save**.

4. Repeat steps 2 and 3 to define the following VLANs:
   - Port = LAN port, VLAN ID = 20 (Net2)
   - Port = LAN port, VLAN ID = 30 (Net3)
   - Port = LAN port, VLAN ID = 2 (APs)
5. When done, the list of VLANs should look like this:



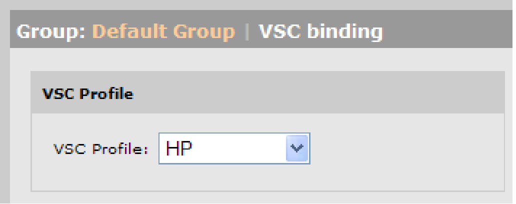
VLAN configuration

	Name	Port	VLAN	IP address	Mask
●	Net2	LAN port	20	[none]	[none]
●	Net3	LAN port	30	[none]	[none]
●	APs	LAN port	2	[none]	[none]

AP configuration

VSC binding

1. Select **Controller > Controlled APs > Default Group >> VSC bindings** and then select **HP**. The **VSC binding** page appears.



Group: Default Group | VSC binding

VSC Profile

VSC Profile: HP

(For complete screenshot see *Binding a VSC to a group on page 6-26*.)

   - Set **VSC profile** to **HP**.

2. Select **Save**.

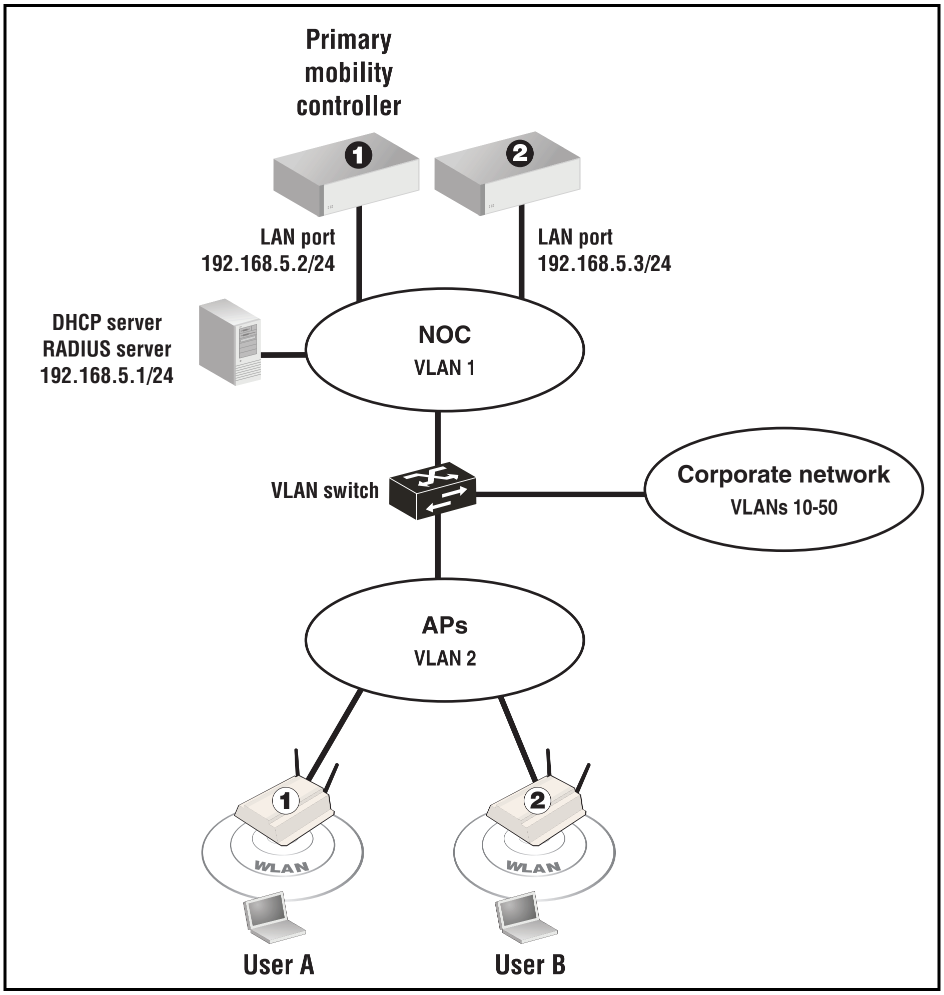
Scenario 6: Distributing traffic using VLAN ranges

This scenario explains how to automatically distribute wireless network traffic onto multiple VLANs on the wired network.

How it works

In this scenario, traffic on a corporate network is segmented onto multiple VLANs to address performance and scalability issues. Traffic from the users on wireless APs needs to be deployed in the same manner. Rather than manually assigning APs and/or groups of users to specific VLANs, MTM can be configured to automatically disperse traffic across a VLAN range. In fact, by defining multiple network profiles, traffic can be mapped to several different ranges, allowing groups of users or APs to be mapped to specific VLAN ranges.

The following diagram provides a logical overview of the setup. (Only two APs are shown for clarity).



Wireless clients receive their DHCP address from the DHCP server on the network.

A single VSC is used. It is configured with the It is configured with the **Wireless mobility, Mobility traffic manager** option enabled. The home network for users is defined by setting the Egress network when the VSC is bound to the APs. The Egress network is mapped to a network profile that defines a range of VLANs on the LAN port on the controller.

Network profile name	Assigned to LAN port on	Assigned to VLAN range
Net1	Controller 1	10-30
Net2	Controller 2	31-50

By assigning a different profile name to AP groups, traffic can be split between controllers. In this example, the APs are split into two groups:

- Group 1: The VSC binding is configured with Egress network set to Net1, putting traffic from this group onto VLAN range 10-30.
- Group 2: The VSC binding is configured with Egress network set to Net2, putting traffic from this group onto VLAN range 11-51.

MTM uses a round-robin mechanism to distribute traffic across the VLANs range. The first wireless user is assigned to the first VLAN in the range. Subsequent users are assigned to the next VLAN in the range. When the range is exhausted, assignment starts with the first VLAN again. For example, if the VLAN range is defined as VLAN IDs 1 to 20, the first user is assigned to VLAN 1. The second is assigned to VLAN 2. The 21st user is assigned to VLAN 1 again. Although VLAN assignment is sequential through the range, from the user's point of view, VLAN assignment will appear to be random.

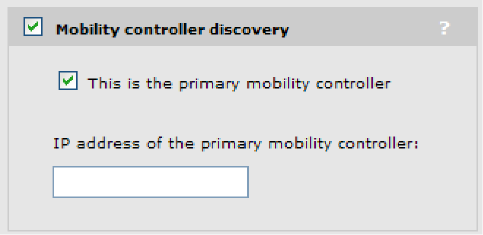
Configuration overview

The following sections provide a summary of the configuration settings needed to enable mobility support only. It is assumed that installation and configuration of all controllers and APs so that they are fully operational on the network was performed as explained in the other chapters in this guide.

Controller 1 configuration

Mobility domain

1. Select **Controller >> Management > Device discovery**.
   - Select **Mobility controller discovery**.
   - Select **This is the primary mobility controller.**



☑ Mobility controller discovery

☑ This is the primary mobility controller

IP address of the primary mobility controller:

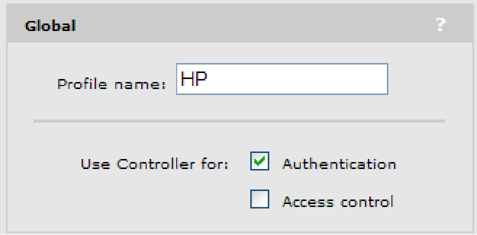
(For complete screenshot see *Defining the mobility domain on page 9-9*.)

2. Select **Save**.

VSC

1. Select **Controller >> VSCs > HP**.

Under Global
- Clear **Access control**.



Global

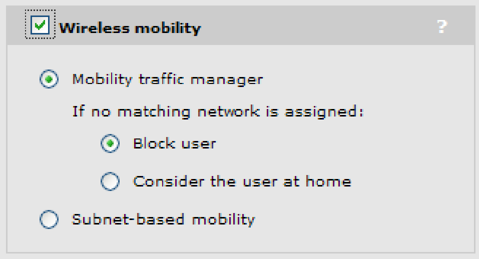
Profile name: HP

Use Controller for: ☑ Authentication

☐ Access control

(For complete screenshot see *VSC configuration options on page 5-5*.)

- Select **Wireless mobility**, then under it:
- Select **Mobility traffic manager**.
- Select **Block user.**



☑ Wireless mobility

● Mobility traffic manager

If no matching network is assigned:

● Block user

○ Consider the user at home

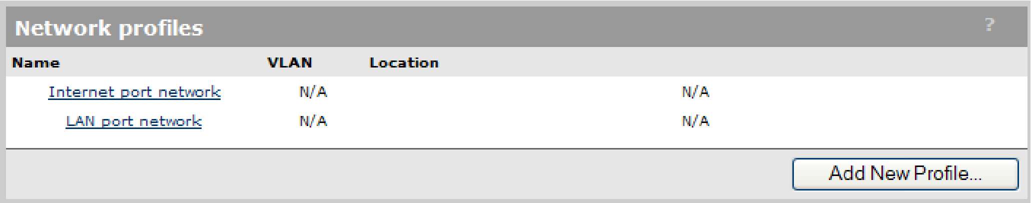
○ Subnet-based mobility

(For complete screenshot see *VSC configuration options on page 5-5*.)

2. Either disable **Wireless security filters** or set it to **Custom**.
3. Select **Save**.

Network profiles

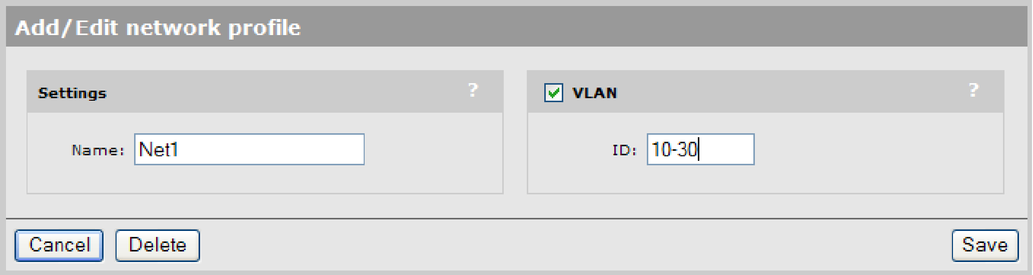
1. Select **Controller >> Network > Network profiles**.



Network profiles

Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A

2. Select **Add New Profile**.



Add/Edit network profile

Settings

Name: Net1

☑ VLAN

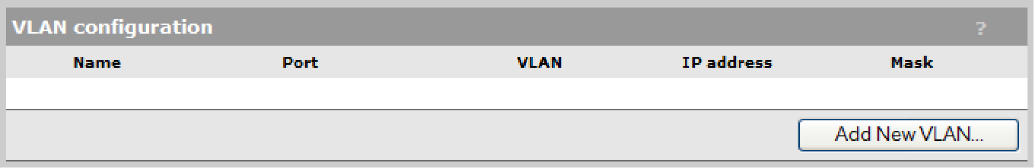
ID: 10-30

- Under **Settings**, set **Name** to **Net1**.
- Select **VLAN**.
- Under **VLAN**, set **ID** to **10-30**.

3. Select **Save**.

VLANs

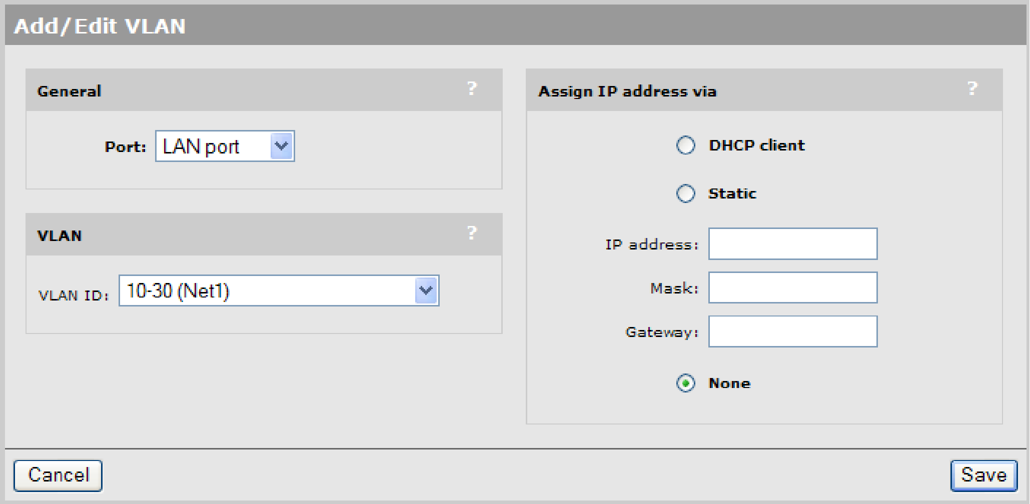
1. Select **Controller >> Network > Ports**. Initially, the VLAN configuration list will be empty.



VLAN configuration

Name	Port	VLAN	IP address	Mask

2. Select **Add New VLAN**.



Add/Edit VLAN

General

Port: LAN port

VLAN

VLAN ID: 10-30 (Net1)

Assign IP address via

○ DHCP client

○ Static

IP address:

Mask:

Gateway:

● None

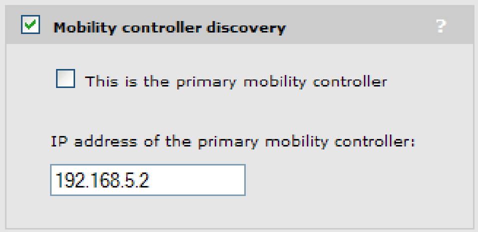
- Under **General**, set **Port** to **LAN port**.
- Under **VLAN**, set **VLAN ID** to **10-30 (Net1)**.

3. Select **Save**.

Controller 2 configuration

Mobility domain

1. Select **Controller >> Management > Device discovery**.



☑ **Mobility controller discovery**

□ This is the primary mobility controller

IP address of the primary mobility controller:

192.168.5.2

(For complete screenshot see *Defining the mobility domain on page 9-9*.)

- Select **Mobility controller discovery**.
- Clear **This is the primary mobility controller.**
- Set the **IP address of the primary mobility controller** to **192.168.5.2**.

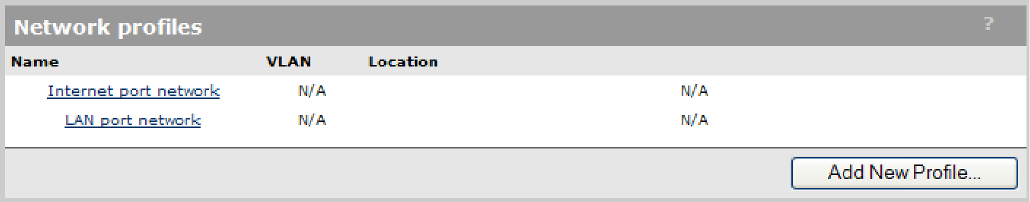
2. Select **Save**.

VSC

Configuration is the same as for controller 1.

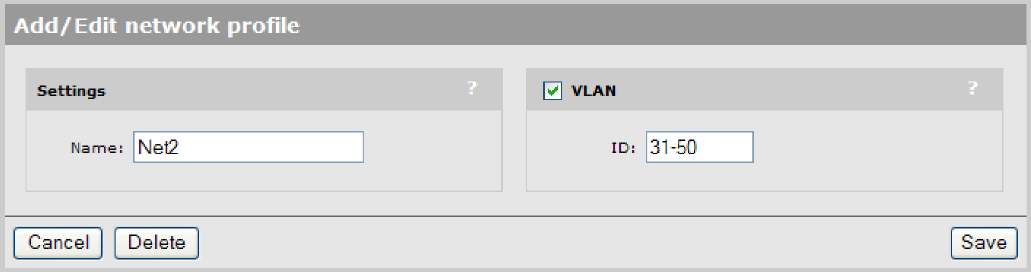
Network profiles

1. Select **Controller >> Network > Network profiles**.



Name	VLAN	Location
Internet port network	N/A	N/A
LAN port network	N/A	N/A

2. Select **Add New Profile**.



Settings

Name: Net2

☑ VLAN

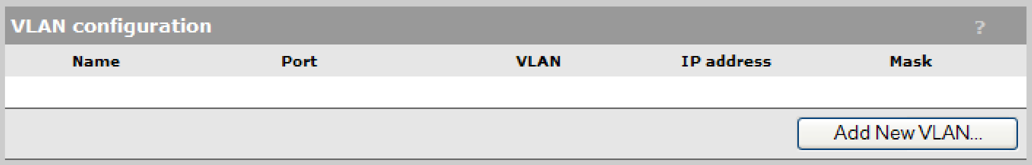
ID: 31-50

- Under **Settings**, set **Name** to **Net2**.
- Select **VLAN**.
- Under **VLAN**, set **ID** to **31-50**.

3. Select **Save**.

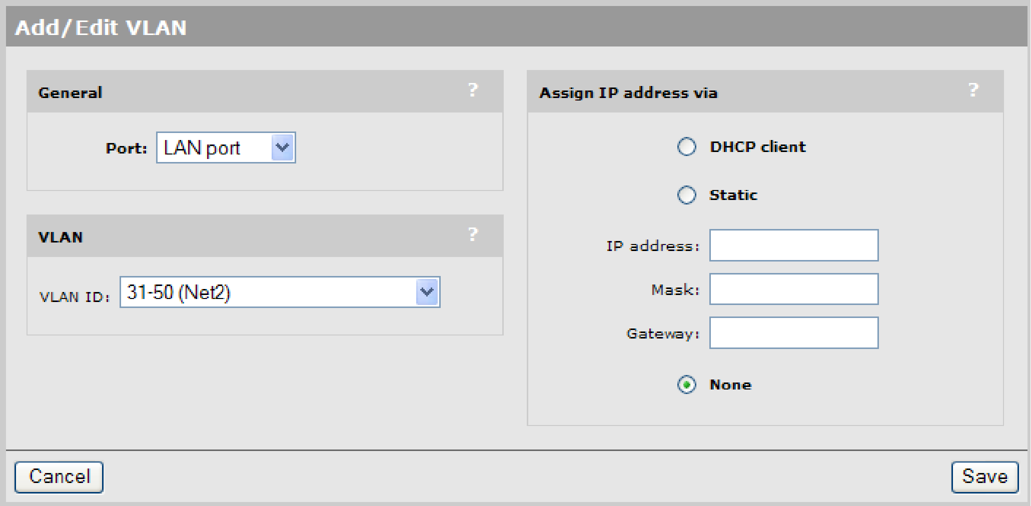
VLANs

1. Select **Controller >> Network > Ports**. Initially, the VLAN configuration list will be empty.



Name	Port	VLAN	IP address	Mask

2. Select **Add New VLAN**.



Add/Edit VLAN

General

Port: LAN port

VLAN

VLAN ID: 31-50 (Net2)

Assign IP address via

○ DHCP client

○ Static

IP address:

Mask:

Gateway:

● None

- Under **General**, set **Port** to **LAN port**.
- Under **VLAN**, set **VLAN ID** to **31-50 (Net2)**.

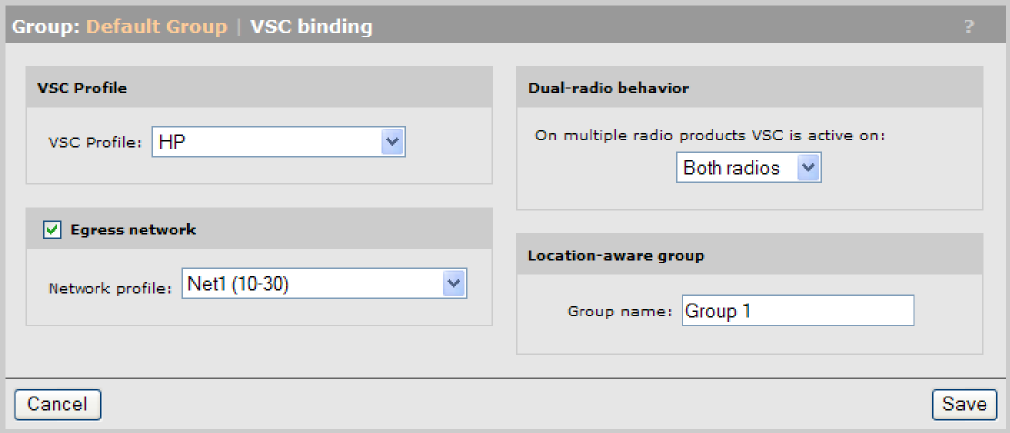
3. Select **Save**.

AP configuration

Split the APs into two groups as explained in *Working with groups on page 6-25*. Call them Group 1 and Group 2.

VSC binding for Group 1

1. Select **Controller > Controlled APs > Group 1 >> VSC bindings** and then select **HP**. The **VSC binding** page appears.



Group: Default Group | VSC binding

VSC Profile

VSC Profile: HP

☑ Egress network

Network profile: Net1 (10-30)

Dual-radio behavior

On multiple radio products VSC is active on: Both radios

Location-aware group

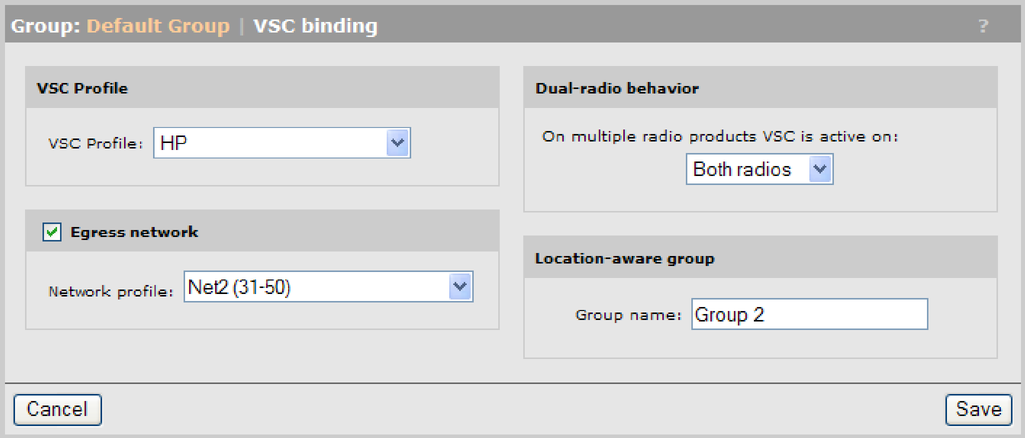
Group name: Group 1

- Set **VSC profile** to **HP**.
- Select **Egress network**, then for **Network profile**, select **Net1 (10-30)**.

2. Select **Save**.

VSC binding for Group 2

1. Select **Controller > Controlled APs > Group 2 >> VSC bindings** and then select **HP**. The **VSC binding** page appears.



Group: Default Group | VSC binding

VSC Profile

VSC Profile: HP

Dual-radio behavior

On multiple radio products VSC is active on: Both radios

☑ **Egress network**

Network profile: Net2 (31-50)

Location-aware group

Group name: Group 2

- Set **VSC profile**, to **HP**.
- Select **Egress network**, then for **Network profile**, select **Net2 (31-50)**.

2. Select **Save**.

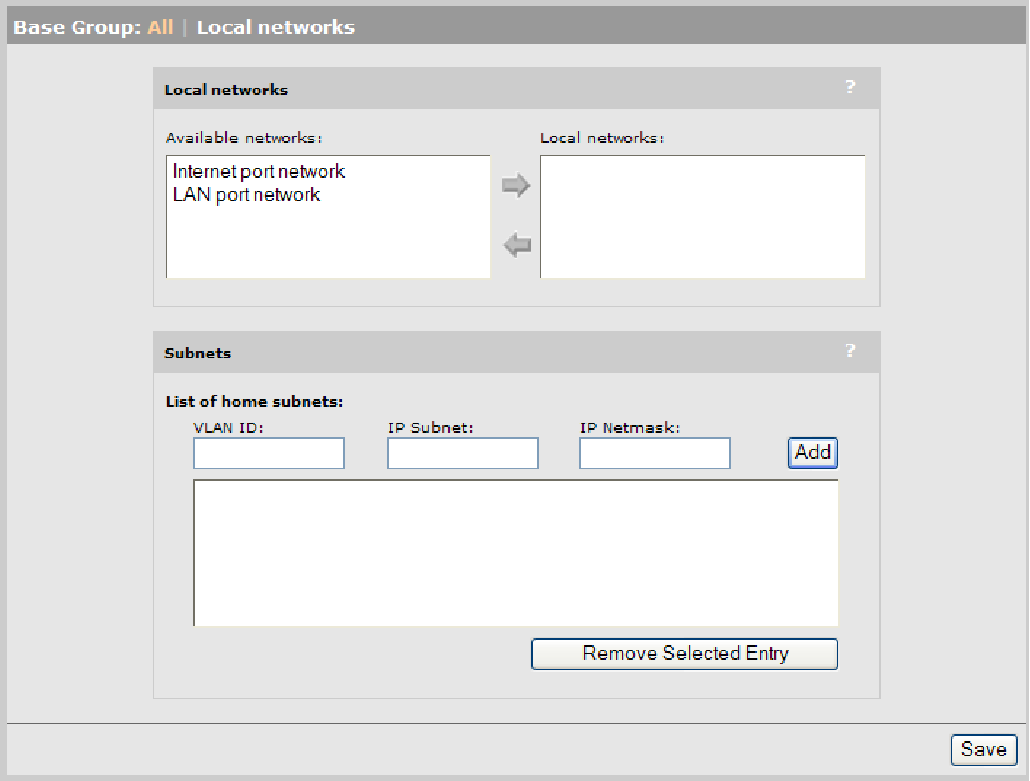
Subnet-based mobility

This feature has been deprecated.

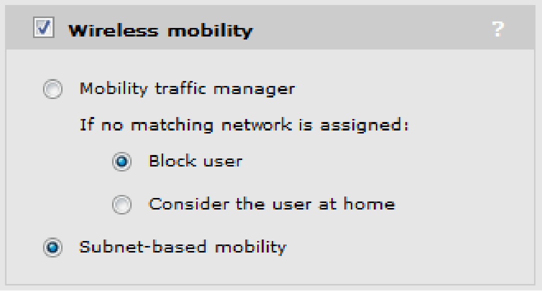
If you are creating a new installation, use Mobility Traffic Manager. If you are upgrading from a previous release, your subnet-based configuration will still work. However, for added benefits and greater flexibility you should migrate your setup to Mobility Traffic Manager.

For reference, subnet-based mobility configuration options appear on the following pages:

- **Controller > Controlled APs >> Configuration > Local networks**
- **Controller > Controlled APs > [*group*] >> Configuration > Local networks**
- **Controller > Controlled APs > [*AP*] >> Configuration > Local networks**



- **Controller > VSCs >> [*VSC-name*]**



☑ **Wireless mobility**

○ Mobility traffic manager

If no matching network is assigned:

● Block user

○ Consider the user at home

● Subnet-based mobility

10

User authentication, accounts, and addressing

Contents

Introduction

Note

This chapter discusses user authentication as it applies to the controller and controlled APs only. For information on authentication when working with autonomous APs, see *Chapter 19: Working with autonomous APs*.

User authentication tasks can be handled either by the AP or by the controller. This is controlled by the settings of the access control and authentication options on the VSC to which a user is connected. See *About access control and authentication on page 5-6*.

Authentication support

The following table lists all authentication types that are supported for user authentication and indicates how they apply to wired and wireless users.

Auth type	**The *Use controller for* option is set to:**			**For more information, see ...**
	Authentication	**Authentication and Access control**	**Neither**	
802.1X (VSC)	Wireless + wired* users authenticated via: ■ Local user accounts ■ External RADIUS server ■ Active Directory	Wireless + wired* users authenticated via: ■ Local user accounts ■ External RADIUS server ■ Active Directory	Wireless + wired users authenticated via: ■ External RADIUS server	*Configuring 802.1X support on a VSC on page 10-10*.
802.1X (Switch port)	Only supported when the switch port is not bound to a VSC. Supports wired users only.			*Configuring 802.1X support on an MSM317 switch port on page 10-14*.
MAC-based (Global)	Not supported	Wireless + wired* users authenticated via: ■ Local user accounts ■ External RADIUS server ■ Active Directory	Not supported	*Configuring global MAC-based authentication on page 10-16*.

Auth type	**The *Use controller for* option is set to:**			**For more information, see ...**
	Authentication	**Authentication and Access control**	**Neither**	
MAC-based (VSC)	Wireless users authenticated via: ■ Local user accounts ■ External RADIUS server ■ Active Directory	Wireless users authenticated via: ■ Local user accounts ■ External RADIUS server ■ Active Directory	Wireless + wired users authenticated via: ■ External RADIUS server	*Configuring MAC-based authentication on a VSC on page 10-17.*
MAC-based (Switch port)	Only supported when the switch port is not bound to a VSC. Supports wired users only.			*Configuring MAC-based authentication on an MSM317 switch port on page 10-19.*
HTML-based	Not supported	Wireless users authenticated via: ■ Local user accounts on the controller ■ External RADIUS server ■ Active Directory	Not supported	*Configuring HTML-based authentication on a VSC on page 10-22.*
VPN-based	Not supported	Wireless + wired* users authenticated via: ■ Local user accounts on the controller ■ External RADIUS server ■ Active Directory	Not supported	*Configuring global MAC-based authentication on page 10-16.*
No authentication	Wireless + wired users*			*No authentication on page 10-26.*

** Wired users are only supported on the default VSC, unless their traffic is on a VLAN that matches the VSC ingress defined on another VSC. (On a controller team, wired users are only supported via the MSM317 switch ports.)*

Other access control methods

Although not authentication options, the following features can also be used to limit access to the wireless port.

Feature	**The *Use controller for* option is set to:**			**For more information, see ...**
	Authentication	**Authentication and Access control**	**Neither**	
MAC lockout (Global)	Not supported	Wireless/wired users connected via: ■ Wireless ports on controlled APs ■ Wired ports (including switch ports) on controlled APs ■ Local mesh ports on controlled APs ■ The LAN port on the controller MAC lockout does not apply to the Internet port on the controller.	Not supported	*MAC lockout on page 12-13*
MAC filtering (VSC)	Not supported	Wireless users authenticated via: ■ Local user accounts on the controller ■ External RADIUS server ■ Active Directory	Not supported	*MAC-based filtering on page 10-16* *Configuring MAC-based filters on a VSC on page 10-19*. *Configuring MAC-based filters on an MSM317 switch port on page 10-20*
IP filtering (VSC)	Not supported	Wireless users authenticated via: ■ Local user accounts on the controller ■ External RADIUS server ■ Active Directory	Not supported	*Wireless IP filter on page 5-30*.

Using more than one authentication type at the same time

For added flexibility, you can enable multiple authentication types on a VSC at the same time to support users with different needs. How this works depends on setting of the **Use Controller for** option in the VSC. The following table lists all possible combinations of authentication types (and other features) that can be activated, and shows the order in which they are applied.

The *Use controller for* option is set to:		
Authentication	**Authentication and Access control**	**Neither**
■ MAC lockout **+** Wireless MAC filter **+** MAC-based (VSC) **+** 802.1X (VSC)	■ MAC lockout **+** Wireless MAC filter **+** MAC-based (Global) **+** HTML-based *or* ■ MAC lockout **+** Wireless MAC filter **+** 802.1X **+** HTML-based *or* ■ MAC lockout **+** Wireless MAC filter **+** 802.1X **+** MAC-based (VSC) *or* ■ MAC lockout **+** VPN-based	■ MAC lockout **+** Wireless MAC filter **+** MAC-based (VSC) **+** 802.1X (VSC)

When MAC-based authentication and 802.1X authentication are enabled

Clients stations only gain access when they are successfully authenticated by both methods. If one method fails, then access is denied.

When MAC-based authentication and Wireless MAC filter are enabled

The following table describes how the Wireless MAC filter option interacts with MAC-based authentication.

Wireless MAC filter setting	**Result**
Client address is in the list and the filter is set to **block**.	Client access is denied. MAC-based authentication is not performed.

Wireless MAC filter setting	Result
Client address is in the list and the filter is set to **allow**.	Client access is granted. MAC-based authentication is not performed.
Client address not in the list.	Client access is granted or denied based on result of MAC-based authentication.

Switch port not bound to a VSC

When a switch port is not bound to a VSC, the following authentication options are supported:

- 802.1X (Switch port)
- MAC-based (Switch port)

If both options are enabled at the same time, then:

- 802.1X takes priority for client stations that are 802.1X enabled. If 802.1X authentication fails, MAC authentication is not checked and the client station fails to authenticate.
- MAC authentication takes priority for client stations that are not 802.1X enabled. If MAC authentication fails, then the client station fails to authenticate.

User authentication limits

The following limits apply:

Controller	Maximum number of controlled APs	Maximum number of locally defined user accounts	Maximum number of active user sessions
710	10	500	100
730	40	2000	500
750	200	2000	2000
760	200	2000	2000
765	200	2000	2000
Controller Team	800	2000	2000

802.1X authentication

802.1X is a popular protocol for user authentication that is natively supported on most client stations. 802.1X authentication can be configured at different levels as described in the following table.

VSC	Switch port
Authentication tasks are managed by either the controller or the AP. (Depends on how the VSC is configured.)	Authentication tasks are managed by the MSM317.
Applies to wireless and wired users.	Applies to wired users only.
Settings are defined on a per-VSC basis.	Settings are defined on a per-port basis.
Can be used on access-controlled and non-access-controlled VSCs.	Can only be used when a switch port is not bound to a VSC.
Configured using the **Add/Edit Virtual Service Community** configuration page in the management tool.	Configured by selecting **Controlled APs > [*MSM317-AP*] >> Configuration > Switch ports > [*switch-port*]** in the management tool.
User credentials can be validated using: ■ Local user accounts on the controller ■ External RADIUS server ■ Active Directory (Depends on how the VSC is configured.)	User credentials can be validated using: ■ External RADIUS server
See: ■ *Configuring 802.1X support on a VSC on page 10-10*. ■ *Configuring global 802.1X settings for wired users on page 10-12*. ■ *Configuring global 802.1X settings for wireless users on page 10-13*.	See *Configuring 802.1X support on an MSM317 switch port on page 10-14*.

Supported 802.1X protocols

The following table lists the 802.1X protocols supported by the internal RADIUS server on the controller, and when using a third-party RADIUS server.

Protocol	Local user accounts (via Internal RADIUS server)	Third-party RADIUS server	Certificates required
EAP-MD5	×	✔	No
EAP-TLS	✔	✔	Client and Server
EAP-TTLS	✔	✔	Server
LEAP	×	✔	No
PEAPv0	✔	✔	Server
PEAPv1	×	✔	Server
EAP-FAST	×	✔	Optional
EAP-SIM	×	✔	Server
EAP-AKA	×	✔	Server

The EAP protocols in this table are known to work with the controller. Other EAP protocols may also work but have not been tested.

Protocol definitions

The following are brief definitions for the supported protocols. For more detailed information, see the appropriate RFC for each protocol.

- EAP-MD5: Extensible Authentication Protocol Message Digest 5. Offers minimum security. Not recommended.
- EAP-TLS: Extensible Authentication Protocol Transport Layer Security. Provides strong security based on mutual authentication. Requires both client and server-side certificates.
- EAP-TTLS: Extensible Authentication Protocol Tunnelled Transport Layer Security. Provides excellent security with less overhead than TLS as client-side certificates can be used, but are not required.
- LEAP: Lightweight Extensible Authentication Protocol. Provides mutual authentication between a wireless client and the RADIUS server. Supports WEP, TKIP, and WPA2 keys.

Note

LEAP is not supported on access-controlled VSCs.

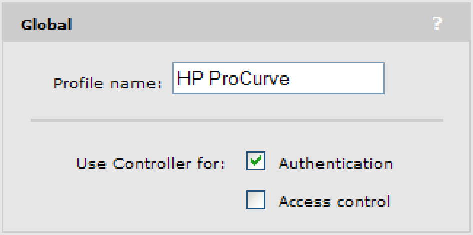
- PEAPv0: Protected Extensible Authentication Protocol. One of the most supported implementations across all client platforms. Uses MSCHAPv2 as the inner protocol.
- PEAPv1: Protected Extensible Authentication Protocol. Alternative to PEAPv0 that permits other inner protocols to be used.

- EAP-FAST: Extensible Authentication Protocol Flexible Authentication via Secure Tunneling. Can use a pre-shared key instead of server-side certificate.

Configuring 802.1X support on a VSC

Each VSC can have unique settings for 802.1X authentication. These settings are defined on the VSC profile page. (To open this page, see *Viewing and editing VSC profiles on page 5-4*).

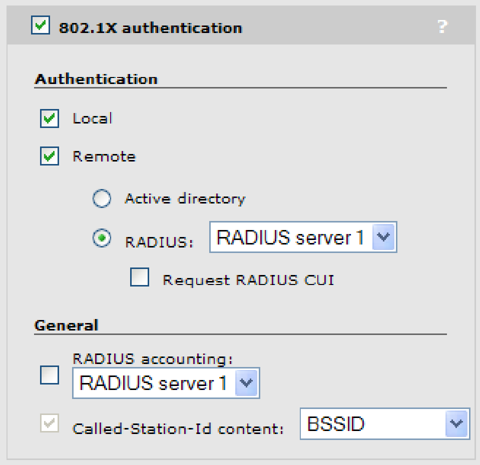
- When the **Use controller for Authentication** option is enabled under **General**, 802.1X authentication tasks are handled by the controller. APs forward all authentication requests to the controller which validates user login credentials using the local user accounts or a third-party authentication server (RADIUS or Active Directory).



Global

Profile name: HP ProCurve

Use Controller for: ☑ Authentication
□ Access control



☑ **802.1X authentication**

Authentication

☑ Local

☑ Remote

○ Active directory

● RADIUS: RADIUS server 1

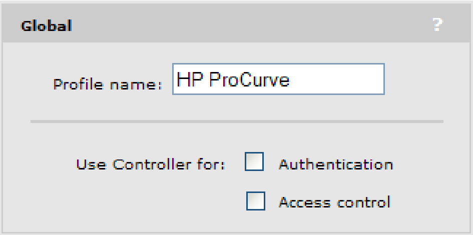
□ Request RADIUS CUI

General

□ RADIUS accounting: RADIUS server 1

☑ Called-Station-Id content: BSSID

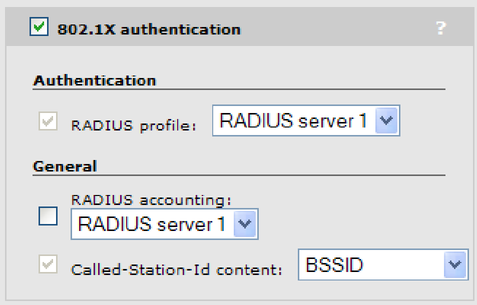
- When the **Use controller for Authentication** option is disabled under **General**, 802.1X authentication tasks are handled directly by the AP. The AP uses the services of a third-party RADIUS server (configured by defining a RADIUS profile on the **Controller >> Authentication > RADIUS profiles** page) to validate user login credentials.



Global

Profile name: HP ProCurve

Use Controller for: □ Authentication
□ Access control



☑ **802.1X authentication**

Authentication

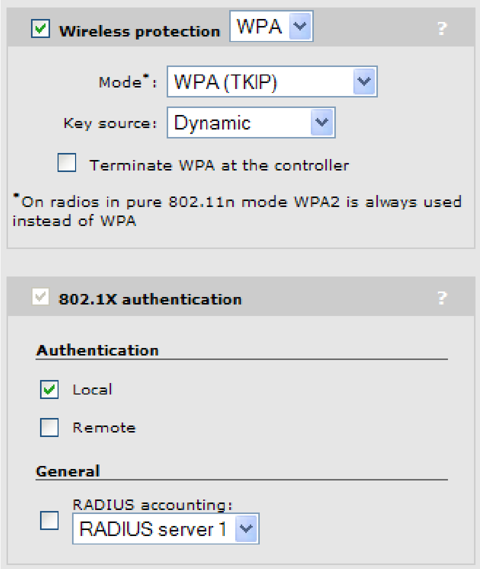
☑ RADIUS profile: RADIUS server 1

General

□ RADIUS accounting: RADIUS server 1

☑ Called-Station-Id content: BSSID

Note When the **Wireless protection** option in a VSC is set to **WPA** with a **Key source** of **Dynamic**, 802.1X is automatically enabled.



☑ Wireless protection: WPA

Mode*: WPA (TKIP)

Key source: Dynamic

□ Terminate WPA at the controller

*On radios in pure 802.11n mode WPA2 is always used instead of WPA

☑ 802.1X authentication

Authentication

☑ Local

□ Remote

General

□ RADIUS accounting: RADIUS server 1

Authentication

Local

User logins are authenticated with the list defined on the **Controller >> Users > User accounts** page.

Remote

- **Active Directory:** User logins are authenticated via Active Directory. To setup Active Directory support go to the **Controller >> Security > Active Directory** page.
- **RADIUS:** User logins are authenticated via an external RADIUS server. To setup the connection to an external RADIUS server, go to the **Controller >> Authentication > RADIUS profiles** page.
  - **Request RADIUS CUI:** Enable this option to support the Chargeable User Identity (CUI) attribute as defined in RFC-4372. The CUI is used to associate a unique identifier with a user so that the user can be identified (for billing, authentication or other purposes) when roaming outside of their home network.

General

RADIUS accounting

Enable this option to have the controller generate a RADIUS START/STOP and interim request for each user. The controller respects the RADIUS interim-update-interval attribute if present inside the RADIUS access accept of the authentication.

Called-Station-ID content

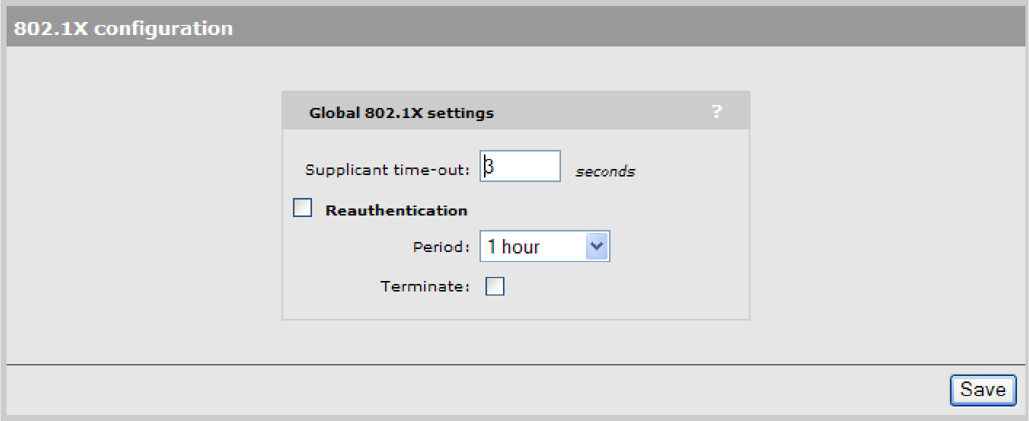
(Only available when **Access control** is disabled under **Global**)

Select the value that the AP (with which the user has established a wireless connection) will return as the called station ID.

- **Port 1**: MAC address of the first Ethernet port on the AP.
- **Port 2**: MAC address of the second Ethernet port on the AP. (Not supported on all APs.)
- **Wireless Radio**: MAC address of the wireless radio on the AP on which this VSC is operating.
- **BSSID**: Basic service set ID of the wireless network defined for this VSC.
- **macaddress:ssid:** The MAC address of the AP radio, followed by a colon, followed by the SSID configured on this VSC.

Configuring global 802.1X settings for wired users

Global 802.1X settings selecting **Controller >> Authentication > 802.1X.**



802.1X configuration

Global 802.1X settings

Supplicant time-out: 3 seconds

□ Reauthentication

Period: 1 hour

Terminate: □

These settings only apply to:

- Wired clients connected to the service controller via the LAN port.
- Wireless clients using an access-controlled VSC with **Wireless protection** set to **WPA** and the **Terminate WPA at the controller** option enabled. See *Terminate WPA at the controller on page 5-24*.

These settings do not apply to clients connected to the switch port on an MSM317.

Supplicant timeout

Specify the maximum length of time that the service controller will wait for a client station to respond to an EAPOL packet before resending it.

If client stations are configured to manually enter the 802.1X username and/or the password, you must increase the value of the timeout to between 15 and 20 seconds.

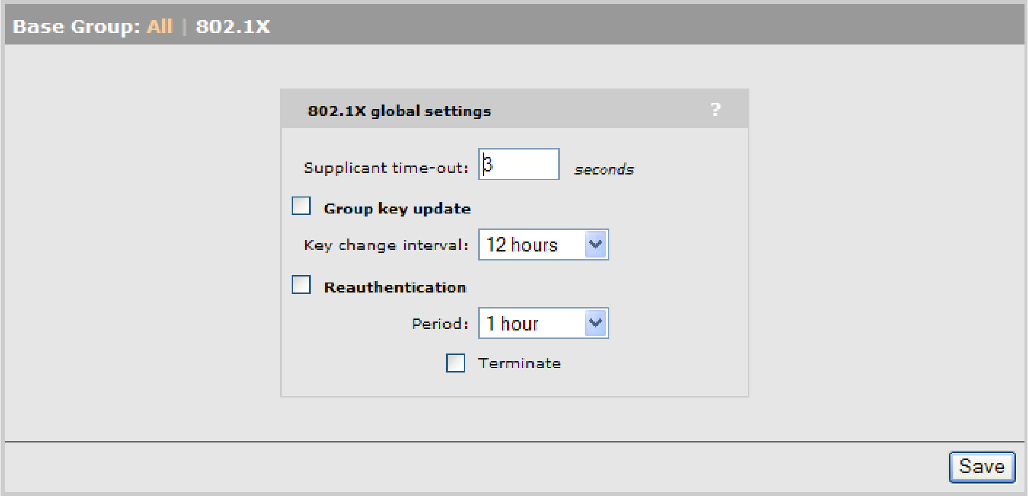
Reauthentication

Enable this option to force 802.1X clients to re-authenticate after the specified **Period**.

- **Period:** Client stations must reauthenticate after this amount of time has passed since their last reauthentication.
- **Terminate**
  - **Disabled:** Client stations remain connected during re-authentication and client traffic is blocked only when re-authentication fails.
  - **Enabled:** Client traffic is blocked during re-authentication and is only activated again if authentication succeeds.

Configuring global 802.1X settings for wireless users

Global 802.1X settings for wireless users connected to controlled APs are defined by selecting **Controlled APs >> Configuration > 802.1X.**



Base Group: All | 802.1X

802.1X global settings

Supplicant time-out: 3 seconds

□ **Group key update**

Key change interval: 12 hours

□ **Reauthentication**

Period: 1 hour

□ Terminate

Supplicant timeout

Specify the maximum length of time for the to wait for a client station to respond to an EAPOL packet before resending it.

EAPOL (Extensible Authentication Protocol over LAN) is used for 802.1X port access control. 802.1X can be used to authenticate at "network connect time" when using either wired or wireless LAN adapters.

If client stations are configured to manually enter the 802.1X username or password or both, increase the value of the timeout to 15 to 20 seconds.

Group key update

Enable this option to force updating of 802.1X group keys at the specified **Key change interval**.

Reauthentication

Enable this option to force 802.1X clients to reauthenticate.

Period

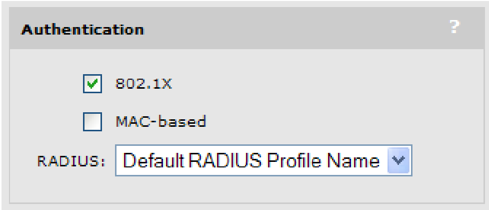
Specify the interval at which client stations must reauthenticate.

Terminate

- **Disabled**: Client station remains connected during reauthentication. Client traffic is blocked only when reauthentication fails.
- **Enabled**: Client traffic is blocked during reauthentication and is only reactivated if authentication succeeds.

Configuring 802.1X support on an MSM317 switch port

If a switch on the MSM317 port is not bound to a VSC, then 802.11X can be enabled on it.



Authentication

☑ 802.1X

□ MAC-based

RADIUS: Default RADIUS Profile Name

802.1X authentication tasks are handled by the MSM317. The MSM317 uses the services of a third-party RADIUS server (configured by defining a RADIUS profile on the **Controller >> Authentication > RADIUS profiles** page) to validate user login credentials.

MAC-based authentication

MAC-based authentication can be used to automatically authenticate wired or wireless devices as soon as they appear on the network, eliminating the need for manual login. This is useful for authenticating devices that do not have a Web browser and are permanently installed on a network (a printer or point-of-sale terminal, for example), but can also be used for regular users.

MAC authentication can be configured at several different levels as described in the following table.

Global	**VSC**	**Switch port**
Authentication is handled by the controller.	Authentication is handled by either the controller or the AP. (Depends on how the VSC is configured.)	Authentication is handled by the MSM317.
Applies to both wireless and wired users.	Applies to wireless users if the VSC is configured for either Authentication and/or Access control. If neither are configured, applies to both wireless and wired users.	Applies to wired users only.
Settings apply globally to all VSCs, except for the authentication server which is defined on a per-VSC basis.	Settings are defined on a per-VSC basis.	Settings are defined on a per-port basis.
Can only be used on access-controlled VSCs that have HTML-based user logins enabled.	Can be used on non-access-controlled VSCs, or on access-controlled VSCs that have HTML-based user logins disabled.	Can only be used when the switch port is not bound to a VSC.
Configured using a RADIUS attribute or local public access attribute.	Configured using the **Add/Edit Virtual Service Community** configuration page in the management tool.	Configured by selecting **Controlled APs > [*MSM317-AP*] >> Configuration > Switch ports > [*switch-port*]** in the management tool.
User credentials can be validated using: ■ Local user accounts on the controller ■ External RADIUS server ■ Active Directory	User credentials can be validated using: ■ Local user accounts on the controller ■ External RADIUS server (Depends on how the VSC is configured.)	User credentials can be validated using: ■ External RADIUS server
See *Configuring global MAC-based authentication on page 10-16*.	See *Configuring MAC-based authentication on a VSC on page 10-17*.	See *Configuring MAC-based authentication on an MSM317 switch port on page 10-19*.

MAC-based filtering

In addition, MAC-based filters can also be used to manage access to the network.

VSC	Switch port
Filtering occurs on the AP wireless interfaces.	Filtering occurs individually on each MSM317 switch port.
Applies to wireless client stations only.	Applies to wired client stations only.
Settings are defined on a per-VSC basis.	Settings are defined on a per-port basis.
Can be used on both access-controlled and non-access-controlled VSCs.	Can only be used when the switch port is not bound to a VSC.
Configured using the **Add/Edit Virtual Service Community** configuration page in the management tool.	Configured by selecting **Controlled APs >** **[*MSM317-AP*] >> Configuration > Switch ports > [*switch-port*]** in the management tool.
MAC addresses are validated against a custom list for each VSC.	MAC addresses are validated against a global list that is defined on the controller and applies across all devices.
See *Configuring MAC-based filters on a VSC on page 10-19*.	See *Configuring MAC-based filters on an MSM317 switch port on page 10-20*.

Note MAC-based filter are always applied before MAC-based authentication.

Configuring global MAC-based authentication

You define global MAC-based authentication settings using the Colubris-AVPair value string `mac-address`, which you must add to the RADIUS account for the controller. See *Global MAC-based authentication on page 15-56*.

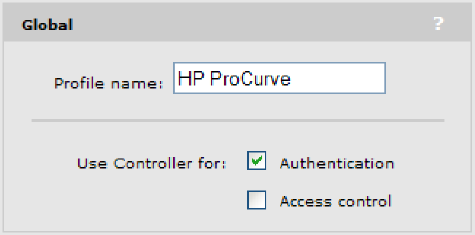
Although the global MAC-based authentication settings apply to all VSCs that have HTML-based user logins enabled, each VSC can use a different authentication server to validate user credentials. To define an authentication server for a VSC, open the **Add/Edit Virtual Service Community** page and use the **HTML-based user logins** box to select the authentication method. See *HTML-based user logins on page 5-27*.

MAC authentication is performed before HTML authentication. If MAC authentication fails, the user’s connection is terminated. If it succeeds, and HTML authentication is enabled, HTML authentication is performed next.

Configuring MAC-based authentication on a VSC

Each VSC can have unique settings for MAC authentication of wireless client stations. These settings are defined on the VSC profile page. (To open this page, see *Viewing and editing VSC profiles on page 5-4*).

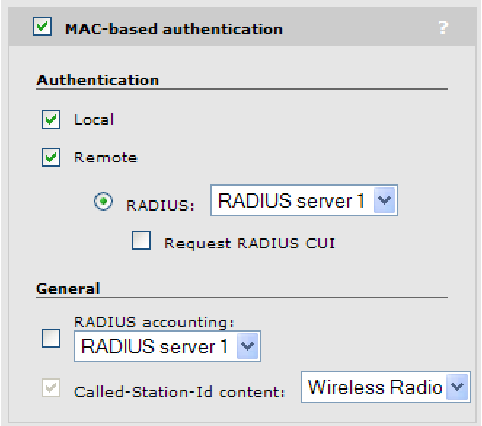
- When the **Use Controller for Authentication** option is enabled under **Global**, MAC-based authentication tasks are managed by the controller. APs forward all authentication requests to the controller which validates user login credentials using the local user accounts or a third-party RADIUS server.



Global

Profile name: HP ProCurve

Use Controller for: ☑ Authentication
☐ Access control



☑ MAC-based authentication

Authentication

☑ Local

☑ Remote

● RADIUS: RADIUS server 1

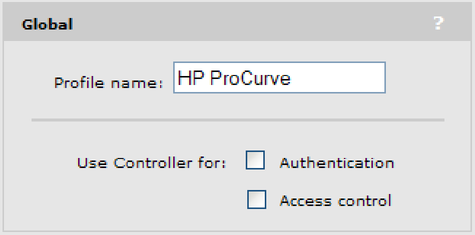
☐ Request RADIUS CUI

General

☐ RADIUS accounting: RADIUS server 1

☑ Called-Station-Id content: Wireless Radio

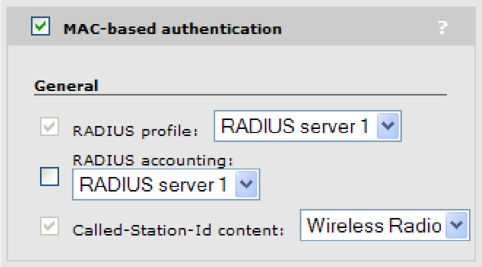
- When the **Use Controller for Authentication** option is disabled under **Global**, MAC-based authentication tasks are managed by the AP. The AP uses the services of a third-party RADIUS server (configured by defining a RADIUS profile on the **Controller >> Authentication > RADIUS profiles** page) to validate user login credentials.



Global

Profile name: HP ProCurve

Use Controller for: ☐ Authentication
☐ Access control



☑ MAC-based authentication

General

☑ RADIUS profile: RADIUS server 1

☐ RADIUS accounting: RADIUS server 1

☑ Called-Station-Id content: Wireless Radio

Note Reauthentication of client stations does not automatically occur upon session timeout.

Authentication

Local

User logins are authenticated with the list defined on the **Controller >> Users > User accounts** page. Define both the username and password as the MAC address of the device. Use the following format: 12 hexadecimal numbers, with the values “a” to “f” in lowercase. For example: 0003520a0f01.

Remote

User logins are authenticated via an external RADIUS server. To define the connection to an external RADIUS server, go to the **Controller >> Authentication > RADIUS profiles** page.

To successfully authenticate a client station, an account must be created on the RADIUS server with both username and password set to the MAC address of the client station.

The MAC address sent by the controller or controlled AP in the RADIUS REQUEST packet for both username and password is 12 hexadecimal numbers, with the values “a” to “f” in lowercase. For example: 0003520a0f01.

The RADIUS server will reply to the REQUEST with either an ACCEPT or REJECT RADIUS RESPONSE packet. In the case of an ACCEPT, the RADIUS server can return the session-timeout RADIUS attribute (if configured for the account). This attribute indicates the amount of time, in seconds, that the authentication is valid for. When this period expires, the controller or controlled AP will re-authenticate the wireless station.

- **Request RADIUS CUI:** Enable this option to support the Chargeable User Identity (CUI) attribute as defined in RFC-4372. The CUI is used to associate a unique identifier with a user so that the user can be identified (for billing, authentication or other purposes) when roaming outside of their home network.

General

RADIUS accounting

Enable this option to have the controller generate a RADIUS START/STOP and interim request for each user. The controller respects the RADIUS interim-update-interval attribute if present inside the RADIUS access accept of the authentication.

Called-Station-ID content

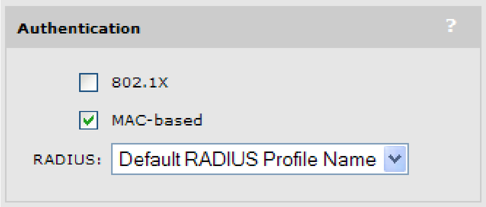
(Only available when **Access control** is disabled under **Global**)

Select the value that the AP (with which the user has established a wireless connection) will return as the called station ID.

- **Port 1**: MAC address of the first Ethernet port on the AP.
- **Port 2**: MAC address of the second Ethernet port on the AP. (Not supported on all APs.)
- **Wireless Radio**: MAC address of the wireless radio on the AP on which this VSC is operating.
- **BSSID**: Basic service set ID of the wireless network defined for this VSC.
- **macaddress:ssid:** The MAC address of the AP radio, followed by a colon, followed by the SSID configured on this VSC.

Configuring MAC-based authentication on an MSM317 switch port

If a switch port on the MSM317 is not bound to a VSC, then MAC-based authentication can be enabled on it. Select **Controlled APs > [*MSM317-AP*] >> Configuration > Switch ports > [*switch-port*]** in the management tool.



Authentication

□ 802.1X

☑ MAC-based

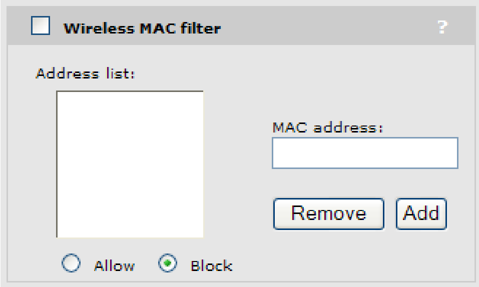
RADIUS: Default RADIUS Profile Name

MAC authentication tasks are handled by the MSM317. The MSM317 uses the services of a third-party RADIUS server (configured by defining a RADIUS profile on the **Controller >> Authentication > RADIUS profiles** page) to validate user login credentials.

Configuring MAC-based filters on a VSC

The Wireless MAC filter option enables you to control access to the wireless network based on the MAC address of a wireless device. You can either block access or allow access, depending on your requirements.

This feature is configured on the VSC profile page. (To open this page, see *Viewing and editing VSC profiles on page 5-4*).



□ Wireless MAC filter

Address list:

MAC address:

○ Allow ● Block

Note

When both this option and the MAC-based authentication option are enabled, MAC filtering occurs first.

Address list

Contains the list of MAC addresses that are checked when filtering is enabled. Up to 64 MAC addresses can be defined per VSC.

MAC address

Specify the MAC address as six pairs of hexadecimal digits separated by colons. For example: 00:00:00:0a:0f:01.

Filter behavior

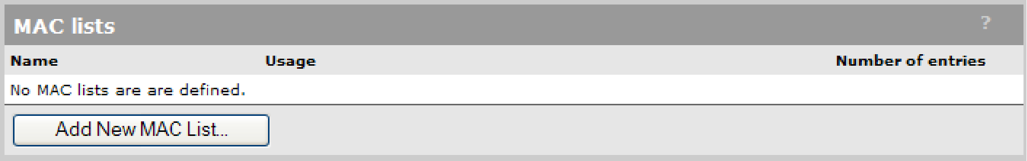
- **Allow:** Only devices whose MAC addresses appear in the Address list can connect to the wireless network.
- **Block:** Devices whose MAC addresses appear in the Address list are blocked from accessing the wireless network.

Configuring MAC-based filters on an MSM317 switch port

This option lets you control port access based on client station MAC addresses. Addresses are checked against one or more lists stored on the controller. If the MAC address of a connected device appears in any configured list, then the device is permitted to send and receive traffic on the port.

To configure MAC-based filters on an MSM317 switch port, do the following:

1. Open the management tool on the MSM7xx Controller.
2. Select **Controller >> Authentication > MAC lists**.

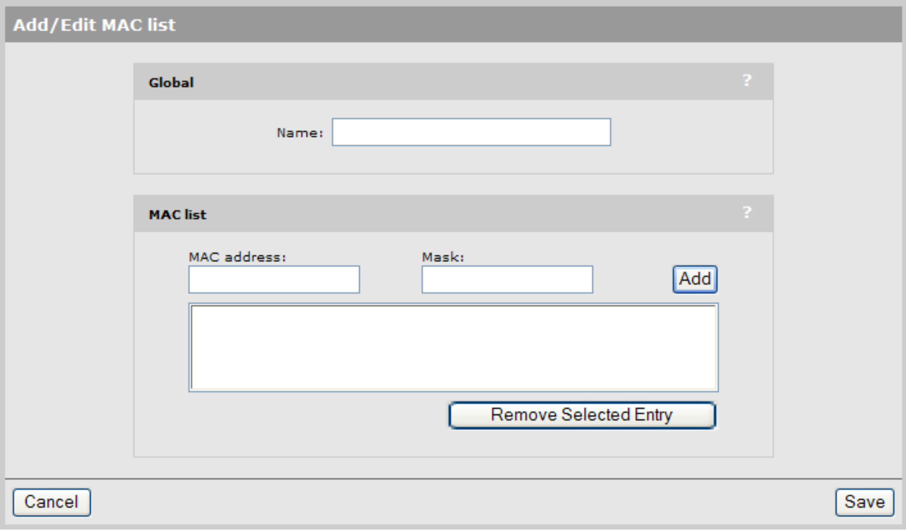


MAC lists

Name	Usage	Number of entries
No MAC lists are are defined.		

3. Select **Add New MAC List**. The Add/Edit MAC list page opens.

   Each entry in the MAC list contains a MAC address and its associated mask. By varying the mask, an entry can be defined to match a single address or a range of addresses.



4. Under **Global**, specify a name to identify the MAC address list.

5. Under **MAC list**, specify the MAC address and mask that you want to match, then select **Add**. For example:

   - The following definition matches a single MAC address:
     MAC address = 00:03:52:07:2B:43
     Mask = FF:FF:FF:FF:FF:FF

   - By changing the last digit of the mask, the definition now matches a range of MAC addresses from **00:03:52:07:2B:40** to **00:03:52:07:2B:4F**:
     MAC address = 00:03:52:07:2B:43
     Mask = FF:FF:FF:FF:FF:F0

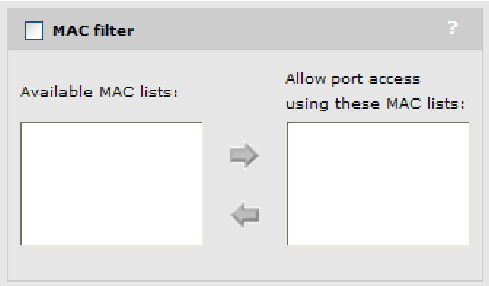
   - The following definition matches all the devices with the MAC prefix (OUI) of **00:03:52**:
     MAC address = 00:03:52:00:00:00
     Mask = FF:FF:FF:00:00:00

6. Repeat step 5 until you have defined all needed entries.

7. Select **Save**.

8. Select **Controlled APs > [*MSM317-AP*] >> Configuration > Switch ports > [*switch-port*]** in the management tool.

9. Select the **MAC filter** checkbox.



10. Select the MAC filter checkbox.

11. Under Available MAC lists, select each MAC list you want to use and select the right arrow icon.

12. Select **Save**.

HTML-based authentication

HTML-based authentication is used with the public/guest access feature described in *Chapter 14: Public/guest network access*. It enables users to login to the public access interface using a standard Web browser.

HTML-based authentication has the following properties:

- Authentication is handled by the controller.
- Settings are defined on a per-VSC basis.
- Can only be used on access-controlled VSCs.
- Configured using the **Add/Edit Virtual Service Community** configuration page in the management tool.
- User credentials can be validated using:
  - Local user accounts on the controller
  - External RADIUS server
  - Active Directory

See *Configuring global access control options on page 14-8* for more configuration settings that affect HTML-based users.

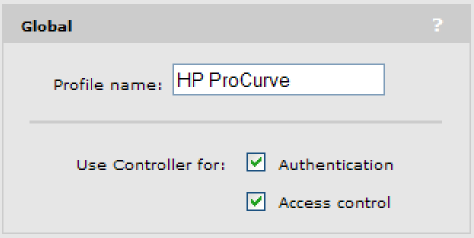
Note

The global MAC-based authentication feature only applies on VSCs that have HTML-based user logins enabled.

Configuring HTML-based authentication on a VSC

Each VSC can have unique settings for HTML-based user logins. These settings are defined on the VSC profile page. (To open this page, see *Viewing and editing VSC profiles on page 5-4*).

When the **Use controller for Authentication** option is enabled under **General**, HTML-based user login options can be defined.

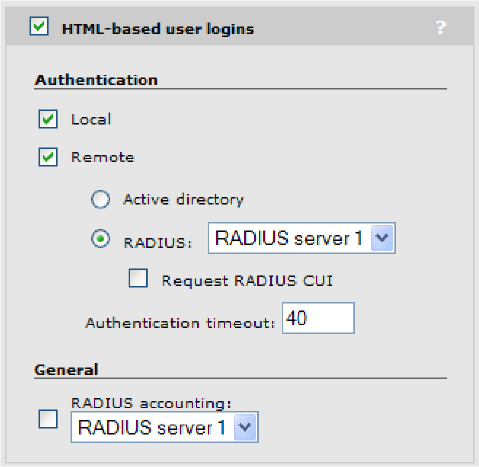


Global

Profile name: HP ProCurve

Use Controller for: ☑ Authentication

☑ Access control



☑ HTML-based user logins

Authentication

☑ Local

☑ Remote

○ Active directory

● RADIUS: RADIUS server 1

□ Request RADIUS CUI

Authentication timeout: 40

General

□ RADIUS accounting: RADIUS server 1

Authentication

If both the **Local** and **Remote** options are active, the controller first checks the local user accounts (defined on the **Controller >> Users > User accounts** page). If the user does not appear in the list, then the controller queries the remote server (Active Directory or RADIUS).

Local

User logins are authenticated with the list defined on the **Controller >> Users > User accounts** page.

Remote

- **Active Directory:** User logins are authenticated via Active Directory. To setup Active Directory support go to the **Controller >> Security > Active Directory** page.
- **RADIUS:** User logins are authenticated via an external RADIUS server. To setup the connection to an external RADIUS server, go to the **Controller >> Authentication > RADIUS profiles** page.
  - **Request RADIUS CUI:** Enable this option to support the Chargeable User Identity (CUI) attribute as defined in RFC-4372. The CUI is used to associate a unique identifier with a user so that the user can be identified (for billing, authentication or other purposes) when roaming outside of their home network.
- **Authentication timeout:** Specify length of time (in seconds) that the controller will wait for the RADIUS server to respond to authentication requests. If the RADIUS server does not respond within this time period logins are refused.

General

- **RADIUS accounting:** Enable this option to have the controller generate a RADIUS START/STOP and interim request for each user. The controller respects the RADIUS interim-update-interval attribute if present inside the RADIUS access accept of the authentication.

VPN-based authentication

VPN-based authentication can be used to provide secure access for client stations on VSCs that do not have encryption enabled.

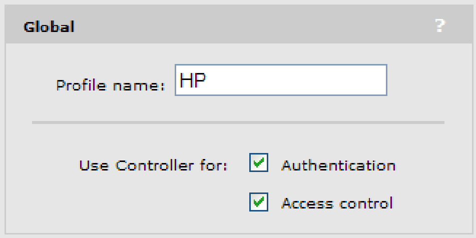
VPN-based authentication has the following properties:

- Authentication is managed by the controller.
- Applies to wireless and wired users.
- Settings are defined on a per-VSC basis.
- Can only be used on access-controlled VSCs.
- Configured using the **Add/Edit Virtual Service Community** configuration page in the management tool.
- User credentials can be validated using:
  - Local user accounts on the controller
  - External RADIUS server
  - Active Directory
- If you enable this option for a VSC, all wireless users on the VSC must establish a VPN connection. No other authentication methods (HTML, MAC, 802.1X) can be used on the VSC.
- When users configure their VPN software, they must specify the controller’s LAN port address as the address of the VPN server.
- To use this option, one or more of the following VPN features must be enabled and configured on the **Controller >> VPN** menu: L2TP server, PPTP server, or IPSec. Once this is done, VPN support can be enabled on a per-VSC basis and users can connect to any active VPN server.
- On the MSM760 and MSM765 a maximum of 50 user sessions are supported across all VSCs. On the MSM710 the limit is 10 sessions.

Configuring VPN-based authentication on a VSC

Each VSC can have unique settings for VPN-based user logins. These settings are defined on the VSC profile page. (To open this page, see *Viewing and editing VSC profiles on page 5-4*).

When the **Use controller for Authentication** and **Access control** options are enabled under **General**, VPN-based user login options can be defined.

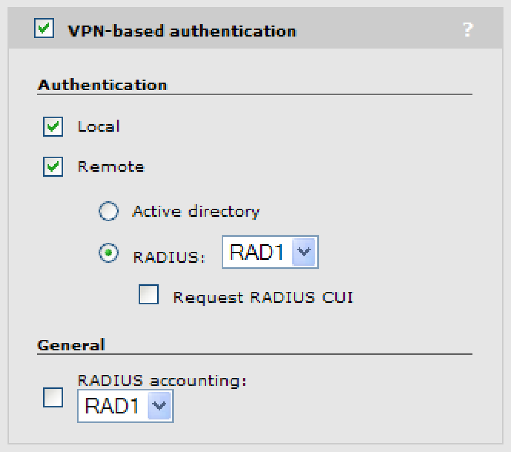


Global

Profile name: HP

Use Controller for: ☑ Authentication

☑ Access control



☑ **VPN-based authentication**

Authentication

☑ Local

☑ Remote

○ Active directory

● RADIUS: RAD1

□ Request RADIUS CUI

General

□ RADIUS accounting: RAD1

Authentication

Local

User logins are authenticated with the list defined on the **Controller >> Users > User accounts** page.

Remote

- **Active Directory:** User logins are authenticated via Active Directory. To setup Active Directory support go to the **Controller >> Security > Active Directory** page.
- **RADIUS:** User logins are authenticated via an external RADIUS server. To setup the connection to an external RADIUS server, go to the **Controller >> Authentication > RADIUS profiles** page.
  - **Request RADIUS CUI:** Enable this option to support the Chargeable User Identity (CUI) attribute as defined in RFC-4372. The CUI is used to associate a unique identifier with a user so that the user can be identified (for billing, authentication or other purposes) when roaming outside of their home network.

General

- **RADIUS accounting:** Enable this option to have the controller generate a RADIUS START/STOP and interim request for each user. The controller respects the RADIUS interim-update-interval attribute if present inside the RADIUS access accept of the authentication.

No authentication

For applications where a remote device performs all authentication functions, it can be useful to disable authentication on the controller and instead, forward all traffic on a VSC into an egress GRE tunnel or egress VLAN for authentication by the remote device.

Note

Because the controller routes traffic to the VSC egress, L2 information from the user is lost and only L3 information is available to the remote authentication device.

Locally-defined user accounts

The controller provides support for locally-defined user accounts with a wide range of customizable options. Locally-defined user accounts use the integrated RADIUS server. Configuration of these accounts is done using the options on the **Controller >> Users** menu, which includes the following configuration pages: User accounts, Account profiles, Subscription plans, and Session persistence.

Each user account:

- Obtains account properties from one or more **account profiles**.
- Obtains account durations from one or more **subscription plans**.
- Is restricted for use with one or more **VSCs**.

Features

Access control

Two types of local user accounts are available: access-controlled and not access-controlled.

- Access-controlled accounts must be used with a VSC that is configured to provide access control.
- Non-access-controlled accounts must be used with a VSC that is *not* configured to provide access control. These accounts are used to handle authentication directly at the AP and cannot make use of the access control capabilities of the controller (the controller must not be in the traffic data path).

Validity and subscription plans

Each user account can be associated with a subscription plan that defines:

- The time period during which the account is available.
- The total amount of time a user can be online when logged in with the account.

VSC usage

User accounts can be restricted to specific VSCs. if a the specified VSC is not available, then the user will not be able to connect with the account.

Account profiles

An account profile is used to define a specific set of features for a user account. Multiple account profiles can be applied to a user account allowing the feature sets of each profile to be added to the account.

Note

Each profile that is applied to a user account must have a unique feature set. The same feature cannot be present in two different profiles.

About the Default AC profile

The **Default AC profile** is defined by default, and is always applied to all access-controlled user accounts. You can view the settings for the **Default AC profile** by selecting it in the profile list. However, you cannot edit any of its settings directly. All settings for this profile are defined by setting attributes on the **Controller >> Public access > Attributes** page.

Supported attributes

The **Public access > Attributes** page allows a wide variety of attributes to be defined. However, only attributes that pertain to user configuration are applied to the **Default AC profile**. This includes the following attributes:

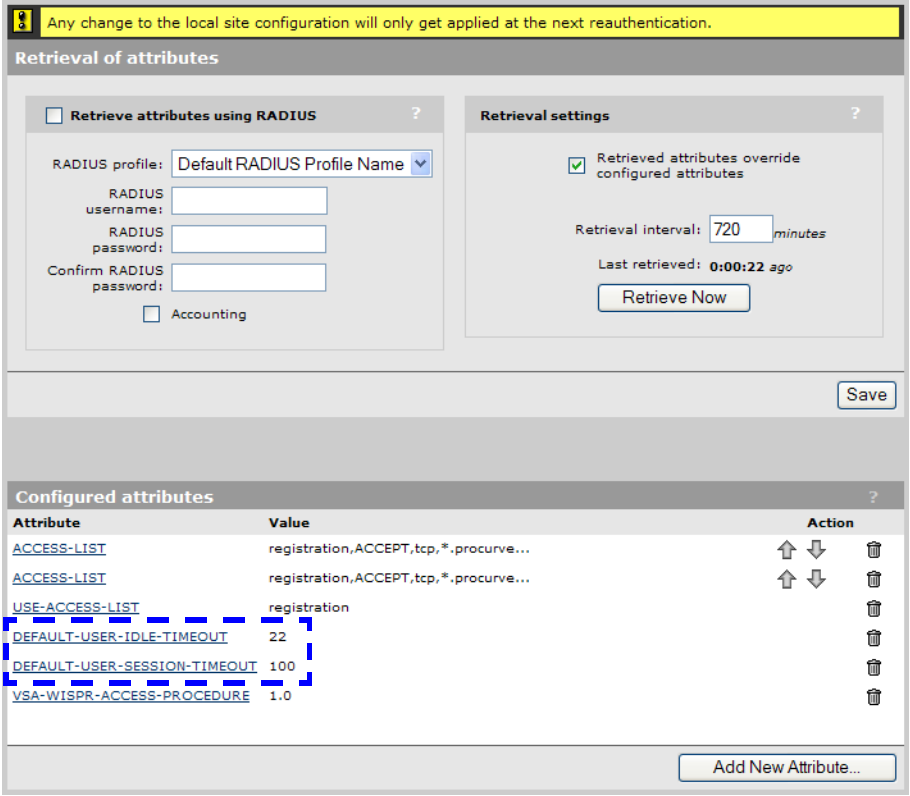
Attribute	For more info see
default-user-use-access-list	*Access list on page 15-34.*
default-user-welcome-url	*Default user URLs on page 15-55.*
default-user-goodbye-url	*Default user URLs on page 15-55.*
default-user-one-to-one-nat	*Default user one-to-one NAT on page 15-53.*
default-user-idle-timeout	*Default user idle timeout on page 15-52.*
default-user-session-timeout	*Default user session timeout on page 15-54.*
default-user-acct-interim-update	*Default user interim accounting update interval on page 15-51.*
default-user-max-output-packets	*Default user quotas on page 15-52.*
default-user-max-input-packets	*Default user quotas on page 15-52.*
default-user-max-total-packets	*Default user quotas on page 15-52.*
default-user-max-output-octets	*Default user quotas on page 15-52.*
default-user-max-input-octets	*Default user quotas on page 15-52.*
default-user-max-total-octets	*Default user quotas on page 15-52.*
default-user-max-input-rate	*Default user data rates on page 15-53.*

Attribute	For more info see
default-user-max-output-rate	*Default user data rates on page 15-53.*
default-user-bandwidth-level	*Default user bandwidth level on page 15-51.*
default-user-use-public-ip-subnet	*Default user bandwidth level on page 15-51*

Example

This example illustrates how to indirectly customize the Default AC profile by defining several attributes, and shows how these settings are then reflected in a the Default AC profile and the user account.

The following sample page shows several attributes defined on the **Public access > Attributes** page under **Configured attributes**. The two of interest for this example are highlighted below.



Any change to the local site configuration will only get applied at the next reauthentication.

Retrieval of attributes

☐ **Retrieve attributes using RADIUS**

RADIUS profile: Default RADIUS Profile Name
RADIUS username:
RADIUS password:
Confirm RADIUS password:
☐ Accounting

Retrieval settings

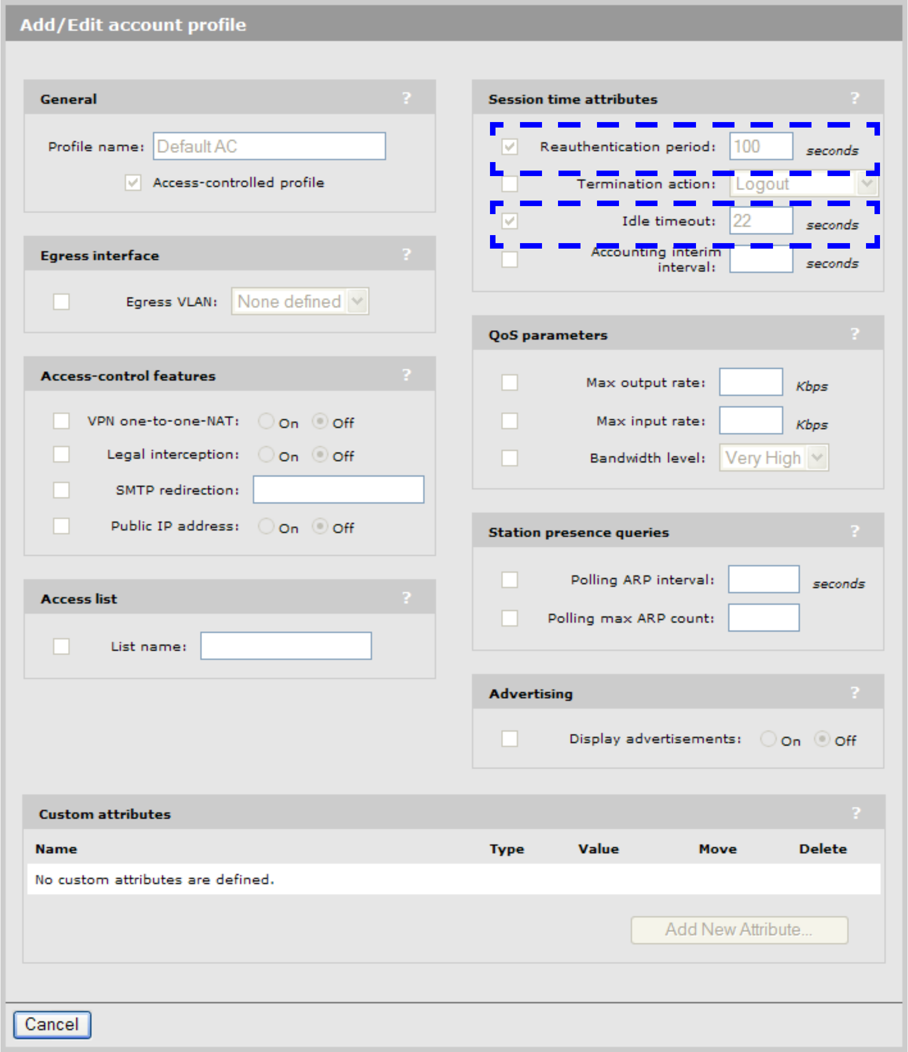
☑ Retrieved attributes override configured attributes

Retrieval interval: 720 *minutes*
Last retrieved: **0:00:22** *ago*

Configured attributes

Attribute	Value	Action
ACCESS-LIST	registration,ACCEPT,tcp,*.procurve...	⇧ ⇩ 🗑
ACCESS-LIST	registration,ACCEPT,tcp,*.procurve...	⇧ ⇩ 🗑
USE-ACCESS-LIST	registration	🗑
DEFAULT-USER-IDLE-TIMEOUT	22	🗑
DEFAULT-USER-SESSION-TIMEOUT	100	🗑
VSA-WISPR-ACCESS-PROCEDURE	1.0	🗑

These two attributes appear in the **Default AC** profile under **Session time attributes**:



Add/Edit account profile

General

Profile name: Default AC

☑ Access-controlled profile

Egress interface

□ Egress VLAN: None defined

Access-control features

□ VPN one-to-one-NAT: ○ On ● Off

□ Legal interception: ○ On ● Off

□ SMTP redirection:

□ Public IP address: ○ On ● Off

Access list

□ List name:

Session time attributes

☑ Reauthentication period: 100 seconds

□ Termination action: Logout

☑ Idle timeout: 22 seconds

□ Accounting interim interval: seconds

QoS parameters

□ Max output rate: Kbps

□ Max input rate: Kbps

□ Bandwidth level: Very High

Station presence queries

□ Polling ARP interval: seconds

□ Polling max ARP count:

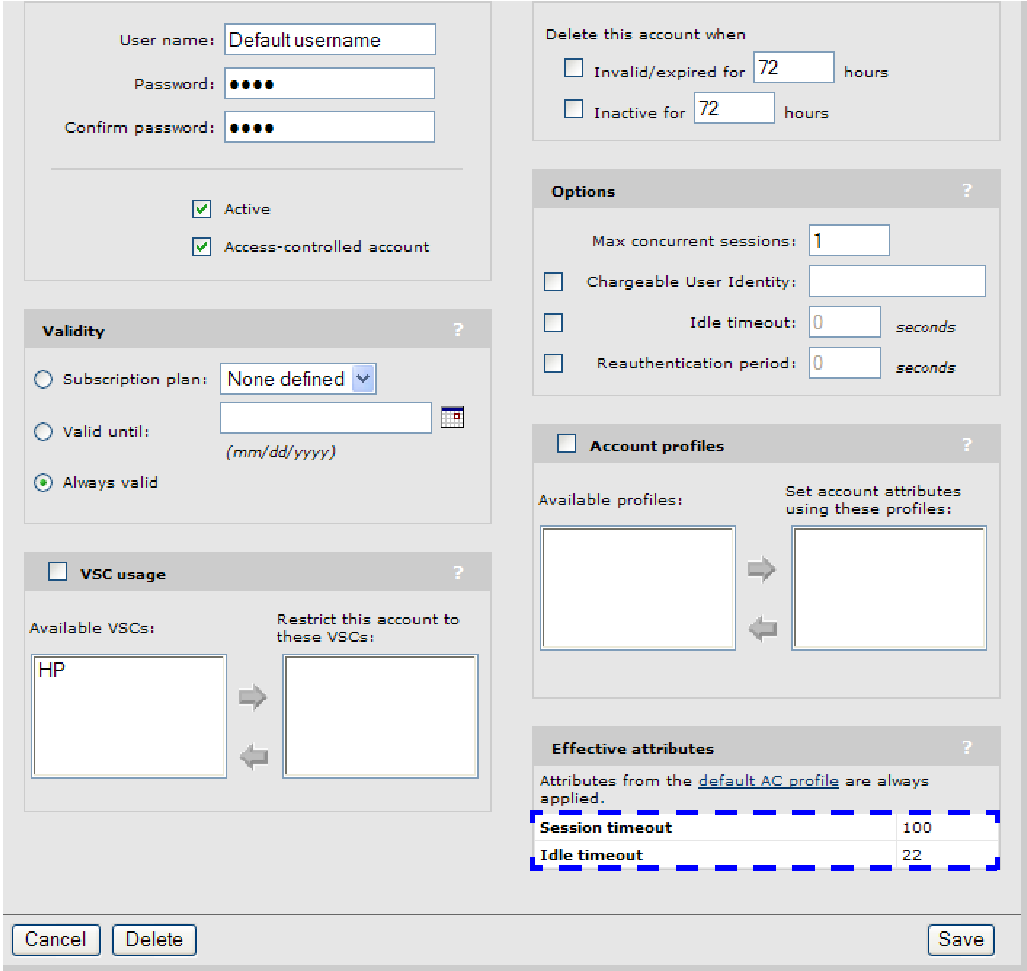
Advertising

□ Display advertisements: ○ On ● Off

Custom attributes

Name	Type	Value	Move	Delete
No custom attributes are defined.				

And the attributes appear in access-controlled user accounts under **Effective attributes**:



User name: Default username

Password: ●●●●

Confirm password: ●●●●

☑ Active

☑ Access-controlled account

Validity

○ Subscription plan: None defined

○ Valid until: (mm/dd/yyyy)

● Always valid

□ **VSC usage**

Available VSCs: HP

Restrict this account to these VSCs:

Delete this account when

□ Invalid/expired for 72 hours

□ Inactive for 72 hours

Options

Max concurrent sessions: 1

□ Chargeable User Identity:

□ Idle timeout: 0 *seconds*

□ Reauthentication period: 0 *seconds*

□ **Account profiles**

Available profiles:

Set account attributes using these profiles:

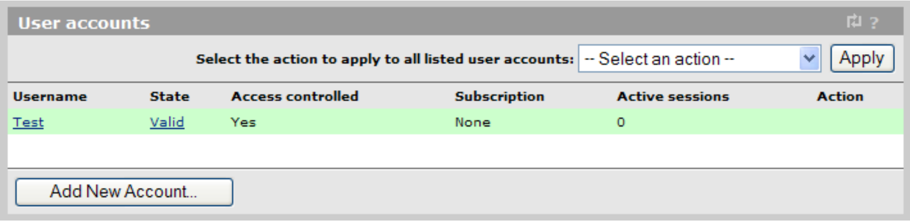
Effective attributes

Attributes from the default AC profile are always applied.

Session timeout	100
Idle timeout	22

Defining a user account

1. Select **Controller >> Users > User accounts**. The User accounts page opens. It presents a list of all defined user accounts. Initially this list is empty.

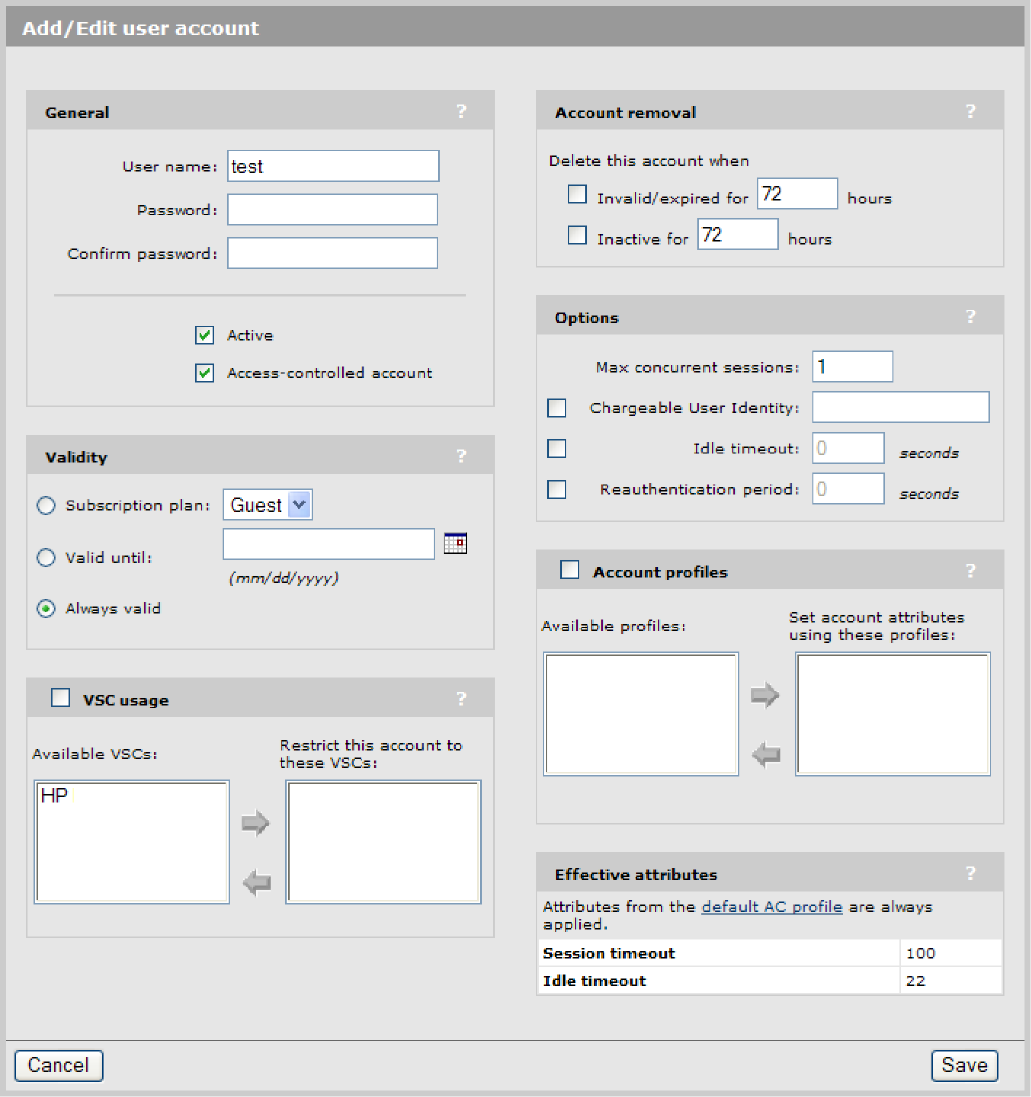


User accounts

Select the action to apply to all listed user accounts: -- Select an action --

Username	State	Access controlled	Subscription	Active sessions	Action
Test	Valid	Yes	None	0	

2. Select **Add New Account**. The **Add/Edit user account** page opens.



Add/Edit user account

General ?

User name: test

Password:

Confirm password:

☑ Active

☑ Access-controlled account

Validity ?

○ Subscription plan: Guest

○ Valid until: (mm/dd/yyyy)

● Always valid

□ **VSC usage** ?

Available VSCs: HP

Restrict this account to these VSCs:

Account removal ?

Delete this account when

□ Invalid/expired for 72 hours

□ Inactive for 72 hours

Options ?

Max concurrent sessions: 1

□ Chargeable User Identity:

□ Idle timeout: 0 *seconds*

□ Reauthentication period: 0 *seconds*

□ **Account profiles** ?

Available profiles:

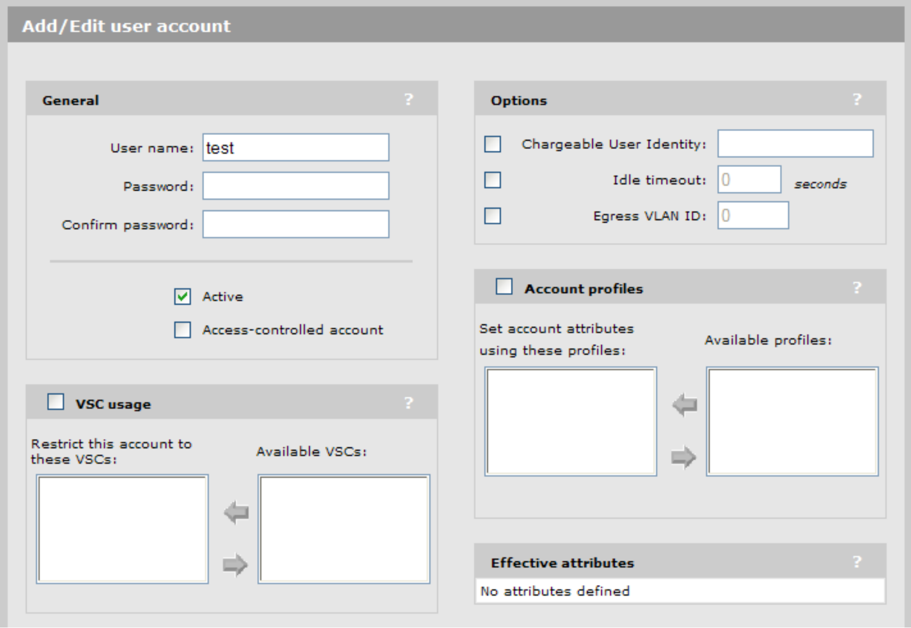
Set account attributes using these profiles:

Effective attributes ?

Attributes from the default AC profile are always applied.

Session timeout	100
Idle timeout	22

If you disable the Access-controlled account option, the page will look like this:



Add/Edit user account

General

User name: test

Password:

Confirm password:

☑ Active

☐ Access-controlled account

☐ VSC usage

Restrict this account to these VSCs:

Available VSCs:

Options

☐ Chargeable User Identity:

☐ Idle timeout: 0 seconds

☐ Egress VLAN ID: 0

☐ Account profiles

Set account attributes using these profiles:

Available profiles:

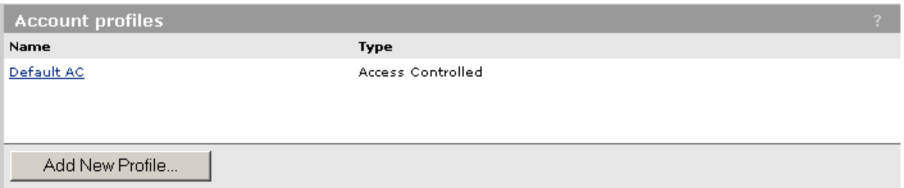
Effective attributes

No attributes defined

3. Configure account options as described in the online help.

Defining account profiles

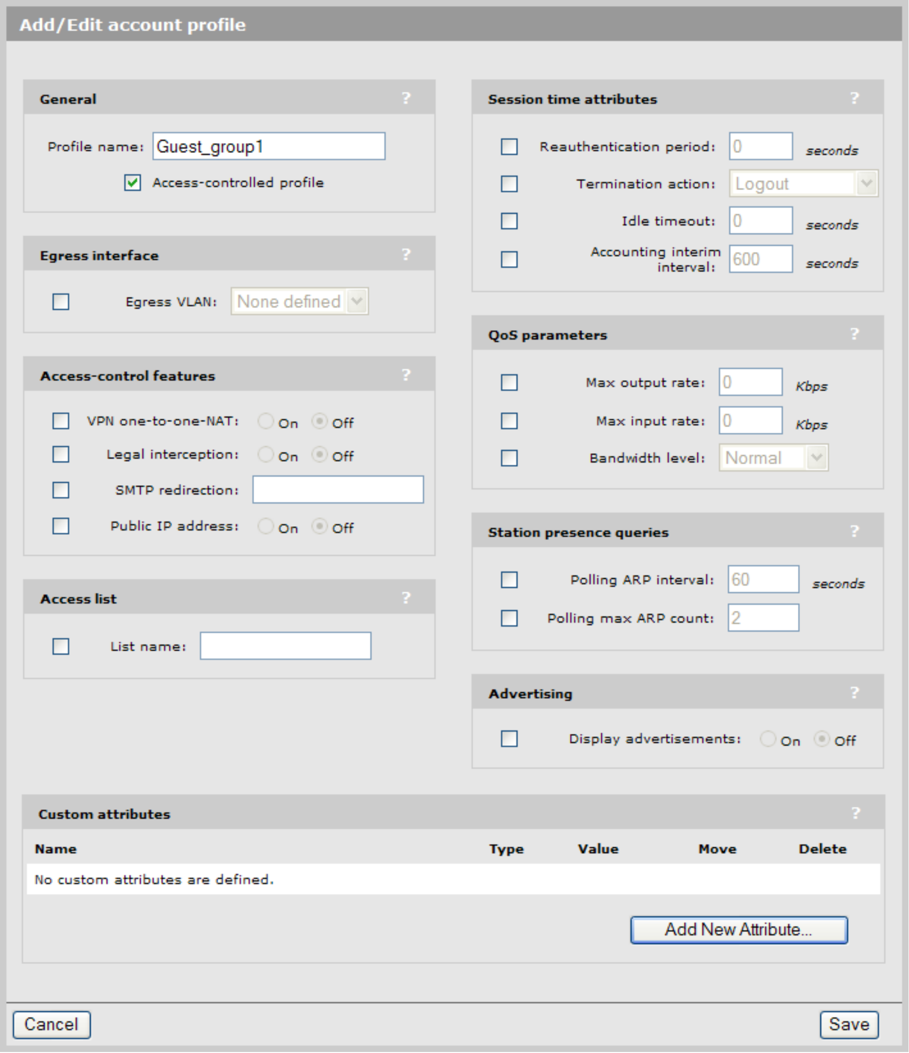
1. Select **Controller >> Users > Account profiles**. The Account profiles page opens. It presents a list of all defined profiles. Initially this list will contain the profile **Default AC**.



Account profiles

Name	Type
Default AC	Access Controlled

2. Select **Add New Profile**. The **Add/Edit account profile** page opens.



Add/Edit account profile

General

Profile name: Guest_group1

☑ Access-controlled profile

Egress interface

☐ Egress VLAN: None defined

Access-control features

☐ VPN one-to-one-NAT: ○ On ● Off

☐ Legal interception: ○ On ● Off

☐ SMTP redirection:

☐ Public IP address: ○ On ● Off

Access list

☐ List name:

Session time attributes

☐ Reauthentication period: 0 seconds

☐ Termination action: Logout

☐ Idle timeout: 0 seconds

☐ Accounting interim interval: 600 seconds

QoS parameters

☐ Max output rate: 0 Kbps

☐ Max input rate: 0 Kbps

☐ Bandwidth level: Normal

Station presence queries

☐ Polling ARP interval: 60 seconds

☐ Polling max ARP count: 2

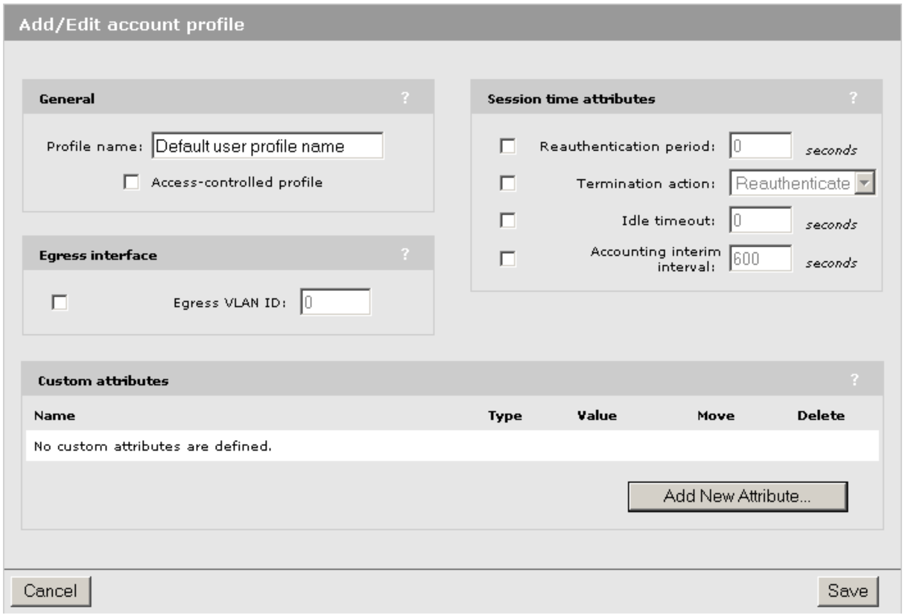
Advertising

☐ Display advertisements: ○ On ● Off

Custom attributes

Name	Type	Value	Move	Delete
No custom attributes are defined.				

If you disable the Access-controlled account option, the page will look like this:



Add/Edit account profile

General

Profile name: Default user profile name

□ Access-controlled profile

Egress interface

□ Egress VLAN ID: 0

Session time attributes

□ Reauthentication period: 0 seconds

□ Termination action: Reauthenticate

□ Idle timeout: 0 seconds

□ Accounting interim interval: 600 seconds

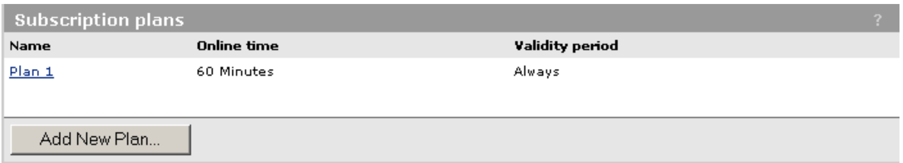
Custom attributes

Name	Type	Value	Move	Delete
No custom attributes are defined.				

3. Configure profile options as described in the online help.

Defining subscription plans

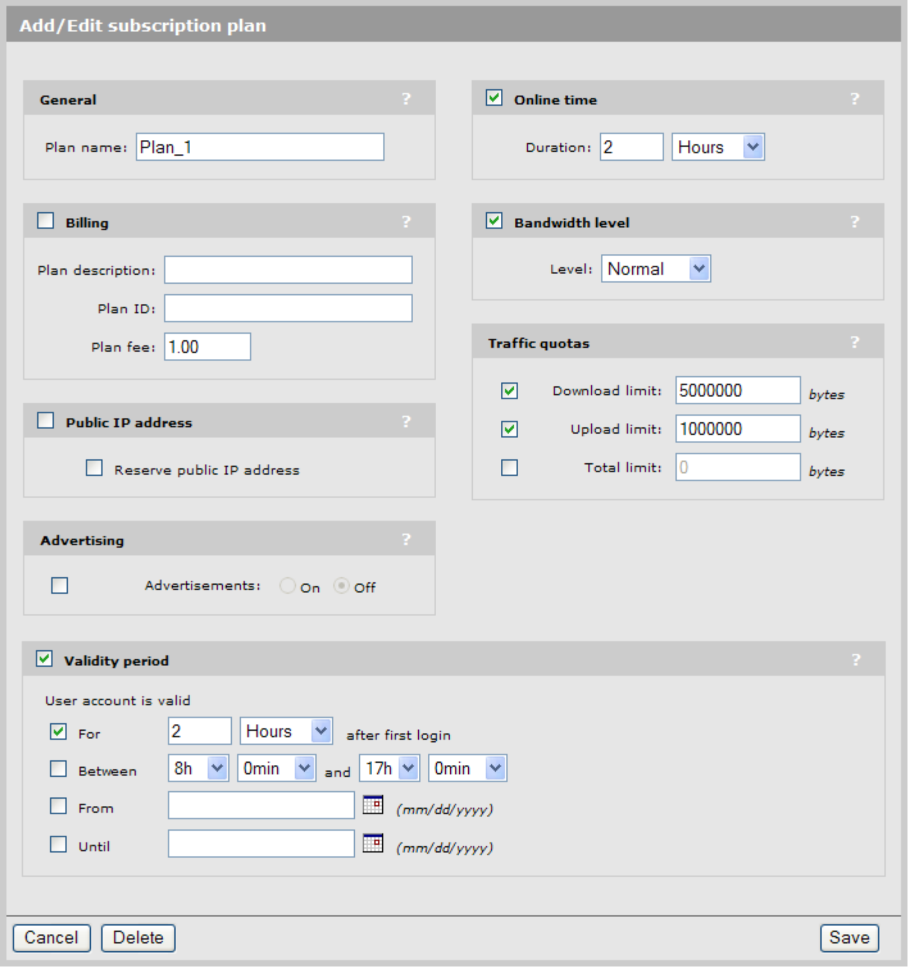
1. Select **Controller >> Users > Subscription plans**. The Subscription plans page opens. It presents a list of all defined subscription plans.



Subscription plans

Name	Online time	Validity period
Plan 1	60 Minutes	Always

2. Select **Add New Plan**. The Add/Edit subscription plan page opens.



Add/Edit subscription plan

General
Plan name: Plan_1

☑ Online time
Duration: 2 Hours

□ Billing
Plan description:
Plan ID:
Plan fee: 1.00

☑ Bandwidth level
Level: Normal

Traffic quotas
☑ Download limit: 5000000 *bytes*
☑ Upload limit: 1000000 *bytes*
□ Total limit: 0 *bytes*

□ Public IP address
□ Reserve public IP address

Advertising
□ Advertisements: ○ On ● Off

☑ Validity period
User account is valid
☑ For 2 Hours after first login
□ Between 8h 0min and 17h 0min
□ From (mm/dd/yyyy)
□ Until (mm/dd/yyyy)

3. Configure plan options as described in the online help.

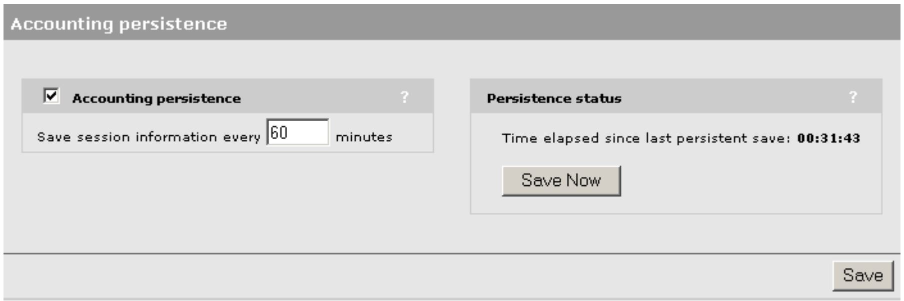
Public IP address

This feature enables a public IP address to be assigned to any client station. This makes the client station address visible to devices on the external network, allowing external devices to create connections with the client station. For more information, see *Public IP address on page 3-10*.

Accounting persistence

Enable this option to have the controller save accounting information to its internal flash memory so that can be recovered in case of abnormal system shutdown. Restarting the controller via its management tool (**Controller >> Maintenance > System**) saves before restarting.

The minimum save time is 30 minutes.



Save session information every 60 minutes

Time elapsed since last persistent save: **00:31:43**

User addressing and related features

The controller provides a number of features related to user addressing, including:

Feature	Description	For more information, see ...
DHCP server	Enables the controller to dynamically assign IP addresses to users.	*DHCP server on page 3-14*
Fixed leases	The controller assigns the same IP addresses to specific users each time they connect.	*Fixed leases on page 3-15*
DHCP relay	The controller to users a third-party DHCP server to dynamically assign IP addresses to users.	*DHCP relay agent on page 3-16*
Static IP address support	Allows users with a static IP address to connect to the network even if the user's address is on a different subnet than the controller or AP.	*Support users that have a static IP address on page 14-11*

Feature	**Description**	**For more information, see ...**
NAT	Hides the IP addresses of all users on the protected network from the public network.	*Network address translation (NAT) on page 3-30*
Extend Internet port subnet to LAN port	Enables a third-party DHCP server to assign an IP address to users that makes them visible on the controller's Internet port.	*Extend Internet port subnet to LAN port on page 3-18*
VPN one-to-one NAT	Assigns a unique IP address to each IPSec or PPTP VPN connection made by a user to a remote server via the Internet port.	*VPN one-to-one NAT on page 3-9*
Public IP address	Assigns an IP address to users that makes them visible on the controller's Internet port.	*Public IP address on page 3-10*

11

Authentication services

Contents

Introduction

This chapter explains how to configure the different authentication services that the controller can use to authenticate user logins and administrator logins. The following table summarizes the services that are available and what they can be used for.

Service	Description	For details, see ...
Integrated RADIUS server	User authentication via the local user lists.	*Using the integrated RADIUS server on page 11-2*
Third-party RADIUS server	User authentication via accounts on a third-party RADIUS server. Administrator authentication via accounts on a third-party RADIUS server.	*Using a third-party RADIUS server on page 11-5*
Active Directory	User authentication via an Active Directory server.	*Using an Active Directory server on page 11-10*

All authentication services support the following authentication types:

Service	For details, see ...
802.1X (VSC)	*802.1X authentication on page 10-8*
MAC-based (Global)	*MAC-based authentication on page 10-14*
MAC-based (VSC)	*MAC-based authentication on page 10-14*
HTML-based	*HTML-based authentication on page 10-22*
VPN-based	*VPN-based authentication on page 10-24*

When configuring 802.1X or MAC-based authentication on an MSM317 switch port, authentication services must be provided by a third-party RADIUS server. (For more information on each authentication type, see *Configuring 802.1X support on an MSM317 switch port on page 10-14* and *Configuring MAC-based authentication on an MSM317 switch port on page 10-19*.)

Using the integrated RADIUS server

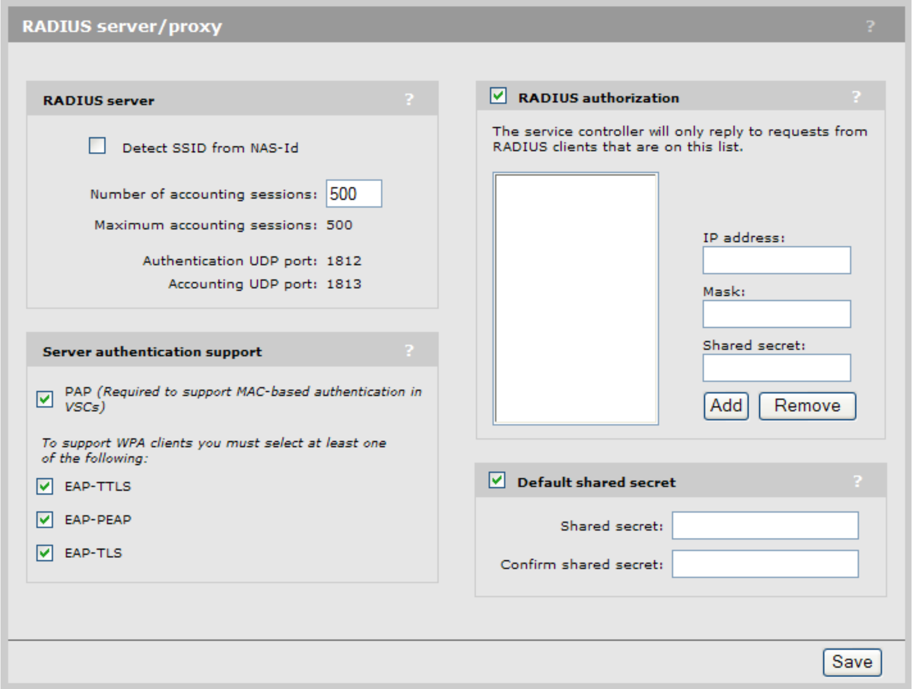
The internal RADIUS server is not intended as a replacement for the high-end/high-performance RADIUS server required for large scale deployments. Rather, it is offered as a cost-effective solution for managing user authentication for small hotspots or enterprise networks.

Primary features

- Provides termination of 802.1X sessions at the controller for clients using WPA/WPA2 with EAP-PEAP, EAP-TLS and EAP-TTLS. Support for other EAP protocols is available using proxy mode.
- Provides MAC-based authentication of wireless users connected to both controlled and autonomous APs.
- Can be used to validate login credentials for HTML-based users.
- All locally defined user account options (user accounts, account profiles, and subscription plans) presented on the **Controller >> Users** menu are handled by the internal RADIUS server.
- Allows RADIUS accounting data to be sent to an external RADIUS server. (The internal RADIUS server does not provide support for accounting.)
- Local user accounts and account profiles have been designed to match the same functionality and support as can be provided by an external RADIUS server. Most of the AVPairs supported on an external RADIUS server are also supported by the integrated RADIUS server.

Server configuration

Configuration of the integrated RADIUS server is done using the **Controller >> Authentication > RADIUS server** page. In most cases, the default settings on this page will not need to be changed.



RADIUS server/proxy

RADIUS server

□ Detect SSID from NAS-Id

Number of accounting sessions: 500

Maximum accounting sessions: 500

Authentication UDP port: 1812

Accounting UDP port: 1813

Server authentication support

☑ PAP *(Required to support MAC-based authentication in VSCs)*

To support WPA clients you must select at least one of the following:

☑ EAP-TTLS

☑ EAP-PEAP

☑ EAP-TLS

☑ RADIUS authorization

The service controller will only reply to requests from RADIUS clients that are on this list.

IP address:

Mask:

Shared secret:

☑ Default shared secret

Shared secret:

Confirm shared secret:

Configuration parameters

RADIUS server

Detect SSID from NAS-Id

Enable this option when working with third-party APs to permit the controller to retrieve the SSID assigned to the AP, and therefore assign user traffic to the appropriate VSC. For this to work, the AP must be configured to send its SSID as the NAS ID in all authentication and accounting requests. See *Working with third-party autonomous APs on page 19-6*.

Number of accounting sessions

Specify the maximum number of sessions for which the controller will track accounting information.

Maximum accounting sessions

Specify the maximum number of accounting sessions that the controller supports.

Authentication UDP port

Indicates the port the controller uses for authentication. This port is always set to the standard value of 1812.

Accounting UDP port

Indicates the port the controller uses for accounting. This port is always set to the standard value of 1813.

Server authentication support

Select the authentication protocols that the internal RADIUS server will support:

- PAP: This protocol must be enabled if any VSCs are configured to use MAC-based authentication or HTML authentication.
- EAP-TTLS
- EAP-PEAP
- EAP-TLS

RADIUS authorization

Note Applies to autonomous and third-party APs. Requests from controlled APs are always accepted because they use the management tunnel.

Enable this option to restrict access to the RADIUS server. The RADIUS server will only respond to requests from RADIUS clients that appear in the list, or that match the default shared secret, as described below.

IP address

Specify the IP address of the RADIUS client.

Mask

Specify the network mask.

Shared secret
Specify the secret (password) that RADIUS client must use to communicate with the RADIUS server.

Default shared secret

Note

Applies to autonomous APs only. Requests from controlled APs are always accepted because they use the management tunnel.

Enable this option to set a shared secret to safeguard communications between the internal RADIUS server and clients not in the RADIUS authorization list.

Shared secret/Confirm shared secret
Specify the secret (password) that controller will use when communicating with RADIUS clients that do not appear in the RADIUS authorization list. The shared secret must match on both the clients and the controller.

User account configuration

User accounts for the internal RADIUS server are defined using the **Controller >> Users** menu. See *Chapter 10: User authentication, accounts, and addressing*.

Using a third-party RADIUS server

A third-party RADIUS server can be used to perform a number of authentication and configuration tasks, as shown in the following table.

Task	For more information, see ...
Validating administrative user credentials	*Administrative user authentication on page 2-4*.
Validating user credentials for 802.1X, MAC, and HTML authentication types	*Wireless protection on page 5-23.* *HTML-based user logins on page 5-27.* *MAC-based authentication on page 5-28.*
Storing custom configuration settings for the public access interface	*Chapter 15: Working with RADIUS attributes*.
Storing custom configuration settings for each user	
Storing accounting information for each user	

The following authetication types can make use of an external third-party RADIUS server:

Service	For details, see ...
802.1X (VSC)	*802.1X authentication on page 10-8*
MAC-based (Global)	*MAC-based authentication on page 10-14*
MAC-based (VSC)	*MAC-based authentication on page 10-14*
HTML-based	*HTML-based authentication on page 10-22*
VPN-based	*VPN-based authentication on page 10-24*

Configuring a RADIUS server profile on the controller

The controller enables you to define a maximum of 16 RADIUS profiles. Each profile defines the settings for a RADIUS client connection. To support a client connection, you must create a client account on the RADIUS server. The settings for this account must match the profile settings you define on the controller.

For backup redundancy, each profile supports a primary and secondary server.

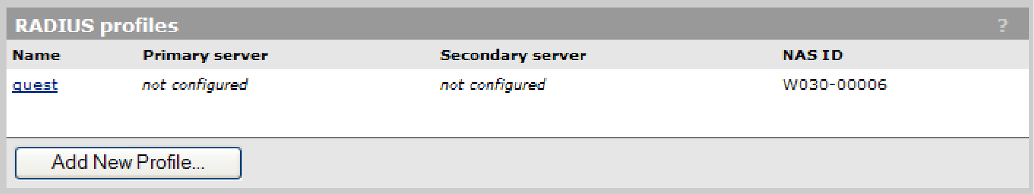
The controller can function with any RADIUS server that supports RFC 2865 and RFC 2866. Authentication occurs via authentication types such as: EAP-MD5, CHAP, MSCHAP v1/v2, PAP, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA, EAP-FAST, and EAP-GTC.

Caution To safeguard the integrity of RADIUS traffic it is important that you protect communications between the controller and the RADIUS server. The controller lets you use PPTP or IPSec to create a secure tunnel to the RADIUS server. For complete instructions on how to accomplish this, see *Securing wireless client sessions with VPNs on page 16-3*.

Note If you change a RADIUS profile to connect to a different server while users are active, all RADIUS traffic for active user sessions is immediately sent to the new server.

Configuration procedure

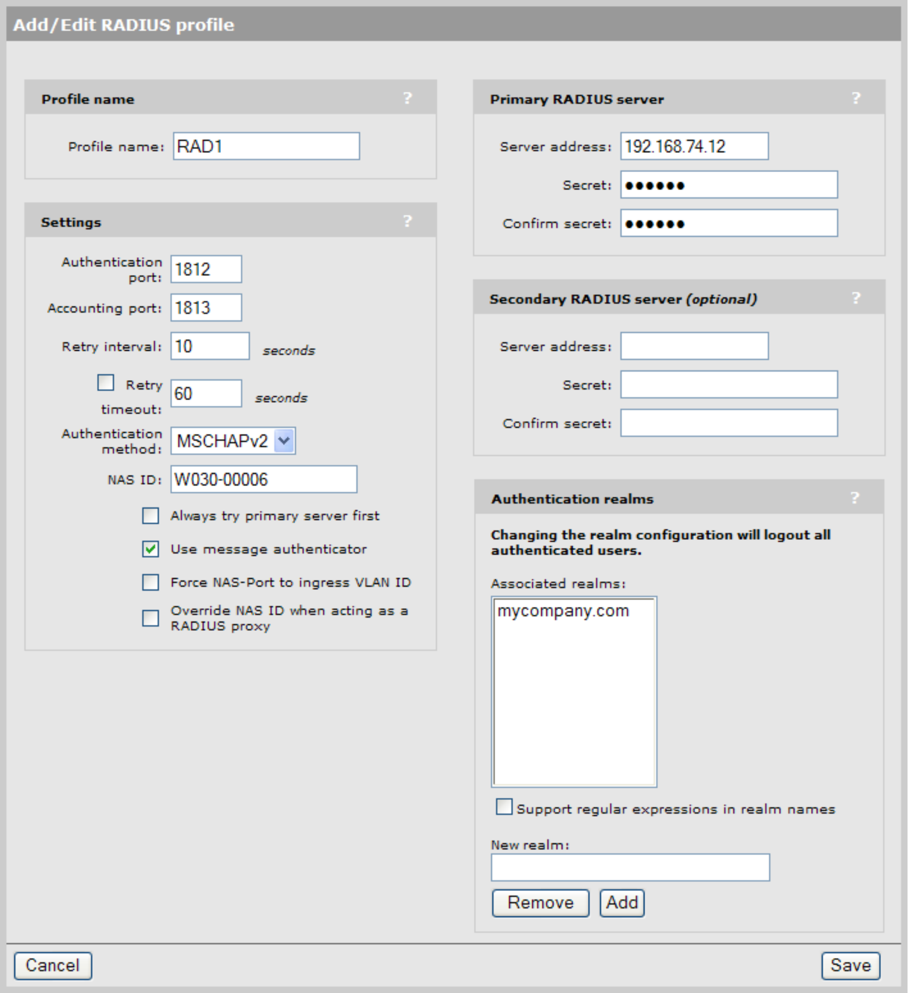
1. Select **Controller >> Authentication > RADIUS profiles.** The RADIUS profiles page opens.



RADIUS profiles

Name	Primary server	Secondary server	NAS ID
guest	*not configured*	*not configured*	W030-00006

2. Select **Add New Profile.** The Add/Edit RADIUS Profile page opens.



Add/Edit RADIUS profile

Profile name

Profile name: RAD1

Settings

Authentication port: 1812

Accounting port: 1813

Retry interval: 10 *seconds*

□ Retry timeout: 60 *seconds*

Authentication method: MSCHAPv2

NAS ID: W030-00006

□ Always try primary server first

☑ Use message authenticator

□ Force NAS-Port to ingress VLAN ID

□ Override NAS ID when acting as a RADIUS proxy

Primary RADIUS server

Server address: 192.168.74.12

Secret: ●●●●●●

Confirm secret: ●●●●●●

Secondary RADIUS server *(optional)*

Server address:

Secret:

Confirm secret:

Authentication realms

Changing the realm configuration will logout all authenticated users.

Associated realms: mycompany.com

□ Support regular expressions in realm names

New realm:

3. Configure the profile settings as described in the following section.

4. Select **Save**.

Configuration parameters

Profile name

Specify a name to identify the profile.

Settings

- **Authentication port:** Specify a port on the RADIUS server to use for authentication. By default RADIUS servers use port 1812.
- **Accounting port:** Specify a port on the RADIUS server to use for accounting. By default RADIUS servers use port 1813.
- **Retry interval:** Specify the number of seconds that the controller waits before access and accounting requests time out. If the controller does not receive a reply within this interval, the controller switches between the primary and secondary

RADIUS servers, if a secondary server is defined. A reply that is received after the retry interval expires is ignored.

Retry interval applies to access and accounting requests that are generated by the following:

- Manager or operator access to the management tool
- User authentication by way of HTML
- MAC-based authentication of devices
- Authentication of the controller
- Authentication of the controlled AP.

You can determine the maximum number of retries as follows:

- HTML-based logins: Calculate the number of retries by taking the setting for the HTML-based logins **Authentication Timeout** parameter and dividing it by the value of this parameter. Default settings result in 4 retries (40 / 10).
- MAC-based and controller authentication: Number of retries is infinite.
- 802.1X authentication: Retries are controlled by the 802.1X client software.

- **Authentication method:** Select the default authentication method that the controller uses when exchanging authentication packets with the RADIUS server defined for this profile. For 802.1X users, the authentication method is always determined by the 802.1X client software and is not controlled by this setting. If traffic between the controller and the RADIUS server is not protected by a VPN, it is recommended that you use either EAP-MD5 or MSCHAP V2 (if supported by your RADIUS Server). PAP and MSCHAP V1 are less secure protocols.
- **NAS ID:** Specify the identifier for the network access server that you want to use for the controller. By default the serial number of the controller is used. The controller includes the NAS-ID attribute in all packets that it sends to the RADIUS server.
- **Always try primary server first:** Enable this option if you want to force the controller to contact the primary server first.

  Otherwise, the controller sends the first RADIUS access request to the last known RADIUS server that replied to any previous RADIUS access request. If the request times out, the next request is sent to the other RADIUS server if defined.

  For example, assume that the primary RADIUS server was not reachable and that the secondary server responded to the last RADIUS access request. When a new authentication request is received, the controller sends the first RADIUS access request to the secondary RADIUS server.

  If the secondary RADIUS server does not reply, the controller retransmits the RADIUS access request to the primary RADIUS server. When two servers are configured, the controller always alternates between the two.

Primary/Secondary RADIUS server

- **Server address:** Specify the IP address or fully-qualified domain name of the RADIUS server.
- **Secret/Confirm secret:** Specify the password for the controller to use to communicate with the RADIUS server. The shared secret is used to authenticate all packets exchanged with the server, proving that the packets originate from a valid/trusted source.

Authentication realms

When authentication realms are enabled for a profile, selection of the RADIUS server to use for authentication is based on the realm name, rather than the RADIUS profile name configured. This applies to any VSC authentication setting that uses the profile.

- Realm names are extracted from user names as follows: if the username is **person1@mydomain.com** then **mydomain.com** is the realm. The authentication request is sent to the RADIUS profile with the realm name **mydomain.com**. The username sent for authentication is still the complete **person1@mydomain.com**.
- For added flexibility, regular expressions can be used in realm names, enabling a single realm name to match many users. For example, if a realm name is defined with the regular expression **^per.*** then all usernames beginning with **per** followed by any number of characters will match. The following usernames would all match:

  per123.biz
  per321.lan
  per1

Important

- Realms names are not case-sensitive and can be a maximum of 64 characters long.
- You can define a maximum of 200 realms across all RADIUS profiles. There is no limit to the number of realms that you can define for each RADIUS profile.
- Each RADIUS profile can be associated with one or more realms. However, a realm cannot be associated with more than one profile.
- A realm overrides the authentication RADIUS server only. The server used for accounting is not affected.
- When realm configuration is changed in any way, all active user sessions are terminated.

Support for regular expressions in realm names

Standard regular expressions can be used in realm names. For example:

Expression	Matches
mycompany[1-3].com	mycompany1.com mycompany2.com mycompany3.com
.*mycompany.com	Matches **mycompany.com** with any number of characters in front of it. For example: **headoffice.mycompany.com** or **server-mycompany.com**.
.*\.mycompany.com	Matches with any number of characters in front of it. For example: **headoffice.mycompany.com** or **server.mycompany.com**, but not **server-mycompany.com**.

Using an Active Directory server

Active Directory is the Windows service that is used by many organizations for user authentication. The controller can communicate with an Active Directory server to authenticate user login credentials and retrieve configurations settings (attributes) that are applied to a user's session.

An active directory server can be used to support the following authentication types:

Service	For details, see ...
802.1X (VSC)	*802.1X authentication on page 10-8*
MAC-based (Global)	*MAC-based authentication on page 10-14*
MAC-based (VSC)	*MAC-based authentication on page 10-14*
HTML-based	*HTML-based authentication on page 10-22*
VPN-based	*VPN-based authentication on page 10-24*

Supported protocols

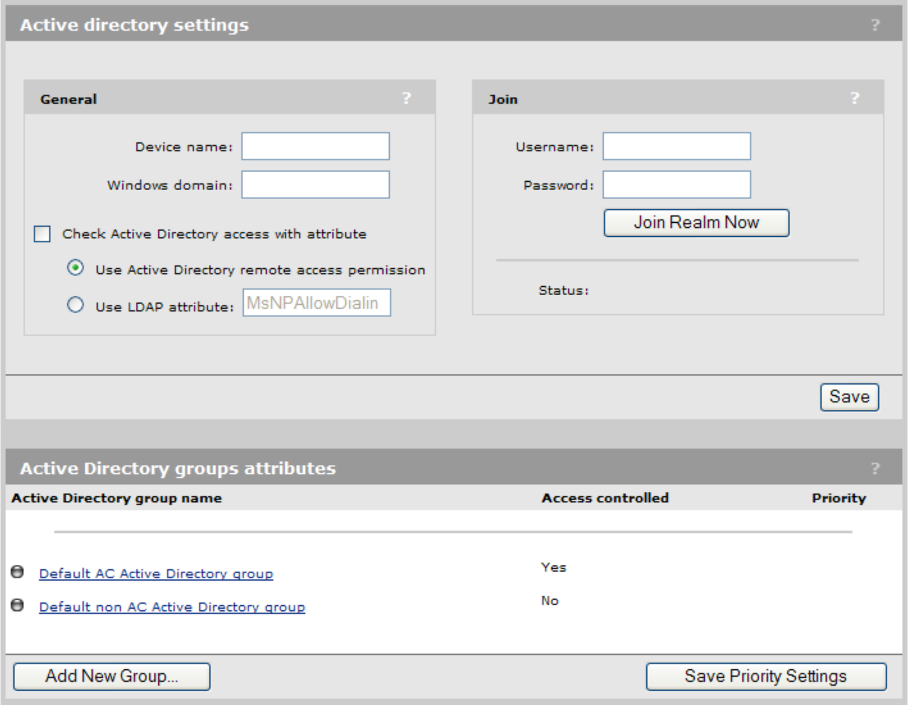
- EAP-PEAP
- EAP-TLS
- EAP-TTLS: Requires that client stations are configured to use MS-CHAP or MS-CHAP-V2.

Active Directory configuration

To configure active directory support, select **Controller >> Authentication > Active Directory**.

Note

It is important that the system time on the controller is accurate when an Active Directory server is being used. To set the time select **Controller >> Management > System time.**



Device name:
Windows domain:
□ Check Active Directory access with attribute
● Use Active Directory remote access permission
○ Use LDAP attribute: MsNPAllowDialin

Username:
Password:
Status:

Active Directory group name	Access controlled	Priority
Default AC Active Directory group	Yes	
Default non AC Active Directory group	No	

Active directory settings

General

Device name

Specify a name that identifies the controller to Active Directory. The controller uses this name to connect to the active directory server, just like any standard active directory client does.

Windows domain

Specify the Windows domain to which the controller belongs. The controller must be part of a Windows domain (**mydomain.com**, for example) to authenticate users that belong to that domain.

Check Active Directory access with attribute

Enable this option to have the controller only accept users with a specific setting in their account.

- **Use Active Directory remote access permission:** Use the standard attribute defined in Active Directory for remote access (MsNPAllowDIalin). If this attribute is set, then the user can be authenticated via Active Directory.

- **Use LDAP attribute:** For non-standard implementation of Active Directory, set this according to the equivalent setting on the Active Directory server.

Join

Before the controller can process user authentication using Active Directory, you must join the controller with the Active Directory server. Fill in the required parameters and select **Join Realm Now**. This is usually a one-time event.

Username

Username the controller will use to join Active Directory.

Password

Password the controller will use to join Active Directory.

Note For security reasons, **Username** and **Password** are not stored on the controller.

Join Realm Now

Select to join the realm immediately.

Status

Shows the status of the join operation as follows:

- **Unknown:** System is processing, no status to report. Refresh the page to update the status.
- **DNS unavailable:** DNS not working, cannot access Active Directory.
- **Missing Config:** No configuration, so join cannot proceed.
- **Never Joined:** Administrator never selected **Join Realm Now**.
- **Not joined:** Not joined: May be joined with the domain, but the join is not confirmed yet. Status will change to **Joined** once confirmed. If the **Not Joined** status persists, check connectivity between the controller and Active Directory or re-join.
- **Joined:** Active Directory reports that controller successfully joined.

Active Directory groups attributes

Displays all Active Directory groups that are defined on the controller. These groups are used to assign attributes to a user once they have been authenticated by Active Directory.

Note Group names on the controller must be identical to existing Active Directory Organizational Units configured on the Active Directory Server.

Once a user is authenticated by Active Directory, the controller retrieves the names of all the active directory groups of which the user is a member.

- If the user is a member of only one Active Directory group, and that group name appears in the list, the controller applies the attributes from that group.
- If the user is a member of more than one Active Directory group, the controller applies the attributes from the matching group name with the highest priority (highest in the list).

- If no match is found, the attributes defined for one of the default groups are applied as follows:
  - If the VSC the user logged in on is access-controlled then the **Default AC Active Directory** group is used.
  - If the VSC the user logged in on is not access-controlled then the **Default non AC Active Directory** group is used.

Note

The default groups are disabled by default. You need to enable them before they can be used.

Add New Group

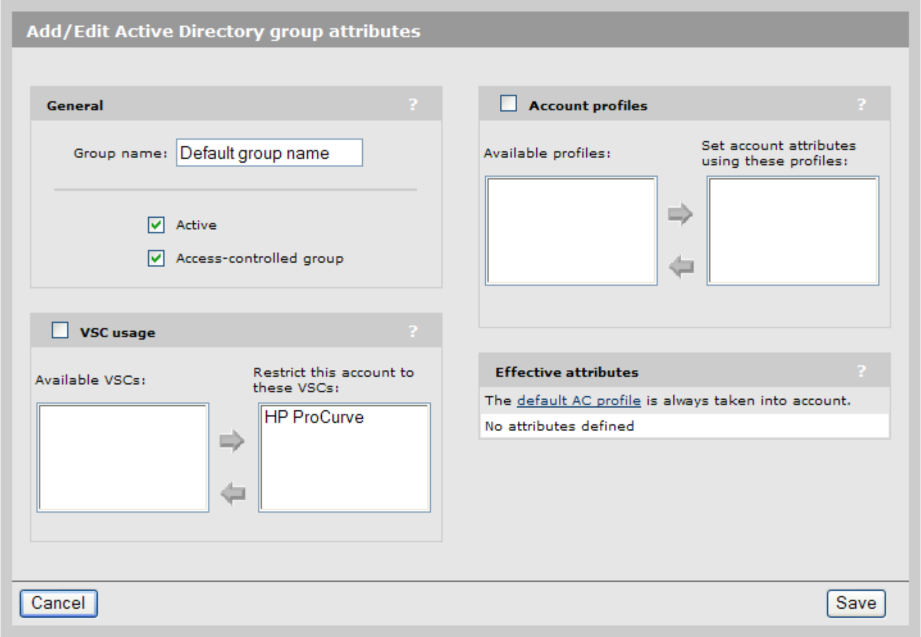
Select to add a new group. See *Configuring an Active Directory group on page 11-13*.

Save Priority Settings

After using the up/down arrows to change the priority of groups, save your changes by selecting this button.

Configuring an Active Directory group

An active directory group defines the characteristics of a user session. To make group configuration easy, account profiles (*Account profiles on page 10-27*) can be applied to set group attributes.



Add/Edit Active Directory group attributes

General

Group name: Default group name

☑ Active

☑ Access-controlled group

□ VSC usage

Available VSCs:

Restrict this account to these VSCs: HP ProCurve

□ Account profiles

Available profiles:

Set account attributes using these profiles:

Effective attributes

The default AC profile is always taken into account.

No attributes defined

Configuration parameters

General

Group name

Specify a name to identify the group. This name must match an existing Active Directory Organizational Unit configured on the Active Directory Server.

Active

Enable this option to activate the group. The group cannot be used until it is active.

Access-controlled group

Determines whether the group is access-controlled or not.

- Access-controlled groups can only be used to log in on VSCs that are access-controlled.
- Non access-controlled groups can only be used to log in on VSCs that are not access-controlled.

VSC usage

Enable this option to restrict this group to one or more VSCs. If the selected VSCs are not defined on an AP, users will not be able to log in on this account.

The **Available VSCs** list shows all defined VSCs that you can select from.

To move VSCs between the two lists:

- Double-click the profile you want to move.
- Or, select the profile you want to move and then select the left or right arrow.

Account profiles

Enable this option to set the attributes of this group using one or more account profiles.

The **Available profiles** list shows all defined profiles that you can select from. To add a new profile, open the **Controller >> Users > Account profiles** page.

To move profiles between the two lists, double-click the profile you want to move, or select the profile you want to move and then select the left or right arrow.

Effective attributes

This list shows all attributes that are active for this Active Directory group. Each time you add an account profile for use by this group, all attributes configured in the profile are added to the **Effective attributes** list.

Note Each profile that is applied to a group must have a unique set of attributes. The same attribute cannot be present in two different account profiles.

About the Default AC profile

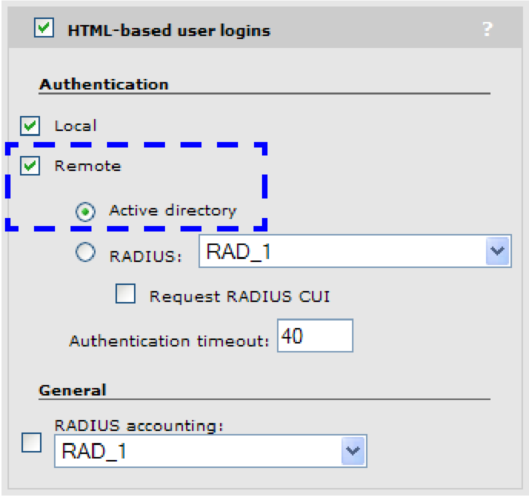
The **Default AC profile** is always present and is always applied to all Active Directory groups. You can use this profile to add additional attributes that are not configurable in an account profile. Instead, these attributes are configured on the **Controller >> Public access > Attributes** page. Once added there, they will automatically appear in the **Effective attributes** list.

The following attributes can be added using this method:

Attribute	For information, see
default-user-use-access-list	*Access list on page 15-34*
default-user-welcome-url	*Default user URLs on page 15-55.*
default-user-goodbye-url	*Default user URLs on page 15-55.*
default-user-one-to-one-nat	*Default user one-to-one NAT on page 15-53.*
default-user-idle-timeout	*Default user idle timeout on page 15-52.*
default-user-session-timeout	*Default user session timeout on page 15-54.*
default-user-acct-interim-update	*Default user interim accounting update interval on page 15-51.*
default-user-max-output-packets	*Default user quotas on page 15-52.*
default-user-max-input-packets	*Default user quotas on page 15-52.*
default-user-max-total-packets	*Default user quotas on page 15-52.*
default-user-max-output-octets	*Default user quotas on page 15-52.*
default-user-max-input-octets	*Default user quotas on page 15-52.*
default-user-max-total-octets	*Default user quotas on page 15-52.*
default-user-max-input-rate	*Default user data rates on page 15-53.*
default-user-max-output-rate	*Default user data rates on page 15-53*
default-user-bandwidth-level	*Default user bandwidth level on page 15-51.*
default-user-use-public-ip-subnet	*Default user public IP address on page 15-54.*

Configuring a VSC to use Active Directory

Any VSC feature that can be configured to support remote authentication can be configured to use Active Directory. For example, with HTML logins.



☑ HTML-based user logins

Authentication

☑ Local

☑ Remote

● Active directory

○ RADIUS: RAD_1

□ Request RADIUS CUI

Authentication timeout: 40

General

□ RADIUS accounting: RAD_1

12

Security

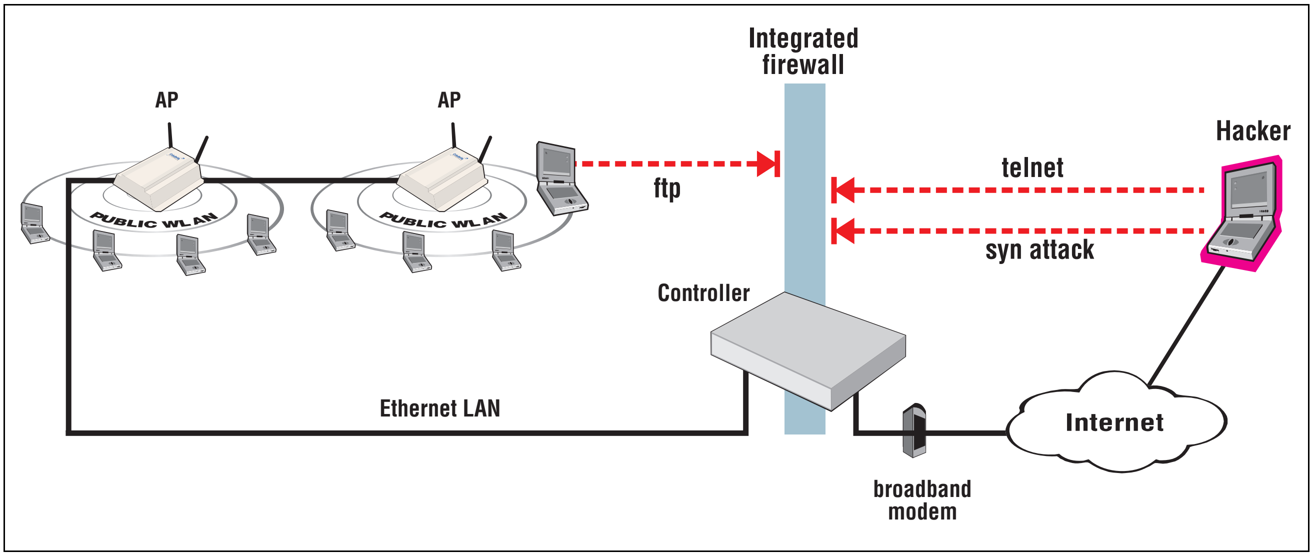
Contents

Firewall

To safeguard your network from intruders, the controller features a customizable stateful firewall. The firewall operates on the traffic streaming through the Internet port. It can be used to control both incoming and outgoing data.

A number of predefined firewall rules let you achieve the security level you need without going to the trouble of designing your own rules. However, you can create a completely custom set of firewall rules to suit your particular networking requirements, if necessary.

If the controller is connected to a wired LAN, the firewall protects the wired LAN as well.



Firewall presets

The easiest way to use the firewall is to use one of the preset settings. Two levels of security are provided:

- **High**: Permits all outgoing traffic, except NetBIOS (TCP and UDP). Blocks all externally initiated connections.
- **Low**: Permits all incoming and outgoing traffic, except for NetBIOS traffic. Use this option if you require active FTP sessions.

The following tables indicate how some common applications are affected by the preset firewall settings.

Outgoing traffic

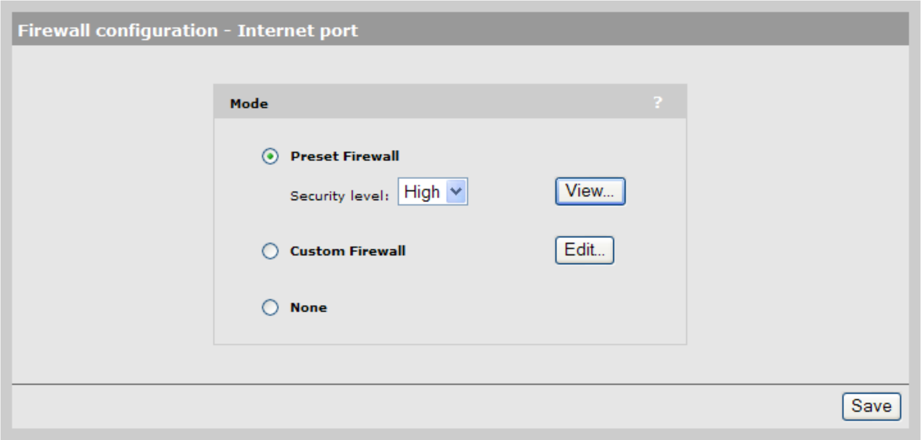
<table>
<tr><th></th><th colspan="2">Firewall setting</th></tr>
<tr><th>Application</th><th>Low</th><th>High</th></tr>
<tr><td>FTP (passive mode)</td><td colspan="2">Passed</td></tr>
<tr><td>FTP (active mode)</td><td colspan="2">Passed</td></tr>
<tr><td>Web (HTTP, HTTPS)</td><td colspan="2">Passed</td></tr>
<tr><td>SNMP</td><td colspan="2">Passed</td></tr>
<tr><td>Telnet</td><td colspan="2">Passed</td></tr>
<tr><td>Windows networking</td><td colspan="2">Blocked</td></tr>
<tr><td>ping</td><td colspan="2">Passed</td></tr>
<tr><td>PPTP from client station to remote server</td><td colspan="2">Passed</td></tr>
<tr><td>NetMeeting (make call)</td><td colspan="2">Passed</td></tr>
<tr><td>IPSec pass-through</td><td colspan="2">Passed</td></tr>
<tr><td>NetBIOS</td><td colspan="2">Blocked</td></tr>
</table>

Incoming traffic

	Firewall setting	
Application	**Low**	**High**
FTP (passive mode)	Passed	Blocked
FTP (active mode)	Passed	Blocked
Web (HTTPS)	Passed	Blocked
Web (HTTP)	Passed	Blocked
Telnet	Passed	Blocked
Windows networking	Passed	Blocked
PPTP from remote client to a server on the local network	Passed	Blocked
ping client on local network	Passed	Blocked
IPSec pass-through	Passed	Blocked
NetBIOS	Passed	Blocked
NetMeeting (receive call)	Passed	Blocked

Firewall configuration

To configure a firewall, select **Controller >> Security > Firewall**. The **Firewall configuration** page opens.



Firewall configuration - Internet port

Mode ?

● Preset Firewall

Security level: High

○ Custom Firewall

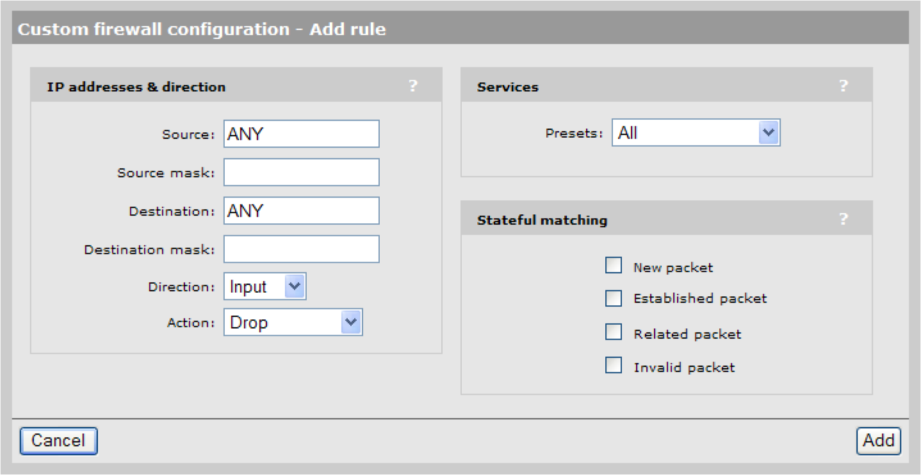
○ None

- Select **Preset firewall** to use a preconfigured firewall setting of **High** or **Low.** Select **View** to see the firewall rules for the selected setting.
- Select **Custom firewall** if you have specific security requirements. This setting enables you to target specific protocols or ports.

Customizing the firewall

To customize the firewall, you define one or more rules. A rule lets you target a specific type of data traffic. If the controller finds data traffic that matches the rule, the rule is triggered, and the traffic is rejected or accepted by the firewall.

To add a rule, select **Custom Firewall** on page **Security > Firewall**, select **Edit**, and then select **Add New Rule**.



Custom firewall configuration - Add rule

IP addresses & direction ?

Source: ANY

Source mask:

Destination: ANY

Destination mask:

Direction: Input

Action: Drop

Services ?

Presets: All

Stateful matching ?

□ New packet

□ Established packet

□ Related packet

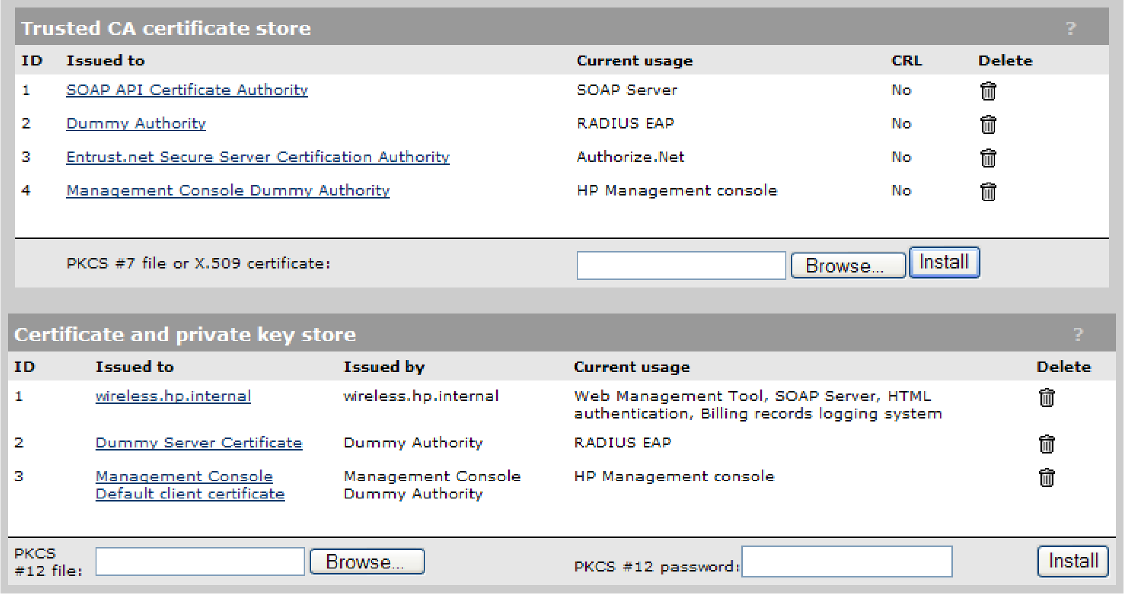
□ Invalid packet

Rules operate on IP datagrams (sometimes called *packets*). Datagrams are the individual packages of data that travel on an IP network. Each datagram contains addressing and control information along with the data it is transporting. The firewall analyses the addressing and control information to apply the rules you define.

The controller applies the firewall rules in the order that they appear in the list. An intelligent mechanism automatically adds the new rules to the list based on their scope. Rules that target a large amount of data are added at the bottom. Rules that target specific datagram attributes are added at the top.

Working with certificates

The certificate stores provide a repository for managing all certificates (except for those used by IPSec and NOC authentication). To view the certificate stores, select **Controller >> Security > Certificate stores**.



Trusted CA certificate store

ID	Issued to	Current usage	CRL	Delete
1	SOAP API Certificate Authority	SOAP Server	No	🗑
2	Dummy Authority	RADIUS EAP	No	🗑
3	Entrust.net Secure Server Certification Authority	Authorize.Net	No	🗑
4	Management Console Dummy Authority	HP Management console	No	🗑

PKCS #7 file or X.509 certificate: [ ] Browse... Install

Certificate and private key store

ID	Issued to	Issued by	Current usage	Delete
1	wireless.hp.internal	wireless.hp.internal	Web Management Tool, SOAP Server, HTML authentication, Billing records logging system	🗑
2	Dummy Server Certificate	Dummy Authority	RADIUS EAP	🗑
3	Management Console Default client certificate	Management Console Dummy Authority	HP Management console	🗑

PKCS #12 file: [ ] Browse... PKCS #12 password: [ ] Install

Trusted CA certificate store

This list displays all root CA (certificate authority) certificates installed on the controller. The controller uses these CA certificates to validate the certificates supplied by client stations during authentication. Multiple CA certificates can be installed to support validation of clients with certificates issued by different CAs.

The controller uses these certificates to validate certificates supplied by:

- Managers or operators accessing the controller's management tool.
- HTML users accessing the public access interface.
- SOAP clients communicating with the controller's SOAP server.
- RADIUS EAP

The following information is presented for each certificate in the list:

- **ID:** A sequentially assigned number to help identify certificates with the same common name.
- **Issued to:** Name of the certificate holder. Select the name to view the contents of the certificate.
- **Current usage:** Lists the services that are currently using this certificate.
- **CRL:** Indicates if a certificate revocation list is bound to the certificate. An X.509 certificate revocation list is a document produced by a certificate authority (CA) that provides a list of serial numbers of certificate that have been signed by the CA but that should be rejected.
- **Delete:** Select to remove the certificate from the certificate store.

Installing a new CA certificate

1. Specify the name of the certificate file or select **Browse** to choose from a list. CA certificates must be in X.509 or PKCS #7 format.
2. Select **Install** to install a new CA certificate.

CA certificate import formats

The import mechanism supports importing the ASN.1 DER encoded X.509 certificate directly or as part of two other formats:

- PKCS #7 (widely used by Microsoft products)
- PEM, defined by OpenSSL (popular in the Unix world)
- The CRL can be imported as an ASN.1 DER encoded X.509 certificate revocation list directly or as part of a PEM file.

Content and file format	Items carried in the file	Description
ASN.1 DER encoded X.509 certificate	One X.509 certificate	This is the most basic format supported, the certificate without any envelope.
X.509 certificate in PKCS #7 file	One X.509 certificate	Popular format with Microsoft products.

Content and file format	Items carried in the file	Description
X.509 certificate in PEM file	One or more X.509 certificates	Popular format in the Unix world. X.509 DER certificate is base64 encoded and placed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines. Multiple certificates can be repeated in the same file.
ASN.1 DER encoded X.509 CRL	One X.509 CRL	Most basic format supported for CRL.
X.509 CRL in PEM file	One X.509 CRL	Same format as X.509 certificate in PEM format, except that the lines contain BEGIN CRL and END CRL.

Default CA certificates

The following certificates are installed by default:

- **SOAP API Certificate Authority:** Before allowing a SOAP client to connect, the controller checks the certificate supplied by a SOAP client to ensure that it is issued by a trusted certificate authority (CA).
- **Dummy Authority:** Used by the internal RADIUS server. You should replace this with your own CA certificate.
- **Entrust.net Secure Server Certification Authority:** This is the Authorize.Net CA certificate. It is used to support credit card payments via Authorize.Net.
- **Management Console Dummy Authority:** Used when the management tool communicates with HP PCM/PMM software.

Note For security reasons, you should replace the default certificates with your own.

Certificate and private key store

This list displays all certificates installed on the controller. The controller uses these certificates and private keys to authenticate itself to peers.

Items provided in this list are as follows:

ID

A sequentially assigned number to help identify certificates with the same common name.

Issued to

Name of the certificate holder. Select the name to view the contents of the certificate.

Issued by

Name of the CA that issued the certificate.

Current usage

Lists the services that are currently using this certificate.

Delete

Select to remove the certificate from the certificate store.

Installing a new private key/public key certificate chain pair

Note RADIUS EAP certificates must have the X.509 extensions. Information about this is available in the Microsoft knowledgebase at: http://support.microsoft.com/kb/814394/en-us

The certificate you install must:

- Be in PKCS #12 format.
- Contain a private key (a password controls access to the private key).
- Not have a name that is an IP address. The name should be a domain name containing at least one dot. If you try to add a certificate with an invalid name, the default certificate is restored.

The common name in the certificate is automatically assigned as the domain name of the controller.

1. Specify the name of the certificate file or select **Browse** to choose one from a list. Certificates must be in PKCS #7 format.
2. Specify the **PKCS #12 password**.
3. Select **Install** to install the certificate.

Default installed private key/public key certificate chains

The following private key/public key certificate chains are installed by default:

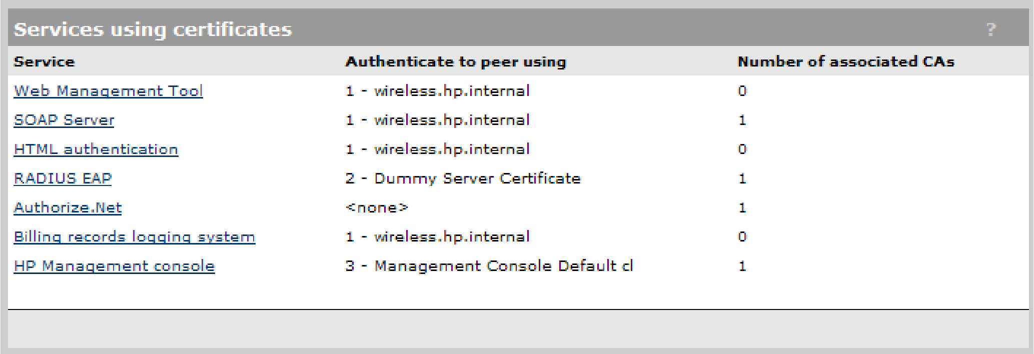
- **wireless.hp.internal:** Default certificate used by the management tool, SOAP server, and HTML-based authentication.
- **Dummy Server Certificate:** Used by the internal RADIUS server. This certificate is present only to allow EAP-PEAP to work if the client chooses not to verify the server's certificate. You should replace this with your own certificate for maximum security.
- **Management Default client certificate:** This certificate is used to identify the management tool when it communicates with HP PCM/PMM software.

Note When a Web browser connects to the controller using SSL/TLS, the controller sends only its own X.509 certificate to the browser. This means that if the certificate has been signed by an intermediate certificate authority, and if the Web browser only knows about the root certificate authority that signed the public key certificate of the intermediate certificate authority, the Web browser does not get the whole certificate chain it needs to validate the identity of the controller. Consequently, the Web browser issues security warnings.
To avoid this problem, make sure that you install the entire certificate chain when you install a new certificate on the controller.

Note An SNMP notification is sent to let you know when the controller SSL certificate is about to expire if you enable the **Notifications** option on the **Controller >> Management > SNMP** page and then select **Configure Notifications** and enable the **Certificate about to expire** notification under **Maintenance**.

Certificate usage

To see the services that are associated with each certificate, select **Security > Certificate usage**. With the factory default certificates installed, the page will look like this:



Services using certificates

Service	Authenticate to peer using	Number of associated CAs
Web Management Tool	1 - wireless.hp.internal	0
SOAP Server	1 - wireless.hp.internal	1
HTML authentication	1 - wireless.hp.internal	0
RADIUS EAP	2 - Dummy Server Certificate	1
Authorize.Net	<none>	1
Billing records logging system	1 - wireless.hp.internal	0
HP Management console	3 - Management Console Default cl	1

Service

Name of the service that is using the certificate. To view detailed information on the certificate select the service name.

Authenticate to peer using

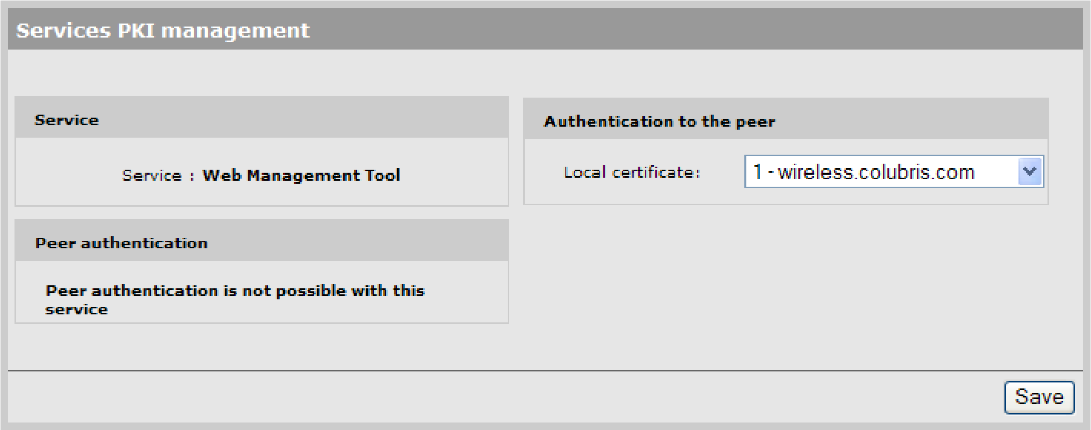
Name of the certificate and private key. The controller is able to prove that it has the private key corresponding to the public key in the certificate. This is what establishes the controller as a legitimate user of the certificate.

Number of associated CAs

Number of CA certificates used by the service.

Changing the certificate assigned to a service.

Select the service name to open the Certificate details page. For example, if you select **Web management tool**, you will see:



Services PKI management

Service

Service : **Web Management Tool**

Peer authentication

Peer authentication is not possible with this service

Authentication to the peer

Local certificate: 1 - wireless.colubris.com

Under **Authentication to the peer**, select a new **Local certificate** and then select **Save**.

About certificate warnings

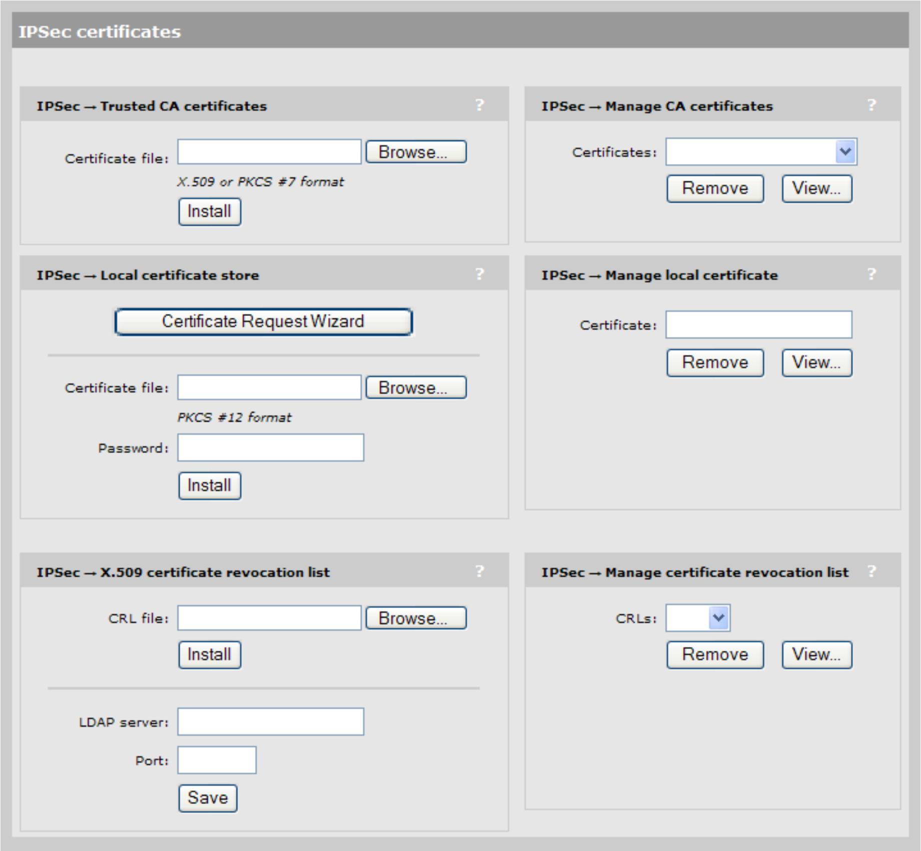
Access to the management tool and the public access interface Login page occur through a secure connection (SSL/TLS). An X.509 certificate is used to validate this connection. The default X.509 certificate installed on the controller for SSL/TLS for access to the management tool and the public access interface is not registered with a certificate authority. It is a self-signed certificate that is attached to the default IP address (192.168.1.1) for the controller's LAN port. As a result, certificate warnings will appear at login until you install a valid, trusted certificate on the controller.

The host name in the currently installed SSL certificate is automatically assigned as the domain name of the controller. You do not have to add this name to your DNS server for it to be resolved. The controller intercepts all DNS requests it receives on the wireless or LAN ports. It resolves any request that matches the certificate host name by returning the IP address assigned to the wireless port. All other DNS requests are forwarded to the appropriate DNS servers as configured on the **Network > DNS** page.

This means that once a valid, trusted certificate is installed on the controller, users will no longer see a certificate warning message when logging in.

IPSec certificates

IPSec certificates are managed on the lower portion of the **Controller >> VPN > IPSec** page.



IPSec — Trusted CA certificates

The controller uses the CA certificates to validate the certificates supplied by peers during the authentication process. Multiple CA certificates can be installed to support validation of peers with certificates issued by different CAs.

- **Certificate file**: Specify the name of the certificate file or select **Browse** to choose from a list. CA certificates must be in X.509 or PKCS #7 format.
- **Install**: Select to install the specified certificate.

IPSec — Manage CA certificates

Use this box to manage the root CA certificate.

- **Certificate**: Select from a list of installed certificates.
- **Remove**: Delete the item shown under **Certificate.**
- **View:** Open the item shown under **Certificate** for viewing.

IPSec — Local certificate store

This is the certificate that the controller uses to identify itself to IPSec peers.

Note If the local certificate includes a CA certificate, both certificates are installed.

- **Certificate Request Wizard**: Helps you to generate a certificate request that can be used to obtain a signed certificate from a certificate authority. Once you obtain the certificate, you can use the **Certificate Request Wizard** to install it on the controller.
- **Certificate file**: Specify the name of the certificate file or select **Browse** to choose from a list.
- **Password**: Specify the certificate password.
- **Install**: Select to install the certificate.

IPSec — Manage local certificate

Use this box to manage the local certificate.

- **Certificate**: Shows the common name of the installed certificate.
- **Remove**: Delete the item shown under **Certificate.**
- **View**: Open the item shown under **Certificate** for viewing.

IPSec — X.509 certificate revocation list

Use this box to update the certificate revocation list (CRL) that is issued by the certificate authority.

The controller uses the CRL to determine if the certificates provided by clients during the authentication process have been revoked. The controller will not establish a security association with a client that submits a revoked certificate.

The controller can obtain a CRL in two ways:

- You can manually install it.
- The controller can automatically install a CRL based on information contained in a client certificate. This occurs only if a CRL is not installed, or if the installed CRL is expired.
- **CRL file**: Specify the name of the CRL file or select **Browse** to choose from a list.
- **Install**: Select to install the specified CRL.
- **LDAP server**: A client certificate may contain a list of locations where the CRL can automatically be retrieved. This location may be specified as an HTTP URL, FTP URL, LDAP URL, or LDAP directory. If the LDAP URL or directory is incomplete, the controller uses the location you specify to resolve the request. Incomplete HTTP or FTP URLs fail.
- **Port**: Port on the LDAP server. Default is 389.

IPSec — Manage certificate revocation list

Use this box to manage the CRL.

- **CRLs**: Shows a list of installed certificate revocation lists.
- **Remove**: Deletes the item shown under **CRLs.**
- **View**: Opens the item shown under **CRLs** for viewing.

MAC lockout

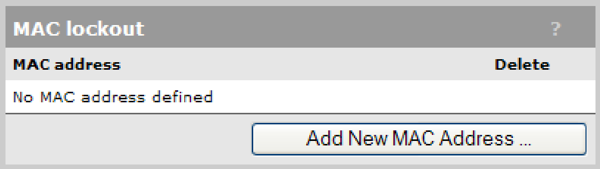
This feature lets you to block traffic from client stations based on their MAC address. MAC lockout applies to client stations connected to:

- Wireless ports on controlled APs
- Wired ports (including switch ports) on controlled APs
- Local mesh ports on controlled APs
- The LAN port on the controller

Note MAC lockout does not apply to the Internet port on the controller.

Adding a MAC lockout address

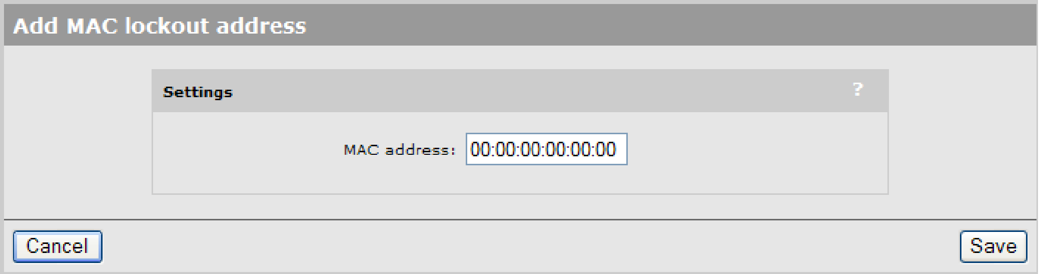
1. Select **Controller >> Security > MAC lockout**.



MAC lockout

MAC address	Delete
No MAC address defined	

2. Select **Add New MAC Address**.



Add MAC lockout address

Settings

MAC address: 00:00:00:00:00:00

3. Specify the MAC address as six pairs of hexadecimal digits separated by colons. For example: 00:00:00:0a:0f:01.
4. Select **Save**.

13

Local mesh

Contents

Key concepts

The local mesh feature enables you to create wireless links between two or more APs. These links provide a wireless bridge that interconnects the networks connected to the Ethernet port on each AP.

The local mesh feature replaces the need for Ethernet cabling between APs, making it easy to extend your network in hard-to-wire locations or in outdoor areas.

Key local mesh features include:

- **Automatic link establishment:** Nodes automatically establish wireless links to create a full-connected network. A dynamic network identifier (local mesh group ID) restricts connectivity to groups of nodes, enabling distinct groups to be created with nodes in the same physical area.
- **Provides fall-back operation to recover from node failure.** In a properly designed implementation, redundant paths can be provided. If a node fails, the mesh will automatically reconfigure itself to maintain connectivity.
- **Maintains network integrity when using DFS channels.** In accordance with the 802.11h standard, dynamic frequency selection (DFS) detects the presence of certain radar devices on a channel and automatically switches the network node to another channel if such signals are detected. 802.11h is intended to resolve interference issues with military radar systems and medical devices.

Note Depending on the radio regulations of some countries, DFS channels are only available on the 802.11a/n bands, which are the preferred band for local mesh backhaul. If more than one node detects radar simultaneously and must switch channels, each node does not necessarily switch to the same channel, and the network might never reconverge. To avoid this problem, local mesh detects a change in channel and provides a means to reconnect on other channels by scanning on multiple channels. See *Operating channel on page 13-6*.

Simultaneous AP and local mesh support

APs can be configured to support both access point and local mesh functionality whether they have a single radio, or multiple radios.

Single radio APs

A single radio can be configured to simultaneously support wireless users and one or more local mesh links. Although this offers flexibility it does have the following limitations:

- The total available bandwidth on the radio is shared between all local mesh links and wireless users. This can result in reduced throughput if lots of traffic is being sent by both wireless users and the local mesh links. You can use the QoS feature to prioritize traffic.
- It limits you to using the same radio options for both wireless clients and local meshes.

Multiple radio APs

On APs with more than one radio, one radio can be dedicated to support wireless users and another to provide local mesh links. Each radio can be configured optimally according to its application.

Using 802.11a/n for local mesh

It is recommended that 802.11a/n in the 5 GHz band be used for local mesh links whenever possible. This optimizes throughput and reduces the potential for interference because:

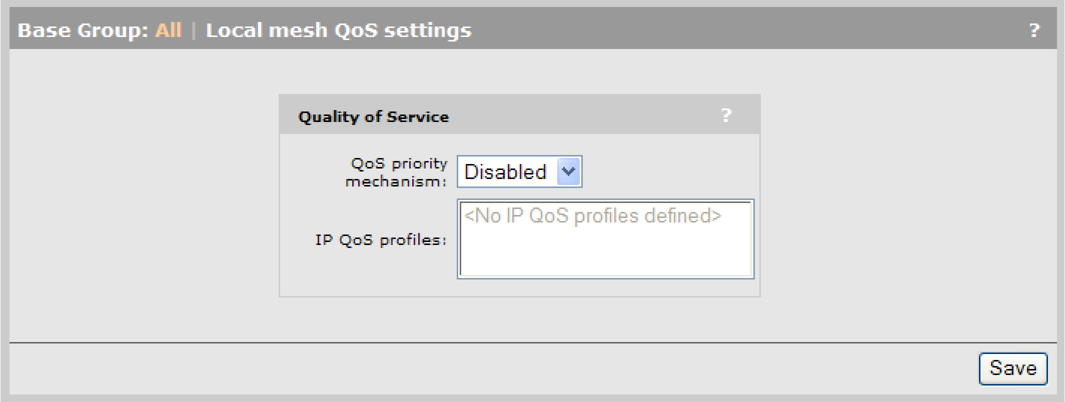
- Most Wi-Fi clients support 802.11b or b/g, therefore most APs are set to operate in the 2.4 GHz band. This frees the 5 GHz (802.11a/n) band for other applications such as local mesh.
- 802.11a/n channels in the 5 GHz band are non-overlapping.
- 802.11a/n provides increased data throughput, providing a *fat pipe* for traffic exchange.

The main limitations in using the 5 GHz band are:

- Since the same radio options must be used for both wireless clients and local mesh links, support for 802.11b/g clients is not possible on APs with a single radio.
- The 5 GHZ band has a shorter reach when compared to the 2.4 GHz band. This could be a factor depending on the distance your links must span.

Quality of service

The local mesh feature enables you to define a quality of service (QoS) setting that will govern how traffic is sent on all wireless links.



Base Group: All | Local mesh QoS settings

Quality of Service

QoS priority mechanism: Disabled

IP QoS profiles: <No IP QoS profiles defined>

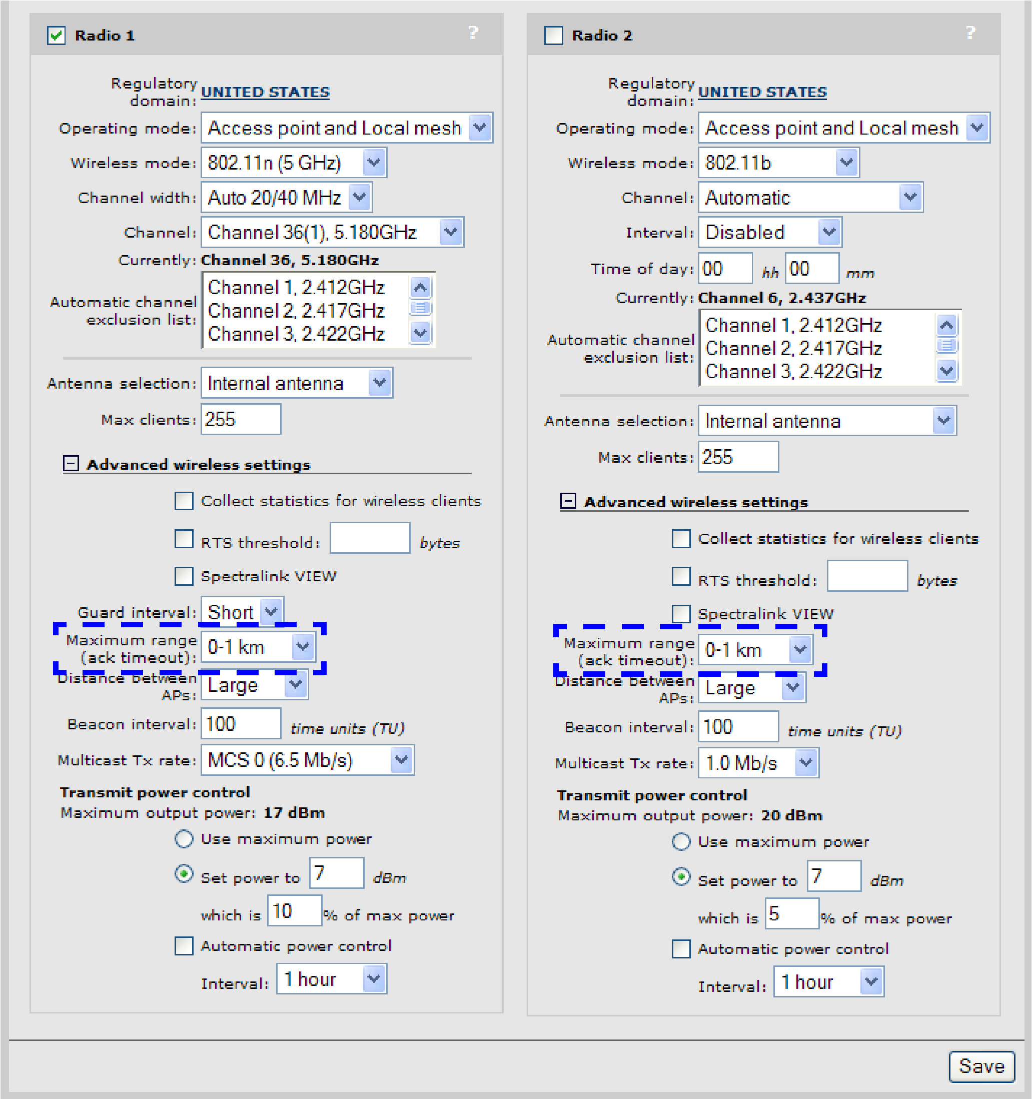
Note

When traffic is forwarded onto a local mesh link from a VSC, the QoS settings on the VSC take priority. For example, if you define a VSC with a QoS setting of **VSC-based High**, then traffic from this VSC will traverse the local mesh on queue 2 even if the QoS setting on the local mesh is **VSC-based Low** (queue 4).

Maximum range (ack timeout)

This is a global setting that is configurable on the **Radio** page when the **Operating mode** is set to support **Local mesh**. It fine tunes internal timeout settings to account for the distance that a link spans. For normal operation, it is set to less than 1 km.

This is a global setting that applies to all wireless connections made with a radio, not just for local mesh links. Therefore, if you are also using a radio to access an AP, adjusting this setting may lower the performance for users with marginal signal strength or when interference is present. (Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)



☑ **Radio 1**

Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11n (5 GHz)
Channel width: Auto 20/40 MHz
Channel: Channel 36(1), 5.180GHz
Currently: **Channel 36, 5.180GHz**
Automatic channel exclusion list: Channel 1, 2.412GHz / Channel 2, 2.417GHz / Channel 3, 2.422GHz
Antenna selection: Internal antenna
Max clients: 255

⊟ **Advanced wireless settings**

□ Collect statistics for wireless clients
□ RTS threshold: *bytes*
□ Spectralink VIEW
Guard interval: Short
Maximum range (ack timeout): 0-1 km
Distance between APs: Large
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: MCS 0 (6.5 Mb/s)

Transmit power control
Maximum output power: **17 dBm**
○ Use maximum power
● Set power to 7 *dBm*
which is 10 % of max power
□ Automatic power control
Interval: 1 hour

□ **Radio 2**

Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11b
Channel: Automatic
Interval: Disabled
Time of day: 00 *hh* 00 *mm*
Currently: **Channel 6, 2.437GHz**
Automatic channel exclusion list: Channel 1, 2.412GHz / Channel 2, 2.417GHz / Channel 3, 2.422GHz
Antenna selection: Internal antenna
Max clients: 255

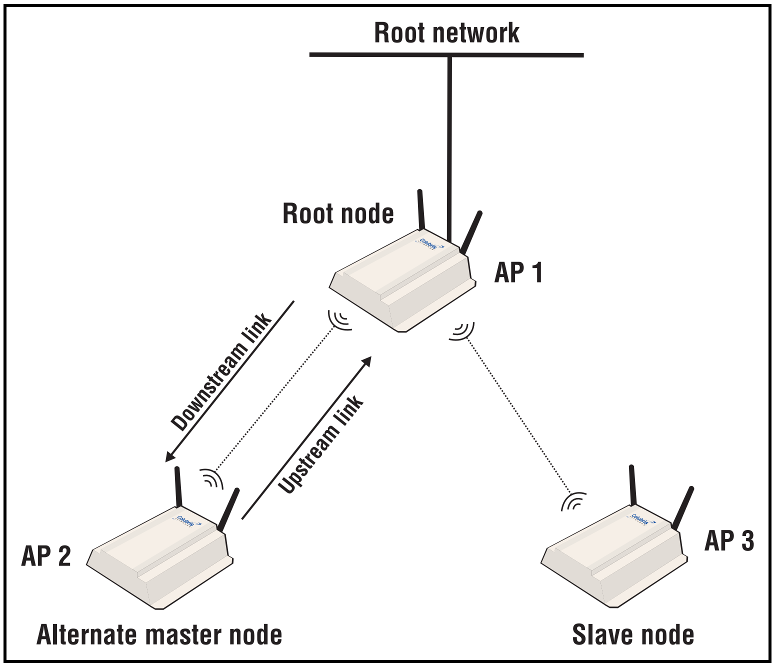
⊟ **Advanced wireless settings**

□ Collect statistics for wireless clients
□ RTS threshold: *bytes*
□ Spectralink VIEW
Maximum range (ack timeout): 0-1 km
Distance between APs: Large
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 1.0 Mb/s

Transmit power control
Maximum output power: **20 dBm**
○ Use maximum power
● Set power to 7 *dBm*
which is 5 % of max power
□ Automatic power control
Interval: 1 hour

Local mesh terminology

The following table defines terms that are used in this guide when discussing the local mesh feature.



Term	Definition
Node	An AP that is configured to support local mesh connections.
Root node	The root node is configured in **Master** mode and provides access to the root network.
Alternate master node	A node that is configured in **Alternate master** mode which enables it to make upstream and downstream connections.
Slave node	A node that is configured in **Slave** mode which enables it to make upstream connections only.
Root network	Wired network to which the root node is connected. This is the network to which the local mesh provides access for all connected alternate master and slave nodes.
Mesh	A series of nodes that connect to form a network. Each mesh is identified by a unique mesh ID.
Link	The wireless connection between two nodes.
Downstream link	A link that transports data away from the root network.
Upstream link	A link that transports data towards the root network.
Peer	Any two connected nodes are peers. In the diagram, AP 1 is the peer of both AP 2 and AP 3.

Local mesh operational modes

Three different roles can be assigned to a local mesh node: **Master, Alternate Master,** or **Slave.** Each role governs how upstream and downstream links are established by the node.

- **Master**: Root node that provides the upstream link to the *ground network* that the other nodes want to reach. The master never tries to connect to any other node. It waits for links from downstream alternate master or slave nodes.

Note

It is possible to have several masters for the same mesh ID connected to the ground network. This can be used to provide redundant paths to the ground network for downstream nodes.

- **Alternate Master**: First establishes an upstream link with a master or alternate master node. Next, operates as a master node waiting for links from downstream alternate master or slave nodes.
- **Slave**: Can only establish an upstream link with master or alternate master node. Slave nodes cannot establish downstream links with other nodes.

Node discovery

Discovery of another node to link with is limited to nodes with the same mesh ID. The link is established with the node that has the best score based on the following calculation:

```
Score = SNR - (Number of hops x SNR cost of each hop)
```

If a node looses its upstream link, it automatically discovers and connects to another available node.

Note

A master or alternate master must be seen with an SNR of 20 or higher before a slave will attempt to connect to it.

Operating channel

If a mesh operates on a dynamic frequency selection (DFS) channel, the master node selects the operating channel. If another node detects radar and switches channels, that node reports the channel switch to the master node, which initiates a channel switch for the nodes connected to it. This allows the local mesh to converge on a specific channel.

A node that uses a DFS channel and that loses connection with its master, scans channels to find a master on another channel, which can be a new master or the same master.

If the local mesh does not operate on a DFS channel, configure the radios in one of the following ways:

- Configure the radios on all nodes to use the same fixed channel.
- Configure the radios for automatic channel selection. In this case the master selects the least noisy channel. Slaves and alternate masters scan channels until they find the master, then tune to the master channel and link with the master.

Local mesh profiles

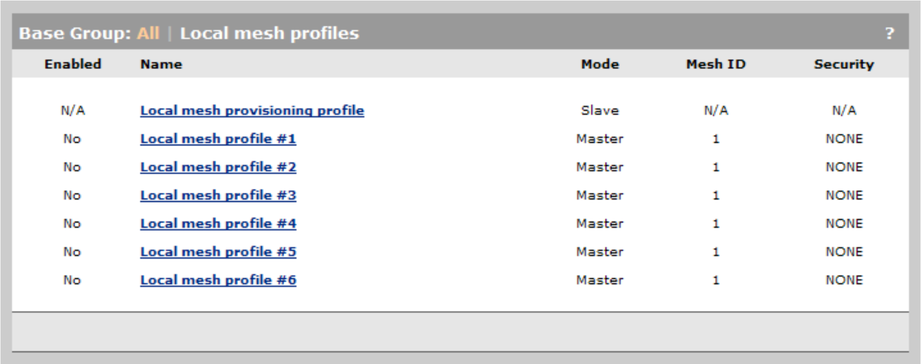
A local mesh profile defines the characteristics for the type of links that can be established with other nodes as follows:

Role	Upstream link	Downstream link
Master	None.	Up to nine links with alternate master or slave nodes per profile.
Alternate master	A single link to a master node or alternate master node.	Up to eight links with alternate master or slave nodes.
Slave	A single link to a master node or alternate master node.	None.

Each node supports up to six profiles plus one provisioning profile. When a profile is active, a node constantly scans and tries to establish links as defined by the profile.

The **local mesh provisioning profile** is used by the wireless link created on a provisioned AP to support discovery of the controller. Initially, this link operates in slave mode. If you configure this profile as an alternate master, then it can also be used to establish up to nine downstream links with alternate master or slave nodes. See *Provisioning local mesh links on page 13-12* for more information.

Local mesh profiles are configurable at the controlled APs, group, or AP level. To view all profiles select **Controller > Controlled APs >> Configuration > Local mesh**. Or you can expand **Controlled APs** and select a group or specific AP. The following is an example of the profile list displayed when selecting **Controlled APs >> Configuration > Local mesh**.



Base Group: All | Local mesh profiles ?

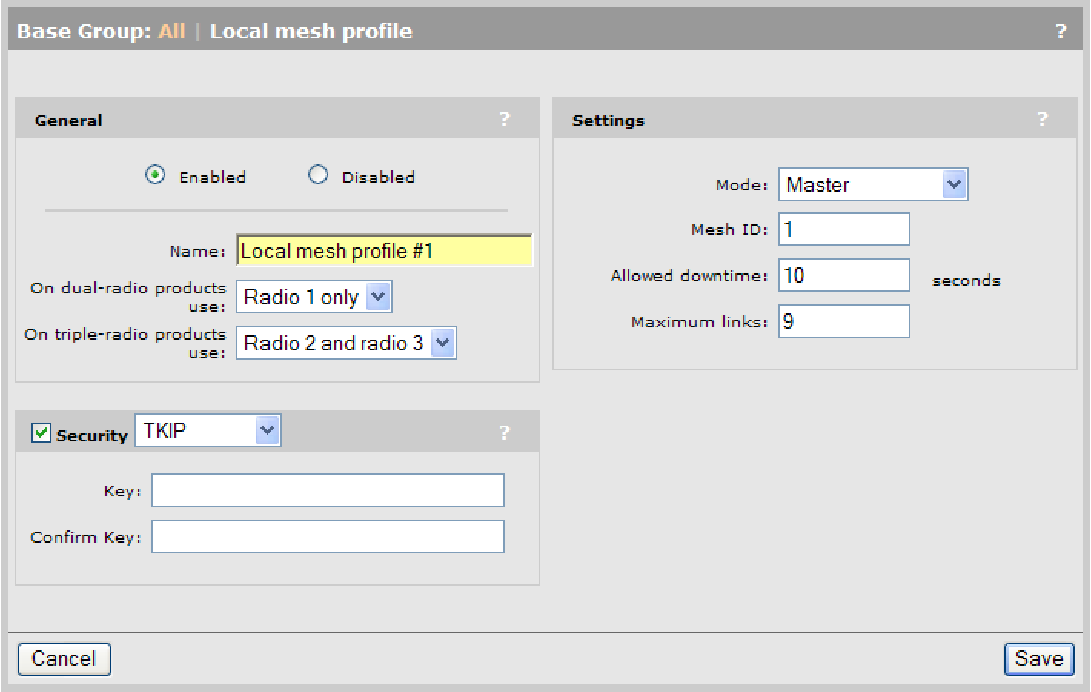
Enabled	Name	Mode	Mesh ID	Security
N/A	Local mesh provisioning profile	Slave	N/A	N/A
No	Local mesh profile #1	Master	1	NONE
No	Local mesh profile #2	Master	1	NONE
No	Local mesh profile #3	Master	1	NONE
No	Local mesh profile #4	Master	1	NONE
No	Local mesh profile #5	Master	1	NONE
No	Local mesh profile #6	Master	1	NONE

Configuration guidelines

- In addition to the provisioning profile, you can configure a total of six local mesh profiles on each node.
- Each local mesh profile (on a master or alternate master) can be used to establish up to nine links with other nodes.
- The same security settings must be used on all nodes in the same mesh.
- Any node that reaches the controller through the local mesh and uses local mesh itself, must be provisioned prior to discovery.
- Daisy-chaining of nodes using local mesh links dramatically reduces throughput (which is typically divided by two for each hop) especially when one or more of the following are true:
  - Nodes provide both upstream and downstream links on the same radio.
  - Nodes share a radio with AP functionality.
  - IP traffic originating from a node can be sent on the link on which the controller was discovered.

Configuring a local mesh profile

To configure profiles #1 to #6, select a name in the list. The **Local mesh profile** page opens.



Base Group: All | Local mesh profile

General

● Enabled ○ Disabled

Name: Local mesh profile #1

On dual-radio products use: Radio 1 only

On triple-radio products use: Radio 2 and radio 3

☑ **Security** TKIP

Key:

Confirm Key:

Settings

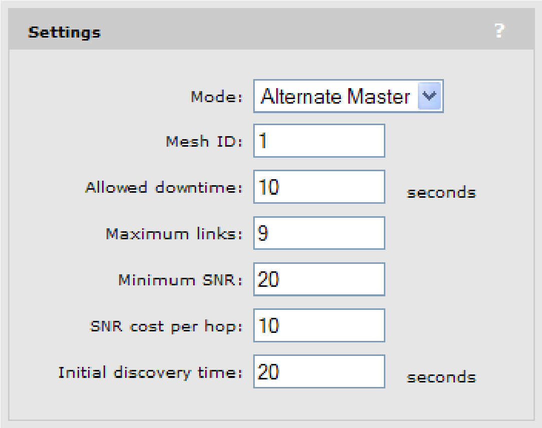
Mode: Master

Mesh ID: 1

Allowed downtime: 10 seconds

Maximum links: 9

For **Slave** and **Alternate Master**, the **Settings** box shows the additional options, for example Alternate Master:



Settings

Mode: Alternate Master

Mesh ID: 1

Allowed downtime: 10 seconds

Maximum links: 9

Minimum SNR: 20

SNR cost per hop: 10

Initial discovery time: 20 seconds

General

Enabled/Disabled

Specify if the profile is enabled or disabled. The profile is only active when enabled.

Name

Name of the profile.

On dual-radio products use

Select the radio to use for this link.

Settings

Mode

Three different roles can be assigned to a node: master, alternate master, or slave. Each role governs how links are established. Links are defined as either upstream or downstream.

- **Master:** The master is the root node that provides the upstream connection to the *ground network* that the other nodes want to reach. The master will only create downstream local mesh links to alternate master or slave nodes.
- **Slave:** Slave nodes can only establish upstream links with master or alternate master nodes. Slave nodes cannot establish downstream links with other nodes.
- **Alternate Master:** An alternate master node must first establish an upstream link with a master or alternate master node before it can establish downstream connections with an alternate master or slave node.

Mesh ID

Unique number that identifies a series of nodes that can connect together to form a local mesh network.

Allowed downtime

The maximum time (in seconds) that a link can remain idle before the link actually gets deleted. When a slave (or alternate master) looses its link to its master, the discovery phase is re-initiated.

Minimum SNR

(Alternate master or slave nodes)

This node will only connect with other nodes whose SNR is above this setting (in dB).

SNR cost per hop

(Alternate master or slave nodes)

This value is an estimate of the cost of a hop in terms of SNR. It indicates how much SNR a node is willing to sacrifice to connect to node one hop closer to the root node, because each hop has an impact on performance, especially when using a single radio.

Initial discovery time

(Alternate master or slave nodes)

Amount of time that will be taken to discover the best available master node. The goal of this setting is to delay discovery until all the nodes in the surrounding area have had time to startup, making the identification of the best master more accurate. If this period is too short, a slave may connect to the first master it finds, not necessarily the best.

Security

Enable this option to secure data transmitted on the wireless link. The APs on both sides of the wireless link must be configured with the same security options.

WEP

This feature has been deprecated. *If you are creating a new installation, use AES/ CCMP. If you are upgrading from a previous release, your existing configuration will still work.*

Enables WEP to secure traffic on the wireless link.

Specify the encryption key the node will use to encrypt/decrypt all data it sends and receives. The key is 128 bits long and must be specified as 26 hexadecimal digits.

TKIP

This feature has been deprecated. *If you are creating a new installation, use* ***AES/CCMP*** *instead. If you are upgrading from a previous release, your existing configuration will still work.*

Enables TKIP encryption to secure traffic on the wireless link.

The node uses the key you specify in the PSK field to generate the TKIP keys that encrypt the wireless data stream.

Specify a key that is between 8 and 63 ASCII characters in length. It is recommended that the key be at least 20 characters long, and be a mix of letters and numbers.

AES/CCMP

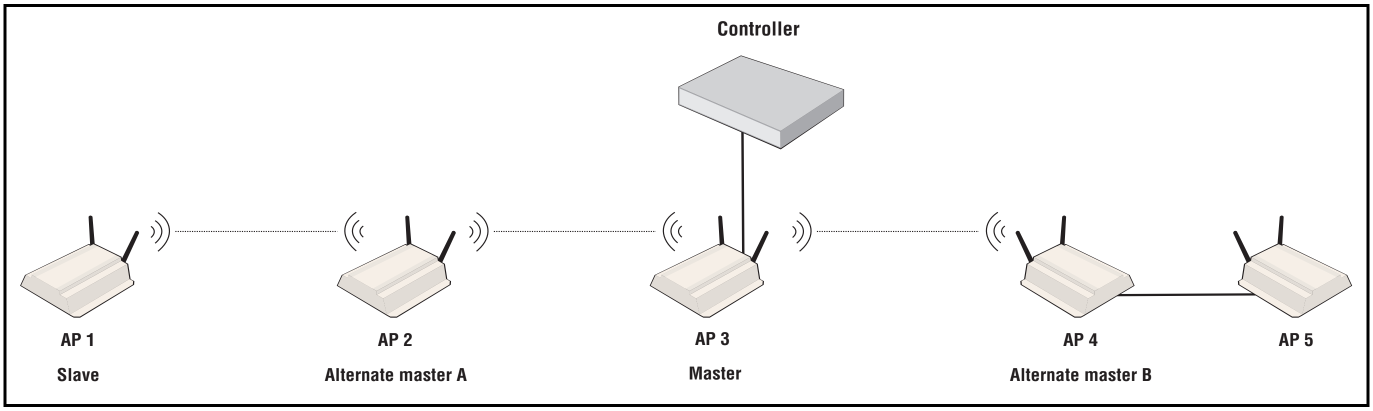
Enables AES with CCMP encryption to secure traffic on the wireless link. This is the most secure method.

The node uses the key you specify in the PSK field to generate the keys that encrypt the wireless data stream.

Specify a key that is between 8 and 63 ASCII characters in length. It is recommended that the key be at least 20 characters long and be a mix of letters and numbers.

Provisioning local mesh links

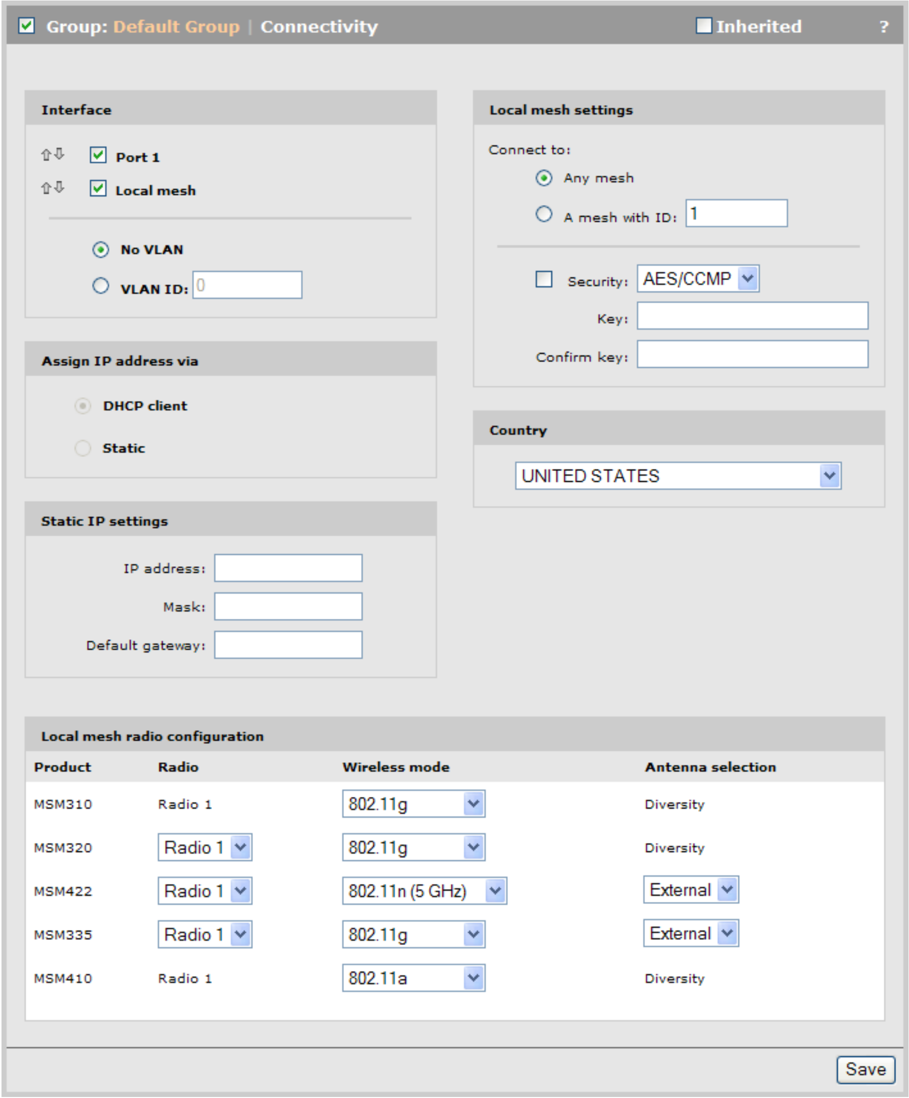
APs operating in controlled mode must be able to discover and connect with a controller. When operating as part of a local mesh, *any AP that can* ***only*** *discover the controller via a wireless link must be provisioned* before being deployed. In this example, AP 1, AP 2, AP 4, and AP 5 must be provisioned prior to deployment for discovery to be successful. (Since AP 3 is using a wired link, it does not need to be provisioned for this scenario.)



Provisioning is done before APs are deployed using either of the following methods:

- Directly connect to each AP and use its management tool to define provisioning settings.
- Connect the APs to the controller (either directly via the LAN port or through a local area network). After the APs are discovered, use the controller management tool to define provisioning settings by opening the **Provisioning > Connectivity** page at either the group or AP level.

In the this example, AP 1, AP 2, and AP 4 are all provisioned with the same settings as follows:



☑ Group: Default Group | Connectivity ☐ Inherited ?

Interface

☑ Port 1
☑ Local mesh

● No VLAN
○ VLAN ID: 0

Assign IP address via

● DHCP client
○ Static

Static IP settings

IP address:
Mask:
Default gateway:

Local mesh settings

Connect to:
● Any mesh
○ A mesh with ID: 1

☐ Security: AES/CCMP
Key:
Confirm key:

Country

UNITED STATES

Local mesh radio configuration

Product	Radio	Wireless mode	Antenna selection
MSM310	Radio 1	802.11g	Diversity
MSM320	Radio 1	802.11g	Diversity
MSM422	Radio 1	802.11n (5 GHz)	External
MSM335	Radio 1	802.11g	External
MSM410	Radio 1	802.11a	Diversity

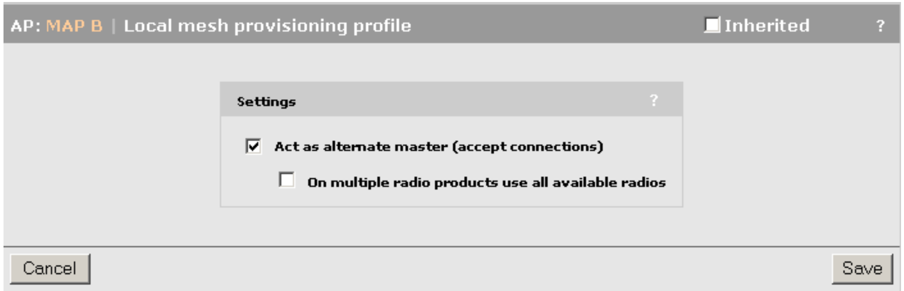
Use the Local mesh radio configuration table to define local mesh settings for each product type.

- **Product:** Indicates the product type.
- **Radio:** Select the radio that will be used for the local mesh.
- **Wireless mode:** Select the wireless mode that will be used for the local mesh.
- **Antenna selection:** Select the antenna(s) on which the radio transmits and receives.
  - **Internal:** The internal antenna is used to transmit and receive.
  - **External:** The external antenna is used to transmit and receive.

Note

All APs must all be configured for the same country so that the local mesh established respects local RF regulations. To define the country setting, see *Assigning country settings to a group on page 6-30*.

The local mesh provisioning profile for AP 2 needs to be set to alternate master mode so that it can support a connection from AP 1. Select AP 2 in the **Network Tree** and then open the **Configuration > Local mesh** page and select **Local mesh provisioning profile.**



AP: MAP B | Local mesh provisioning profile

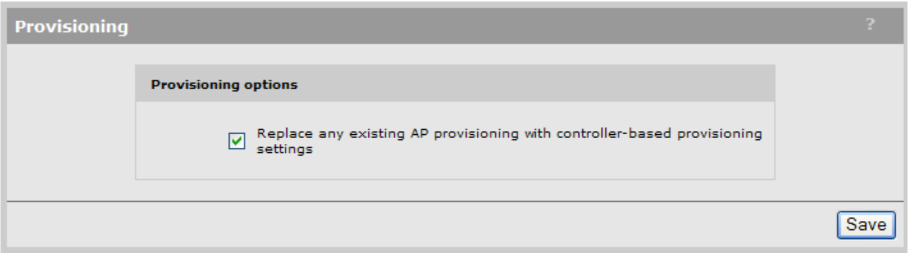
Settings

☑ Act as alternate master (accept connections)

□ On multiple radio products use all available radios

Note

To enable the controller to send provisioned settings to controlled APs, activate the **Enable provisioning of controlled APs** option on the **Controller >> Controlled APs > Provisioning** page.



Provisioning

Provisioning options

☑ Replace any existing AP provisioning with controller-based provisioning settings

Until this option is enabled, provisioned settings defined on the controller are not sent to any controlled APs.

Once provisioning settings have been defined you need to update all controlled APs with the new settings by synchronizing them as described in *Synchronizing APs on page 6-24*.

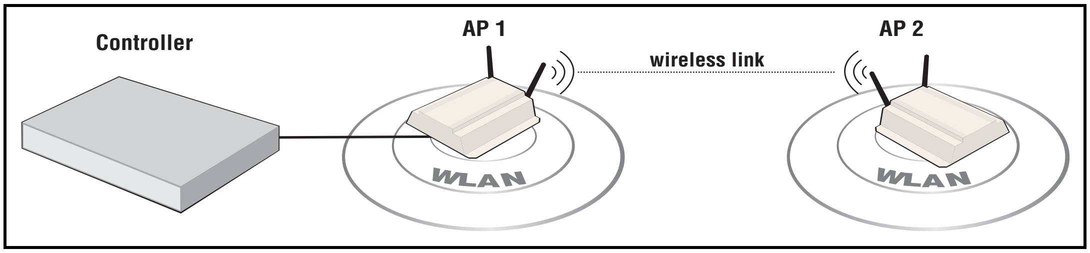
After an AP has been updated with provisioned settings, the provisioned settings do not become active until the AP is restarted, or a **Remove and rediscover** action is executed on the **Controlled APs >> Configured APs** page.

Sample local mesh deployments

RF extension

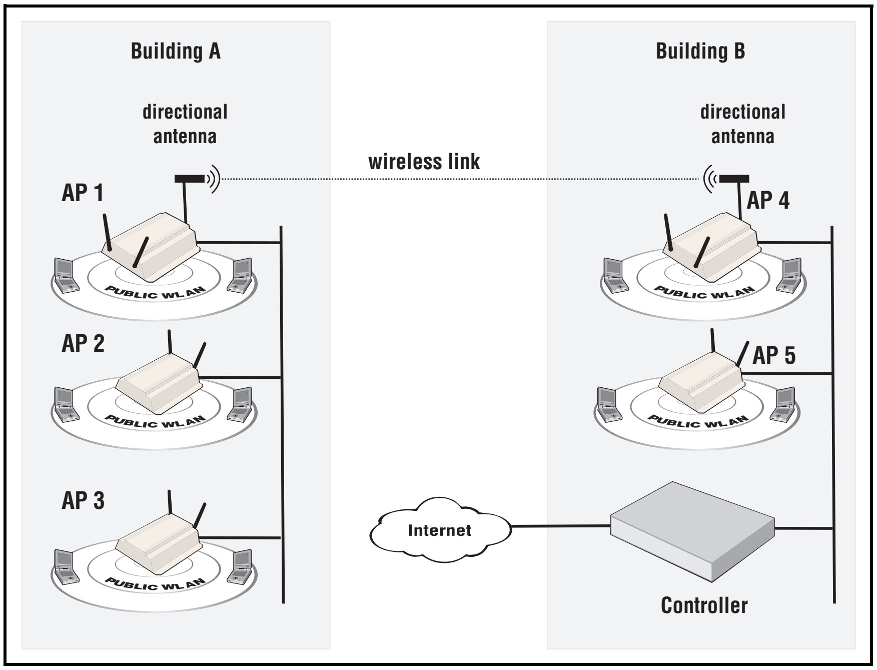
Local mesh provides an effective solution for extending wireless coverage in situations where it is impractical or expensive to run cabling to an AP.

In this scenario, a wireless bridge is used to extend coverage of the wireless network. Both APs are equipped with omni-directional antennas, enabling them to deliver both AP capabilities and wireless bridging using local mesh capabilities.



Building-to-building connection

You can also use local mesh to create point-to-point links over longer distances. in this scenario, two dual-radio APs create a wireless link between networks in two adjacent buildings. Each AP is equipped with a directional external antenna attached to radio 1 to provide the wireless link. Omnidirectional antennas are installed on radio 2 to provide AP capabilities. The two APs are placed within line of sight.



Note

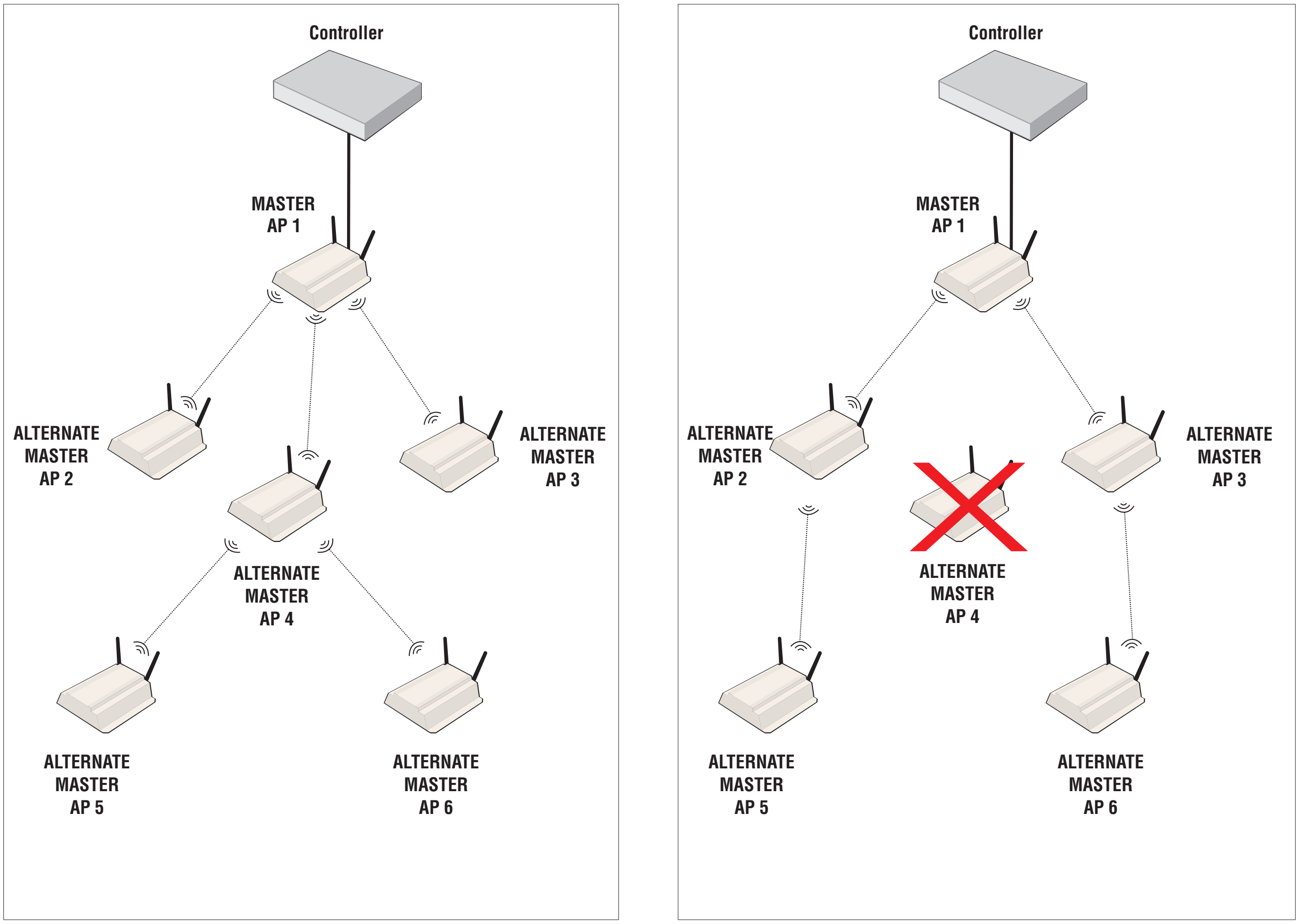
In the above example, all APs must connect to the backbone network via port 1.

Dynamic network

In this scenario, a controller is deployed with several APs to provide wireless coverage of a large area. Instead of using a backbone LAN, wireless links are used to interconnect all APs.

AP 1 is the *master*. It provides the connection to the wired network and a wireless link to the other APs. The other APs automatically established their links to the master based on a balance between SNR (signal to noise ratio) and hops, to provide the most efficient network topology.

If a node becomes unavailable, the links dynamically adjust to find the optimum path to the master.



Initial network configuration is automatically established.

When AP 4 is unavailable, the network dynamically reconfigures itself.

14

Public/guest network access

Contents

Introduction

The *Public/Guest Network Access* feature enables you to provide controlled network access for a variety of deployments. Some common applications of this feature are:

- Providing Internet access to wireless customers in airports, restaurants, train stations, conference halls, etc.
- Providing wireless and wired access to staff and guests in hospitals, corporations, and government buildings.
- Providing wireless and wired access to students, staff, and teachers in schools and universities.
- Providing outdoor wireless access for an entire town, enabling city workers, police, fire, public security, and the general public to connect.

This chapter provides describes the public/guest network access feature and how it can be used. For detailed information on the RADIUS attributes that can be used to customize the public access interface, see *Chapter 15: Working with RADIUS attributes on page 15-1*.

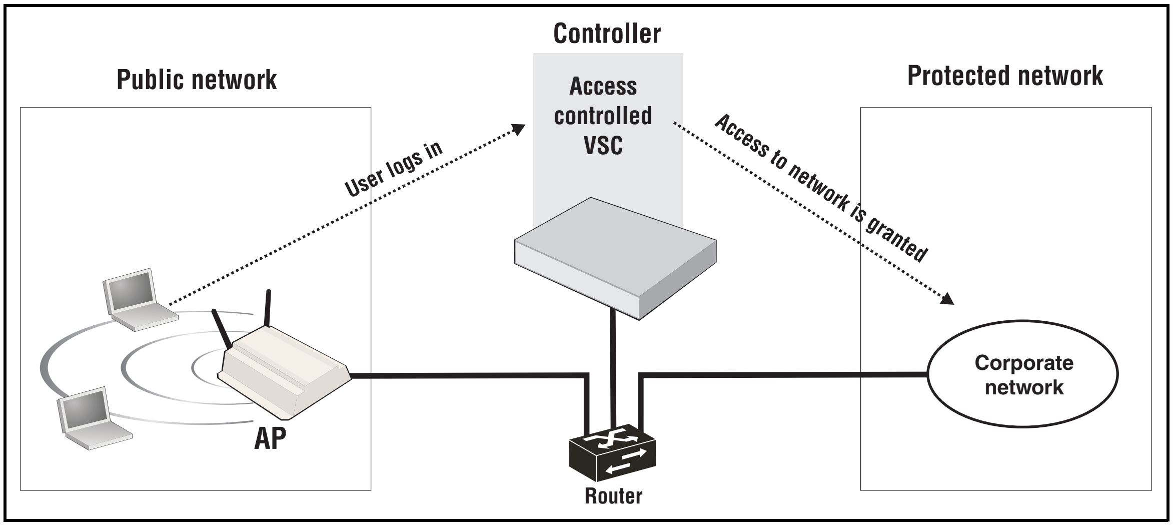
Key concepts

Access control

When the **Access control** option is enabled on a VSC, it creates an **access-controlled VSC**. This means that for all traffic on the VSC, the controller acts as the gatekeeper between two distinct network segments: the *public network* and the *protected network.*

- **Public network:** Access to the public network and its resources is generally made available to all unauthenticated wireless users once they successfully connect to the wireless network. Access is also generally made available to unauthenticated wired users on any network that is connected to the controller's LAN port.
- **Protected network:** Access to the protected network is restricted by the controller and typically requires that users be authenticated by the controller before they gain access. Various authentication methods are available (HTML-based, MAC-based, 802.1X). The most commonly used method is HTML-based, which enables users to login through their Web browsers via the public access interface Login page. The controller can validate user login credentials using locally defined user accounts or by using the services of a third-party authentication server (RADIUS or Active Directory).

The following diagrams illustrates a basic setup in which a wireless user is authenticated by an access-controlled VSC and then gains access to a corporate network.



For more information on access control, see *Configuring global access control options on page 14-8*.

Note

If authentication is not enabled on a VSC, all users connected to the VSC can access the protected network.

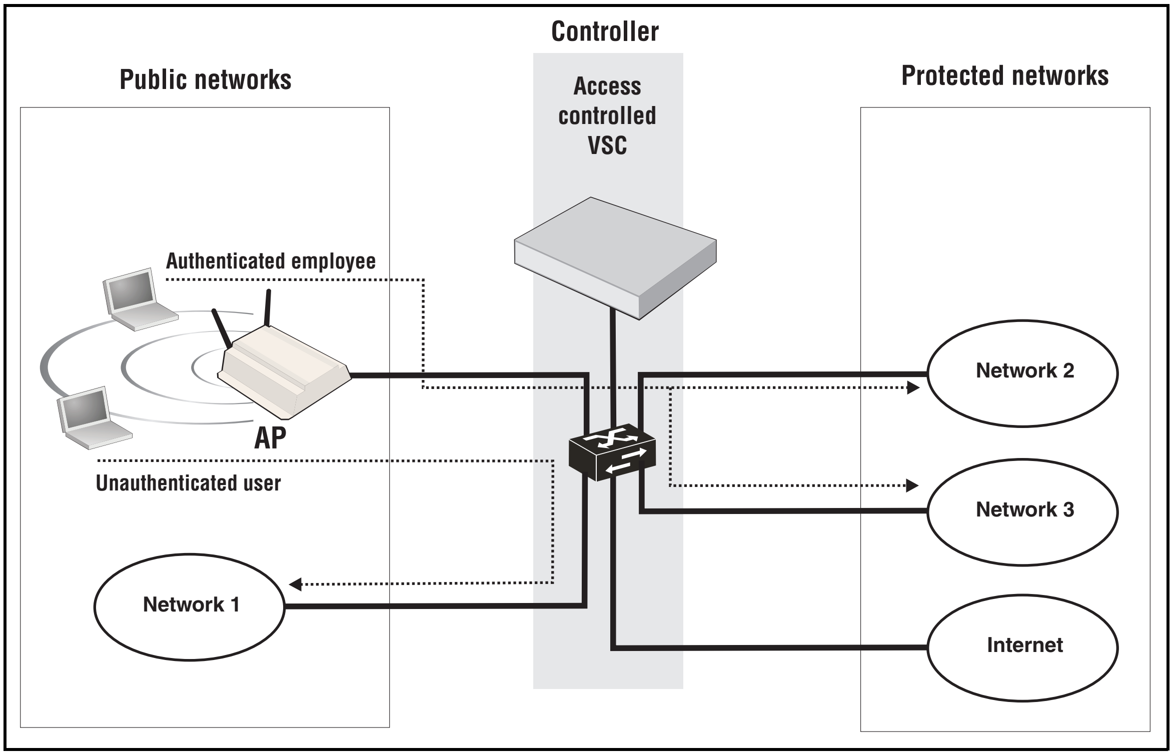
Access lists

An access list is a set of rules that governs how the controller manages access to the public and private network resources. You can create multiple access lists, each with multiple rules, enabling you to create public areas on your network that all users can browse, and protected areas that are restricted to specific user accounts or groups.

For more information, see *Access list on page 15-34*.

In the following example, access lists are defined to allow the following levels of access:

- Unauthenticated users can access Network 1.
- Authenticated employees can access Network 2 and the Internet.
- Authenticated guests can access the Network 3 and the Internet.

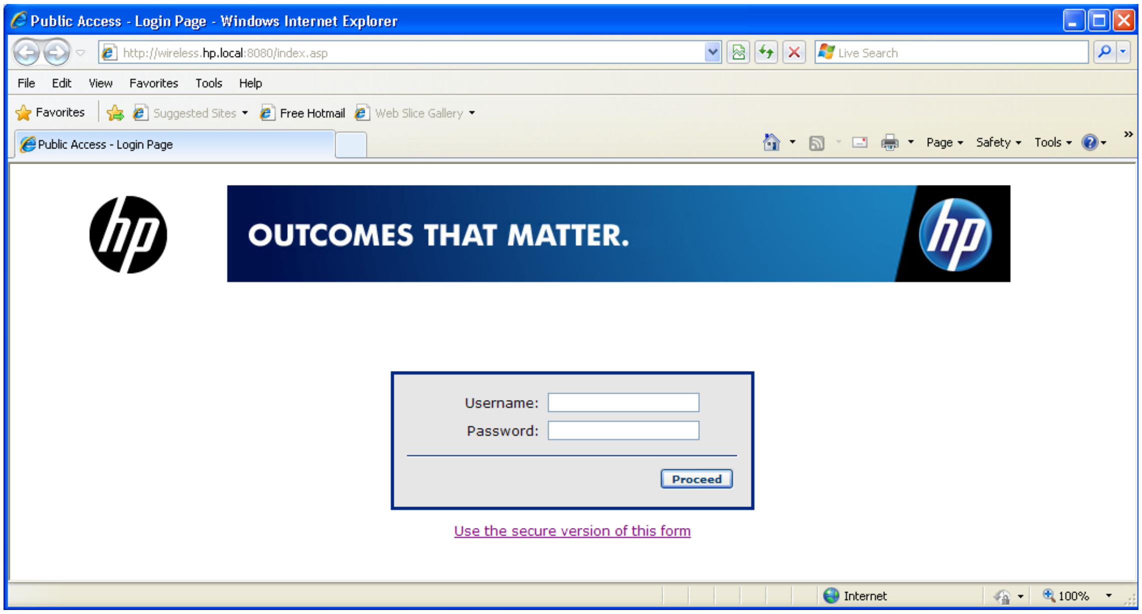


The public access interface

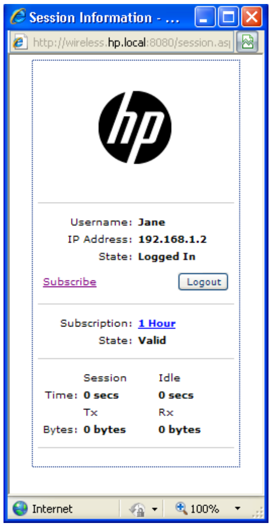
The *public access interface* is the sequence of Web pages through which access-controlled users can log in, log out, and view the status of their wireless connections to the public access network. By default, these Web pages are hosted on the controller's Web server. However, pages can also be hosted on external servers for added flexibility. The pages, error messages, images, and workflow are all customizable.

Standard pages are provided for common tasks such as login, service purchase, and display of session information. As well, advertisements can be displayed if required.

When a wireless user attempts to browse a Web site that is on the protected network, the user is redirected to the public access interface Login page. The following screen shot shows the default login page provided with the controller.


Public Access - Login Page - Windows Internet Explorer
http://wireless.hp.local:8080/index.asp
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
Public Access - Login Page
Page
Safety
Tools
OUTCOMES THAT MATTER.
Username:
Password:
Proceed
Use the secure version of this form
Internet
100%

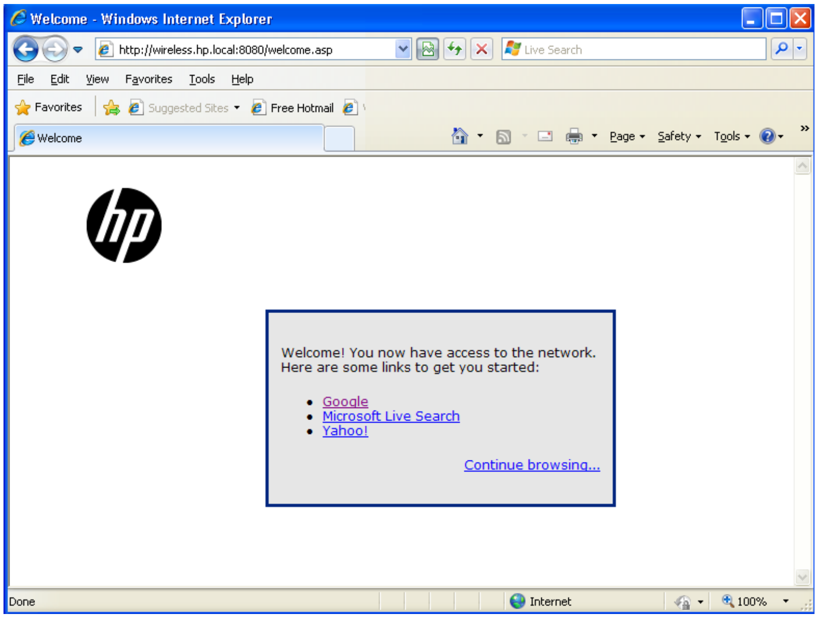
After the user successfully logs in, the session and welcome pages appear.


Session Information - ...
http://wireless.hp.local:8080/session.asp
Subscribe
Logout
Internet
100%

Username: **Jane**
IP Address: **192.168.1.2**
State: **Logged In**

Subscription: **1 Hour**
State: **Valid**

	Session	Idle
Time:	**0 secs**	**0 secs**
	Tx	Rx
Bytes:	**0 bytes**	**0 bytes**


Welcome - Windows Internet Explorer
http://wireless.hp.local:8080/welcome.asp
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Welcome
Page
Safety
Tools
Done
Internet
100%

Welcome! You now have access to the network.
Here are some links to get you started:

- Google
- Microsoft Live Search
- Yahoo!

Continue browsing...

The session page provides details on the user’s session, and a Logout button. The welcome page is the starting point for the user once logged in. You can customize this page to present important information about your network.

If the user selects **Continue browsing**, they are redirected to the original Web site that they were attempting to reach after they associated with the wireless network.

When done browsing, the user selects **Logout** on the session page to terminate their session.

For more information on the public access Web pages, see:

- *Public access interface control flow on page 14-13*
- *Customizing the public access interface on page 14-14*

Location-aware

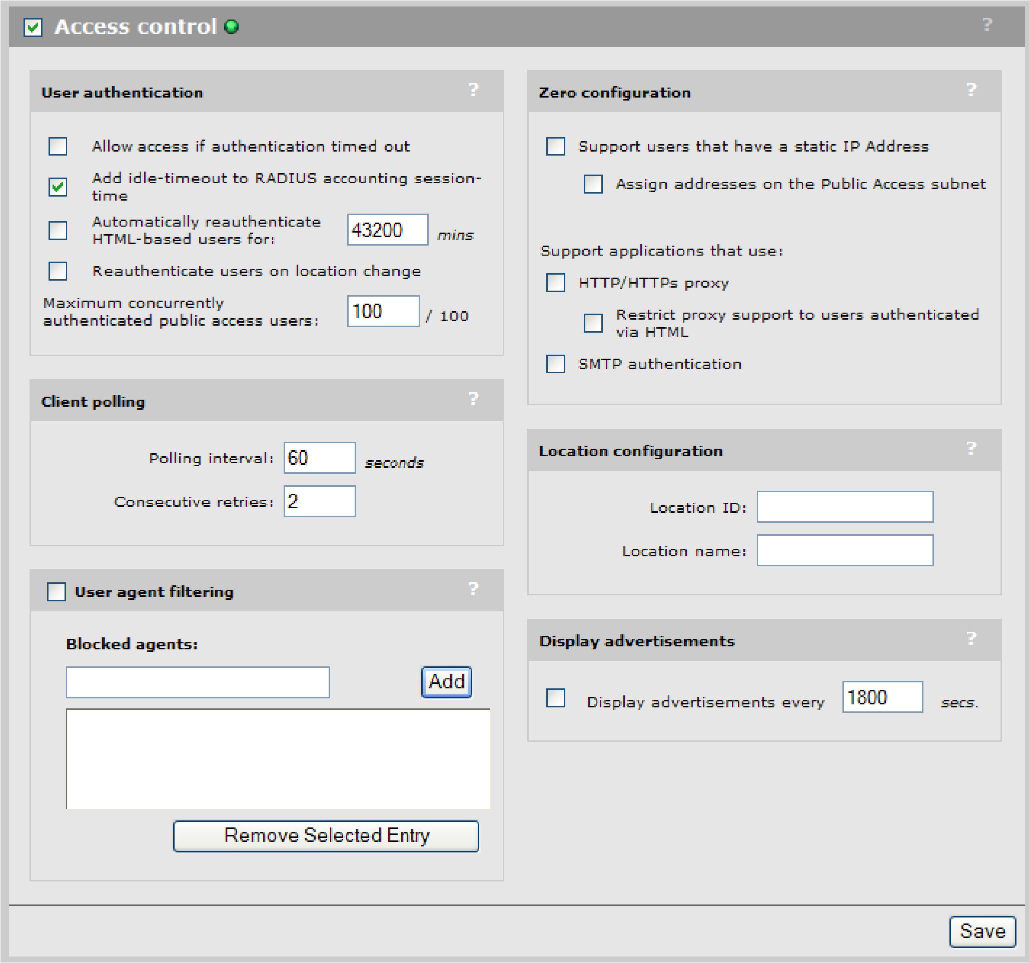
The location-aware feature enables you to control logins to the public access network based on the wireless AP to which a user is connected. It is configured on a per-VSC basis.

When enabled, the controller returns location-specific information for RADIUS-authenticated users. This information can be retrieved and processed by server side scripts to manage network access.

For more information, see *Location-aware authentication on page 14-48*.

Configuring global access control options

Global access control settings are managed by selecting **Controller >> Public access > access control**.



☑ Access control ●

User authentication

□ Allow access if authentication timed out

☑ Add idle-timeout to RADIUS accounting session-time

□ Automatically reauthenticate HTML-based users for: 43200 *mins*

□ Reauthenticate users on location change

Maximum concurrently authenticated public access users: 100 / 100

Client polling

Polling interval: 60 *seconds*

Consecutive retries: 2

□ **User agent filtering**

Blocked agents:

Zero configuration

□ Support users that have a static IP Address

□ Assign addresses on the Public Access subnet

Support applications that use:

□ HTTP/HTTPs proxy

□ Restrict proxy support to users authenticated via HTML

□ SMTP authentication

Location configuration

Location ID:

Location name:

Display advertisements

□ Display advertisements every 1800 *secs.*

The access control mechanism is used by the controller to manage user access to network resources. Access control is applied on a per-VSC basis. When the **Use Controller for Access control** option is enabled on a VSC, the configuration options on this page take effect with regards to client station configuration, authentication, and authorization.

Use the checkbox in the title bar to globally enable or disable the access control mechanism:

- When enabled, the controller provides access control functionality which can then be configured on a per-VSC basis.
- When disabled, the Public/Guest Network Access feature is disabled for all VSCs that are configured to use access control.

The status light indicates the state of the authentication system.

- **Green:** Access control is working and authentication requests can be processed.
- **Red:** Access control cannot process authentication requests at this time.

User authentication

Allow access if authentication timed out

Enable this option to give users free access to the protected network if authentication services configured for a VSC are unavailable. Once the authentication services are available again, free user sessions remain active until the user logs out.

For example, if a user is connected to a VSC configured for HTML-based authentication using a RADIUS server, and the RADIUS server is not responding, the user will be granted free access to the network using the settings from the default user profile (Default AC).

Note This feature does not work for users configured to use 802.1X or WPA when the encryption keys are provided by the RADIUS server.

Add idle-timeout to RADIUS accounting session-time

When enabled, the controller includes the idle time-out in the total session time for a user when the session is terminated due to idle time-out.

To remove the idle time-out from the total session time, disable this option.

Automatically reauthenticate HTML-based users for *nn* min

When this option is enabled, you can specify the amount of time that the controller will remember the login credentials for an HTML-based user after they log out. If the user reconnects to the network before this timeout expires, they are automatically logged in, and instead of being redirected to the Login page, they are redirected to the Welcome-back page.

For this feature to work, users must have successfully been logged in at least once via HTML and must have the same IP address and MAC address as their initial login when they return. Also, the session must have been terminated involuntarily. For example, by the user moving out of range, or their computer being restarted. If the user terminates their session, they will not be automatically reauthenticated.

To support this functionality, the DHCP server on the controller needs to be enabled. It will attempt to reserve a user’s assigned DCHP addresses even after their lease time has expired. As long as free addresses remain in the DHCP address pool, the expired address will not be reassigned to a new user.

Note

- The controller remembers login credentials even if the controller is restarted for administrative reasons.
- This feature may not work for users whose actual IP or MAC address is hidden by an intervening router or other network device.

Reauthenticate users on location change

When this option is enabled, the controller will automatically reauthenticate users when they switch to:

- a wireless cell with a different SSID
- a different VLAN ID on the same VSC
- an AP with a different MAC address
- an AP with a different group name
- a different wireless mode

Note This feature is only supported when using an external RADIUS server for authentication tasks.

Maximum concurrently authenticated public access users

Specify the maximum number of users that can be authenticated and logged into the public access interface at the same time.

Client polling

The controller polls authenticated client stations to ensure that they are active. If no response is received and the number of specified retries is reached, the client station is disconnected. To use this feature, client stations must have L2 connectivity to the controller.

This feature enables the controller to detect if two client stations are using the same IP address but have different MAC addresses. If this occurs, access is terminated for this IP address removing both stations from the network.

Changing these values may have security implications. A large interval provides a greater opportunity for a session to be hijacked.

The initial query is always done after the client station has been idle for 60 seconds. If there is no answer to this query, the settings for **Interval** and **Retries** are used to control additional retries.

Polling interval

Specify how long to wait between polls.

Consecutive retries

Specify how many consecutive polls to which a client station can fail to reply before it is disconnected.

User agent filtering

Enable this option to filter and stop redirection of HTTP login requests coming from unauthorized client applications. Filtering occurs via the user-agent string that web-based applications use to identify themselves to their peers.

Blocked agents

This is the list of user-agent strings that the controller will use to block client applications. If an application's user-agent string appears in this list, it will be blocked.

When the list is empty, all valid HTTP login requests are redirected.

For example, add the word **Torrent** to the list to stop HTTP login requests coming from the BitTorrent 6.3 client application.

A list of user agents strings can be found here:
http://www.useragentstring.com/pages/useragentstring.php

Zero configuration

Support users that have a static IP address

Enable this option to allow client stations with static IP addresses that are not on the same subnet as the controller to connect to the controller. This permits users to access the network without reconfiguring their network settings.

For example, by default the controller creates a network on the subnet 192.168.1.0. A client station that is preconfigured with the address 10.10.4.99 can connect to the controller without changing addresses.

Assign addresses on the Public Access subnet

Enable this option to provide network address translation for client stations with static IP addresses. This permits the controller to assign an alias address to the client station that puts it on the same subnet as the VSC the client station is associated with. This subnet is defined by configuring the DHCP server option in the VSC.

Note This option cannot be used if NAT is enabled on the Internet port.

Support applications that use

- **HTTP/HTTPS proxy:** Enable this option to allow the controller to support client stations that use application software (such as a web browser) configured to use a proxy server for HTTP and HTTPS, without reconfiguration of the application software.

  When this feature is enabled, ensure that client stations:

  - Do not use a proxy server on ports 21, 23, 25, 110, 443, 8080, or 8090. To support ports 8080 and 8090, change the port settings under **Controller >> Public access > Web server > Ports**.
  - Use the same proxy server address and port number for both HTTP and HTTPS.
  - **Restrict proxy support to users authenticated via HTML:** Enable this option to restrict proxy support to users who logged in via the public access login page. Proxy traffic from users authenticated via other methods is blocked.

- **SMTP authentication:** When the controller redirects user SMTP traffic, the server to which the traffic is redirected may need to authenticate the controller. Enable this option to allow the controller to supply a username and password to the server. You can define the username and password in the RADIUS account for the controller or for the user.

Location configuration

These values are returned to IPass clients, and are also sent in RADIUS Authentication Access Requests and Accounting Requests for all users authenticated by this controller.

Location ID
Specify the WISPr location ID assigned to the controller.

Location name
Specify the WISPr location name assigned to the controller.

Display advertisements

When this option is enabled, it causes users to be redirected to an ad content page while they are browsing.

The ads page can be either **ads.asp** or **ads-frameset.asp**, depending on the setting of **Use frames when presenting ads** under **Site options** on the **Public access > Web content** page.

Redirection occurs on TCP port 80.

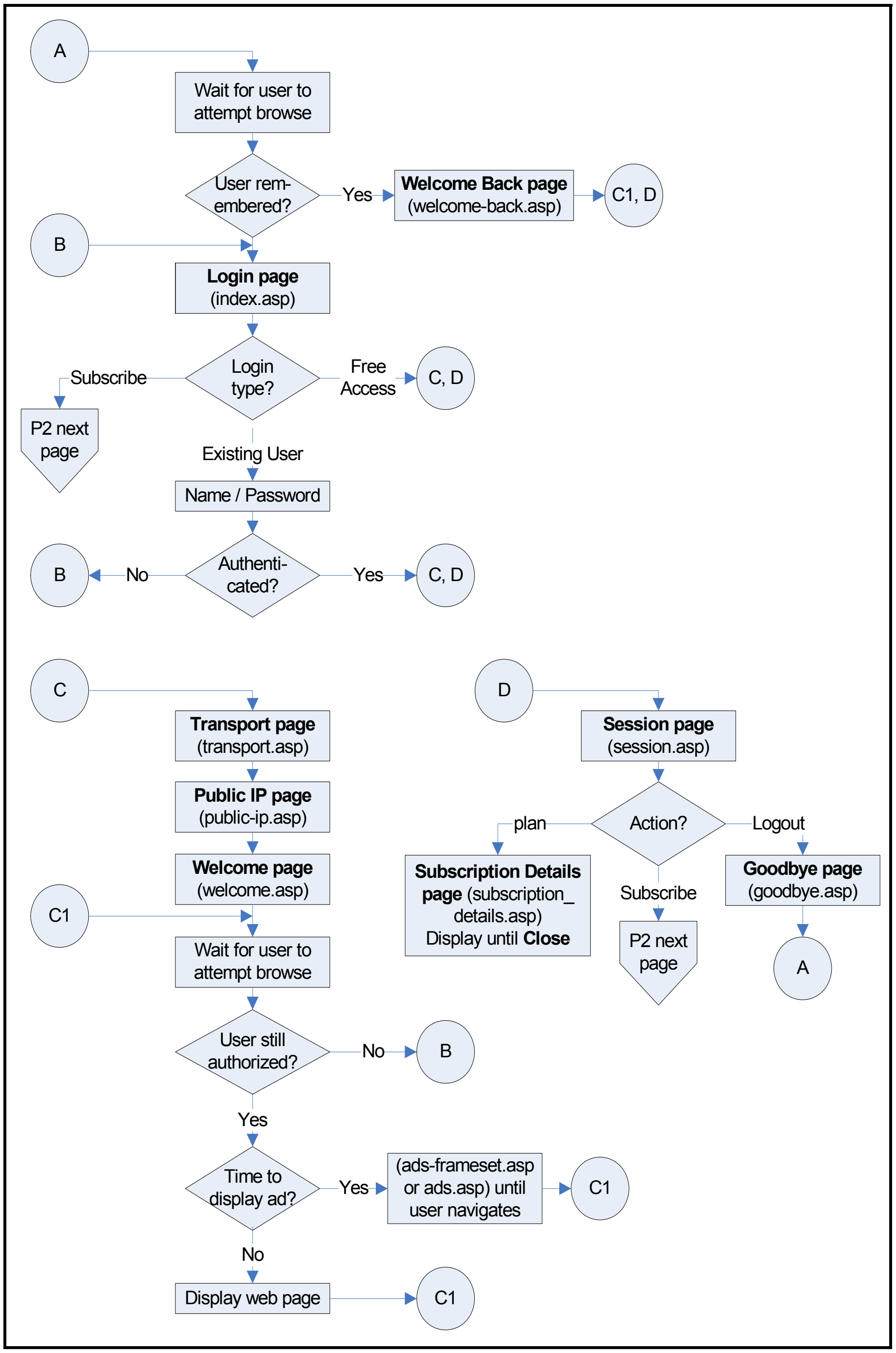
Display advertisements every *nnn* sec
Specify the interval at which users are redirected to the ads page.

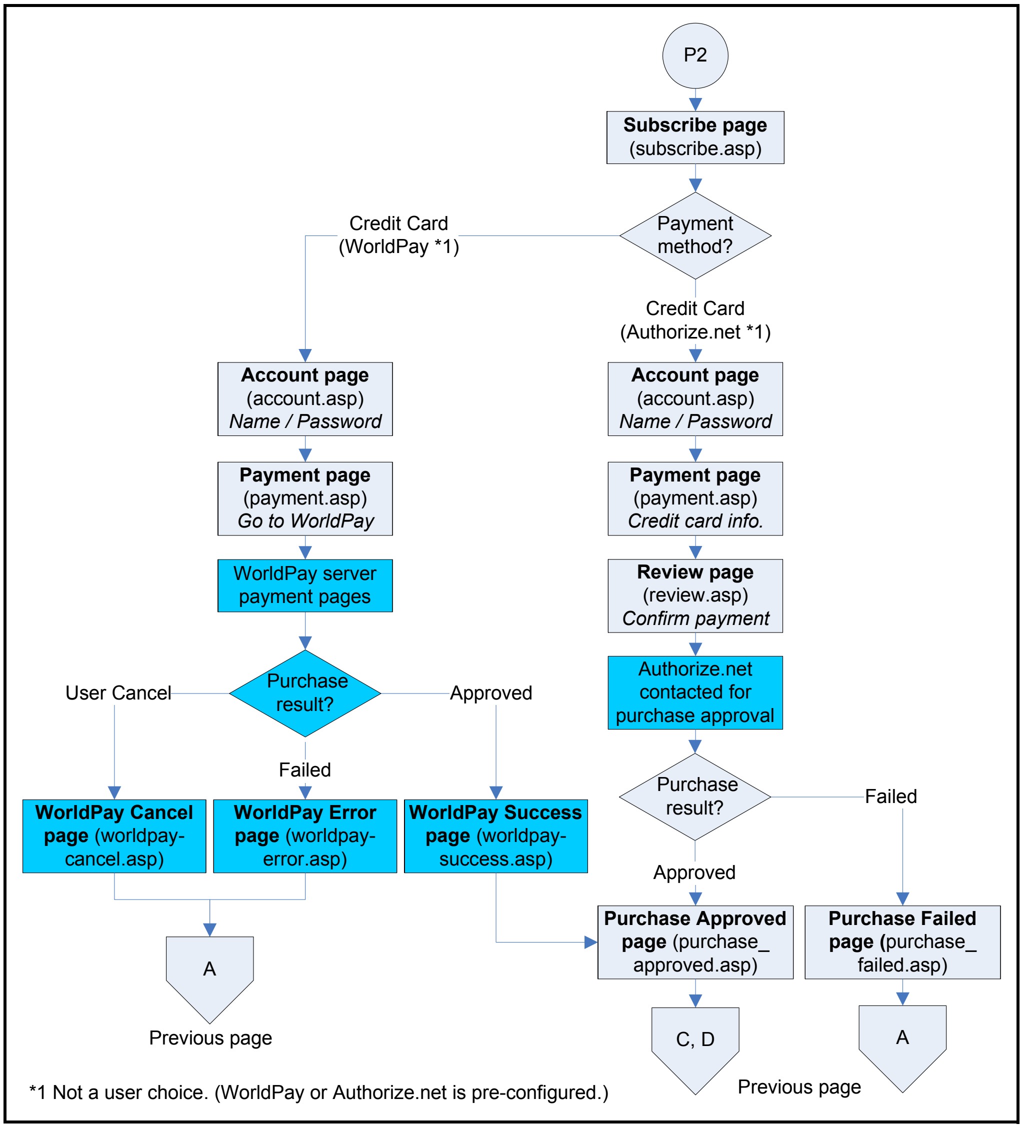
Note Once the **Display advertisements** option is enabled, advertisements are displayed for all users. You can selectively disable the display of advertising in user profiles (**Controller >> Users > Account profiles**), subscription plans (**Controller >> Users > Subscription plan**), or via attributes set in a user's RADIUS account.

Public access interface control flow

The two following diagrams provide an overview of the default public access interface Web page flow. All site Web pages are identified by their role: **Login**, **Welcome**, **Logout**, etc. This abstraction is used because the name of the actual page used for a particular role is configurable in many cases. (For reference, the page name used by the factory default configuration is provided in parenthesis.)

For a description of the individual pages, see *Current site files on page 14-25*.


A
Wait for user to attempt browse
User rem-embered?
Yes
Welcome Back page (welcome-back.asp)
C1, D
B
Login page (index.asp)
Subscribe
Login type?
Free Access
C, D
P2 next page
Existing User
Name / Password
B
No
Authenti-cated?
Yes
C, D
C
Transport page (transport.asp)
Public IP page (public-ip.asp)
Welcome page (welcome.asp)
C1
Wait for user to attempt browse
User still authorized?
No
B
Yes
Time to display ad?
Yes
(ads-frameset.asp or ads.asp) until user navigates
C1
No
Display web page
C1
D
Session page (session.asp)
plan
Action?
Logout
Subscription Details page (subscription_ details.asp) Display until Close
Subscribe
P2 next page
Goodbye page (goodbye.asp)
A


P2
Subscribe page (subscribe.asp)
Payment method?
Credit Card (WorldPay *1)
Credit Card (Authorize.net *1)
Account page (account.asp) Name / Password
Account page (account.asp) Name / Password
Payment page (payment.asp) Go to WorldPay
Payment page (payment.asp) Credit card info.
WorldPay server payment pages
Review page (review.asp) Confirm payment
Purchase result?
User Cancel
Approved
Failed
Authorize.net contacted for purchase approval
WorldPay Cancel page (worldpay-cancel.asp)
WorldPay Error page (worldpay-error.asp)
WorldPay Success page (worldpay-success.asp)
Purchase result?
Failed
Approved
Purchase Approved page (purchase_approved.asp)
Purchase Failed page (purchase_failed.asp)
A
Previous page
C, D
A
Previous page
*1 Not a user choice. (WorldPay or Authorize.net is pre-configured.)

Customizing the public access interface

The public access interface can be customized using the methods described below. You might use one or more of these methods, depending on the type of customization that you want to perform.

- **Setting site configuration options:** The site configuration options on the **Controller >> Public access > Web content** page can be used to quickly enable/disable certain public access features.

  See *Setting site configuration options on page 14-19*.

- **Customizing the public access interface Web pages:** The Web pages hosted on the controller internal Web server can be modified, allowing the entire public access interface to be customized. Simple modifications can be made with basic knowledge of HTML. Users with advanced HTML skills and knowledge of ASP and Javascript will be able to fully-customize all site operations.

  See *Customizing the public access Web pages on page 14-24*.

- **Setting public access attributes:** Configuration of a number of public access features can be accomplished by setting various RADIUS attributes. There categories of attributes are available:

  - **Site attributes:** These attributes are used to configure site-related options and global settings that apply to all user sessions. They can be defined in the RADIUS account for the controller or reside locally on the controller.

    See *Controller attributes overview on page 15-4*.

  - **User attributes:** These attributes are used to customize settings on a per-user basis. These attributes can reside locally on the controller or be retrieved from a third-party RADIUS server.

    See *Defining and retrieving user attributes on page 15-14*.

Sample public access pages

Some of the examples in this chapter make use of files contained in the Public Access Examples zip file. This file is available at www.hp.com/networking/public-access-examples.

Common configuration tasks

Customizing the login, welcome, or goodbye page

1. Select **Controller >> Public access > Web content.**
2. Under **Current site files**, select one of the following files:

Login page:	**index.asp**
Welcome page:	**welcome.asp**
Goodbye page:	**goodbye.asp**

3. The file will appear in the built-in text editor. Change the file to meet the requirements of your site.
4. Select **Save**.

Customizing the logo

1. Create a file called **logo.gif** that contains your logo (recommended size less than 20K).
2. Select **Controller >> Public access > Web content.**

3. Under **Current site files**, select the garbage can icon to the right of **logo.gif** to delete it.
4. Select **Add New File**.
5. For **Filename**, specify **logo.gif.**
6. Next to **Load content from file**, select **Browse**.
7. Select the **logo.gif** file that you created in Step 1.
8. Select **Load**.

Displaying custom welcome and goodbye pages

This example shows how to display unique welcome and goodbye pages for specific users or groups of users. This example assumes that you are hosting the web pages are hosted on a remote server and that you are using a RADIUS server to authenticate users.

For this example, assume that you have two sets of users: basic and premium. To distinguish the two groups, you have set up the user accounts on the RADIUS server accordingly. (Perhaps you are using access lists to restrict each group to a different section of the public network as described in *Access list example on page 15-40*).

1. Retrieve the Public Access Examples zip file at www.hp.com/networking/public-access-examples.
2. Create the following two folders on your Web sever: **basic** and **premium**.
3. Copy the files **welcome.html** and **goodbye.html** from the Examples zip file into both the **basic** and **premium** folders on the web server.
4. Edit the pages to present customized welcome and goodbye content for each set of users.
5. Add the following entry to the RADIUS profile for the basic users:

   ```
   welcome-url=web_server_URL/basic/welcome.html
   goodbye-url=web_server_URL/basic/goodbye.html
   ```

6. Add the following entry to the RADIUS profile for the premium users:

   ```
   welcome-url=web_server_URL/premium/welcome.html
   goodbye-url=web_server_URL/premium/goodbye.html
   ```

7. Add the following entry to the RADIUS profile for the controller. This gives all unauthenticated users access to the Web server hosting the goodbye page.

   ```
   access-
   list=loginserver,ACCEPT,tcp,web_server_IP_address,port_number
   ```

Delivering dynamically generated content

Another way to generate custom pages is to add placeholders in the URLs for the custom external pages and then use server-side scripting to dynamically create the pages. This method provides a powerful mechanism to automatically generate completely customized pages on a per-user basis. Rather than designing one or more static pages, as in the previous example, the custom pages in this example can be built on-the-fly based on user preferences stored in a central database, or based on a user's location within the network.

For example, if you want to generate a custom welcome page for each user:

1. Add the following entry to the RADIUS profile for the controller.

   ```
   welcome-url=web_server_URL/custom/
   welcome.html?loginname=%u&IPaddress=%i
   ```

2. Create a server-side script to retrieve the user's login name (%u) and the controller IP address or domain name (%u). The script can use this information to then display a custom page based on user's preferences (stored in the server database) and the user's location within the wireless network.

Supporting PDAs

Users using PDAs that only support a single browser window will have difficulty using the public access interface in its standard configuration.

Once a user logs in to the public access interface, two Web pages are sent to their browser: the Welcome page and the Session page.

The Session page contains a logout button. Users who are unable to view this page will not be able to log out.

To solve the problem, modify the Welcome page to include a logout button.

1. Create a folder called **PDAusers** on your Web sever.
2. See *Sample public access pages on page 14-15*. Copy public access sample files **welcome.html** and **goodbye.html** into the **PDAusers** folder.
3. Edit **welcome.html** to include a logout link with the target:

   ```
   http://controller_name:port/goform/HtmlLogout.
   ```

   For example:

   ```
   http://wireless.mycompany.com:8080/goform/HtmlLogout.
   ```

   Adds a warning to this page that tells PDA users to bookmark the Welcome page so that they can logout.

4. Add the following entry to the RADIUS profile for all PDA users:

   ```
   welcome-url=web_server_URL/PDAusers/welcome.html
   ```

Customizing error messages

To customize the error messages, edit the appropriate messages in the files listed in the following table, using the **Controller >> Public access > Web content** page**.**

If an error occurs on	Messages are taken from
Login page (index.asp)	login_error_message.asp
Subscription page (subscribe.asp), Account page (account.asp), Payment page (payment.asp), Review page (review.asp), Purchase failed page (purchase_failed.asp)	subscription_error_message.asp
Other pages	Messages.txt

Logout host name
Logout IP address

These two options enable easy logout from the public access network. Users can logout by pointing their browsers to a specific host name or its IP address.

Host names must be fully-qualified, which means they must include the domain name suffix (**.suffix**). For example: **mydomain.com** is fully qualified, **mydomain** is not.

If a user that is logged in via HTML sends an HTTP request to the specified host name or IP address, the controller will log the user out.

To use this option you must define an access list with the DNAT option. For example, if the controller's LAN port is at **192.168.1.1** and you want to logout users when they access **network.logout** (which has an IP address of 10.10.1.1) you would define the following:

Logout host name = network.logout
Logout IP address = 10.10.1.1

On the **Controller >> Public access > Attributes** page, add the following attributes under **Configured attributes**:

dnat-server = logout, 192.168.1.1, 8081

> *The DNAT-SERVER has to point to the* controller*'s LAN port on TCP port 8081. This is where the logout service is located on the controller.*

access-list = logout,DNAT-SERVER,tcp,10.10.1.1,80

> *Indicates that TCP traffic on port 80 that is addressed to 10.10.1.1 will be forwarded to the DNAT-SERVER (192.168.1.1).*

use-access-list=logout

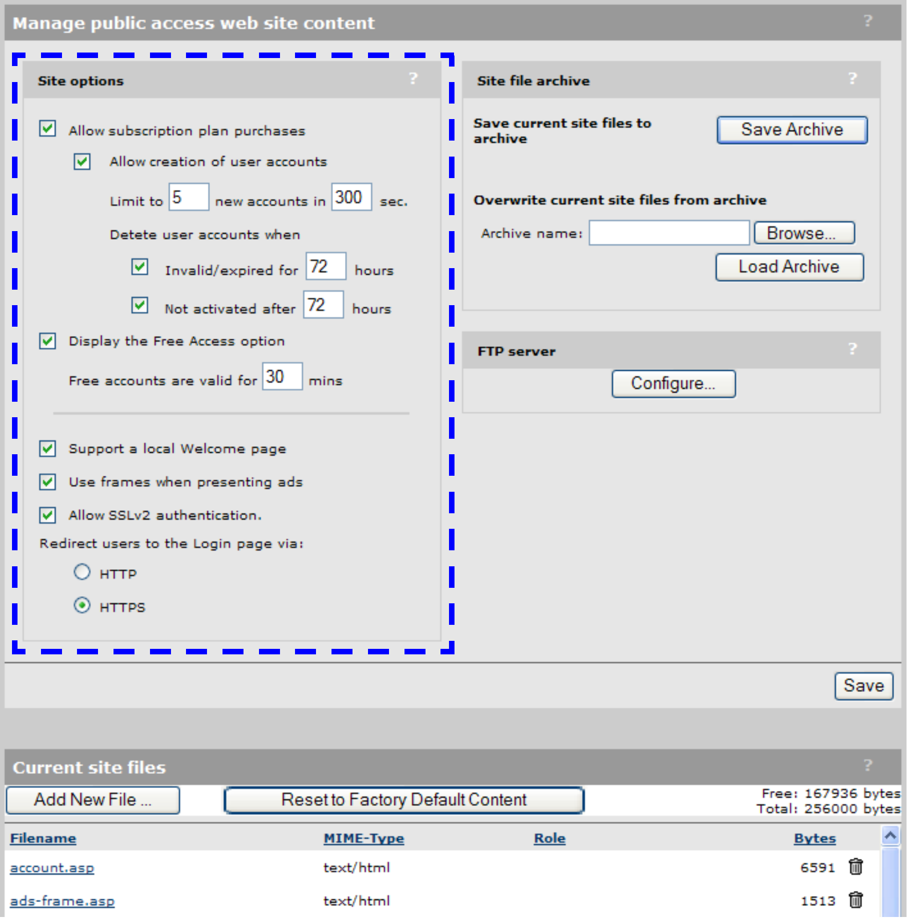
> *Activates the access list for all user's on the controller.*

How it works

1. When a user enters **http://network.logout** in their browser, the controller resolves it to to **10.10.1.1**.
2. The controller then intercepts any TCP traffic destined for 10.10.1.1 on port 80 and redirects it to 192.168.1.1 on port 8081.
3. The logout service running on controller port 8081 then logs the user out.

Setting site configuration options

To view, edit, and manage site options, select **Controller >> Public access > Web content** and configure the settings under **Site options**.



Site options

☑ Allow subscription plan purchases

☑ Allow creation of user accounts

Limit to 5 new accounts in 300 sec.

Detete user accounts when

☑ Invalid/expired for 72 hours

☑ Not activated after 72 hours

☑ Display the Free Access option

Free accounts are valid for 30 mins

☑ Support a local Welcome page

☑ Use frames when presenting ads

☑ Allow SSLv2 authentication.

Redirect users to the Login page via:

○ HTTP

● HTTPS

Save current site files to archive

Overwrite current site files from archive

Archive name:

Free: 167936 bytes
Total: 256000 bytes

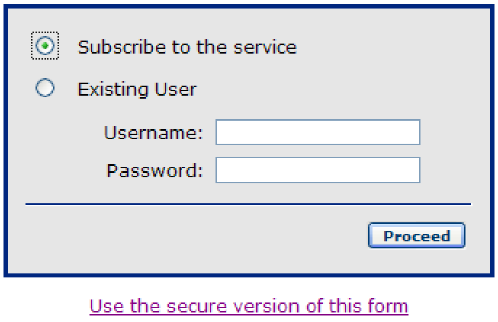
Filename	MIME-Type	Role	Bytes
account.asp	text/html		6591
ads-frame.asp	text/html		1513

About ASP variables

A number of ASP variables are defined for use by the public access interface pages. These variables are used to make configuration and status information available via ASP function calls, allowing for customization of the Web pages. Some of the site configuration options set the values of these variables. See *Public access interface ASP functions and variables on page 15-75*.

Allow subscription plan purchases

When enabled, the **Subscribe to this service** option is displayed on the default Login page (index.asp).



● Subscribe to the service

○ Existing User

Username:

Password:

This option provides a link to the default Subscription page (subscribe.asp), where users can choose one of the subscription plans defined on the **Controller >> Users > Subscription plans** page. Existing users must enter their username and password to update their current account. New users enter a username and password to create a new account.

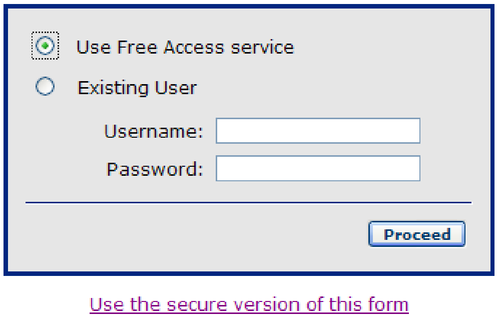
Pre-requisites

To use this feature, the following items must be pre-configured:

- One or more subscription plans must be defined by selecting **Controller >> Users > Subscription plans**.
- To support *credit card* payments, the credit card payment service must be enabled and configured by selecting **Controller >> Public access > Payment services**.

Display the Free Access option

When enabled, the Free Access option is displayed on the default Login page (index.asp). This enables users to login to the public access interface without paying.



● Use Free Access service

○ Existing User

Username:

Password:

A user account is automatically created for each user that selects the Free Access option. Each account has the following properties:

- The account name and password are set to the MAC address of the user's device.
- The account is valid for up to 30 minutes from the time it is created. To change this time use the **Free accounts are valid for *nn* minutes** option. When a Free Access account expires, the user can choose Free Access again and continue browsing.
- Account settings are imported from the **Default AC** profile. See *About the Default AC profile on page 10-27*.

Free accounts are valid for *nn* minutes

Specify how many minutes a free account is valid, starting from the time the user logs in with the Free Access option.

Support a local Welcome page

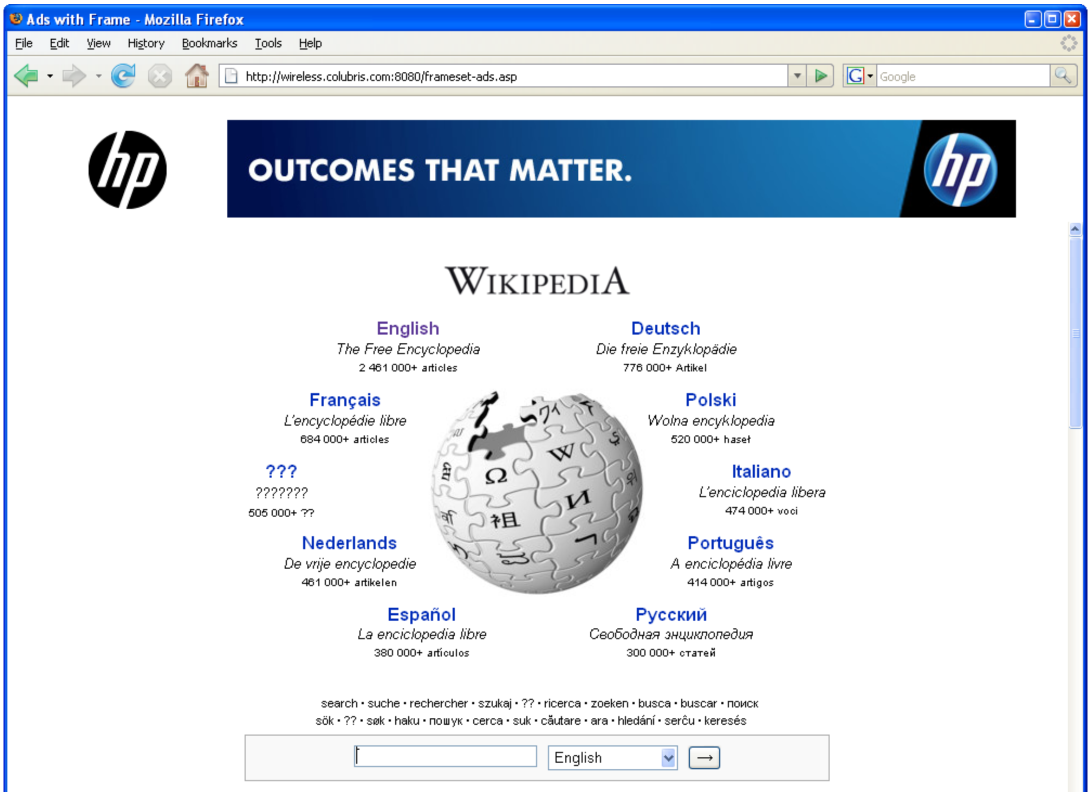
Use this feature to host the Welcome page on the controller Web server.

- When enabled, users are redirected to **welcome.asp** on the controller Web server.
- When disabled, you can use the welcome-url attribute (see *Default user URLs on page 15-55*) to define a remotely hosted welcome page.

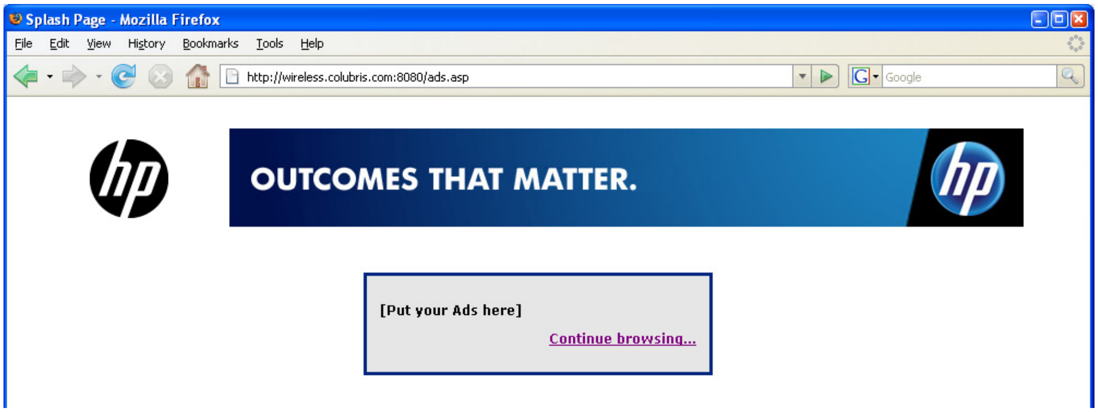
Use frames when presenting ads

This option controls how advertising is displayed:

- When this option is enabled, the logo and advertisement displayed in a frame at the top of the page.



- When this option is disabled, the logo and advertisement are displayed on a separate page. The user selects **Continue browsing** to return to the page they were viewing.


Splash Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://wireless.colubris.com:8080/ads.asp
Google
OUTCOMES THAT MATTER.

[Put your Ads here]

Continue browsing...

For more information on how advertising works, see *Display advertisements on page 14-12*.

Allow SSLv2 authentication

Enable this option to support client stations that use SSL v2 for their HTTPS connections. When disabled, the controller only supports client stations that are using SSL v3 for HTTPS connections. SSL v2 clients are refused.

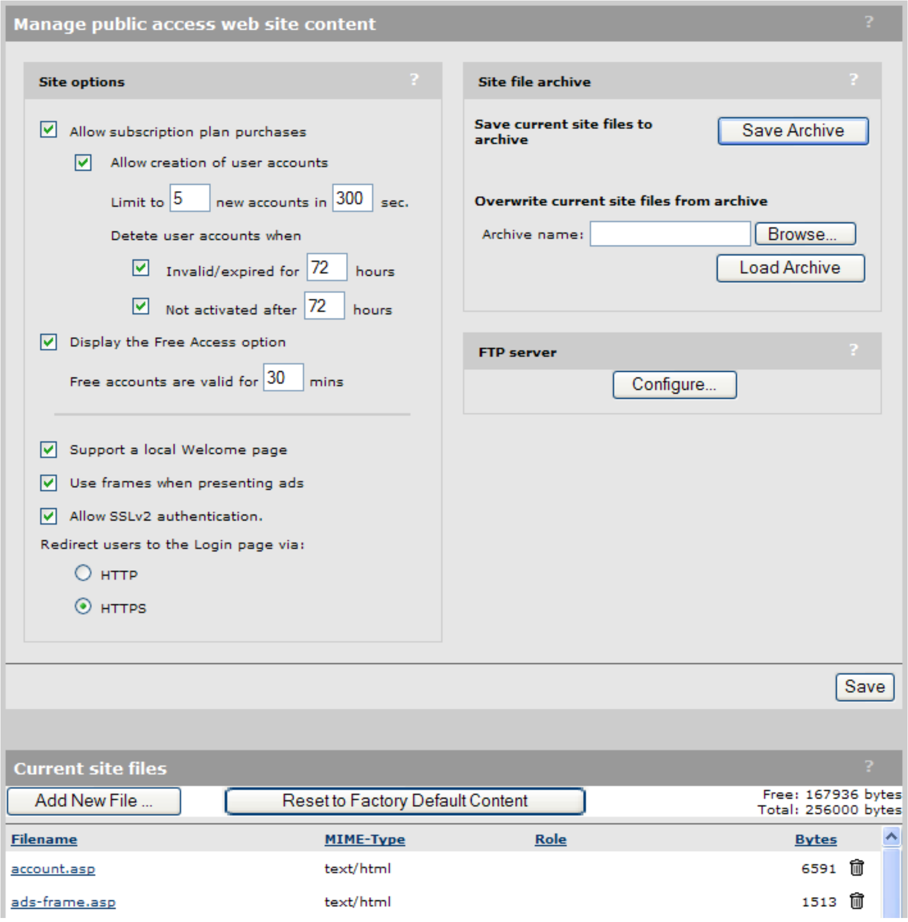
Redirect users to the Login page via

Select the protocol that will be used when redirecting users to the default Login page (index.asp).

- **HTTP:** This option does not provide any encryption for protecting user login credentials.
- **HTTPS:** Provides a secure connection to protect user login credentials. However, until the default SSL certificate that is installed on the controller is replaced with a certificate signed by a well-known certificate authority, users will see a certificate warning message each time they attempt to log in. See *Working with certificates on page 12-5* for more information on replacing the SSL certificate.

Customizing the public access Web pages

To view, edit, and customize the public access interface Web pages, select **Controller >> Public access > Web content**.



Manage public access web site content

Site options

☑ Allow subscription plan purchases

☑ Allow creation of user accounts

Limit to 5 new accounts in 300 sec.

Detete user accounts when

☑ Invalid/expired for 72 hours

☑ Not activated after 72 hours

☑ Display the Free Access option

Free accounts are valid for 30 mins

☑ Support a local Welcome page

☑ Use frames when presenting ads

☑ Allow SSLv2 authentication.

Redirect users to the Login page via:

○ HTTP

● HTTPS

Site file archive

Save current site files to archive

Overwrite current site files from archive

Archive name:

FTP server

Current site files

Free: 167936 bytes
Total: 256000 bytes

Filename	MIME-Type	Role	Bytes
account.asp	text/html		6591
ads-frame.asp	text/html		1513

Site file archive

Use these options to manage the files on the Web server as a single archive file (zip format).

Save current site files to archive

Saves all the current site files to an archive file.

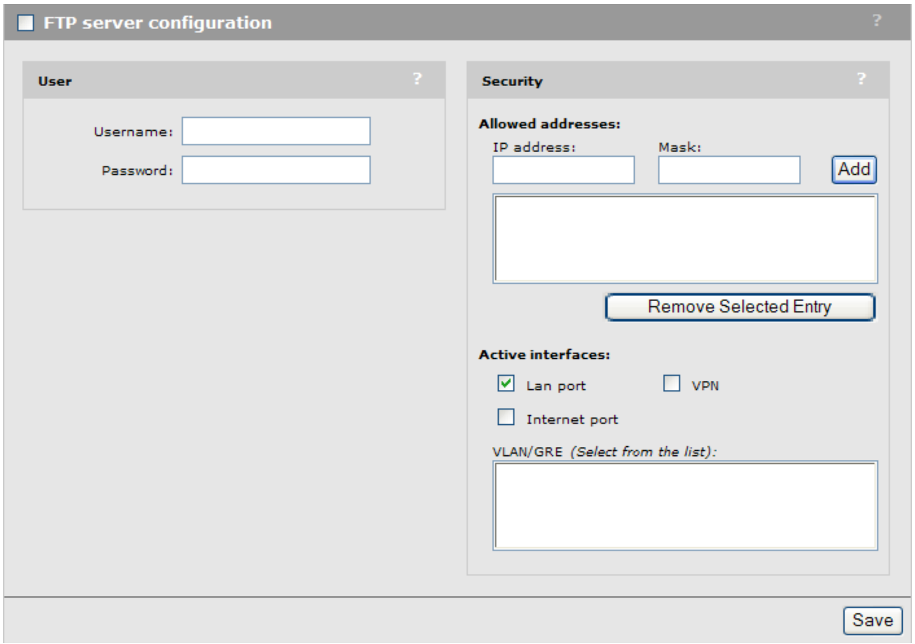
Overwrite current site files from archive

Select **Load Archive** to load all the site files from an archive, overwriting the currently installed site files.

FTP server

The FTP server provides an easy way to manage the public access interface files on the Web server, allowing you to use third-party Web site editing tools to customize content.

Select **Configure** to its define operational settings.



□ FTP server configuration

User

Username:

Password:

Security

Allowed addresses:

IP address: Mask:

Active interfaces:

☑ Lan port □ VPN

□ Internet port

VLAN/GRE *(Select from the list)*:

Note For security reasons you should disable the FTP server once the controller is deployed. Or at minimum, define security filters to restrict FTP access.

User

Specify the username and password that will be required when connecting to the FTP server.

Note When using FTP, the username and password are not encrypted. They are sent as clear text.

Security

Allowed addresses

Enables you to define a list of IP address from which to permit access to the FTP server. To add an entry, specify the IP address and appropriate mask and select **Add**.

When the list is empty, access is permitted from any IP address.

Active interfaces

Select the interfaces through which client stations can access the FTP server.

To select multiple entries, hold down the shift or control key as you select each entry.

Current site files

These are the files that are currently installed on the Web server and make up the public access interface. You can edit and create text files using the built-in editor. Other files must be created offline and uploaded via FTP.

For an overview of the default site structure and control flow, see *Public access interface control flow on page 14-13*.

Add New File

Select this button to create a new text-based file on the server.

Reset to Factory Default Content

Select this button to reset the site files to factory default content. You should make a backup copy of the current content using the **Site file archive** options before restoring factory defaults.

About ASP variables

A number of ASP variables are defined for use by the public access interface pages. These variables are used to make configuration and status information available via ASP function calls, allowing for customization of Web page content. Some of the site configuration options set the values of these variables. See *Public access interface ASP functions and variables on page 15-75*.

Site file descriptions

account.asp

text/html

This page is launched by **subscribe.asp** when the user selects **Next**. It displays a summary of the subscription plan that was chosen and prompts for a username and password to create a new user account.

- Selecting **Cancel** launches **index.asp**.
- Selecting **Next** launches **payment.asp**.

ads-frame.asp

text/html

This file contains the frame content for ads when using **ads-frameset.asp**.

ads-frameset.asp

text/html

Page that is used to display advertisements using frames. Users see the ad in a frame and their original Web site in second frame.

Users can select the **Continue Browsing** button to return to their original Web page, or continue browsing within the frame.

ads.asp

text/html

Page that is used to display advertisements without frames. Users are redirected to this page while browsing and must select the **Continue Browsing** button to return to their original Web page.

ads.jpg

image/jpeg

This is the default advertisement that is displayed.

fail.asp

text/html

This is a generic error reporting page that is called by various other pages to present an error message.

goodbye.asp

text/html

When a user logs out (by selecting the **Logout** button on the **session.asp** page, for example), if no **goodbye-url** attribute is defined (which specifies the location of a goodbye page), the user is redirected to this page. If this page is missing, than **fail.asp** is presented.

graceful_ending.js

application/javascript

Provides a graceful ending to subscription plans that are about to expire. When a subscription plan has only 10 minutes left or reaches 80% of its transfer quota (these limits are configurable in this script), a warning appears encouraging the user to purchase another plan before their existing one expires.

index.asp

text/html

This is the Login page that users see when they are first redirected to the public access interface.

The Login page contains a single graphic element suitable for a logo or other identifying element and two fields (username and password) that enable users with an existing account to log in. Additional choices may be visible on the Login page if the following features are enabled on the **Controller >> Public access > Web conten**t page under **Site options:**

- Allow subscription plan purchases
- Display the Free Access option.

login_error_message.asp

text/html

Error messages and the code that is used to display them. Used by **index.asp**.

logo.gif

image/gif

Re-usable image shared by a number of pages.

payment.asp

text/html

This page is called by **account.asp** when a user selects **Next**.

It displays a summary of the user's subscription selection.

For the Authorize.Net payment service

- Credit card information is requested.
- Selecting **Review**, launches **review.asp.**
- Errors in payment information cause this page to be redisplayed.
- Selecting **Cancel** returns the user to the Login page (index.asp).

For the WorldPay payment service

- Selecting **Go to WorldPay** launches the payment processing page on the WorldPay site.
- Selecting **Cancel** returns the user to the Login page (index.asp).

See *WorldPay-cancel.asp/ WorldPay-error.asp/ WorldPay-success.asp on page 14-32*.

For the PayPal payment service

- Selecting **Checkout with PayPal** redirects the user to the PayPal site.
- Selecting **Cancel** returns the user to the Login page (index.asp).

See *paypal-cancel.asp on page 14-28*, *paypal-return.asp on page 14-28*, and *paypal_error.asp on page 14-28*.

paypal-cancel.asp

The user is redirected to this page if they cancel the PayPal transaction when on the PayPal site or on **paypal-return.asp**.

paypal-return.asp

Once a user has completed setting up payment details on the PayPal site, the PayPal server redirects the user to this page which then displays a summary of the transaction.

- Selecting **Confirm** finalizes the transaction. A request is sent to PayPal, and if approved, the user is redirected to **purchase_approved.asp**. If not approved, the user is sent to **paypal-error.asp**.
- Selecting **Cancel** redirects the user to **paypal-cancel.asp**.

paypal_error.asp

In the case where PayPal detects any error, the user is redirected to this page and PayPal error messages are displayed. Error messages are defined by PayPal here:

https://cms.paypal.com/us/cgi-bin/?cmd=_render-content&content_ID=developer/e_howto_api_nvp_errorcodes

prototype.js

application/javascript

Javascript library used to support AJAX for use in **session_ajax.asp** and **subscription_details.asp**.

public-ip.asp

text/html

Message page that is displayed explaining the steps a user must follow to activate a public IP address. This page is only displayed if a public IP address is assigned in the user's account or account profile. See *Public IP address on page 3-10*.

purchase_approved.asp

text/html

This page is displayed as soon as payment is approved. The user selects **Login** on this page to open **welcome.asp**.

purchase_failed.asp

text/html

This page is displayed if payment fails.

redirect.asp

text/html

This is the page that is sent when the controller intercepts a connection from a non-authenticated user. Its function is to redirect the browser to the Login page.

review.asp

text/html

This page is called by **payment.asp** and applies to Authorize.Net payments only.

It displays a summary of the user's subscription selections and presents a **Pay** button. Selecting **Pay** completes the Authorize.Net transaction. If the transaction is approved, **purchase_success.asp** page is called, otherwise, **purchase_failed.asp** is called.

session.asp

text/html

This page shows usage statistics for the session, as well as the logout button that the user selects to terminate the session.

session.js

application/javascript

Included by **session.asp.** Provides smart updates for Javascript-based browsers.

session_ajax.asp

text/html

This page is specially designed for AJAX, and provides a JSON page format for use by **session.js** to provide the same content as **session.asp** but for Javascript-enabled browsers. This enables smart refresh of the session data; only changed data is updated, not the entire page, eliminating screen flickering.

Session.asp includes **session.js** which calls **session_ajax.asp**.

sessionwindow.js

application/javascript

Contains Javascript functions used to control opening and closing of the session page.

setfocus.js

application/javascript

Contains Javascript functions used to set the focus to the first form on a page.

style.css

text/css

Stylesheet for all public access interface Web pages.

subscribe.asp

text/html

This page is called by **index.asp** and **session.asp** if **Allow subscription plan purchases** is enabled on the **Controller >> Public access > Web content** page under **Site options**.

The page displays all defined subscription plans so that the user can choose one.

The user can select **Next** to proceed to **account.asp**, or **Cancel** in which case they are redirected to **index.asp**.

subscription_details.asp

text/html

This page is called by **session.asp**. it provides information on the subscription plan selected by a user, as well as running totals for data transfer and online time.

subscription_details.js

application/javascript

Included by **subscription_details.asp**. Provides smart updates for Javascript-based browsers.

subscription_details_ajax.asp

text/html

Included by **subscription_details.asp**. Provides smart updates for Javascript-based browsers.

This page is specially designed for AJAX, and provides a JSON page format for use by **subscription_details.js** to provide the same content as subscription_details.asp but for Javascript-enabled browsers. This enables smart refresh of the data; only changed data is updated, not the entire page, eliminating screen flickering.

subscription_details.asp includes **subscription_details.js** which calls **subscription_details _ajax.asp**. Also, **session.asp** includes **gracefulending.js** which calls **subscription_details_ajax.asp**.

subscription_details_window.js

application/javascript

Included by **session.asp**. Contains Javascript functions used to control opening and closing of the subscription details page.

subscription_error_message.asp

text/html

Error messages and code to display them. Used by: **subscribe.asp**, **account.asp**, **payment.asp**, **review.asp**, and **purchase_failed.asp**.

transport.asp

text/html

This page appears briefly after the login is approved and redirects the user to the local or external welcome page.

utils.js

application/javascript

Contains Javascript utility functions used by various public access pages.

welcome-back.asp

text/html

If the **Automatically reauthenticate HTML-based users for *nnn* minutes** option is enabled on the **Controller >> Public access > Access control** page under **User authentication**, this page is displayed for returning users instead of the Login page (index.asp).

welcome.asp

text/html

This page is called after the login process is complete if **Support a local Welcome page** is enabled on the **Controller >> Public access > Web content** page under **Site options**.

WorldPay-cancel.asp/ WorldPay-error.asp/ WorldPay-success.asp

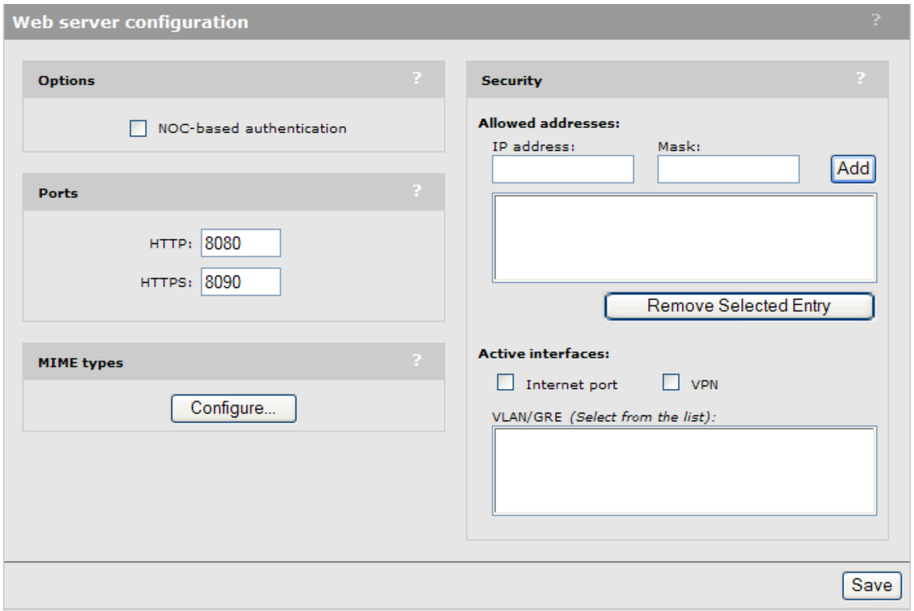
text/html

These pages are retrieved by the WorldPay service during the payment process. This means that the Web server must be accessible to the WorldPay server. Generally this is done by assigning a public IP address to the Internet port. Modifications to these pages must follow WorldPay guidelines.

Configuring the public access Web server

The controller features an integrated Web server that, by default, is used to host the Web pages that make up the public access interface. Public access Web pages can also be hosted on third-party Web servers.

Web server configuration settings are defined on the **Controller >> Public access > Web server** page.



Web server configuration

Options

□ NOC-based authentication

Ports

HTTP: 8080

HTTPS: 8090

MIME types

Security

Allowed addresses:

IP address:

Mask:

Active interfaces:

□ Internet port □ VPN

VLAN/GRE *(Select from the list)*:

Options

NOC-based authentication
Enable this option to support NOC-based authentication.

NOC-based authentication must be used in conjunction with the remote login page feature. The remote login page feature enables users to be redirected to a remote Web server to log in instead of using the internal login page on the controller.

To validate user logins, a login application on the remote server must collect user login information and send it to the controller for authentication.

See *NOC authentication on page 15-62* and *Appendix D: NOC authentication*.

Ports

Specify the port number the Web server uses for each protocol.

If you enable support for proxy settings under **Controller >> Public access > Access control > Zero configuration,** you must change the selected port to support client stations that are using proxy servers on the standard port (8080 or 8090). The following mappings are recommended:

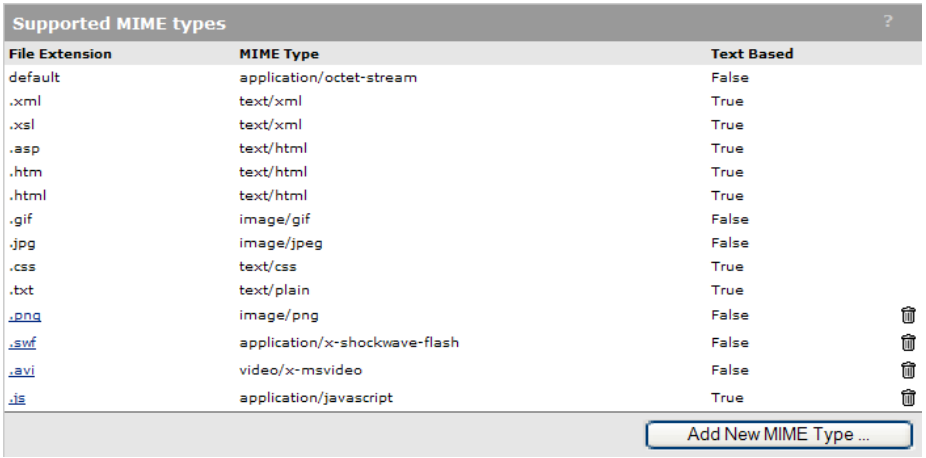
- Map the unsecure port 8080 to port 81
- Map the secure port 8090 to port 444

Make sure that you do not remap these ports to values already in use on your network.

MIME types

MIME (Multipurpose Internet Mail Extensions) is an Internet standard that is used to describe the type of information that a message or file contains.

By default, the controller contains the definitions for a number of common MIME types. If you need to add your own definition, select **Configure**.

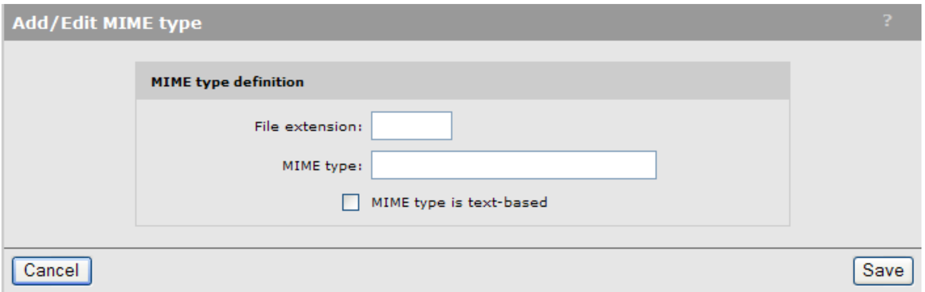


Supported MIME types

File Extension	MIME Type	Text Based	
default	application/octet-stream	False	
.xml	text/xml	True	
.xsl	text/xml	True	
.asp	text/html	True	
.htm	text/html	True	
.html	text/html	True	
.gif	image/gif	False	
.jpg	image/jpeg	False	
.css	text/css	True	
.txt	text/plain	True	
.png	image/png	False	🗑
.swf	application/x-shockwave-flash	False	🗑
.avi	video/x-msvideo	False	🗑
.js	application/javascript	True	🗑

This page lists all MIME types that are currently defined on the Web server. A number of common MIME types are defined by default. (Some of the default definitions cannot be changed.)

Select **Add New MIME Type** to define your own MIME type.



File extension
Specify the file extension that identifies this MIME type.

MIME type
Specify the content-type string that identifies this MIME-type. This is the value that must appear in an HTTP Content-type header for the controller to recognize this MIME type.

Types should be specified in the following format: **type/subtype**

For example: **text/xml**

MIME type is text-based
Enable this option if the MIME type identifies files that are text-based.

Security

Use this option to control access to the Web server.

Allowed addresses
The Web server will only accept connections from devices whose IP addresses appear in this list.

When the list is empty, authentication requests are accepted from any address.

Active interfaces
Select the interface(s) on which the controller will accept connections.

When NOC authentication is active, this is the interface on which the remote login Web server application can be reached. For more information on NOC authentication, see *NOC authentication on page 15-62* and *Appendix D: NOC authentication*.

Note Ingress interfaces configured inside VSCs (including the LAN port) always have access to the Web server when NOC-based authentication is disabled.

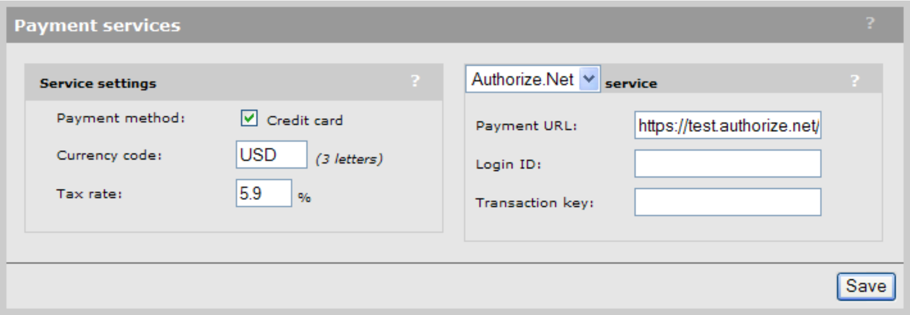
Managing payment services

The controller can directly interact with payment processing services service such as Authorize.Net and WorldPay, so that users can pay for network access from within their Web browser.

Payment services configuration

To configure payment services, follow this procedure:

1. Select **Controller >> Public access > Payment services**.



Payment services

Service settings

Payment method: ☑ Credit card

Currency code: USD *(3 letters)*

Tax rate: 5.9 %

Authorize.Net service

Payment URL: https://test.authorize.net/

Login ID:

Transaction key:

Use this page to define the type of payment options that the public access interface will support.

2. Enable **Credit card**. Specify the 3-letter **Currency code** (see online help for list of codes) and **Tax rate**.

3. For Credit card payment authorization, select either Authorize.NET or WorldPay, and specify the appropriate information. Merchant accounts must be set up to use these services (www.authorize.net or www.worldpay.com).

Service settings

Payment method: Credit card
Enable this option to allow users to pay for services via credit card. The controller makes use of a third-party credit card processing service (either Authorize.Net or WorldPay) to handle credit card transactions.

Communications with the credit card service occurs via an SSL connection. In the case of Worldpay, you must purchase the appropriate certificate as required and install it on the **Controller >> Security > Certificates stores** page. The other payment methods do not require installation of a certificate.

The controller does not keep a record of the user’s credit card information. All information handled by the system is securely managed in accordance with the PCI DSS v1.2 standard.

The controller maintains a billing log that provides a simple audit trail of all transactions. The log supports the buffering and retransmission of up to 2000 billing records to an external billing records server. You can configure log options on the **Controller >> Public access > Records** page.

Currency code
Specify the three-letter code for the currency in which all charges will be calculated. See the online help for a complete list of currency codes.

Tax rate
Specify the tax rate to use when calculating sales tax for all charges.

Authorize.Net service

Payment URL
Specify the URL of the Authorize.Net server.

Login ID
Specify the login ID of the Authorize.Net account assigned to the controller.

Transaction key
Specify the transaction key for the Authorize.Net account assigned to the controller.

WorldPay service

Payment URL
Specify the URL of the WorldPay server.

Installation ID
Specify your WorldPay installation ID. This informs WorldPay to which merchant all sales will be credited.

Response password
Specify your WorldPay installation response password.

Other configuration issues
To successfully make use of the WorldPay service you must also address the following issues:

- The Internet port of the controller must be reachable by the WorldPay servers. This is required so that the WorldPay pages stored on the controller can be retrieved, and that the controller can receive an HTTP/HTTPS post with payment details. (To support HTTPS, a certificate signed by a well-known certificate authority must be installed on the controller.)
- An access list must be defined on the controller that gives users access to the WorldPay site without being authenticated. For example:
  `access-list=factory,ACCEPT,tcp,*worldpay.com,all`

  If different, replace `*worldpay.com` with whatever is configured.

- You must configure the payment response URL in your Worldpay customer account to point to the public access web server on the controller. This tells Worldpay where to post information about transactions. The format for the URL is:

  ```
  https://host_name:port/goform/HtmlWorldpayPaymentResponse
  ```

  Where:

  - *host_name* is the name of the public access web server as defined in the X.509 (SSL) certificate installed on the controller.
  - *port* is the HTTPS port number of the public access web server as defined on the **Controller >> Public access > Web server** page.

For complete configuration requirements, see the documentation on the WorldPay site.

PayPal service

Before you can configure and use the PayPal service you need to:

- Open a PayPal business account and obtain a PayPal user ID, user password, and signature.
- Become familiar with your responsibilities as a merchant.
- Obtain basic knowledge of the PayPal Express Checkout API (version 63.0 or higher) in order to successfully customize the PayPal public access web pages, which are: paypal-cancel.asp, paypal-return.asp, and paypal-error.asp. To see the contents of these pages, select **Controller >> Public access > Web server** and look in the Current site files list.

PayPal offers many different methods for deducting funds from a customer account. However, the controller only supports methods that provide immediate resolution. Any kind of deferred payment is not supported. As a result, when PayPal displays payment options to the user, only instant payment options are shown. If a user's PayPal account does not support instant payment, then they will not be able to purchase services.

In order to pay for service with PayPal, users must be able to reach the PayPal server before they are authenticated. Therefore, an access list must be created on the controller to give unauthenticated users access to the PayPal server. For example, you can add the following definition to the default access list called **factory**:

```
access-list=factory,ACCEPT,tcp,*paypal.com,all
```

Add this definition by selecting **Controller >> Public access > Attributes**, and then selecting **Add New Attribute**.

User ID
Specify the user ID assigned to your PayPal business account.

User password
Specify the password assigned to your PayPal business account.

Signature
Specify the signature assigned to your PayPal business account.

Mode

- **Test:** Use this option to test your setup to make sure that everything is working properly. Requests are set to the PayPal test server at: https://api-3t.sandbox.paypal.com/nvp

  When users select the **Checkout with PayPal** button, they are redirected to: https://www.sandbox.paypal.com/

  For more information on using the test server, see the PayPal developer network at https://www.x.com/community/ppx/testing

- **Production:** Requests are set to the PayPal server at: https://api-3t.paypal.com/nvp

  When users select the **Checkout with PayPal** button, they are redirected to: https://www.paypal.com/

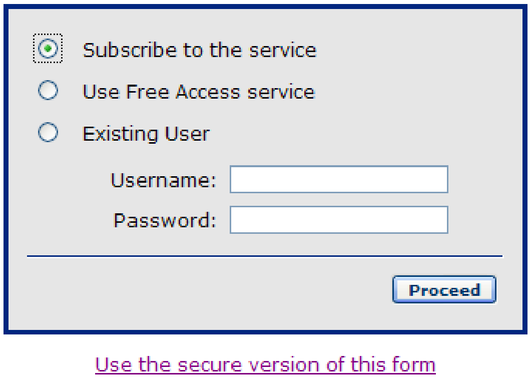
Override default PayPal URLs

Enable this option to override the default PayPal URLs for both Test and Production modes with a custom value.

Paypal example

The following steps illustrate the typical user experience when using the new PayPal feature. To save space the pages have been cropped to remove the browser window and any banners. The name of the public access interface web page is shown for each image.

1. On the Login page, the user selects the **Subscribe to this service** button and then selects **Proceed**.

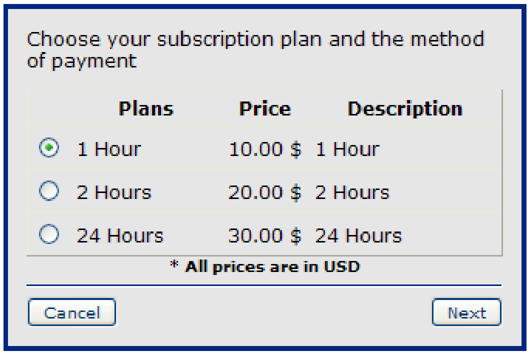


● Subscribe to the service
○ Use Free Access service
○ Existing User

Username:
Password:

page name= *index.asp*

2. The user chooses a subscription plan and then selects **Next**.



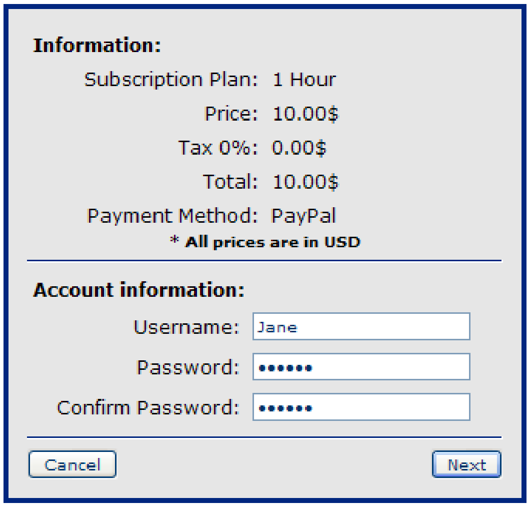
Choose your subscription plan and the method of payment

	Plans	Price	Description
●	1 Hour	10.00 $	1 Hour
○	2 Hours	20.00 $	2 Hours
○	24 Hours	30.00 $	24 Hours

* All prices are in USD

page name= *subscribe.asp*

3. The user reviews the subscription plan information, specifies a username and password for the new account, and then selects **Next**.



Information:

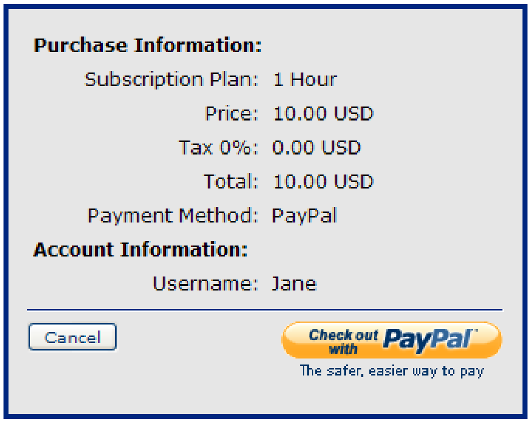
Subscription Plan: 1 Hour
Price: 10.00$
Tax 0%: 0.00$
Total: 10.00$
Payment Method: PayPal
* All prices are in USD

Account information:

Username: Jane
Password: ••••••
Confirm Password: ••••••

page name= *account.asp*

4. The user selects the **Checkout with PayPal** button to pay.



Purchase Information:

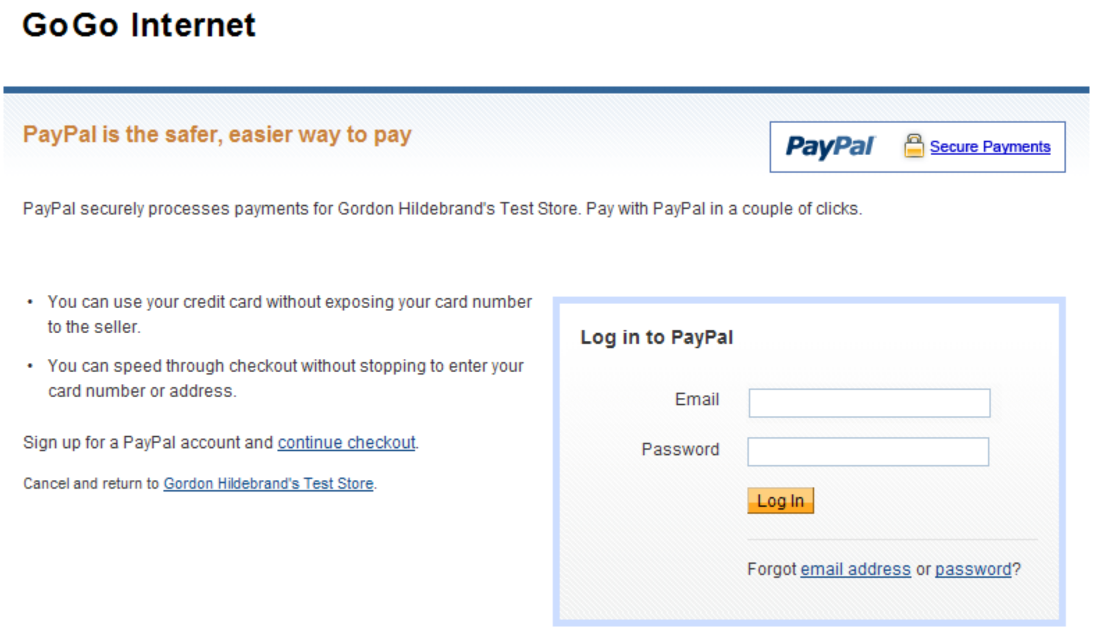
Subscription Plan: 1 Hour
Price: 10.00 USD
Tax 0%: 0.00 USD
Total: 10.00 USD
Payment Method: PayPal

Account Information:

Username: Jane

page name= *payment.asp*

5. The user is redirected to the PayPal site. A banner placed at the top of the page shows the merchant's name. The user enters their PayPal username and password and selects **Log In** to sign into PayPal.



PayPal is the safer, easier way to pay

PayPal securely processes payments for Gordon Hildebrand's Test Store. Pay with PayPal in a couple of clicks.

- You can use your credit card without exposing your card number to the seller.
- You can speed through checkout without stopping to enter your card number or address.

Sign up for a PayPal account and continue checkout.

Cancel and return to Gordon Hildebrand's Test Store.

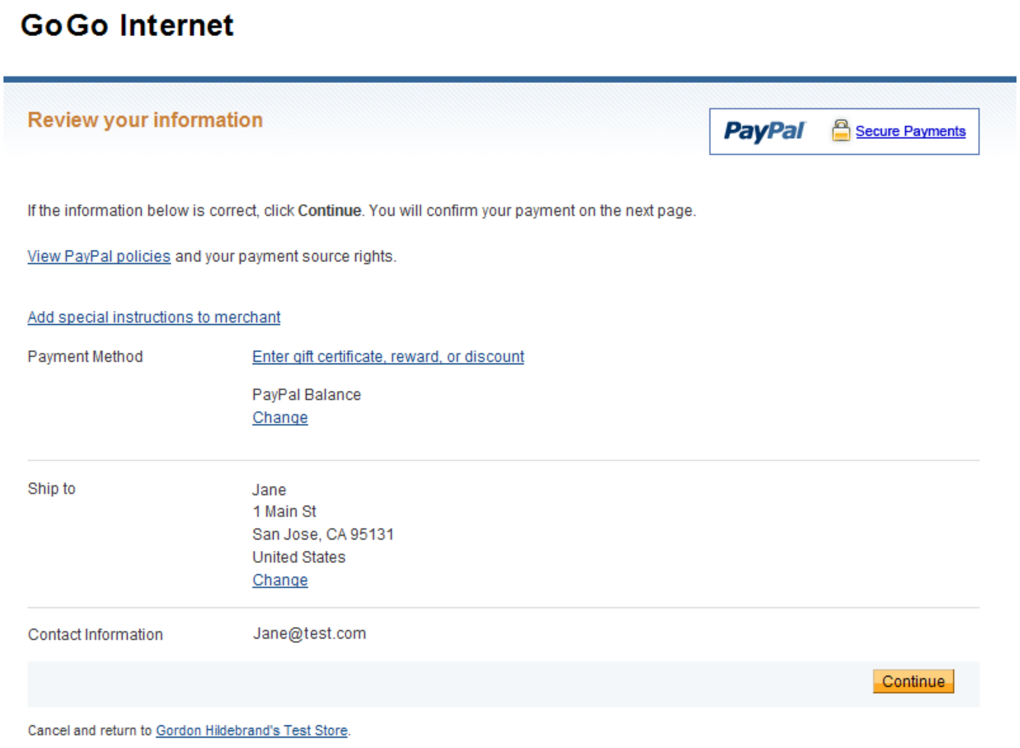
Log in to PayPal

Email

Password

Forgot email address or password?

6. PayPal presents billing information for the user to review. If satisfied, the user selects **Continue** to proceed. PayPal then sends the user’s transaction data back to the controller



Review your information

If the information below is correct, click **Continue**. You will confirm your payment on the next page.

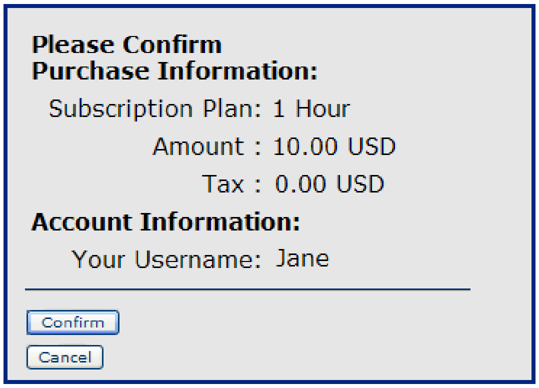
View PayPal policies and your payment source rights.

Add special instructions to merchant

Payment Method	Enter gift certificate, reward, or discount PayPal Balance Change
Ship to	Jane 1 Main St San Jose, CA 95131 United States Change
Contact Information	Jane@test.com

Cancel and return to Gordon Hildebrand's Test Store.

7. The user is redirected back to the controller public access interface, which presents a summary of the transaction. To continue, the user selects **Confirm**. The controller queries the PayPal server to approve the transaction.



Please Confirm
Purchase Information:

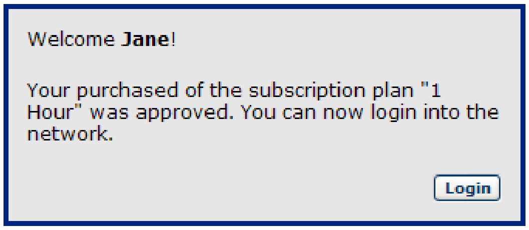
Subscription Plan: 1 Hour
Amount : 10.00 USD
Tax : 0.00 USD

Account Information:

Your Username: Jane

page name= *paypal-return.asp*

8. If the transaction is approved, the user can login to the network by selecting **Login**.

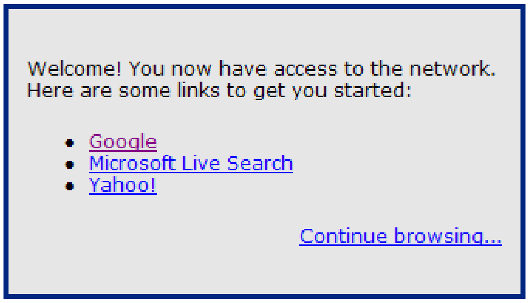


Welcome **Jane**!

Your purchased of the subscription plan "1 Hour" was approved. You can now login into the network.

purchase_approved.asp

9. The user's session starts.



Welcome! You now have access to the network. Here are some links to get you started:

- Google
- Microsoft Live Search
- Yahoo!

Continue browsing...

page name= *welcome.asp*

Billing record logging

The billings records logging system provides a simple audit trail of all billing transactions.

The log supports the buffering and retransmission of up to 2000 billing records to one or more external billing records servers. Log transmission occurs using HTTP/1.1 POST method with a completely customizable data format.

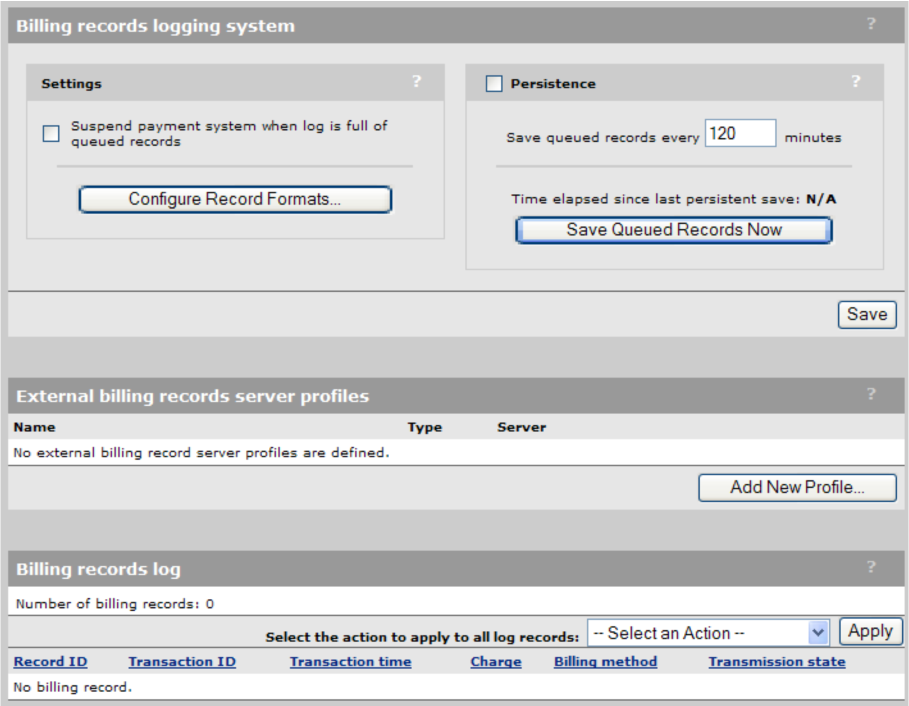
The system will retransmit a billing record until it is successfully acknowledged or until transmission is stopped because of too many failures.

Multiple backup servers can be assigned to a primary server to increase the probability of successfully transmitting a billing record.

To reduce the risk of billing records being lost, data can be mirrored by defining multiple primary servers. A copy of each record is sent to each primary server.

Note Records are always added to the log, even when record transmission is disabled. If required, these records can be saved (exported) to a file, but cannot be transmitted to a billing server.

To configure Billing record logging, select **Controller >> Public access > Billing records**.



Billing records logging system

Settings

□ Suspend payment system when log is full of queued records

Persistence □

Save queued records every 120 minutes

Time elapsed since last persistent save: **N/A**

External billing records server profiles

Name	Type	Server
No external billing record server profiles are defined.		

Billing records log

Number of billing records: 0

Select the action to apply to all log records: -- Select an Action --

Record ID	Transaction ID	Transaction time	Charge	Billing method	Transmission state
No billing record.					

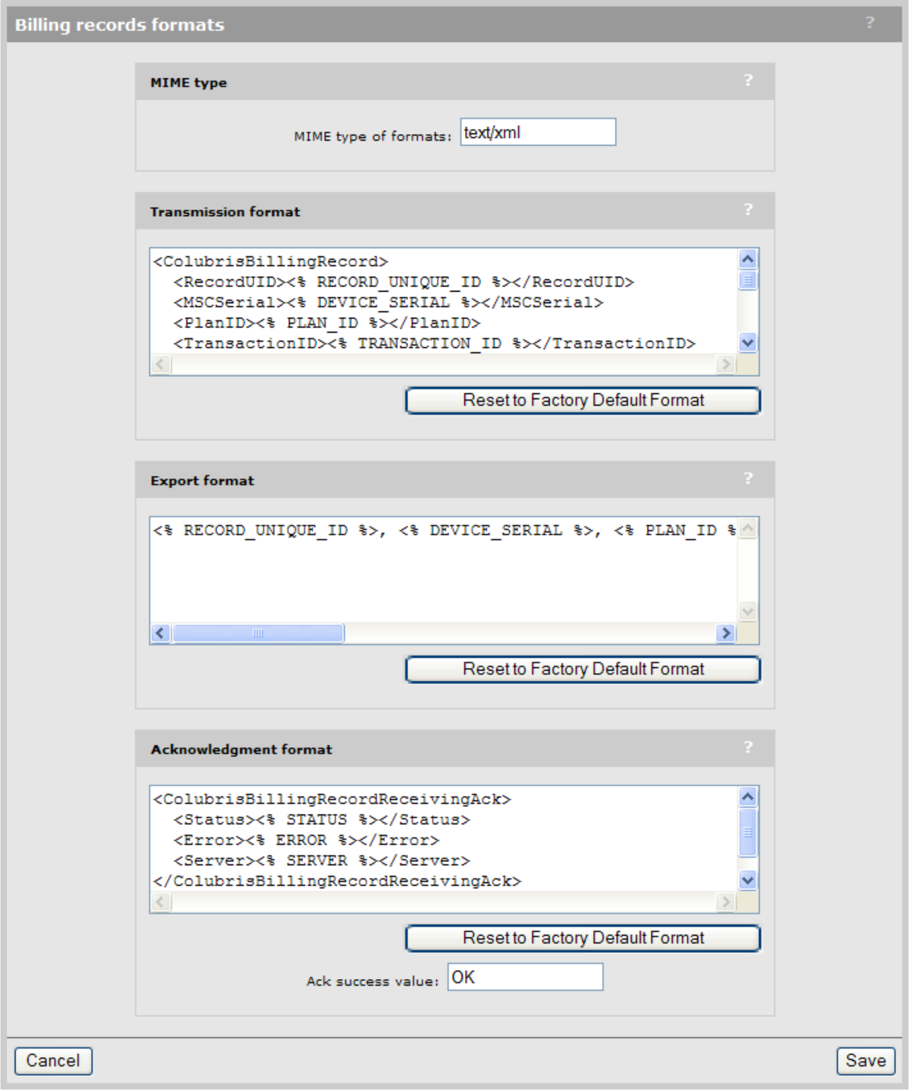
Settings

Suspend payment system when log is full of queued records

Use this option to halt the payment system if external billing servers are unable to receive records and the log is full of **untransmitted** records. (Records with a status of “Queued”). For more information on how the log entries are managed, see *Billing records log on page 14-47*.

When this options is disabled, the oldest untransmitted record is removed from the log to make room for the new record.

Configure Record Formats
Select this button to edit the transmission, export, and acknowledgement formats for the billing records. See the online help for format descriptions.



MIME type of formats: text/xml

```
<ColubrisBillingRecord>
  <RecordUID><% RECORD_UNIQUE_ID %></RecordUID>
  <MSCSerial><% DEVICE_SERIAL %></MSCSerial>
  <PlanID><% PLAN_ID %></PlanID>
  <TransactionID><% TRANSACTION_ID %></TransactionID>
```

```
<% RECORD_UNIQUE_ID %>, <% DEVICE_SERIAL %>, <% PLAN_ID %
```

```
<ColubrisBillingRecordReceivingAck>
  <Status><% STATUS %></Status>
  <Error><% ERROR %></Error>
  <Server><% SERVER %></Server>
</ColubrisBillingRecordReceivingAck>
```

Ack success value: OK

Persistence

Enable this option to have the controller save queued (untransmitted) records in the log to its internal flash memory so that they can be recovered in case of abnormal system shutdown (power failure, for example). See *Billing records log on page 14-47*.

Save queued records every *nn* minutes
Specify the interval at which the log is saved.

Save Queued Records Now
Force the log to be saved immediately.

External billing records server profiles

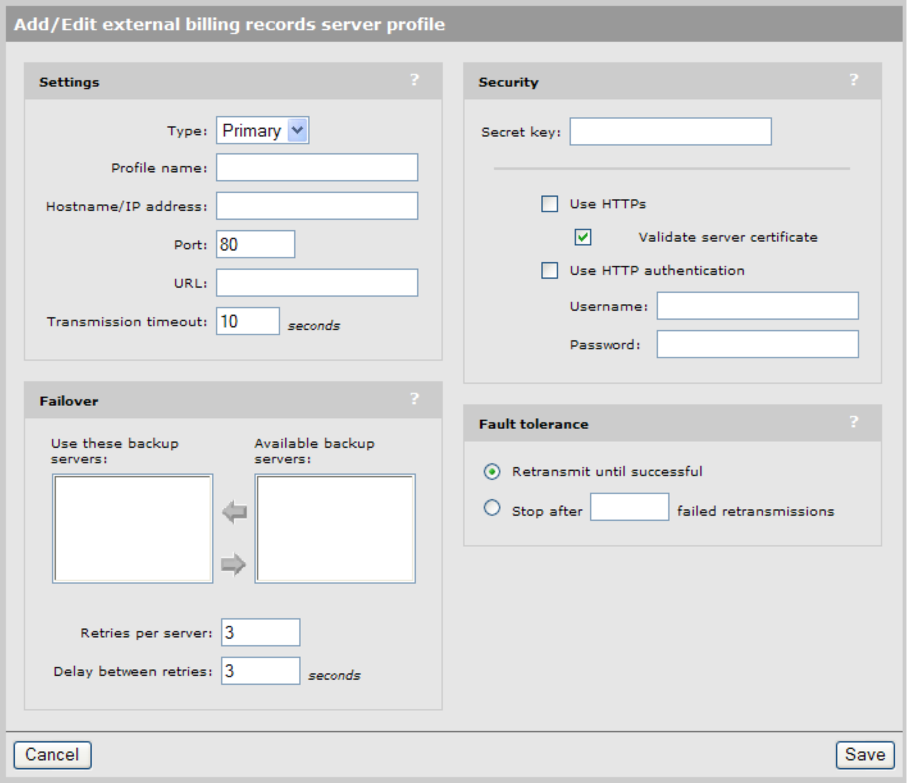
This list displays all configured billing records server profiles. Billing records are sent to the servers defined in this list as follows:

- A copy of the current billing record is sent to each primary server. By adding multiple primary servers you create data mirroring and reduce the risk of a record being lost.
- If a primary server fails to acknowledge the record, the controller retries. Once the retry limit is reached, the record is transmitted to any defined backup servers. Once all retries are attempted for all backup servers, the record is either skipped, or the entire process starts again.

For example, if you configure a primary server “Server A” with “Server B” as a backup, with 2 transmission attempts, the following sequence in used to transmit the billing record:

A-[Delay]-A-[Delay]-B-[Delay]-B-[Delay]-A-[Delay]-A-[Delay]-B-[Delay]-B…

To edit an existing profile, select its **Name**. To add a new profile, select **Add New Profile**. In either case you will see the Add/Edit external billing records server profile page.



Add/Edit external billing records server profile

Settings

Type: Primary

Profile name:

Hostname/IP address:

Port: 80

URL:

Transmission timeout: 10 seconds

Security

Secret key:

□ Use HTTPs

☑ Validate server certificate

□ Use HTTP authentication

Username:

Password:

Failover

Use these backup servers:

Available backup servers:

Retries per server: 3

Delay between retries: 3 seconds

Fault tolerance

● Retransmit until successful

○ Stop after failed retransmissions

Settings

Type

- **Primary:** Defines a primary server. The controller sends a copy of each billing record to all primary servers. See *Record transmission overview on page 14-46*.
- **Backup:** Defines a backup server. Backup servers can be assigned to act as a backup to a primary server by using the **Failover** box.

Profile name
Specify a name to identify the server profile.

Hostname/IP address
IP address or hostname of the server.

Port
Port on which to send the HTTP post.

URL
URL to which the HTTP post will be sent.

Transmission timeout
Amount of time that the controller waits for an HTTP response for a transmitted record. If the response is not received within this period, this is considered as a failed transmission.

Failover

Use this box to define one or more backup server profiles for the current primary server profile.

Use these backup servers
Lists all backup server profiles for this primary server profile. Backup profiles are used in the order that they appear in the list.

Available backup servers
Lists all server profiles of type backup.

Retries per server
Number of times that a record will be retransmitted before the next profile is tried.

Note This parameter also sets the number of retries on the primary.

Delay between retries
Amount of time to wait between retransmitting a record.

Security

Encryption and authentication can be used to increase the transmission security of billing records.

HTTP authentication and secure HTTP using SSLv3 are supported. Also, to make sure that a billing record has not been altered, a secret key, shared between the billing server and the controller, can be defined and used to produce a cryptographic signature of the billing record.

Secret key
Specify the secret key that will be used to generate an encryption signature using HMAC-SHA-1. The signature is generated using the entire contents of the billing record. (The signature field is empty when the signature is calculated.)

Use HTTPS
When enabled, secure HTTP using SSLv3 is used to transmit records to all servers.

Validate server certificate
When enabled, the controller will validate the external billing server certificate. For this to be successful, you must install the billing server CA certificate in the Trusted CA certificate store on the **Security > Certificate stores** page.

Use HTTP authentication
Enable this option if the billing server requires a username and password.

Fault tolerance

Fault tolerance settings control how many times each billing record is retransmitted.

Retransmit until successful
When enabled, the controller will never skip a record due to transmission failure. Retransmission is continuously retried on the primary server and all backup servers until successful.

Enabling this option may cause log entries to be lost if a record fails to be transmitted before the log wraps around. To avoid losing records, enable the **Suspend operation of payment system when log is full** option under **Log settings** on the **Controller >> Public access > Billing records** page.

Stop after failed *nnn* retransmissions
Select this option to have the controller stop retransmitting a record when the total number of retransmissions on all servers (primary and backup) exceeds the specified number.

When this occurs the record is flagged as **Transmission Failed** in the log.

Record transmission overview

Transmission of a billing record occurs as follows:

- Billing record is transmitted to the primary server.
- If the primary server does not send an HTTP reply within the **Transmission timeout**, then the transmission is considered to have failed. If a response is received, but the status field does not match the value of **Ack success value**, then the transmission is considered to have failed.
- Failed transmissions are retried on the primary server until the **Retries per server** limit is met, after which each backup server is tried in order. Once all backups are tried, the sequence resumes again with the primary server.
- Retransmissions only stop if the selected condition under **Fault tolerance** is met: either the record is successfully transmitted or the total number of retires on all servers passes a predetermined limit.

Note A billing record is considered to be successfully transmitted only when it has been successfully transmitted to **every primary server** (or one of its backups).

Billing records log

This table displays the contents of the billing records log. The log can hold up to 2000 records. When full, records are deleted in the following order:

1. Records that have been successfully transmitted.
2. Records that do not have to be transmitted, because transmission is disabled.
3. Records for which transmission has failed.

If transmissions to remote billing server(s) is interrupted, the log can become full of untransmitted records only. (Records with status set to "Queued".) What happens next is controlled by the **Suspend payment system when log is full of queued records** when log is full setting under **Settings**.

- If enabled, payment services are suspended.
- If disabled, the oldest queued record is removed.

Number of billing records
Lists the total number of billing records in the log.

Select the action to apply to all log records

- **Clear log:** Delete all records in the log.
- **Save log:** Save the log to a file using the export format defined by selecting **Controller >> Public access > Billing records > Configure Records Format**.
- **Retransmit failed records:** Force the retransmission of records that have transmission state set to **Transmission Failed**. This starts the complete transmit cycle all over again for the record.
- **Cancel current transmission:** Terminates the record transmission that is currently in progress.

Table

Record ID
Unique number that identifies each record.

Transaction ID
Credit card transaction ID generated by the credit card service.

Transaction time
Date and time of the transaction.

Charge
Amount charged on the transaction.

Billing method

Identifies the billing method:

- CC_WORLDPAY
- CC_AUTHORIZE_NET
- CC_PAYPAL

Transmission state

- **Transmitting:** The record is being transmitted.
- **Queued:** The record is queued for transmission.
- **Transmission Disabled:** Transmission of the record was disabled. Once records fall into this category they cannot be retransmitted.
- **Successful:** The record was successfully transmitted and acknowledged by all primary servers (or their backups).
- **Transmission Failed:** The record was not transmitted successfully and retransmission attempts have stopped due to the setting for **Fault tolerance** in the billing records server profile (**Controller >> Public access > Billing records > External billing records server profiles**).

Location-aware authentication

This feature enables you to control logins to the public access network based on the wireless access point with which a user is associated. Once authenticated, this feature is also used to monitor and control roaming to other access points in the network.

How it works

Location-aware is automatically enabled when a VSC is set to **provide access control**. When enabled, the location-aware feature causes the controller to return location-specific information for RADIUS-authenticated users. This information is returned:

- When the user logs in
- Each time the user roams to a new access point or switches SSIDs on the same access point (which causes the user to be re-authenticated).

Note

Due to security constraints in 802.1X client software, users cannot automatically be re-authenticated when roaming to a new access point. Therefore, location-aware information cannot be returned when these users roam.

Returned information

The controller can return the following attributes in the RADIUS access request for all user authentications (whether initial login or re-authentication due to roaming):

- Called-station-ID (Standard RADIUS attribute)
- HP-specific attribute: SSID
- HP-specific attribute: GROUP

Note When re-authenticating users, the returned RADIUS attribute Service-Type is set to 8744 (decimal).

Called-Station-ID value

By default, this is the MAC address of the wireless port (radio) to which the user is associated. This is the MAC address of the **wvlan0** or **wvlan1** interface in IEEE format as displayed by **Tools > System Tools > Interface info.**

If required, the controller can return other values for this attribute by setting the **Called-Station-Id content** on a per-VSC basis. The other available options are:

- **SSID:** SSID of the access point with which the user is associated.
- **Group:** Group name of the access point with which the user is associated.
- **macaddress:** Returns the MAC address of the wireless port (radio) the user is associated with. This is the MAC address of the wvlan0 or wvlan1 interface as shown by **Controller >> Tools > System Tools > Interface info**.

  If the user is connected via a wired connection, the value returned is the MAC address of the controller wireless/LAN port. To use the MAC address of the Internet port, you must edit the config file and change the setting of **radius-called-station-id-port** to **WAN** in the <ACCESS-CONTROLLER> section.
- **macaddress:ssid:** The MAC address of the wireless AP’s radio, followed by a colon, followed by the SSID configured on this VSC.

HP-specific attribute: SSID

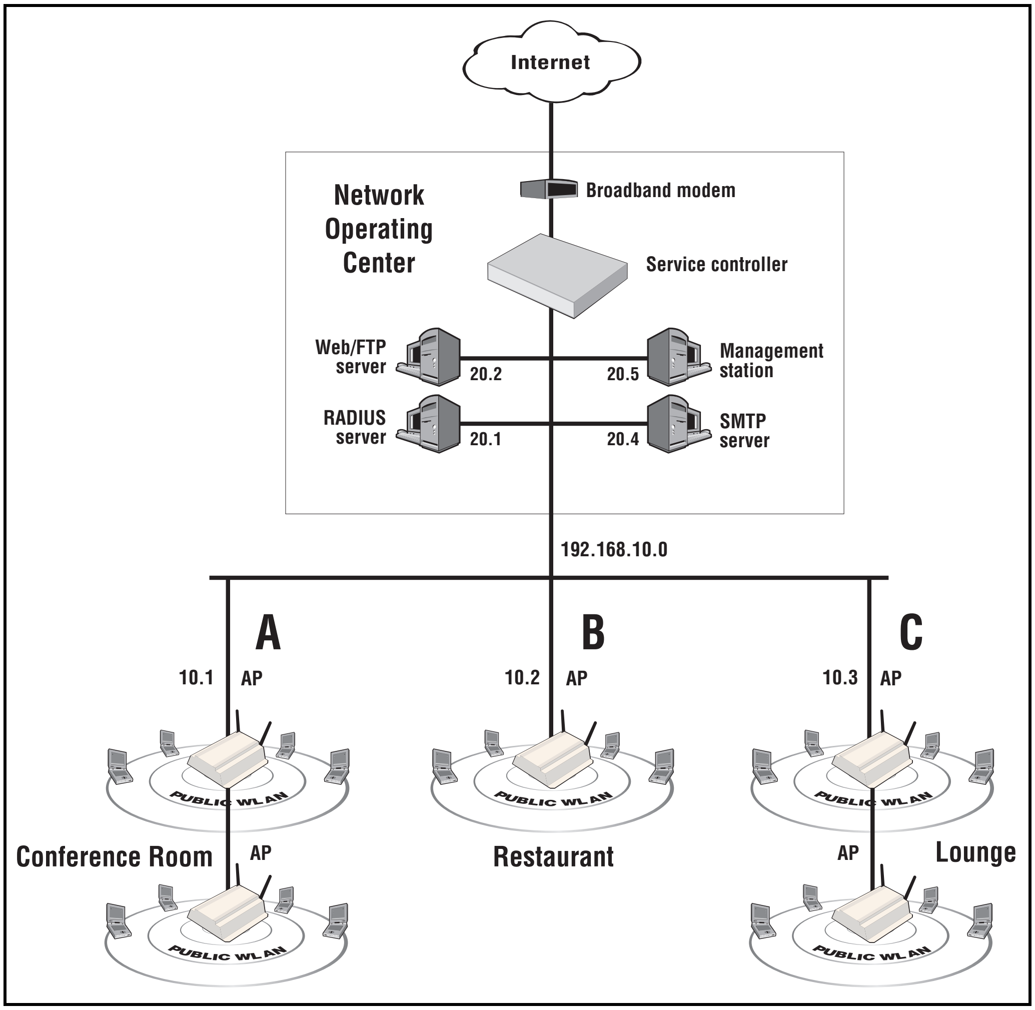
The SSID of the access point with which the user is associated (wireless only).

HP-specific attribute: GROUP

The group name of the access point with which the user is associated (wireless only).

Example

Consider the following topology for a fictional small hotel. The restaurant and lounge are available to all hotel users who subscribe to the wireless service. However, the conference room is available only to a specific group of guests who book it in advance.



In this example, the access points in each area are assigned the following unique group names:

- conference_room
- restaurant
- lounge

When a user logs in, server-side code can be used to determine the access point they are associated with by inspecting the Called-Station-ID. Then, using user's account information, access can either be granted or denied.

Security

The controller accepts location-aware information only from MSM APs that have a matching shared secret to its own.

15

Working with RADIUS attributes

Contents

Introduction

RADIUS attributes can be used to customize a wide range of configuration settings on the controller. This includes defining configuration settings for the public access interface, customizing the settings of access-controlled user accounts, or configuring credentials for the administrative accounts that are used to manage/operate the controller.

Attributes can be defined both locally on the controller or retrieved from a third-party RADIUS server. In certain cases, values can be defined locally and then overwritten by values retrieved from a RADIUS server. This allows, for example, default values on the controller to be dynamically updated on a per-user basis.

This chapter splits the supported RADIUS attributes into three categories:

Category	Description	For information, see...
Controller attributes	Used to customize the operation of the public access interface (creating access lists for walled gardens, for example), and also to define default values that are applied to all user accounts.	■ *Controller attributes overview on page 15-4* ■ *Colubris AV-Pair - Site attribute values on page 15-33*
User attributes	Used to customize the settings of individual access-controlled user accounts.	■ *User attributes on page 15-13* ■ *Colubris AV-Pair - User attribute values on page 15-67*
Administrator attributes	Used to define login credentials for administrative users (mangers and operators).	■ *Administrator attributes on page 15-31* ■ *Colubris AV-Pair - Administrator attribute values on page 15-74*

Controller attributes overview

The controller provides support for a number of standard RADIUS attributes, including those for authentication and accounting. See *Controller attribute definitions on page 15-8* for a list of these attributes and a brief definition. For detailed information on these attributes, refer to RFC2865, or the documentation that came with your RADIUS server.

The controller also supports several vendor-specific attributes, including the special HP attribute (known as the *site attribute*) that is used to customize the behavior of the public access interface and define global default values for user accounts. To find out more about the site attribute, see the following section.

Customizing the public access interface using the site attribute

HP has defined a vendor-specific RADIUS attribute to support configuration of the public access interface and user accounts. This attribute conforms to RADIUS RFC 2865 and is called the **Colubris AV-Pair**.

Multiple instances of the Colubris AV-Pair attribute can be defined on the controller, each with a different **AV-Pair value**. For a complete list of all supported AV-Pair values, see *Colubris AV-Pair - Site attribute values on page 15-33*.

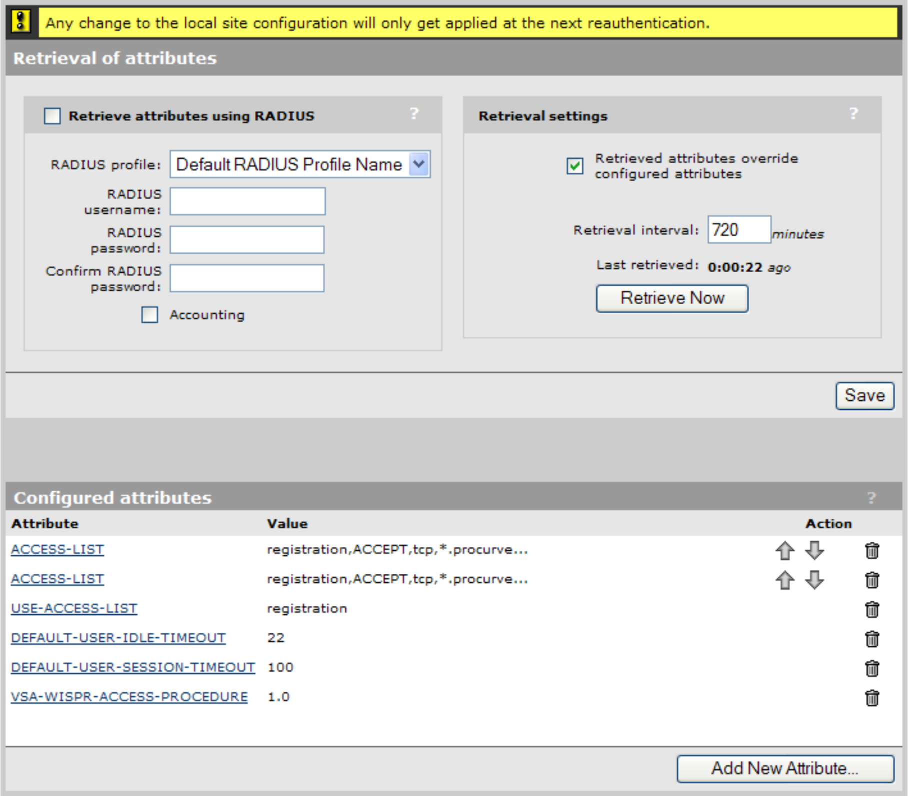
In order for a third-party RADIUS server to support the Colubris AV-Pair attribute you need to define it as described under *Colubris AV-Pair on page 15-11*.

Note The Colubris AV-Pair attribute can be used to define settings on the controller and for users and administrators. This section discuses controller settings only.

Important The documentation for this product frequently uses the terms site attributes and user attributes to refer to the Colubris AV-Pair attribute values depending on whether the AV-Pair attribute values are set with a value that applies to the public access site or to an individual user.

Defining and retrieving site attributes

Site attributes can be retrieved from a third-party RADIUS server or specified directly on the controller. In both cases, configuration settings are defined on the **Public Access > Attributes** page.



Any change to the local site configuration will only get applied at the next reauthentication.

Retrieval of attributes

□ Retrieve attributes using RADIUS

RADIUS profile: Default RADIUS Profile Name
RADIUS username:
RADIUS password:
Confirm RADIUS password:
□ Accounting

Retrieval settings

☑ Retrieved attributes override configured attributes

Retrieval interval: 720 minutes
Last retrieved: 0:00:22 ago

Configured attributes

Attribute	Value	Action
ACCESS-LIST	registration,ACCEPT,tcp,*.procurve...	
ACCESS-LIST	registration,ACCEPT,tcp,*.procurve...	
USE-ACCESS-LIST	registration	
DEFAULT-USER-IDLE-TIMEOUT	22	
DEFAULT-USER-SESSION-TIMEOUT	100	
VSA-WISPR-ACCESS-PROCEDURE	1.0	

Retrieving site attributes from a RADIUS server

To retrieve attributes form a RADIUS server, enable the **Retrieve attributes using RADIUS** option. To use this option, you must also configure a RADIUS profile (see *Using a third-party RADIUS server on page 11-5*) and define an account for the controller on the appropriate RADIUS server. This account must contain all site attributes that you want to retrieve. For a complete list of all supported site attributes and their syntax, see *Colubris AV-Pair - Site attribute values on page 15-33*.

After the controller is authenticated by the RADIUS server it automatically retrieves the site attributes you defined in the controller's RADIUS account. The retrieved attributes are then combined with the attributes defined in the **Configured attributes** list (if any) to build the complete list of attributes that are active on the controller. If the same attribute is defined on both the RADIUS server and in the **Configured attributes** list, the setting of **Retrieved attributes override configured attributes** determines which definition is used.

Note

A maximum of 128 attributes can be active at any one time (including both the RADIUS and the **Configured attributes** list).

The maximum attribute size that the controller can receive in a single RADIUS request is 4096 bytes. However, some networks may limit RADIUS request size to around 1500 bytes because they discard UDP fragments.

Configure the **Retrieve attributes using RADIUS** options as follows:

- **RADIUS profile**: Select a RADIUS profile. The profile is used to establish the connection to a RADIUS server. RADIUS profiles are defined by selecting **Controller >> Authentication > RADIUS profiles**. For details, see *Using a third-party RADIUS server on page 11-5*.
- **RADIUS username**: Specify the username of the RADIUS account assigned to the controller.
- **RADIUS password / Confirm password**: Specify the password of the RADIUS account assigned to the controller.
- **Accounting**: Enable this option to have the controller generate a RADIUS accounting request ON/OFF each time its authentication state changes.
- **Retrieved attributes override configured attributes**: Enable this option to have attributes retrieved from the RADIUS server overwrite settings defined in the **Configured attributes** table.
- **Retrieval interval**: Specify the number of minutes between attribute retrievals. The controller retrieves attributes from its RADIUS account each time this interval expires.

  To avoid potential service interruptions that may occur when new attributes are activated by the controller, it is strongly recommended that you use a large interval (12 hours or more).

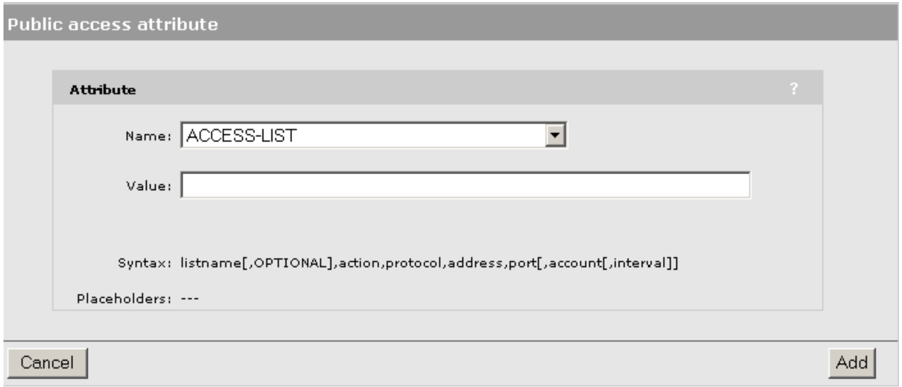
  You can override the value configured on this page by using the RADIUS attribute **Session-timeout**, which enables the following strategy: Configure **Retrieval interval** to a small value (10 to 20 minutes) and set the RADIUS attribute **Session-timeout** to override it with a large value (12 hours) when authentication is successful. Since the **Retrieval interval** is also respected for Access Reject packets, this configuration results in a short reauthentication interval in the case of failure, and a long one in the case of success.
- **Last retrieved**: Shows the amount of time that has passed since the controller last retrieved attributes.
- **Retrieve Now**: Select to force the controller to contact the RADIUS server and retrieve attributes.

Defining site attributes directly on the controller

Site attributes can be defined directly on the controller eliminating the need to use a RADIUS server. If needed, both methods can be used at the same time. In this case, the retrieved attributes are combined with those attributes defined in the **Configured attributes** list to build the complete list of attributes that are active on the controller. If the same attribute is defined on both the RADIUS server and in the **Configured attributes** list, the setting of **Retrieved attributes override configured attributes** determines which definition is used.

To add a new attribute:

1. Select **Add New Attribute.** The **Public access attribute** page opens.
2. Under **Name,** select an AV-Pair value, as shown in the following figure.



Public access attribute

Attribute

Name: ACCESS-LIST

Value:

Syntax: listname[,OPTIONAL],action,protocol,address,port[,account[,interval]]

Placeholders: ---

3. Once you select a **Name,** information appears regarding the correct syntax to specify under **Value.** Use the correct syntax to specify the desired **Value**.

   For a complete list of all supported site attributes and their syntax, see *Colubris AV-Pair - Site attribute values on page 15-33*, or consult the online help.

4. Select **Add.**

Controller attribute definitions

The following table lists all RADIUS attributes supported by the controller. A brief description of each attribute follows the table. For detailed information, refer to RFC2865, or the documentation that came with your RADIUS server.

Access Request

- Acct-Session-Id
- Called-Station-Id
- Calling-Station-Id
- CHAP-Challenge
- CHAP-Password
- Connect-Info
- EAP-Message
- Framed-IP-Address
- Framed-MTU
- NAS-Identifier
- NAS-Ip-Address
- NAS-Port
- NAS-Port-Type
- Message-Authenticator
- Service-Type
- State
- User-Name
- User-Password
- Vendor-specific (Microsoft)
  - MSCHAP-Challenge
  - MSCHAP-Response
  - MSCHAPv2-Response
- Vendor-specific (WISPr)
  - Location-Name
  - Location-ID
  - Logoff-url

Access Accept

- Class
- EAP-Message
- Session-Timeout
- Vendor-specific (Colubris)
  - Colubris AV-Pair

Access Reject

No attributes are supported.

Access Challenge

No attributes are supported.

Accounting Request

- Acct-Authentic
- Acct-Delay-Time
- Acct-Event-Timestamp
- Acct-Session-Id
- Acct-Status-Type
- Called-Station-Id
- Calling-Station-Id
- Class
- Framed-IP-Address
- NAS-Identifier
- NAS-Ip-Address
- NAS-Port
- NAS-Port-Type
- User-Name

Accounting Response

No attributes are supported.

In the attribute descriptions, a *string* is defined as 1 to 253 characters.

Access request

Acct-Session-Id
(32-bit unsigned integer)
Random value generated per authentication by the controller.

Called-Station-Id
(string)
By default, this is set to the MAC address of the controller wireless/LAN port in IEEE format. For example: 00-02-03-5E-32-1A. To use the MAC address of the Internet port, you must edit the config file and change the setting of **radius-called-station-id-port** to **WAN** in the <ACCESS-CONTROLLER> section.

Calling-Station-Id
(string)
The MAC address of the controller LAN port in IEEE format. For example: 00-02-03-5E-32-1A.

CHAP-Challenge
(string)
Randomly generated by the product. As defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to CHAP. Length = 19 bytes.

CHAP-Password
(string)
The password assigned to the controller on the **Public access > Attributes** page. Encoded as defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to CHAP.

Connect-Info
(string)
The string "HTTPS".

EAP-Message
(string)
As defined in RFC 2869. Only present when the authentication method for the RADIUS profile is set to EAP-MD5.

Framed-IP-Address
(32-bit unsigned integer)
IP Address of the controller LAN port.

Framed-MTU
(32-bit unsigned integer)
Hard-coded to 1496 (802.1X). Hard-coded value of 1496. The value is always four bytes lower than the wireless MTU maximum which is 1500 bytes in order to support IEEE802dot1x authentication.

NAS-Identifier
(string)
The NAS ID set on the **Controller >> Authentication > RADIUS profiles > Add New Profile** page for the RADIUS profile being used.

NAS-Ip-Address
(32-bit unsigned integer)
The IP address of the port the controller is using to communicate with the RADIUS server.

NAS-Port
(32-bit unsigned integer)
Always 0.

NAS-Port-Type
(32-bit unsigned integer)
Always set to 19, which represents WIRELESS_802_11.

Message-Authenticator
(string)
As defined in RFC 2869. Always present even when not doing an EAP authentication. length = 16 bytes.

Service-Type
(32-bit unsigned integer)
RADIUS service type.

State
(string)
As defined in RFC 2865.

User-Name
(string)
The RADIUS username assigned to the controller on the **Public access > Attributes** page.

User-Password
(string)
The password assigned to the controller on the **Public access > Attributes** page. Encoded as defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to PAP.

Vendor-specific (Microsoft)
HP supports the following Microsoft vendor-specific attributes.

MSCHAP-Challenge
(string)
As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1 or MSCHAPv2. Length = 8 bytes.

MSCHAP-Response
(string)
As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1. Length = 49 bytes.

MSCHAPv2-Response
(string)
As defined in RFC 2759. Only present when the authentication method for the RADIUS profile is set to MSCHAPv2. Length = 49 bytes.

Vendor-specific (WISPr)
HP supports the following Wi-Fi Alliance vendor-specific attributes.

Location-Name
The WISPr location name assigned to the controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 2
- Attribute type: A string in the format: `wispr-location-name=`*`location_name`*

Location-ID
The WISPr location identifier assigned to the controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 1
- Attribute type: A string in the format: `wispr-location-id=`*`location_id`*

Logoff-url
The WISPr log-off URL that will be used.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 3
- Attribute type: A string in the format: `wispr-logoff-url=`*`URL`*

Access accept

Class
(string)
As defined in RFC 2865. Multiple instances are supported.

EAP-Message
(string)
Only supported when authentication is EAP-MD5. Note that the content will not be read as the RADIUS Access Accept overrides whatever indication is contained inside this packet.

Session-Timeout
(32-bit unsigned integer)
The controller will retrieve RADIUS attributes when this timer expires. Omitting this attribute or specifying **0** disables the feature. (Note that this is configurable directly on the controller by setting **Public access > Attributes** > **Retrieval interval**.

Vendor-specific (Colubris)

Colubris AV-Pair
(string)
HP has defined this vendor-specific attribute to support configuration of special features on the controller, such as the customization of the public access interface and global user session settings. This attribute conforms to RADIUS RFC 2865. You may need to define this attribute on your RADIUS server (if it is not already present) using the following values:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 0
- Attribute type: A string in the following format `<keyword>=<value>`

Multiple instances of the Colubris AV-pair can be defined in a RADIUS account to configure a variety of settings. For a complete list of all supported attributes, see *Colubris AV-Pair - Site attribute values on page 15-33*.

Access reject

No attributes are supported.

Access challenge

No attributes are supported.

Accounting request

Acct-Authentic
(32-bit unsigned integer)
Always set to 1 which means RADIUS.

Acct-Delay-Time
(32-bit unsigned integer)
As defined in RFC 2869.

Acct-Event-Timestamp
(32-bit unsigned integer)
As defined in RFC 2869.

Acct-Session-Id
(32-bit unsigned integer)
Random value generated by the controller.

Acct-Status-Type
(32-bit unsigned integer)
Supported values are: Accounting-On (7) and Accounting-Off (8).

Called-Station-Id
(string)
The MAC address of the controller LAN port in IEEE format. For example: 00-02-03-5E-32-1A.

Calling-Station-Id
(string)
The MAC address of the controller LAN port in IEEE format. For example: 00-02-03-5E-32-1A.

Class
(string)
As defined in RFC 2865. Multiple instances are supported.

Framed-IP-Address
(32-bit unsigned integer)
IP Address of the controller LAN port.

NAS-Identifier
(string)

The NAS ID for the RADIUS profile being used.

NAS-Ip-Address
(32-bit unsigned integer)
The IP address of the port the controller is using to communicate with the RADIUS server.

NAS-Port
(32-bit unsigned integer)
Always 0.

NAS-Port-Type
(32-bit unsigned integer)
Always set to 19, which represents WIRELESS_802_11.

User-Name
(string)
The RADIUS username assigned to the controller on the **Public access > Attributes** page.

Accounting response

No attributes are supported.

User attributes

The controller provides support for a number of standard RADIUS user attributes, including those for authentication and accounting. See *User attribute definitions on page 15-20* for a list of these attributes and a brief definition. For detailed information on these attributes, refer to the documentation that came with your RADIUS server.

The controller also supports several vendor-specific attributes, including the special HP attribute (known as the *user attribute*) that is used to customize the behavior of the public access interface and define values for user accounts. To find out more about the user attribute, see the following section.

Customizing user accounts with the user attribute

HP has defined a vendor-specific RADIUS attribute to support configuration of the public access interface and user accounts. This attribute conforms to RADIUS RFC 2865 and is called the **Colubris AV-Pair**.

Multiple instances of the Colubris AV-Pair attribute can be defined for each user, each with a different **AV-Pair value**. For a complete list of all supported AV-Pair values, see *Colubris AV-Pair - User attribute values on page 15-67*.

In order for a third-party RADIUS server to support the Colubris AV-Pair attribute you need to define it as described under *Colubris AV-Pair on page 15-32*.

Note The Colubris AV-Pair attribute can be used to define settings on the controller and for users and administrators. This section discuses user settings only.

Important The documentation for this product frequently uses the terms site attributes and user attributes to refer to the Colubris AV-Pair attribute values depending on whether the AV-Pair attribute values are set with a value that applies to the public access site or to an individual user.

Defining and retrieving user attributes

User attributes can be retrieved from a third-party RADIUS server or specified directly on the controller in user account profiles.

Defining attributes locally in user accounts

If you are using the local user accounts to authenticate users, then you can define account attributes locally via account profiles.

Each user account can be associated with one or more account profiles. The attributes that are set in each profile are combined in the account to produce the full list of active attributes.

If you are working with access-controlled user accounts, additional attributes can also be defined via the **Default AC** profile.

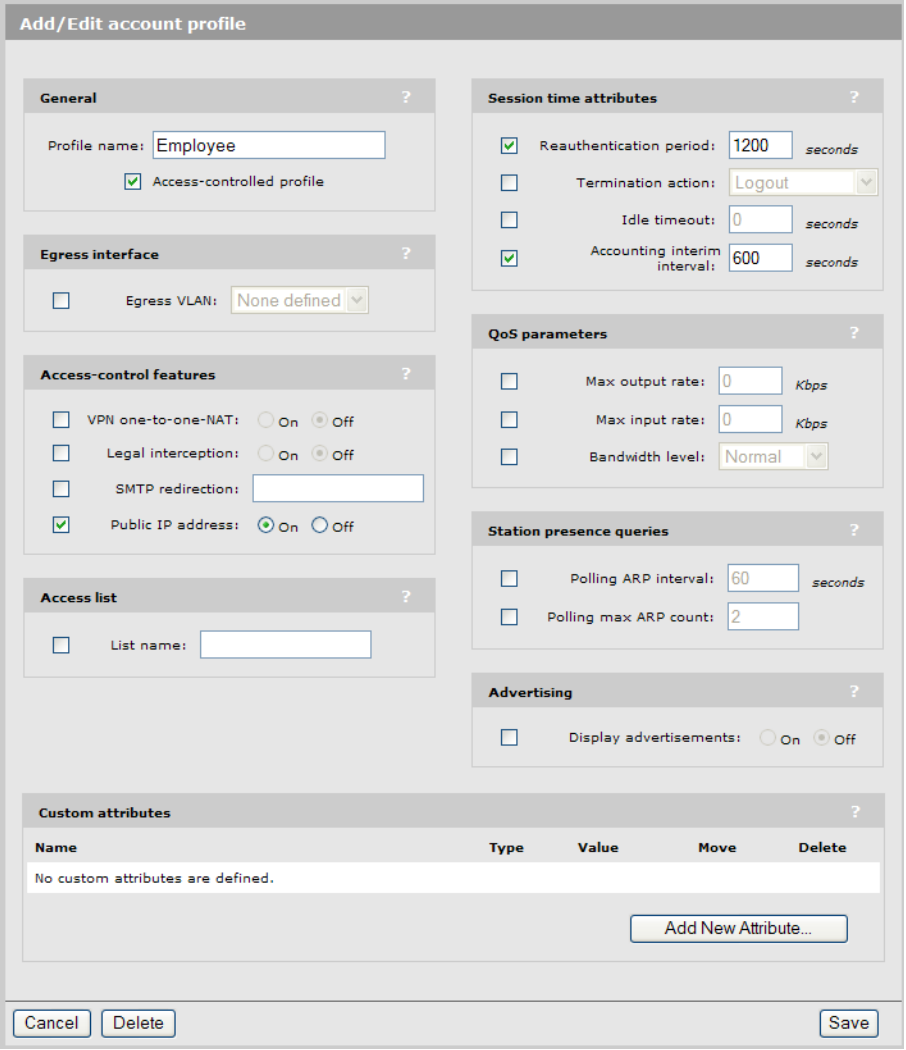
The best way to understand how all this works is to look at an example.

Example

In this example, two user profiles (called **Employee** and **Guest**) are defined on the **Controller >> Users > Account profiles** page. The settings for each profile are shown below.

Employee profile

Sets the attributes that will be used to define employee accounts.



Add/Edit account profile

General

Profile name: Employee
☑ Access-controlled profile

Egress interface

□ Egress VLAN: None defined

Access-control features

□ VPN one-to-one-NAT: ○ On ● Off
□ Legal interception: ○ On ● Off
□ SMTP redirection:
☑ Public IP address: ● On ○ Off

Access list

□ List name:

Session time attributes

☑ Reauthentication period: 1200 seconds
□ Termination action: Logout
□ Idle timeout: 0 seconds
☑ Accounting interim interval: 600 seconds

QoS parameters

□ Max output rate: 0 Kbps
□ Max input rate: 0 Kbps
□ Bandwidth level: Normal

Station presence queries

□ Polling ARP interval: 60 seconds
□ Polling max ARP count: 2

Advertising

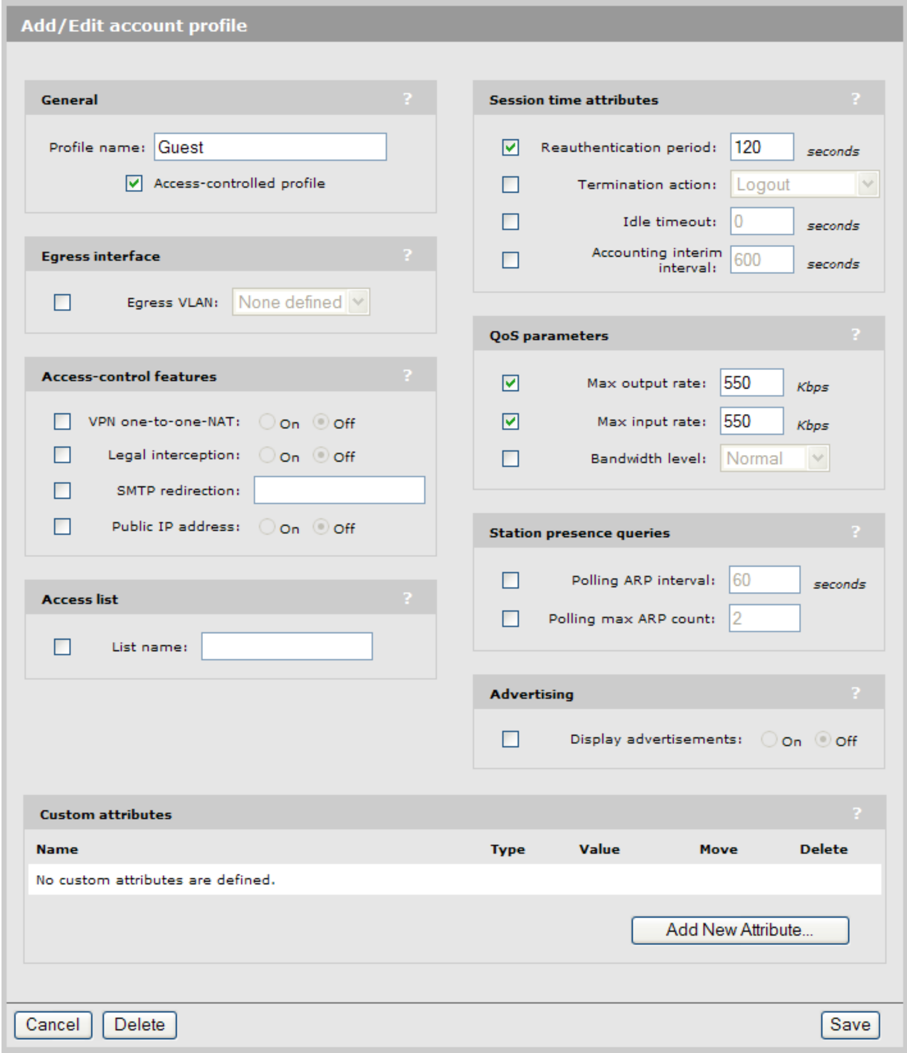
□ Display advertisements: ○ On ● Off

Custom attributes

Name	Type	Value	Move	Delete
No custom attributes are defined.				

Guest profile

Sets the attributes that will be used to define guest accounts.



Add/Edit account profile

General

Profile name: Guest

☑ Access-controlled profile

Egress interface

□ Egress VLAN: None defined

Access-control features

□ VPN one-to-one-NAT: ○ On ● Off

□ Legal interception: ○ On ● Off

□ SMTP redirection:

□ Public IP address: ○ On ● Off

Access list

□ List name:

Session time attributes

☑ Reauthentication period: 120 seconds

□ Termination action: Logout

□ Idle timeout: 0 seconds

□ Accounting interim interval: 600 seconds

QoS parameters

☑ Max output rate: 550 Kbps

☑ Max input rate: 550 Kbps

□ Bandwidth level: Normal

Station presence queries

□ Polling ARP interval: 60 seconds

□ Polling max ARP count: 2

Advertising

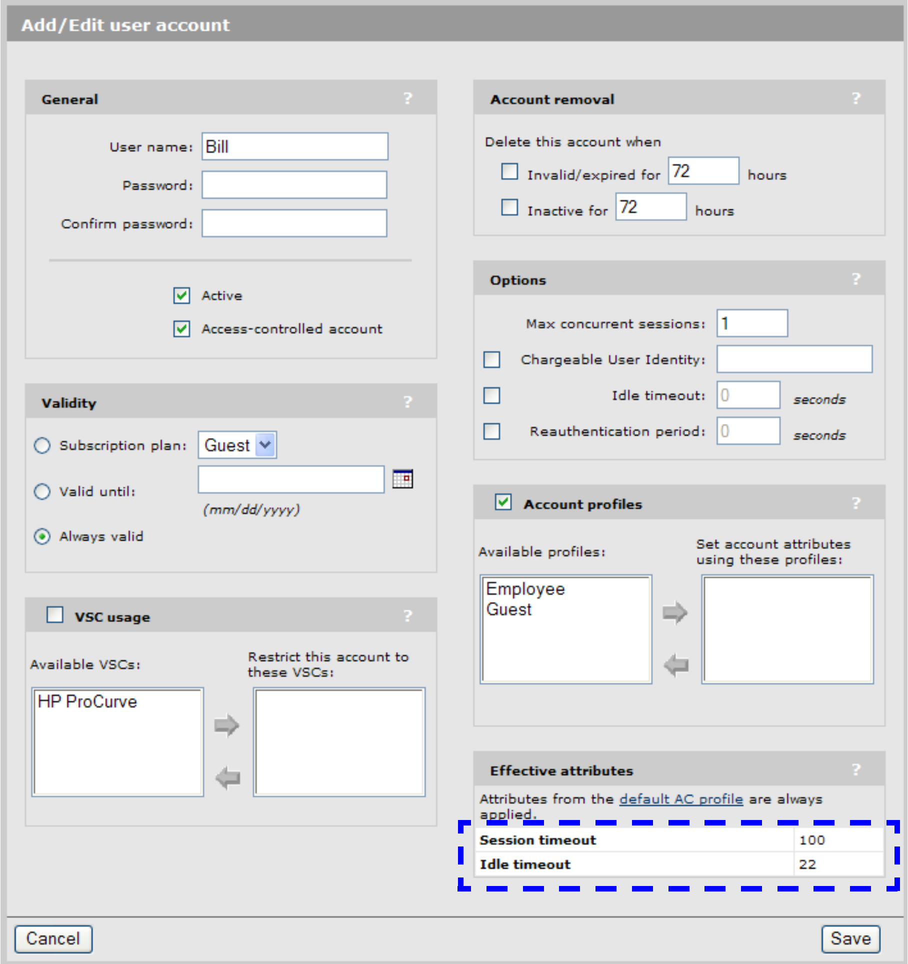
□ Display advertisements: ○ On ● Off

Custom attributes

Name	Type	Value	Move	Delete
No custom attributes are defined.				

Once account profiles have been defined, user accounts can be created.

The following sample page shows the initial configuration of a user account for an employee named **Bill**. Notice that before any account profile is assigned, the **Effective attributes** box shows a couple of active attributes: **Idle timeout**, and **Session timeout**.



Add/Edit user account

General

User name: Bill
Password:
Confirm password:

☑ Active
☑ Access-controlled account

Validity

○ Subscription plan: Guest
○ Valid until: (mm/dd/yyyy)
● Always valid

□ **VSC usage**

Available VSCs: HP ProCurve
Restrict this account to these VSCs:

Account removal

Delete this account when
□ Invalid/expired for 72 hours
□ Inactive for 72 hours

Options

Max concurrent sessions: 1
□ Chargeable User Identity:
□ Idle timeout: 0 seconds
□ Reauthentication period: 0 seconds

☑ **Account profiles**

Available profiles: Employee, Guest
Set account attributes using these profiles:

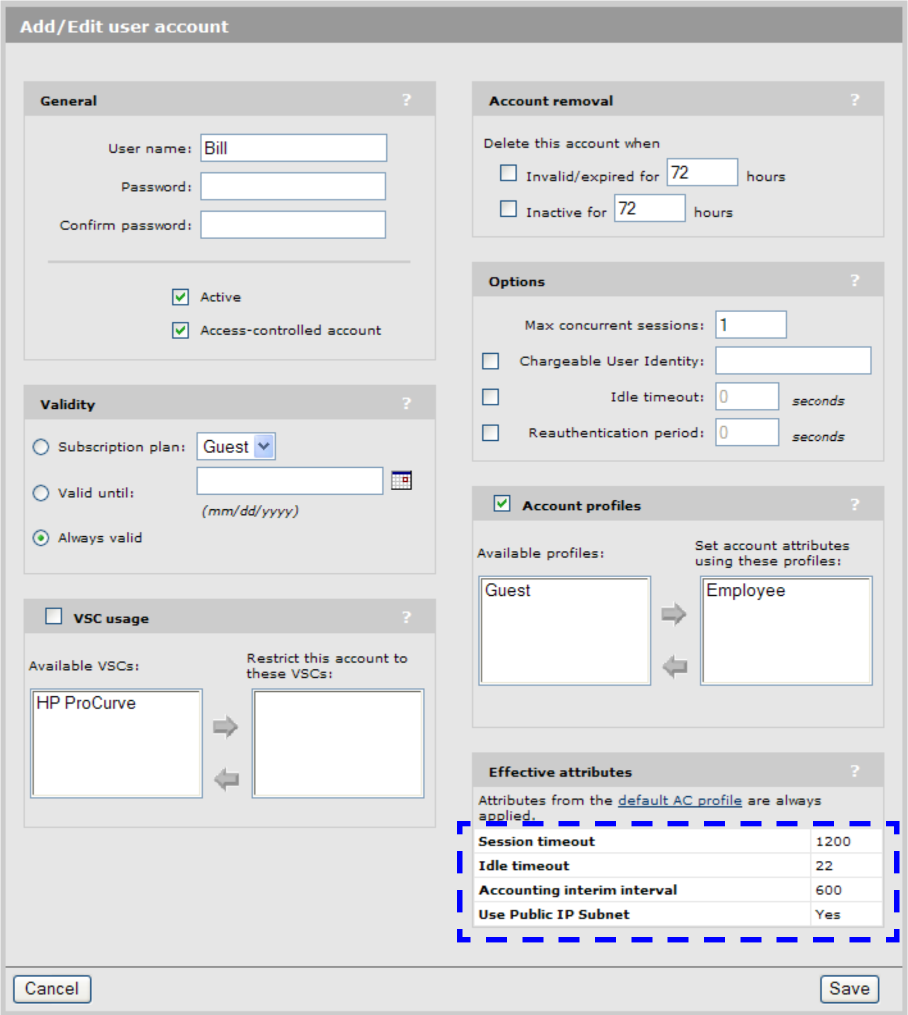
Effective attributes

Attributes from the default AC profile are always applied.

Session timeout	100
Idle timeout	22

These attributes come from the **Default AC** profile. Attributes from this profile are automatically assigned to all access-controlled user accounts. To customize the attributes for the **Default AC** profile you need to select **Controller >> Public access > Attributes**. (The default AC profile cannot be edited via the **Controller >> Users > Account profiles** page.) See *About the Default AC profile on page 10-27*.

To complete the configuration of Bill's account, the **Employee** account profile is assigned, which adds additional attributes to the **Effective attributes** list.



Add/Edit user account

General

User name: Bill
Password:
Confirm password:

☑ Active
☑ Access-controlled account

Validity

○ Subscription plan: Guest
○ Valid until: (mm/dd/yyyy)
● Always valid

☐ VSC usage

Available VSCs: HP ProCurve
Restrict this account to these VSCs:

Account removal

Delete this account when
☐ Invalid/expired for 72 hours
☐ Inactive for 72 hours

Options

Max concurrent sessions: 1
☐ Chargeable User Identity:
☐ Idle timeout: 0 *seconds*
☐ Reauthentication period: 0 *seconds*

☑ Account profiles

Available profiles: Guest
Set account attributes using these profiles: Employee

Effective attributes

Attributes from the default AC profile are always applied.

Session timeout	1200
Idle timeout	22
Accounting interim interval	600
Use Public IP Subnet	Yes

Retrieving attributes from a RADIUS server

When you are using a RADIUS server to authenticate users, attributes can be set in individual user accounts to define the same settings that are available via the local user profiles. These settings are accomplished by adding both standard RADIUS attributes (*User attribute definitions on page 15-20*) and one or more instances of the Colubris AV-Pair (user) attribute (*Colubris AV-Pair - User attribute values on page 15-67*) to the appropriate RADIUS user accounts.

ProCurve Manager IDM support

HP ProCurve Manager (PCM) is a network management solution for managing HP ProCurve devices. HP ProCurve Identity Driven Manager (IDM) is a plug-in to HP ProCurve Manager Plus that enables dynamic provisioning of network security and performance settings based on user, device, location, time, and endpoint posture.

IDM can be used to define settings in a user’s RADIUS account that the controller will retrieve when the user is authenticated, and then apply to the user’s wireless session. The following PCM settings are supported.

PCM setting	**Description**	**Supported on VSCs that are ...**
Tagged VLAN (The Untagged VLAN setting is not supported.)	Specifies a VLAN number only. Names are not supported.	Access controlled and Non-access-controlled
QoS	Sets the bandwidth level for the user’s account. PCM numerical values are mapped to the user account as follows: 6, 7 = VERY-HIGH 4, 5 = HIGH 0, 3 = NORMAL 1, 2 = LOW	Access controlled and Non-access-controlled Requires that the Bandwidth control feature is enabled on the controller (**Controller >> Network > Bandwidth control)** when access-controlled VSCs are used.
Ingress/Egress rate limit	Sets the user’s ingress and egress data rates in bytes.	Access controlled
Network resources access rule	Sets a custom access control list for the user.	Access controlled

Important

When using PCM to configure settings in a user’s RADIUS account, you should **not** use Colubris AV-Pair values to define other settings in the same account. Standard RADIUS attributes can be used however.

User attribute definitions

The following attributes are supported for user accounts.

Access Request

- Acct-Session-Id
- Called-Station-Id
- Calling-Station-Id
- CHAP-Challenge
- CHAP-Password
- Chargeable User Identity (CUI)
- Connect-Info
- EAP-Message
- Framed-IP-Address
- Framed-MTU
- NAS-Identifier
- NAS-Ip-Address
- NAS-Port
- NAS-Port-Type
- Message-Authenticator
- Service-Type
- State
- User-Name
- User-Password
- Vendor-specific (Microsoft)
  - MSCHAP-Challenge
  - MSCHAP-Response
  - MSCHAPv2-Response
- Vendor-specific (WISPr)
  - Location-Name
  - Location-ID
  - Logoff-url

Access Accept

- Acct-Interim-Interval
- Chargeable User Identity (CUI)
- Class
- EAP-Message
- Idle-Timeout
- Reply-Message
- Session-Timeout
- Termination-Action
- Tunnel-Medium-Type
- Tunnel-Private-Group-ID
- Tunnel-Type
- Vendor-specific (Microsoft)
  - MS-MPPE-Recv-Key
  - MS-MPPE-Send-Key
- Vendor-specific (Colubris)
  - Colubris AV-Pair
  - Colubris-Intercept

Access Reject

- EAP-Message
- Vendor-specific (Microsoft)
  - MSCHAP-Error
- Reply-Message

Access Challenge

- EAP-Message
- State

Accounting Response

No attributes are supported.

Accounting Request

- Acct-Authentic
- Acct-Delay-Time
- Acct-Event-Timestamp
- Acct-Session-Id
- Acct-Status-Type
- Calling-Station-Id
- Called-Station-Id
- Chargeable User Identity (CUI)
- Class
- Framed-IP-Address
- NAS-Identifier
- NAS-Ip-Address
- NAS-Port
- NAS-Port-Type
- User-Name
- Vendor-specific (WISPr)
  - Location-Name
  - Location-ID
  - Logoff-url
- Acct-Session-Time
- Acct-Input-Gigawords
- Acct-Input-Octets
- Acct-Input-Packets
- Acct-Output-Gigawords
- Acct-Output-Octets
- Acct-Output-Packets
- Acct-Terminate-Cause

Access request

Acct-Session-Id
(32-bit unsigned integer)
Random value generated per authentication by the controller.

Called-Station-Id
(string)
By default, this is set to the MAC address of the controller wireless/LAN port in IEEE format. For example: 00-02-03-5E-32-1A. To use the MAC address of the Internet port, you must edit the config file and change the setting of **radius-called-station-id-port** to **WAN** in the <ACCESS-CONTROLLER> section. If location-aware authentication is enabled for the VSC the user is logged into, then this value is defined by the VSC.

Calling-Station-Id
(string)
The MAC address of the user's station in IEEE format. For example: 00-02-03-5E-32-1A.

CHAP-Challenge
(string)
Randomly generated. As defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to CHAP. Length = 19 bytes.

CHAP-Password
(string)
The user's password. Encoded as defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to CHAP.

Chargeable User Identity (CUI)
(string)
As defined in RFC-4372. The CUI is used to associate a unique identifier with a user so that the user can be identified (for billing, authentication or other purposes) when roaming outside of their home network.

Connect-Info
(string)
The string "HTTPS" or "IEEE802.1X".

EAP-Message
(string)
As defined in RFC 2869. Only present when the authentication method for the RADIUS profile is set to EAP-MD5.

Framed-IP-Address
(32-bit unsigned integer)
IP Address as configured on the client station (if known by the controller).

Framed-MTU
(32-bit unsigned integer)
Hard-coded value of 1496. The value is always four bytes lower than the wireless MTU maximum which is 1500 bytes in order to support IEEE802dot1x authentication.

NAS-Identifier
(string)
The NAS ID set on the **Controller >> Authentication > RADIUS profiles > Add New Profile** page for the RADIUS profile being used.

NAS-Ip-Address
(32-bit unsigned integer)
The IP address of the port the controller is using to communicate with the RADIUS server.

NAS-Port
(32-bit unsigned integer)
A port number, other than 0.

NAS-Port-Type
(32-bit unsigned integer)
Always set to 19, which represents WIRELESS_802_11.

Message-Authenticator
(string)
As defined in RFC 2869. Always present even when not doing an EAP authentication. length = 16 bytes.

Service-Type
(32-bit unsigned integer)
RADIUS service type.

State
(string)
As defined in RFC 2865.

User-Name
(string)
The username assigned to the user or a device when using MAC authentication.

User-Password
(string)
The password supplied by a user or device when logging in. Encoded as defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to PAP.

Vendor-specific (Microsoft)
HP supports the following Microsoft vendor-specific attributes.

MSCHAP-Challenge
(string)
As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1 or MSCHAPv2. Length = 8 bytes.

MSCHAP-Response
(string)
As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1. Length = 49 bytes.

MSCHAPv2-Response
(string)
As defined in RFC 2759. Only present when the authentication method for the RADIUS profile is set to MSCHAPv2. Length = 49 bytes.

Vendor-specific (WISPr)

HP supports the following Wi-Fi Alliance vendor-specific attributes.

Location-Name
The WISPr location name assigned to the controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 2
- Attribute type: A string in the format: `wispr-location-name=`*`location_name`*

Location-ID
The WISPr location identifier assigned to the controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 1
- Attribute type: A string in the format: `wispr-location-id=`*`location_id`*

Logoff-url
The WISPr log-off URL that will be used.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 3
- Attribute type: A string in the format: `wispr-logoff-url=`*`URL`*

Access accept

Acct-Interim-Interval

(32-bit unsigned integer)
When present, enables the transmission of RADIUS accounting requests of the Interim Update type. Specify the number of seconds between each transmission.

Chargeable User Identity (CUI)

(string)
As defined in RFC-4372. The CUI is used to associate a unique identifier with a user so that the user can be identified (for billing, authentication or other purposes) when roaming outside of their home network.

Class

(string)
As defined in RFC 2865. Multiple instances are supported.

EAP-Message

(string)
Only supported when authentication is EAP-MD5. Note that the content will not be read as the RADIUS Access Accept overrides whatever indication is contained inside this packet.

Idle-Timeout
(32-bit unsigned integer)
Maximum idle time in seconds allowed for the user. Once reached, the user session is terminated with termination-cause IDLE-TIMEOUT. Omitting the attribute or specifying 0 disables the feature.

Reply-Message
(string)
This string (as defined in RFC 2865) is recorded and passed as is to the GetRadiusReplyMessage() asp function. Multiple string are supported to a maximum length of 252 bytes.

Session-Timeout
(32-bit unsigned integer)
Maximum time a session can be active. The user must re-authenticate when this timer expires. Omitting this attribute or specifying **0** disables the feature.

Termination-Action
(32-bit unsigned integer)
As defined by RFC 2865. If set to **1**, a new Access Request is sent. If an Access Accept is returned, the controller then extends the user's session timeout, and if applicable, session quota, according the value returned by the RADIUS server.

Tunnel-Medium-Type
(24-bit unsigned integer)
Only used when assigning a specific VLAN number to a user. In this case it must be set to 802. The **tag** field for this attribute must be set to **0**.

Tunnel-Private-Group-ID
(string)
Only used when assigning a specific VLAN number to a user. In this case it must be set to the VLAN ID. The **tag** field for this attribute must be set to **0**.

Tunnel-Type
(24-bit unsigned integer)
Only used when assigning a specific VLAN number to a user. In this case it must be set to 13 (VLAN). The **tag** field for this attribute must be set to **0**.

Vendor-specific (Microsoft)
HP supports the following Microsoft vendor-specific attributes.

MS-MPPE-Recv-Key
(string)
Use to validate a PMKID inside a 802.11 association request, send EAPOL keys to a wireless station when a VSC has 802.1X WEP enabled, and to perform a four-way handshake.

MS-MPPE-Send-Key
(string)
Use to validate a PMKID inside a 802.11 association request, send EAPOL keys to a wireless station when a VSC has 802.1X WEP enabled, and to perform a four-way handshake.

Vendor-specific (Colubris)
(string)

Colubris AV-Pair
The Colubris AV-Pair is a HP a vendor-specific attribute defined by HP to support configuration of user session settings. This attribute conforms to RADIUS RFC 2865. You may need to define this attribute on your RADIUS server (if it is not already present) using the following values:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 0
- Attribute type: A string in the following format `<keyword>=<value>`

Multiple instances of the Colubris AV-Pair can be defined in a RADIUS account to configure a variety of settings. For a complete list of all supported settings, see *Colubris AV-Pair - Site attribute values on page 15-33*.

Colubris-Intercept
This attribute is used to enable/disable the interception and redirection of traffic for individual users. The destination for intercepted traffic is defined separately for each VSC using the **Interception** option under **VSC egress mapping.** See *VSC egress mapping on page 5-17*.

You may need to define the Colubris-Intercept attribute on your RADIUS server (if it is not already present) using the following values:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 1
- Attribute type = integer with one of the following values:
  - **0**: Do not intercept user traffic.
  - **1**: Intercept user traffic and redirect it to the destination defined by the **Intercepted** option under **VSC egress mapping** in the VSC to which the user is connected.

Access reject

EAP-Message
(string)
Only supported when authentication is EAP-MD5. Note that the content will not be read as the RADIUS Access Reject overrides whatever indication is contained inside this packet.

Vendor-specific (Microsoft)
HP supports the following Microsoft vendor-specific attributes.

MSCHAP-Error
(string)
A MSCHAP specific error as defined by RFC 2433.

Reply-Message
(string)
This string (as defined in RFC 2865) is recorded and passed as is to the GetRadiusReplyMessage() asp function. Multiple string are supported to a maximum length of 252 bytes.

Access challenge

EAP-Message
(string)
One or more occurrences of this attribute is supported inside the same packet. All occurrences are concatenated and transmitted to the IEEE802dot1x client as is. As defined in RFC 2869.

State
(string)
As defined in RFC 2865.

Accounting request

Accounting start, stop. and interim-update

Acct-Authentic
(32-bit unsigned integer)
Always set to 1 which means RADIUS.

Acct-Delay-Time
(32-bit unsigned integer)
As defined in RFC 2869.

Acct-Event-Timestamp
(32-bit unsigned integer)
As defined in RFC 2869.

Acct-Session-Id
(32-bit unsigned integer)
Random value generated by the controller.

Acct-Status-Type
(32-bit unsigned integer)
Supported value are: Start (1), Interim Update (3), and Stop (2).

Calling-Station-Id
(string)
The MAC address of the user’s computer in IEEE format. For example: 00-02-03-5E-32-1A.

Called-Station-Id
(string)
The MAC address of the controller LAN port in IEEE format. For example: 00-02-03-5E-32-1A.

Chargeable User Identity (CUI)
(string)
As defined in RFC-4372. The CUI is used to associate a unique identifier with a user so that the user can be identified (for billing, authentication or other purposes) when roaming outside of their home network.

Class
(string)
As defined in RFC 2865. Multiple instances are supported.

Framed-IP-Address
(32-bit unsigned integer)
IP Address of the user's computer.

NAS-Identifier
(string)

The NAS ID for the RADIUS profile being used.

NAS-Ip-Address
(32-bit unsigned integer)
The IP address of the port the controller is using to communicate with the RADIUS server.

NAS-Port
(32-bit unsigned integer)
A virtual port number starting at 1. Assigned by the controller.

NAS-Port-Type
(32-bit unsigned integer)
Always set to 19, which represents WIRELESS_802_11.

User-Name
(string)
The username assigned to the user or to a device when using MAC authentication.

Vendor-specific (WISPr)
HP supports the following Wi-Fi Alliance vendor-specific attributes.

Location-Name
The WISPr location name assigned to the controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 2
- Attribute type: A string in the format: `wispr-location-name=`*`location_name`*

Location-ID
The WISPr location identifier assigned to the controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 1
- Attribute type: A string in the format: `wispr-location-id=`*`location_id`*

Logoff-url
The WISPr log-off URL that will be used.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 3
- Attribute type: A string in the format: `wispr-logoff-url=`*`URL`*

Accounting stop. and interim-update

Acct-Session-Time
(32-bit unsigned integer)
Number of seconds this session since this session was authenticated. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Acct-Input-Gigawords
(32-bit unsigned integer)
High 32-bit value of the number of octets/bytes received by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Acct-Input-Octets
(32-bit unsigned integer)
Low 32-bit value of the number of octets/bytes received by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Acct-Input-Packets
(32-bit unsigned integer)
Low 32-bit value of the number of packets/bytes received by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Acct-Output-Gigawords
(32-bit unsigned integer)
High 32-bit value of the number of octets/bytes sent by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**. As defined in 2869.

Acct-Output-Octets
(32-bit unsigned integer)
Low 32-bit value of the number of octets/bytes sent by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Acct-Output-Packets
(32-bit unsigned integer)
Low 32-bit value of the number of packets/bytes sent by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Accounting stop only

Acct-Terminate-Cause
(32-bit unsigned integer)
Termination cause for the session See RFC 2866 for possible values. Only present when **Acct-Status-Type** is **Stop**.

ID	Cause	Notes
1	User Request	Supported. Indicates that the user logged out.
2	Lost Carrier	Supported. Indicates that the client station is no longer alive.
3	Lost Service	Supported. When location-aware is enabled and a user switches access points, the controller re-authenticates the user. If authentication fails due to timeout, this code is returned.
4	Idle Timeout	Supported. User exceeded the idle timeout value defined for the session.
5	Session Timeout	Supported. User exceeded maximum time defined for the session.
6	Admin Reset	Supported. User session was terminated by the controller administrator via SNMP or the management tool.
7	Admin Reboot	Not Supported. (not applicable)
8	Port Error	Supported. If two users are detected using the same IP address, both are logged out with this error. Another cause is if an error is encountered in an access list definition. For example, an invalid host was specified.
9	NAS Error	Not Supported. (not applicable)
10	NAS Request	Not Supported. (not applicable)
11	NAS Reboot	Supported. User was logged out because the controller was restarted.
12	Port Unneeded	Not Supported. (not applicable)
13	Port Preempted	Supported. When a user switches AP or SSID with incompatible configurations (authentication type), they are logged out with this code. Also if the user changes authentication type of the same AP.
14	Port Suspended	Not Supported. (not applicable)
15	Service Unavailable	Not Supported. (not applicable)
16	Callback	Not Supported. (not applicable)

ID	Cause	Notes
17	User Error	Supported. An 802.1X client initiated a second authentication request for a user, and this request was refused.
18	Host Request	Not Supported. (not applicable)
0x8744 (34628 decimal)	Termination	HP-specific termination cause.

Accounting response

No attributes are supported.

Administrator attributes

If you want to support multiple administrator names and passwords, you must use a RADIUS server to manage them. The controller only supports a single admin name and password internally (defined on the **Controller >> Management > Management tool** page).

Note

Improper configuration of the administrator profile could expose the controller to access by any user with a valid account. The only thing that distinguishes an administrative account from that of a standard user account is the setting of the service type. Make sure that a user is not granted access if service type is not Administrative, This is the reason why it may be prudent to use a different RADIUS server to handle administrator logins. This practice reduces the risk of a bad configuration on the RADIUS server side creating a security hole.

The following attributes are supported for administrator accounts.

Access Request

- Framed-MTU
- NAS-Identifier
- User-Name
- Service-Type
- Vendor-specific (Microsoft)
  - MSCHAP-Challenge
  - MSCHAP-Response

Access Accept

- Vendor-specific (Colubris)

Access Reject

No attributes are supported.

Access Challenge

No attributes are supported.

Accounting Request

No attributes are supported.

Accounting Response

No attributes are supported.

Access request

Framed-MTU
(32-bit unsigned integer)
Hard-coded value of 1496. The value is always four bytes lower than the wireless MTU maximum which is 1500 bytes in order to support IEEE802dot1x authentication.

NAS-Identifier
(string)
The NAS ID set on the **Controller >> Authentication > RADIUS profiles > Add New Profile** page for the RADIUS profile being used.

User-Name
(string)
The username assigned to the administrator.

Service-Type

(32-bit unsigned integer)
As defined in RFC 2865. Set to a value of 6, which indicates SERVICE_TYPE_ADMINISTRATIVE.

Vendor-specific (Microsoft)

HP supports the following Microsoft vendor-specific attributes.

MSCHAP-Challenge
(string)
As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1 or MSCHAPv2. Length = 8 bytes.

MSCHAP-Response
(string)
As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1. Length = 49 bytes.

Access accept

Vendor-specific (Colubris)

(string)

Colubris AV-Pair
HP has defined a vendor-specific attribute to support configuration of user session settings. This attribute conforms to RADIUS RFC 2865. You may need to define this attribute on your RADIUS server (if it is not already present) using the following values:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 0
- Attribute type: A string in the following format `<keyword>=<value>`

Multiple instances of the Colubris AV-Pair can be defined in a RADIUS account to configure a variety of settings. For a complete list of all supported attributes, see *Colubris AV-Pair - Administrator attribute values on page 15-74*.

Colubris AV-Pair - Site attribute values

Site values let you define global settings that affect operation of the public access network and all user accounts.

Each Colubris AV-Pair value is specified using the following format: `<keyword>=<value>`

The following table lists all supported site value keywords and provides a link to complete descriptions for each one.

Colubris AV-Pair keyword	For more information see

access-list
use-access-list=uselistname
use-access-list-unauth=uselistname
default-user-access-list
	Access list on page 15-34

configuration-file	*Configuration file on page 15-44*
ssl-certificate	*Custom SSL certificate on page 15-44*
custom-pages	*Loading custom pages from an archive on page 15-45*
login-page transport-page session-page fail-page logo	*Loading individual pages on page 15-46* ***These keywords have been deprecated.*** *If you are creating a new installation, use the* **custom-pages** keyword or the *site file archive feature on the* ***Controller >> Public access > Web content*** *page. If you are upgrading from a previous release, your existing configuration will still work.*
welcome-url login-err goodbye-url	*Hosting pages on an external Web server on page 15-47*
login-url	*Remote login page on page 15-47*
messages	*Custom message file on page 15-51*
default-user-acct-interim-update	*Default user interim accounting update interval on page 15-51*
default-user-bandwidth-level	*Default user bandwidth level on page 15-51*
default-user-idle-timeout	*Default user idle timeout on page 15-52*
default-user-one-to-one-nat	*Default user one-to-one NAT on page 15-53*
default-user-use-public-ip-subnet	*Default user public IP address on page 15-54*
default-user-session-timeout	*Default user session timeout on page 15-54*
default-user-smtp-redirect	*Default user SMTP server on page 15-54*

Colubris AV-Pair keyword	For more information see
default-user-welcome-url default-user-goodbye-url	*Default user URLs on page 15-55*
default-user-max-input-packets default-user-max-output-packets default-user-max-total-packets default-user-max-input-octets default-user-max-output-octets default-user-max-total-octets	*Default user quotas on page 15-52*

default-user-max-input-rate=value
default-user-max-output-rate=value
	Default user data rates on page 15-53

http-proxy-upstream	*HTTP proxy upstream on page 15-55*
ipass-login-url	*IPass login URL on page 15-56*
mac-address	*Global MAC-based authentication on page 15-56*
primary-web-server-status-url secondary-web-server-status-url primary-web-server-status-url secondary-web-server-status-url	*Multiple login servers on page 15-57*
redirect-url	*Redirect URL on page 15-59.*
ssl-noc-certificate ssl-noc-ca-certificate	*NOC authentication on page 15-62.*
wispr-login-url wispr-abort-login-url redirect-page access-procedure	*HP WISPr support on page 15-62.*
dnat-server primary-dnat-server-status-url secondary-dnat-server-status-url	*Traffic forwarding (dnat-server) on page 15-63.*

Access list

Access lists enable you to create public areas on your network that all users can browse, and protected areas that are restricted to specific user accounts or groups.

Each access list is a set of rules that governs how the controller controls access to network resources. You can create multiple access lists, each with multiple rules to manage the traffic on your public access network.

Default setting

By default no access lists are defined. This means that:

- If authentication (802.1X, WPA, HTML, MAC) is not enabled on a VSC, all users that connect to the VSC have access to the protected network.
- If authentication (802.1X, WPA, HTML, MAC) is enabled on a VSC, then:
  - Unauthenticated users only reach the public access login page. Access to the protected network is blocked, except for **register.procurve.com** which enables product registration.
  - Authenticated users have access to the protected network.

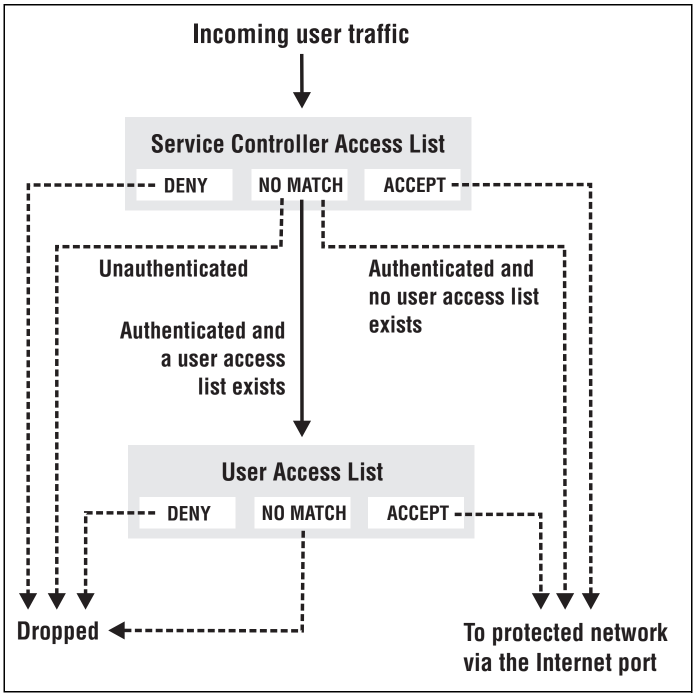
How the access lists work

Access lists can be applied on the controller (site access lists), in which case they affect all user traffic, or individually for each user account (user access lists).

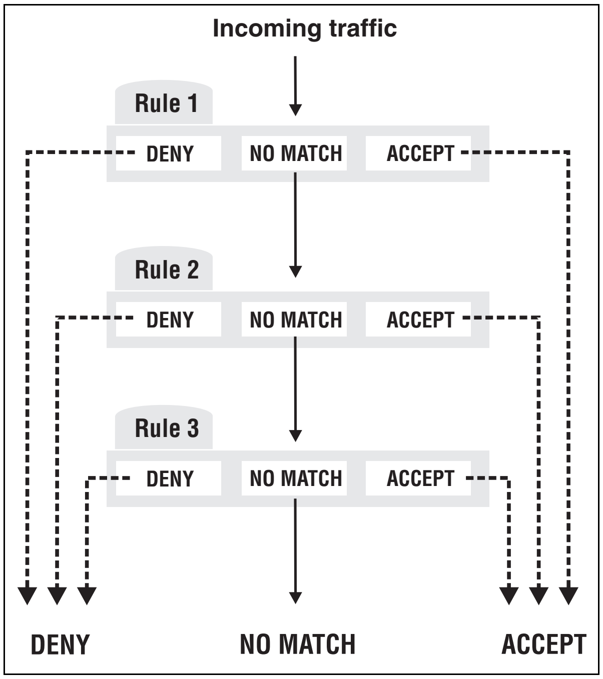
Incoming traffic cascades through the currently active lists. Traffic that is accepted or denied by a list is not available to the list that follows it. Traffic that passes through all lists without being accepted or denied is dropped.

- Access list rules that **accept** traffic are: ACCEPT, ACCEPT-MORE, DNAT-SERVER, and REDIRECT.
- Access list rules that **deny** traffic are: DENY and WARN.

The following diagram illustrates how incoming traffic from a user session is processed by the access list mechanism.


Incoming user traffic
Service Controller Access List
DENY
NO MATCH
ACCEPT
Unauthenticated
Authenticated and no user access list exists
Authenticated and a user access list exists
User Access List
DENY
NO MATCH
ACCEPT
Dropped
To protected network via the Internet port

Within each access list, traffic cascades through the list rules in a similar manner.



Access list rules are numbered according to the order in which they are specified. Only data that is not accepted or denied by a rule is available to the next rule in the list.

Accounting support

Each rule in an access list can be configured with an account name for billing purposes. The controller sends billing information based on the amount of traffic matched by the rule.

This lets you create rules to track and bill traffic to particular destinations.

Tips on using the access list

With certificates

- If you replaced the default SSL certificate on the controller with one signed by a well-known CA, you should define the access list to permit access to the CA certificate for all non-authenticated users. This enables the user's browser to verify that the certificate is valid without displaying any warning messages.
- Users may have configured their Web browsers to check all SSL certificates against the Certificate Revocation List (CRL) maintained by the CA that issued the certificate. The location of the CRL may be configured in the browser, or embedded in the certificate. The access list should be configured to permit access to the CRL, otherwise the user's browser times out before displaying the login page.

Remote login page

If you are using the remote login page feature, make sure that access to the Web server hosting the login page is granted to all unauthenticated users via the site access list.

SMTP redirect

If an unauthenticated user establishes a connection to their email server, the SMTP redirect feature will not work once the user logs in. The user's email is still sent to the original email server.

To avoid this, do not use an access list to open TCP port 25 for unauthenticated users.

Critical access list definitions (such as for a remote login page, certificates) should not use the OPTIONAL setting because if these definitions fail to initialize there is no indication in the log.

Defining access lists

Access lists are defined by adding the following Colubris AV-Pair value string to the RADIUS profile for a controller or to the local list (**Public access > Attributes** page).

```
access-list=value
```

Each value string defines one rule. Up to 99 rules can be defined for an access list.

All rules that make up an access list must be initialized without error for the list to be active. (You can force the controller to ignore initialization errors on a rule-by-rule basis by using the OPTIONAL parameter.)

You can define up to 32 access lists.

Activating site access lists

When an access list is activated on the controller, it applies to all access controlled user traffic handled by the controller.

Access lists are activated by adding the following Colubris AV-Pair value string to the RADIUS profile for a controller or to the local list (**Public access > Attributes** page).

```
use-access-list=uselistname
```

Only one access list can be active on the controller. This list must be initialized without an error.

It is possible to set an access list to apply only for unauthenticated users by specifying the following value string:

```
use-access-list-unauth=uselistname
```

User access lists

Access lists can also be activated on a per-user basis by configuring the appropriate settings for each user account. See *Access list on page 15-67* for more information.

A default access list can defined by adding the following Colubris AV-Pair value string to the RADIUS profile for a controller or to the local list (**Public access > Attributes** page). This defines the access list to use for all users whose profiles do not contain an access list value.

```
default-user-access-list=uselistname
```

Syntax

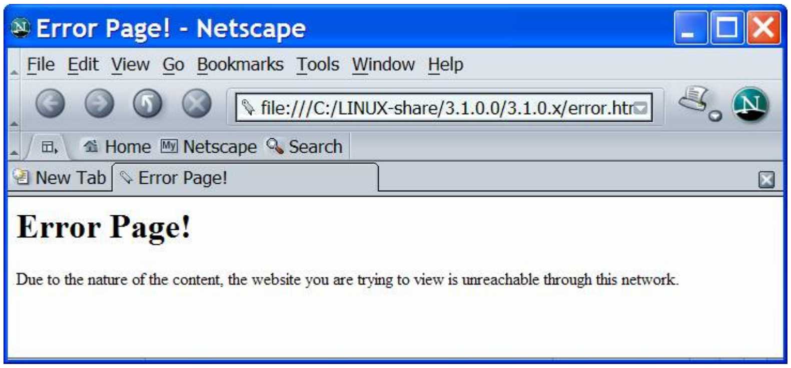
```
access-list=
listname[,OPTIONAL],action,protocol,address,port[,account[,interval]]

use-access-list=uselistname

default-user-access-list=uselistname

use-access-list-unauth=uselistname
```

Note You can use spaces as separators instead of commas.

Where:

Parameter	**Description**
listname	Specify a name (up to 32 characters long) to identify the access list this rule applies to. If a list with this name does not exist, a new list is created. If a list with this name exists, the rule is added to it.
uselistname	Specify the name of an existing access list. This list is activated for the current profile. Lists are checked in the order they are activated.
OPTIONAL	Allows the access list to be activated even if this rule fails to initialize. For example, if you specify a rule that contains an *address* which cannot be resolved for some reason, the other rules that make up the access list will still be initialized. If you do not specify optional, a failed rule will cause the entire list to fail. **Critical access list definitions (such as for a remote login page, certificates) should not use the OPTIONAL setting because if these definitions fail to initialize there will be no indication in the log.**
action	Specify what action the rule takes when it matches incoming traffic. The options are: ■ ACCEPT - Allow traffic matching this rule. ■ ACCEPT-MORE - Allow traffic matching this rule and allocate extra connections (when required) to enable users to connect with the specified *address*. By default the controller allows up to 200 TCP or UDP connections per authenticated or unauthenticated user. If a user has exceeded this connection limit, this parameter allows the controller to permit extra connections from the user when connecting to the specified destination. Connections are assigned from a global pool of 100 connections.

Parameter	**Description**

action
(continued)
	This can be used to make sure that users can always reach an important resource on the network. For example, the following access list definition allows additional connections as needed to any user who is trying to reach **my-web-server.com.**
	`access-list=HP,ACCEPT-MORE,all,my-web-server.com,80`
	`use-access-list=procurve`
	- `DENY` - Reject traffic matching this rule.
	- `DNAT-SERVER`: Traffic matching this rule is forwarded to the destination defined by the **dnat-server** value. See *Traffic forwarding (dnat-server) on page 15-63* for more information.
	Note: SSL traffic cannot be forwarded as this breaks SSL security during connection negotiation resulting in the connection not being established.
	- `REDIRECT`: Reject traffic matching this rule and redirect the user's Web browser to the page specified by **redirect-url**, or **login-url** if **redirect-url** is not defined. See *Redirect URL on page 15-59* for more information. For example, one use for this feature could be to block access to a popular protocol, then prompt the user for additional fees to activate support.
	- `WARN`: Reject traffic matching this rule and return an HTTP error message (which is not customizable) indicating that access to the site is not allowed by the network. For example:
	
	 Error Page! - Netscape
	File Edit View Go Bookmarks Tools Window Help
	file:///C:/LINUX-share/3.1.0.0/3.1.0.x/error.htr
	Home Netscape Search
	New Tab Error Page!
	Error Page!
	Due to the nature of the content, the website you are trying to view is unreachable through this network.

protocol	Specify the protocol to check: `tcp, udp, icmp, all`

Parameter	Description
`address`	Specify one of the following: ■ IP address or domain name (up to 107 characters in length) ■ Subnet address. Include the network mask as follows: `address/subnet mask` For example: 192.168.30.0/24 ■ Use the keyword `all` to match any address. ■ Use the wildcard symbol * to match any sequence of characters at the beginning or the end of a domain name. For example: ***.mydomain** matches any host on the domain **.mydomain**. **myhost.*** matches **myhost** at any domain. For example, **myhost.com** or **myhost.ca** ■ Use the keyword `none` if the protocol does not take an address range (ICMP for example).
`port`	Specify a specific port to check or a port range as follows: ■ `none` - Used with ICMP (since it has no ports). ■ `all` - Check all ports. ■ `1-65535[:1-65535]` - Specify a specific port or port range. **Note:** If you choose all possible protocols for an access-list definition, then you must supply all ports as well.
`account`	Specify the name of the user account the controller will send billing information to for this rule. Account names must be unique and can be up to 32 characters in length.
`interval`	Specify time between interim accounting updates. If you do not enable this option, accounting information is only sent when a user connection is terminated. Range: 5 to 99999 seconds in 15 second increments.

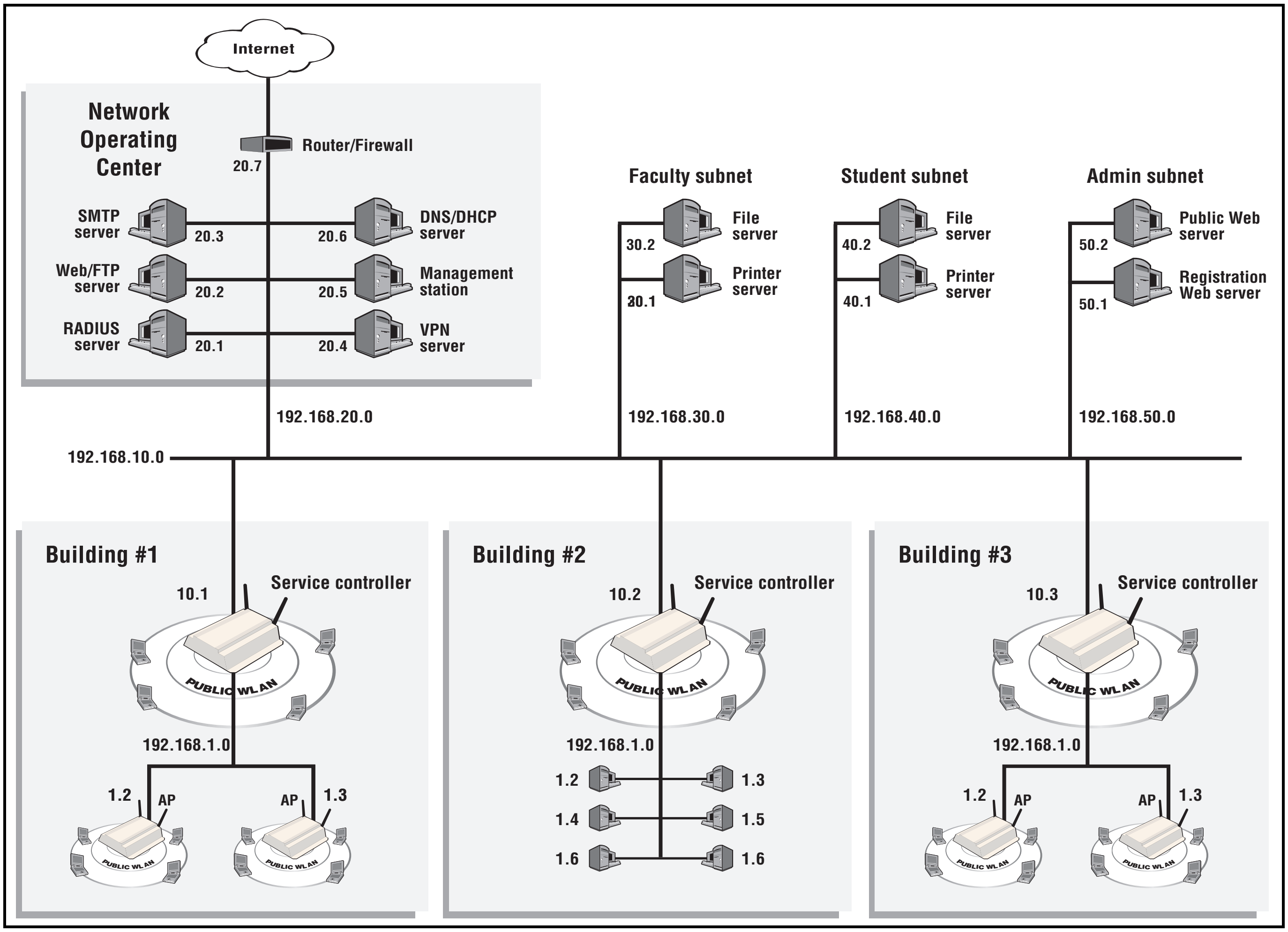
Access list example

This example illustrates how access lists can be used to control access to network resources for different groups of users at a fictitious university campus.

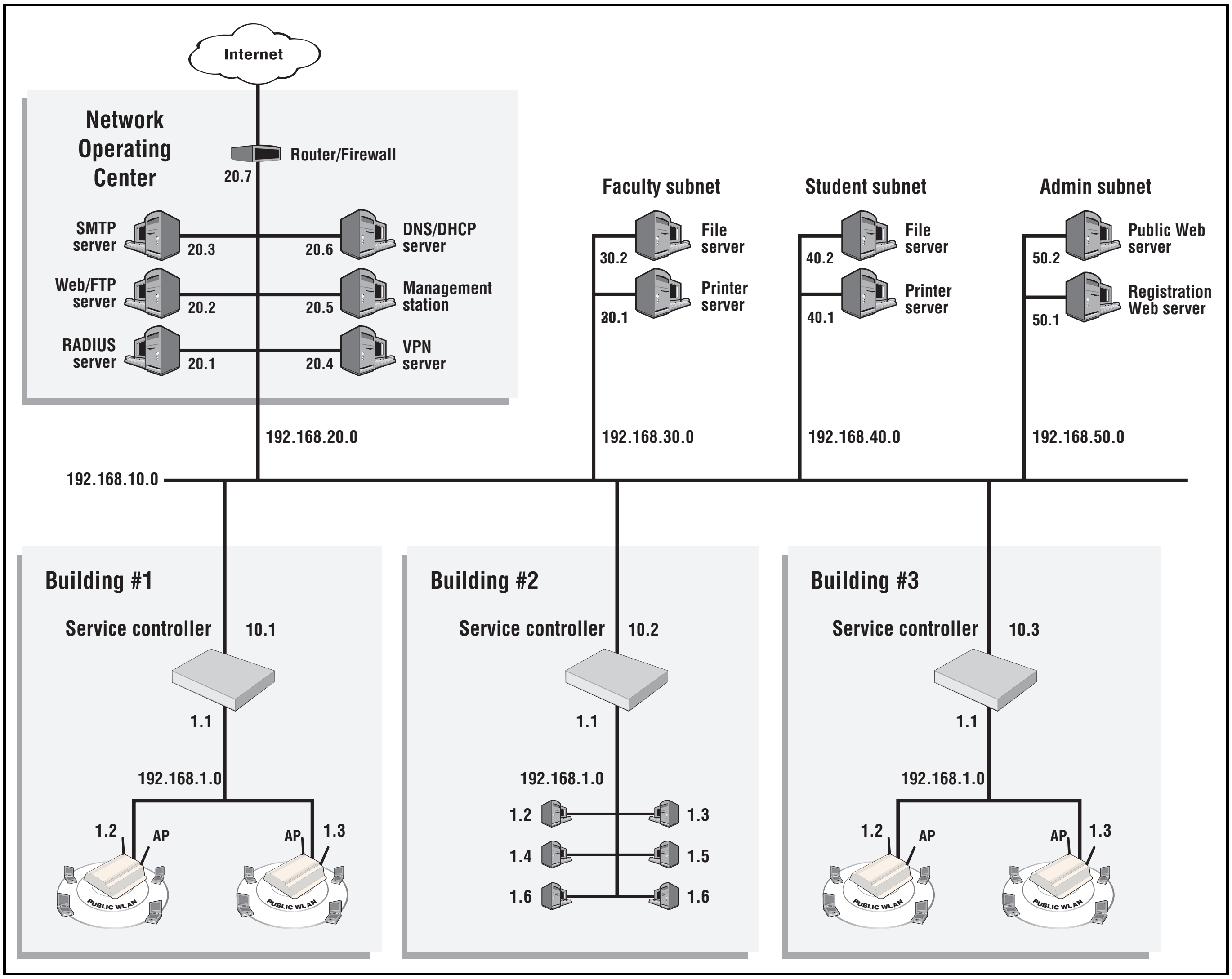
Topology

The following two topologies show potential wireless deployments for the campus using different types of HP equipment. In both cases, a RADIUS server is used to store configuration attributes for the public access network. Although the topologies are slightly different, the same access list definitions are used for both installations.

Topology 1:


Internet
Network Operating Center
Router/Firewall
20.7
SMTP server
20.3
20.6
DNS/DHCP server
Web/FTP server
20.2
20.5
Management station
RADIUS server
20.1
20.4
VPN server
Faculty subnet
File server
30.2
Printer server
30.1
Student subnet
File server
40.2
Printer server
40.1
Admin subnet
Public Web server
50.2
Registration Web server
50.1
192.168.20.0
192.168.30.0
192.168.40.0
192.168.50.0
192.168.10.0
Building #1
Service controller
10.1
PUBLIC WLAN
192.168.1.0
1.2
AP
AP
1.3
Building #2
Service controller
10.2
192.168.1.0
1.2
1.3
1.4
1.5
1.6
1.6
Building #3
Service controller
10.3
192.168.1.0
1.2
AP
AP
1.3

Topology 2:



Access list definitions

The RADIUS profile for the controller contains the following:

```
access-list=everyone,ACCEPT,tcp,192.168.50.2,80

access-list=students,ACCEPT,tcp,192.168.50.1,80,students_reg,500
access-list=students,ACCEPT,all,192.168.40.0/24,all
access-list=students,DENY,all,192.168.20.0/24,all
access-list=students,DENY,all,192.168.30.0/24,all
access-list=students,ACCEPT,all,all.all,student_internet_use,5000

access-list=faculty,ACCEPT,tcp,192.168.50.1,80,faculty_reg,500
access-list=faculty,ACCEPT,all,192.168.30.0/24,all
access-list=faculty,DENY,all,192.168.20.0/24,all
access-list=faculty,DENY,all,192.168.40.0/24,all
access-list=faculty,ACCEPT,all,all.all,faculty_internet_use,5000

use-access-list=everyone
```

The RADIUS profile for every student contains the following:

```
use-access-list=students
```

The RADIUS profile for every faculty member contains the following:

```
use-access-list=faculty
```

This definitions create three access lists: everyone, students, and faculty.

Everyone
This list applies to all users (students, teachers, guests), whether they are authenticated or not. This is because the list is active on the controller, which is accomplished with the entry:

```
use-access-list=everyone
```

It enables everyone to access the public Web server.

Students
This list applies to authenticated students only. It is composed of the following entries:

```
access-list=students,ACCEPT,tcp,192.168.50.1,80,students_reg,500
```

Enables Web traffic to the registration Web server. Accounting data is recorded in the account students_reg.

```
access-list=students,ACCEPT,all,192.168.40.0/24,all
```

Enables traffic to reach the student segment.

```
access-list=students,DENY,all,192.168.20.0/24,all
access-list=students,DENY,all,192.168.30.0/24,all
```

These two entries deny access to the faculty subnet and the NOC.

```
access-list=students,ACCEPT,all,all.all,student_internet_use,5000
```

Enables all other traffic to reach the Internet (via routers on the backbone LAN and the router in the NOC). If this last rule did not exist, this traffic would be dropped.

Faculty
This list applies to authenticated faculty members only. It is composed of the following entries:

```
access-list=faculty,ACCEPT,tcp,192.168.50.1,80,faculty_reg,500
```

Enables Web traffic to the registration Web server. Accounting data is recorded in the account faculty_reg.

```
access-list=faculty,ACCEPT,all,192.168.30.0/24,all
```

Enables traffic to reach the faculty segment.

```
access-list=faculty,DENY,all,192.168.20.0/24,all
access-list=faculty,DENY,all,192.168.40.0/24,all
```

These two entries deny access to the student subnet and the NOC.

```
access-list=faculty,ACCEPT,all,all.all,faculty_internet_use,5000
```

Enables all other traffic to reach the Internet (via routers on the backbone LAN and the router in the NOC). If this last rule did not exist, this traffic would be dropped.

Configuration file

The controller can retrieve and load a new configuration file automatically, based on the URL you specify.

Syntax

```
configuration-file=URL[placeholder]
```

Where:

Parameter	Description
URL	Specify the URL that points to the new configuration file.

By using the following placeholders, you can customize the URL for each controller. This is useful when you need to update multiple units.

Placeholder	Description
%n	Returns the NAS ID assigned to the controller. By default, this is the unit serial number.
%s	Returns the RADIUS login name assigned to the controller on the **Public access > Attributes** page. By default, this is the unit serial number.
%i	Returns the domain name assigned to the controller Internet port.
%a	Returns the IP address of the controller Internet port.

Custom SSL certificate

The controller can retrieve a custom SSL security certificate to replace the HP certificate that is included by default.

Syntax

```
ssl-certificate=URL[placeholder]
```

Where:

Parameter	Description
URL	Specify the URL that points to the new certificate.

By using the following placeholders, you can customize the URL for each controller. This is useful when you need to update multiple units.

Placeholder	Description
`%n`	Returns the NAS ID assigned to the controller. By default, this is its serial number.
`%s`	Returns the RADIUS login name assigned to the controller. By default, this is its serial number.
`%i`	Returns the domain name assigned to the controller Internet port.
`%a`	Returns the IP address of the controller Internet port.

The certificate is encoded using PKCS#12 format, and contains:

- the private key of the Web server
- the certificate of the Web server

The file is locked using a password.

Note The password with which the certificate was locked must be the same as the password specified on the **Public access > Attributes** page. This is the password the controller uses to login to the RADIUS server.

Example

```
ssl-certificate=http://www.mycompany.com/%s_certificate
```

Custom public access interface Web pages

Several options are available to define custom pages.

Loading custom pages from an archive

This option enables you load site files from an external file archive, allowing you to replace the entire public access Web site in one simple operation. The archive must be in .zip format.

Note The contents of the existing public access site is deleted and replaced by the contents of the archive (.zip) file. If the archive does not contain a complete set of valid pages, the public access interface will not function correctly.

Note When unzipped the total size of all files must be less than 1MB.

Syntax

`custom-pages=`*ArchiveURL*

Where:

Parameter	Description
ArchiveURL	URL of the .zip archive to be loaded.

Loading individual pages

These keywords have been deprecated. *If you are creating a new installation, use the* **custom-pages** keyword or the *site file archive feature on the* ***Controller >> Public access > Web content*** *page. If you are upgrading from a previous release, your existing configuration will still work.*

Use the following values to retrieve pages from an external location and load them onto the controller. For descriptions of the individual pages, see *Current site files on page 14-25*.

Note

The maximum length of any page URL is 512 characters. If this is exceeded (when using placeholders for example), the URL is truncated. Therefore, it is recommended that you specify the most-important placeholders first.

The pages can only be changed as a group. You cannot, for example, just specify the login-page value. You must specify all of the following pages:.

Login page

`login-page=`*URL_of_page* `[`*placeholder*`]`

Can be omitted if a remote login page is being used. See *Remote login page on page 15-47*.

Transport page

`transport-page=`*URL_of_page* `[`*placeholder*`]`

Session page

`session-page=`*URL_of_page* `[`*placeholder*`]`

Fail page

`fail-page=`*URL_of_page* `[`*placeholder*`]`

Logo

`logo=`*URL_of_gif_file* `[`*placeholder*`]`

Placeholder

The following placeholder is only available when using a RADIUS server. If these values are specified under **Controller >> Public access > Attributes > Configured attributes**, the placeholder cannot be used.

Placeholder	Description
`%a`	Returns the IP address of the controller's Internet port.

Hosting pages on an external Web server

Use the following values to reference pages that reside on an external Web server.

Note The maximum length of any page URL is 512 characters. If this is exceeded (when using placeholders for example), the URL is truncated. Therefore, it is recommended that you specify the most-important placeholders first.

Note The controller maintains a separate copy of the URLs for external pages for each user. This means it is possible to provide different pages for each user. See *Displaying custom welcome and goodbye pages on page 14-16.*

Welcome page

`welcome-url=`*URL_of_page*`[`*placeholder*`]`

The user is authenticated, so the welcome page can be located on any URL reachable by the user.

Login error page

`login-err-url=`*URL_of_page*`[`*placeholder*`]`

Access to the Web server hosting this page must be granted to all unauthenticated users. Do this with an appropriate access list definition. (Users can see this page *before* they are logged in.)

if the radius server denies user authentication, this is used instead of an error being presented on the login page.

Goodbye page

`goodbye-url=`*URL_of_page*`[`*placeholder*`]`

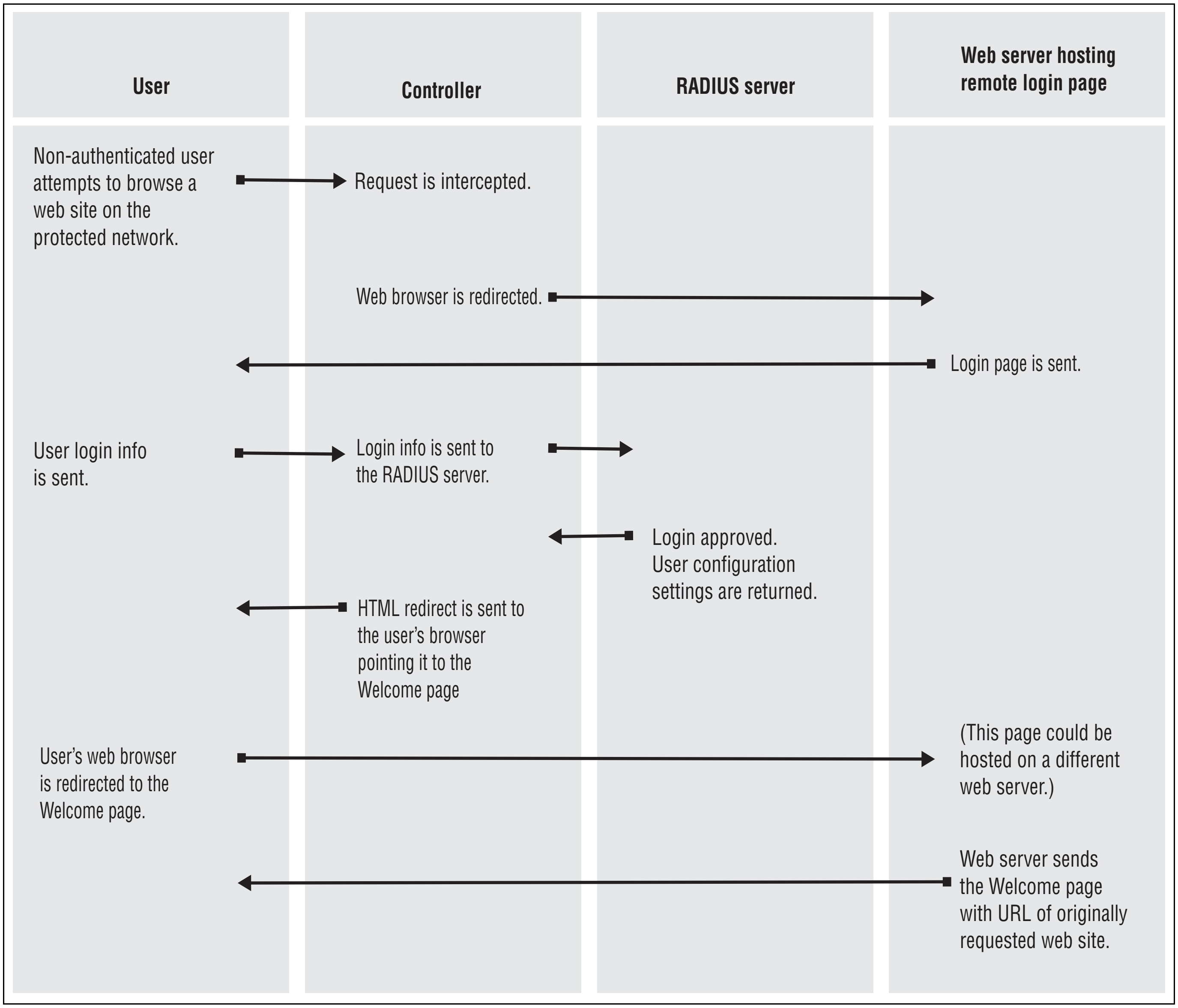
Access to the Web server hosting this page must be granted to all unauthenticated users. Do this with an appropriate access list definition. (Users see this page *after* they are logged out.)

Remote login page

Use this value to redirect users to a remote server to log in to the public access interface instead of using the internal login page.

Although the remote login page feature enables you to host the public access login page on a remote Web server, authentication of users is still performed by the controller through a RADIUS server or using the local user list. To accomplish this, the remote Web server must send user login information back to the controller. There are two ways this can be done: basic remote login (as described in this section), or by using the NOC-based authentication feature (described in *Appendix D: NOC authentication*).

The following diagram shows the sequence of events for a typical user session when using a remote login page and a RADIUS server for authentication.


User
Controller
RADIUS server
Web server hosting remote login page
Non-authenticated user attempts to browse a web site on the protected network.
Request is intercepted.
Web browser is redirected.
Login page is sent.
User login info is sent.
Login info is sent to the RADIUS server.
Login approved. User configuration settings are returned.
HTML redirect is sent to the user's browser pointing it to the Welcome page
User's web browser is redirected to the Welcome page.
(This page could be hosted on a different web server.)
Web server sends the Welcome page with URL of originally requested web site.

Syntax

```
login-url=URL_of_the_page [placeholder]
```

Access to the Web server hosting this page must be granted to all unauthenticated users. Do this with an appropriate access list definition. (Users see this page *before* they are logged in.)

Placeholders

An important feature of these pages is that they make it easy to deliver a unique experience for each user. By appending the following optional placeholders to the Colubris AV-Pair value strings, you can pass important information to the Web server. Server-side code can process this information to generate custom pages on-the-fly.

Placeholder	Description
`%d`	Returns the WISPr location-ID. Supported for login-url only.
`%e`	Returns the WISPr location-Name. Supported for login-url only.
`%l`	Returns the URL on the controller where user login information should be posted for authentication. This option is used with the remote login page feature. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
`%n`	Returns the NAS ID assigned to the controller. By default, this is the unit serial number. Not supported in local mode.
`%s`	Returns the RADIUS login name assigned to the controller. By default, this is the unit serial number.
`%u`	Returns the login name of the user.
`%o`	Returns the original URL requested by the user. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
`%i`	Returns the domain name assigned to the controller Internet port.
`%p`	Returns the IP port number on the controller where user login information should be posted for authentication.
`%a`	Returns the IP address of the controller Internet port.
`%E`	When the location-aware feature is enabled, returns the ESSID of the wireless AP the user is associated with.
`%P`	When the location-aware feature is enabled, returns the wireless mode “ieee802.11a”, “ieee802.11b”, “ieee802.11g”) the user is using to communicate with the AP.
`%G`	When the location-aware feature is enabled, returns the group name of the wireless AP the user is associated with.
`%C`	When the location-aware feature is enabled, returns the Called-station-id content for the wireless AP the user is associated with.
`%r`	Returns the string sent by the RADIUS server when an authentication request fails. The RADIUS server must be configured to support this feature. The information contained in the returned string depends on the configuration of the RADIUS server.

Placeholder	Description
`%m`	Returns the MAC address of the client station that is being authenticated.
`%v`	Returns the VLAN assigned to the client station at the controller ingress (LAN port).

Security issues

- It is recommended that the Web server hosting the remote login page be secured with SSL (requires an SSL certificate from a well-known certificate authority), to ensure that user logins are secure. Without SSL security, logins are exposed and may be compromised, enabling fraudulent use of the network.
- Communications between the user's browser and the controller is always SSL-based. The default certificate on the controller generates a warning on the user's browser unless replaced with a certificate signed by a well-known certificate authority.

Example

1. Create the following folder on your Web sever: **newlogin**.
2. See *Sample public access pages on page 14-15*. Copy the following sample pages into the **newlogin** folder:
   - login.html
   - transport.html
   - session.html
   - fail.html
   - logo.gif
3. Add the following entries to the **Configured attributes** table on the **Public access > Attributes** page. (You can also define these attributes in the RADIUS profile for the controller if you are using a RADIUS server.)

```
login-url=web_server_URL/newlogin/login.html?loginurl=%l
transport-page=web_server_URL/newlogin/transport.html
session-page=web_server_URL/newlogin/session.html
fail-page=web_server_URL/newlogin/fail.html
logo=web server URL/newlogin/logo.gif
access-list=loginserver,ACCEPT,tcp,web_server_IP_address
use-access-list=loginserver
```

4. Customize **login.html** to accept username and password information from users and then send it to the controller. You can use code similar to the following example to redirect the user's Web browser to the login URL on the controller for authentication:

```
<form action="https://wireless.colubris.com:8090/goform/HtmlLoginRequest"
method="POST">
```

   For more flexibility, the remote login page should be written using a server-side scripting language such as ASP, PHP, or PERL. This enables the remote login page to take advantage of any placeholders that may have been defined in the login-url.

Custom message file

Use this value to load a custom message file. These messages are used when various error conditions occur.

`messages=`*URL_of_text_file* `[`*`placeholder`*`]`

If you specify a new message file, you must also specify values for:

- Login page
- Transport page
- Session page
- Fail page
- Logo

Placeholders
The following optional placeholder can be appended to the Colubris AV-Pair value for the message file.

Placeholder	Description
`%a`	Returns the IP address of the controller Internet port.

Default user interim accounting update interval

This keyword lets you define the interim accounting update interval for all users that do not have a specific interval set in their profile.

Syntax

`default-user-acct-interim-update=`*value*

Where:

Parameter	Description
`value`	Number of seconds between interim updates.

Default user bandwidth level

This keyword lets you define the bandwidth level for all users that do not have a specific level set in their profile.

Syntax

`bandwidth-level=`*`level`*

Where:

Parameter	**Description**
level	Specify one of the following the bandwidth levels for the user's session. The actual data rate associated with a bandwidth level is defined on the **Network > Bandwidth control** page. VERY-HIGH HIGH NORMAL LOW

Default user idle timeout

Use this to set the default idle timeout for all users whose RADIUS profile does not contain a value for the RADIUS attribute *idle-timeout*.

Syntax

```
default-user-idle-timeout=seconds
```

Where:

Parameter	**Description**
seconds	Specify the maximum amount of time a user session can be idle. Once this time expires, the session is automatically terminated. A value of 0 means no timeout.

Default user quotas

These keywords let you define upload and download limits for all users that do not have a specific limit set in their profile. Limits can be defined in terms of packets or octets (bytes).

Syntax

```
default-user-max-input-packets=value
default-user-max-output-packets=value
default-user-max-total-packets=value


default-user-max-input-octets=value
default-user-max-output-octets=value
default-user-max-total-octets=value
default-user-max-input-rate=value
default-user-max-output-rate=value
```

Where:

Parameter	Description
value	For packets: 32-bit unsigned integer value. For octets: 64-bit unsigned integer value.

When a user session is terminated based on a quota, a new non-standard termination cause is used. The value for this termination cause is 0x8744. You can customize this by modifying the value of "radius-quota-exceeded-cause" in the "ACCESS-CONTROLLER" section of the configuration file.

Default user data rates

These keywords let you define data rate limits for all users that do not have a specific limit set in their profile.

Syntax

```
default-user-max-input-rate=value
default-user-max-output-rate=value
```

Where:

Parameter	Description
value	For packets: 32-bit unsigned integer value. For octets: 64-bit unsigned integer value.

Default user one-to-one NAT

This keyword lets you define the default setting for one-to-one NAT support for all users that do not have this setting specified in their profile. This feature only applies to users making IPSec or PPTP VPN connections with a remote site via controller Internet port. For more information, see *VPN one-to-one NAT on page 3-9* and *One-to-one NAT on page 15-69*.

Syntax

```
default-user-one-to-one-nat=value
```

Where:

Parameter	Description
value	Set this to 1 to activate one-to-one NAT support.

Default user session timeout

Use this to set the default session timeout for all users whose RADIUS profile does not contain a value for the RADIUS attribute *session-timeout*.

Syntax

`default-user-session-timeout=`*seconds*

Where:

Parameter	Description
seconds	Specify the maximum amount of time a user session can be connected. Once this time expires, the session is automatically terminated. A value of 0 means no timeout.

Default user public IP address

Use this to set the default value for public IP address assignment for users whose RADIUS profile does not contain a value for **use-public-ip-subnet** (*Public IP address on page 15-70*). For more information using public IP addresses, see *Public IP address on page 3-10*.

Syntax

`default-user-use-public-ip-subnet=`*value*

Where:

Parameter	Description
value	Set this to 1 to activate assignment of a public IP address. Set to 0 to disable.

Default user SMTP server

Use this to set the default SMTP server address for all user sessions. This address is used if a specific server is not set for a particular user.

Syntax

`default-user-smtp-redirect=`*hostname*`[:`*port*`][,`*username*`,`*password*`]`

Where:

Parameter	Description
hostname	Specify the IP address or domain name of the e-mail server. Maximum length is 253 characters.

Parameter	Description
port	Specify the port on the e-mail server to relay to. Range: 1 to 65535. Default: 25
username	Specify the username required to log on to the SMTP server. Maximum 32 characters. Only used if the **SMTP authentication** option is enabled on the **Public Access > Access Control** page. Works with SMTP servers that support plain or CRAM-MD5 authentication.
password	Specify the password required to log on to the SMTP server. Maximum 32 characters. Only used if the **SMTP authentication** option is enabled on the **Public Access > Access Control** page. Works with SMTP servers that support plain or CRAM-MD5 authentication.

Default user URLs

Use this to set the default URLs for the welcome and goodbye pages for all users that do not have default pages specified in their profile.

Syntax

```
default-user-welcome-url=URL
default-user-goodbye-url=URL
```

Where:

Parameter	Description
URL	Specify the URL of an external Web page.

HTTP proxy upstream

The HTTP proxy upstream feature can be used to force all outgoing TCP traffic to be sent to a third-party upstream HTTP proxy server. When using this feature, outgoing traffic is automatically translated into HTTP proxy format because many HTTP proxies are not able to handle transparent proxy requests. HTTP requests such as **GET / HTTP/1.0** are transformed into **GET http://www.website.com/ HTTP/1.0** before being forwarded to the thrid-party server.

Note The HTTP proxy upstream feature targets the HTTP protocol and not HTTPS. Because of this, HTTPS only works if users have configured their browsers for HTTP proxy usage. In the case of transparent proxy, the connection will not be detected as HTTP-compatible and will not be redirected to the upstream proxy server.

By default this feature listens to TCP port 8088 on the LAN port. However, it can be configured to capture other ports. This is done by defining an access list and DNAT server. For example:

```
HTTP-Proxy-Upstream=myproxy.com:8888
```

```
Access-List=mylist,DNAT-SERVER,tcp,*mydomain.com,80
```

```
Use-access-list=mylist
```

```
DNAT-Server=mylist,192.168.1.1,8088
```

This example forces any incoming traffic, with a matching target protocol, address, or port number (tcp,*mydomain.com,80) to be redirected to the internal HTTP proxy. Then, because of the HTTP-Proxy-Upstream keyword, the traffic is forwarded to **myproxy.com**.

Note The HTTP-Proxy-Upstream definition must exclude any traffic addressed to the controller public access interface, otherwise HTML-based users will not be able to login.

Syntax

`HTTP-Proxy-Upstream=`*hostname*`:`*port*

Where:

Parameter	Description
hostname	Specify the IP address or domain name of the proxy server. Maximum length is 253 characters.
port	Specify the port on the proxy server. Range: 1 to 65535.

IPass login URL

This keyword lets you define the location of the IPass login page. The controller will automatically redirect users with IPass client software to this page.

Syntax

`ipass-login-url=`*URL_of_page*

Where:

Parameter	Description
URL_of_page	Address of the IPass login page.

Global MAC-based authentication

The global MAC-based authentication feature enables you to define MAC-based authentication settings that apply across all VSCs.

Note You can also define MAC-based authentication settings on a per-VSC basis. See *MAC-based authentication on page 10-14* for a description of all MAC-based authentication options.

To make use of this feature you need to define a local user account or a RADIUS user account for each device as follows:

- username: Set this to the username you specified in the mac-address value string. If no username is specified, set the account name to the MAC address of the device. Use dashes to separate characters in the address. For example: 00-20-E0-6B-4B-44.
- password: Set this to the password you specified in the mac-address value string. If no password is specified, set this to the same password that is used for the user account.

Note The username and password are not encrypted for transmission so it is important that the link with the RADIUS server is secure.

Note MAC authentication only applies to VSCs that have HTML-based authentication enabled.

Syntax

`mac-address=`*address*`[,`*username*`[,`*password*`]]`

Where:

Parameter	Description
address	Specify the MAC address of the device to authenticate. Use dashes to separate characters in the address. Do not use colons (:). For example: 00-20-E0-6B-4B-44.
username	Specify the username to associate with this MAC address. Maximum 32 alphanumeric characters. The username field cannot contain a comma.
password	Specify the password to associate with this MAC address. Maximum 32 alphanumeric characters. The password field cannot contain a comma.

Example
Consider the scenario where several APs are installed with a controller. If the APs are going to perform software updates from a remote Web or FTP server, they will need to log in to the public access network. By using MAC-based authentication, this can easily be accomplished.

Multiple login servers

This feature lets you dynamically set the URL used for retrieving custom external pages or a remote login page based on the status of a primary or secondary Web server.

Syntax

`primary-web-server-status-url=`*URL_of_page*

`secondary-web-server-status-url=`*URL_of_page*

Where:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><i>URL_of_page</i></td><td>Specify the URL that points to the Web server status file. Use HTTP or HTTPS with a port number if required.

The status file must contain the following code:

<pre>
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/
envelope/"
  xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/
encoding/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
<SOAP-ENV:Body>
    <MYCOMPANY:WebServerStatus>
      <MYCOMPANY:result>UP</MYCOMPANY:result>
    </MYCOMPANY:WebServerStatus>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
</pre>
Change the <code>&lt;MYCOMPANY:result&gt;</code> line to indicate the status of the server as follows:

<b>Server is UP</b>
<MYCOMPANY:result>UP</MYCOMPANY:result>

<b>Server is DOWN</b>
<MYCOMPANY:result>DOWN</MYCOMPANY:result>

Do not change any other lines in the file.</td></tr>
</table>

Polling

The controller attempts to retrieve the server status file from the primary server first. If no response is received before the polling timeout expires (30 seconds by default), the controller attempts to retrieve the server status file from the secondary server. If no response is received before the polling timeout expires, unauthenticated users attempting to login will see the Fail page with the message: “Login server is unavailable”.

After initialization, the controller continuously polls the servers to determine their status. As long as the primary server is available, it is used. if the primary server fails to respond or returns status DOWN, then the secondary server will be used, but only until the primary server comes back up.

The polling interval and polling timeout are configured by editing the following entries in the configuration file: **web-server-polling-interval** and **web-server-polling-timeout.**

To change the error message, edit the entry **err-msg-login-server-down** in **messages.txt**.

Setting the URLs of other AV-Pair values

This feature will redefine the URLs in the following AV-Pair values, if they have the same hostname as is specified for the **primary-web-server-status-url**:

- login-url
- welcome-url
- goodbye-url
- logout-url
- login-err-url
- ipass-login-url

For example, if the following values are defined:

```
primary-web-server-status-url=https://srv1.abc.com/status.html

secondary-web-server-status-url=https://srv2.abc.com/status.html

login-url=https://srv1.abc.com/loginpage.html

welcome-url=http://srv1.abc.com/mywelcome.html

login-err-url=http://srv3.xyx.com/mywelcome.html
```

- If the primary server is up, then the URLs are not changed.
- If the primary server is down and the secondary server is up, then login-url and welcome-url are changed as follows:

```
login-url=https://srv2.abc.com/loginpage.html

welcome-url=http://srv2.abc.com/mywelcome.html
```

- If both servers are down, then the URLs are not changed.

Redirect URL

The redirect-url value is used to specify the target URL for redirection when using an access list with the REDIRECT action. Only one **redirect-url** value can be specified in each controller or user RADIUS account.

When an access list rule with the REDIRECT action is processed, the user’s browser is redirected to a different HTTP address in this order:

- redirect-url keyword in the user account, if present
- redirect-url keyword in the controller account, if present
- login-url keyword, in the controller account, if present

The URL can contain any of the applicable placeholders defined here.

Note Placeholders %G, %C, %E, %P, and %v do not produce constant values. These values may vary over time.

Use the following Colubris AV-Pair value string:

`redirect-url=`*`URL_of_the_page`* `[`*`placeholder`*`]`

Where:

Parameter	Description
`URL_of_the_page`	URL of the redirect page. Access to the Web server hosting this page must be granted to all unauthenticated users. Do this with an appropriate access list definition.

The following placeholders can be added to the redirect-url string.

Placeholder	Description
`%c`	Returns the IP address of the user's computer.
`%l`	Returns the URL on the controller where user login information should be posted for authentication. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
`%n`	Returns the NAS ID assigned to the controller. By default, this is the unit serial number. Not supported in local mode.
`%s`	Returns the RADIUS login name assigned to the controller. By default, this is the unit serial number. Not supported in local mode.
`%o`	Returns the original URL requested by the user. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
`%i`	Returns the domain name assigned to the controller Internet port.
`%p`	Returns the port number on the controller where user login information should be posted to for authentication.
`%a`	Returns the IP address of the controller interface that is sending the authentication request.
`%E`	When the location-aware feature is enabled, returns the ESSID of the wireless access point the user is associated with.
`%P`	When the location-aware feature is enabled, returns the wireless mode ("ieee802.11a", "ieee802.11b", "ieee802.11g") the user is using to communicate with the access point.

Placeholder	Description
`%G`	When the location-aware feature is enabled, returns the group name of the wireless access point the user is associated with.
`%C`	When the location-aware feature is enabled, returns the Called-station-id content for the wireless access point the user is associated with.
`%r`	Returns the string sent by the RADIUS server when an authentication request fails. The RADIUS server must be configured to support this feature. The information contained in the returned string depends on the configuration of the RADIUS server.
`%m`	Returns the MAC address of the wireless/wired client station that is being authenticated.
`%v`	Returns the VLAN assigned to the client station at the controller ingress (LAN port).

Note The maximum length of the remote login page URL is 512 characters. If this is exceeded (when using placeholders for example), the URL is truncated. It is therefore recommended that you specify the most-important placeholders first.

Example

One way to use this feature is to offer a premium service for a given (or all) sites. For example, in the controller profile, define two lists, one for normal usage and one for premium usage:

```
access-list=normal,REDIRECT,tcp,www.mypremiumservice.com,80
access-list=normal,ACCEPT,all,all,all
access-list=premium,ACCEPT,all,all,all
redirect-url=http://www.mysite.com/getpremium/
```

In the RADIUS profile for normal users, map them to the “normal” access list:

```
use-access-list=normal
```

In the RADIUS profile for premium users, map them to the “premium” access list:

```
use-access-list=premium
```

The access list only takes effect on an authentication, so a change of service as shown in this example takes effect only at the user’s next authentication (login).

NOC authentication

The NOC authentication feature provides a secure way of authenticating public access users, with strong mutual authentication between the login application on the Web server hosting the remote login page and the controller used for authenticating user logins. This occurs via the two Colubris AV-Pair value strings (**ssl-noc-certificate** and **ssl-noc-ca-certificate**), which define the locations of two certificates. These certificates enable the controller to validate that the user login information does indeed come from a trusted application.

For example, from a login application on the Web server.

`ssl-noc-certificate=`*URL_of_the_certificate*

Certificate issued to the application on the Web server that will send user info to the controller for authentication.

`ssl-noc-ca-certificate=`*URL_of_the_certificate*

Certificate of the certificate authority (CA) that issued the NOC certificate.

For a more detailed example of using NOC authentication, see *Appendix D: NOC authentication*

HP WISPr support

WISPr login URL

This keyword lets you define the location of the WISPr login page. The controller automatically redirects users with WISPr-compatible wireless client software to this page. To customize the redirection use the WISPr redirect page keyword.

Syntax

`wispr-login-url=`*URL_of_page*

Where:

Parameter	Description
URL_of_page	URL of the WISPr login page.

WISPr abort login URL

This keyword lets you define the destination where the WISPr abort login will be POSTed.

Syntax

`wispr-abort-login-url=`*URL_of_page*

Where:

Parameter	Description
URL_of_page	URL where to POST the WISPr abort login.

WISPr redirect page

This keyword lets you define the location of the WISPr redirect page. Use this page to customize the code that the controller includes in the HTTP redirect sent to a user's browser.

Syntax

`redirect-page=`*URL_of_page*

Where:

Parameter	Description
`URL_of_page`	URL of the page containing code to use for WISPr redirect.

If this keyword is not defined, default code is used. To view the default code, open the file **redirect.html,** which is available in the Public Access Examples file. See *Sample public access pages on page 14-15*.

WISPr access procedure

Specifies the version of the WISPr client access procedure supported by the controller.

`access-procedure=`*procedure_version*

Where:

Parameter	Description
`procedure_version`	Specify the WISPr client access procedure supported by the controller. Currently, the controller only supports the value “1.0”.

Traffic forwarding (dnat-server)

This keyword defines the external server to which the controller will forward traffic when an access list rule with the DNAT-SERVER action matches incoming traffic.

Note SSL traffic cannot be forwarded as this breaks SSL security during connection negotiation resulting in the connection not being established.

Two external servers can be defined with this keyword. A status polling mechanism is available that enables the controller to determine the status of the external servers and forward traffic to the one this is operational. To activate the polling mechanism see *Multiple DNAT servers* below.

This keyword can be defined directly on the controller or in the controller RADIUS profile.

Syntax

`dnat-server=`*listname*`,`*hostname*`,`*port*`[,`*hostname2*`,`*port2*`]`

Where:

Parameter	Description
listname	Specify the name of an access list definition that has its action set to DNAT-SERVER.
hostname	Specify the IP address or domain name of the primary server to which traffic will be redirected. Maximum length is 253 characters. If polling is not enabled, traffic is always sent to this server, even if it is down.
port	Specify the port on the primary server to which traffic will be redirected. Range: 1 to 65535.
hostname2	Specify the IP address or domain name of the secondary server to which traffic will be redirected. Maximum length is 253 characters. Traffic will only be sent to the secondary server if polling is enabled and the primary server is down. See *Multiple DNAT servers on page 15-64*.
port2	Specify the port on the secondary server to which traffic will be redirected. Range: 1 to 65535.

Example

The following creates an access list called **redirect** which is used to redirect HTTP traffic for authenticated users to **server1.mycompany.com** on port **8080**.

The following entry is added to the local profile for the controller:

```
access-list=redirect,DNAT-SERVER,tcp,all,80
```

```
dnat-server=redirect,srv1.mycompany.com,8080
```

Multiple DNAT servers

The **dnat-server** keyword supports the definition of two external servers. To make use of these servers a polling mechanism is provided. Two keywords are available to activate and configure the polling mechanism.

Syntax

`primary-dnat-server-status-url=`*listname*`,`*URL_of_page*

`secondary-dnat-server-status-url=`*listname*`,`*URL_of_page*

Where:

Parameter	Description
listname	Specify the name of an access list definition that has its action set to DNAT-SERVER.

Parameter	Description

URL_of_page	Specify the URL that points to a status file on the Web server. Use HTTP or HTTPS with a port number if required.
	The status file must contain the following code:
	`<?xml version="1.0" encoding="UTF-8"?>`
	`<SOAP-ENV:Envelope`
	`  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/`
	`envelope/"`
	`  xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/`
	`encoding/"`
	`  xmlns:xsi="http://www.w3.org/2001/XMLSchema-`
	`instance"`
	`  xmlns:xsd="http://www.w3.org/2001/XMLSchema"`
	`  xmlns:MYCOMPANY="http://www.mycompany.com/SOAP/`
	`NOCAPI/1.0/">`
	`  <SOAP-ENV:Body>`
	`    <MYCOMPANY:WebServerStatus>`
	`      <MYCOMPANY:result>UP</MYCOMPANY:result> <!-`
	`Change this between UP and DOWN to determine the state`
	`of your server !>`
	`    </MYCOMPANY:WebServerStatus>`
	`  </SOAP-ENV:Body>`
	`</SOAP-ENV:Envelope>`
	Change the `<MYCOMPANY:result>` line to indicate the status of the server as follows:
	Server is UP
	<MYCOMPANY:result>UP</MYCOMPANY:result>
	Server is DOWN
	<MYCOMPANY:result>DOWN</MYCOMPANY:result>
	Do not change any other lines in the file.
	If the controller fails to receive an answer to a poll, or receives an incorrect answer (bad format, wrong result setting) it is interpreted as the server being down.

Polling

Initially, the controller polls the primary server at an interval of 10 minutes. As long as the primary is active, it is used. If it is not available, then the secondary server is used, but only until the primary server becomes available again.

If both servers are not available, both are polled in turn with no delay (other than the poll timeout) until one becomes available. When both servers are unavailable the access list DNAT-SERVER definition is skipped with no action taken, and processing moves to the next rule in the access list. This next rule can then be used to define the action taken when both DNAT-SERVERS are down.

The following table shows possible results when polling is active for both the primary and secondary servers.

Server 1	Server 2	Description
UP	UP	Traffic matching the DNAT-SERVER rule is forwarded to server 1.
UP	DOWN	Traffic matching the DNAT-SERVER rule is forwarded to server 1.
DOWN	UP	Traffic matching the DNAT-SERVER rule is forwarded to server 2.
DOWN	DOWN	No action is performed for the DNAT-SERVER rule. Processing moves to the next rule in the list. To accept all traffic if both servers are down, define this rule as: ACCEPT,all,all,all

Example

The following creates an access list called **redirect** which is used to redirect HTTP traffic for authenticated users to either **srv1.mycompany.com** or **srv2.mycompany.com** depending on which one is active. Port **8080** is used to forward traffic. If neither the primary or secondary DNAT-SERVER is available, all traffic is accepted.

The following entry is added to the local profile for the controller:

```
access-list=redirect,DNAT-SERVER,tcp,all,80

access-list=redirect,ACCEPT,all,all,all
```

The following entry is added to the RADIUS profile for each user:

```
dnat-
server=redirect,srv1.mycompany.com,8080,srv2.mycompany.com,8080
```

Colubris AV-Pair - User attribute values

User values let you define settings for individual user accounts.

Each Colubris AV-Pair value is specified using the following format: `<keyword>=<value>`

The following table lists all supported user value keywords and provides a link to complete descriptions for each one.

Colubris AV-Pair keyword	For more information see
access-list	*Access list on page 15-67.*
ads-presentation	*Advertising on page 15-68.*
bandwidth-level	*Bandwidth level on page 15-68.*
max-output-rate max-input-rate	*Data rate on page 15-69.*
one-to-one-nat	*One-to-one NAT on page 15-69.*
use-public-ip-subnet	*Public IP address on page 15-70.*
max-input-packets max-output-packets max-input-octets max-output-octets max-total-octets max-total-packets	*Quotas on page 15-70.*
smtp-redirect	*SMTP redirection on page 15-71.*
polling-arp-interval polling-max-arp-count	*Station polling on page 15-72.*
redirect-url	*Redirect URL on page 15-59.*
welcome-url	*Custom public access interface Web pages on page 15-72.*
goodbye-url	*Custom public access interface Web pages on page 15-72.*

Access list

An access list is a set of rules that govern how the controller controls user access to protected network resources (those attached to the controller Internet port). Access lists are defined in the profile for the controller) and are activated in user profiles as needed.

Only one access list can be activated per user profile. See *Access list on page 15-34*.

Syntax

`use-access-list=`*`uselistname`*

Where:

Parameter	**Description**
`uselistname`	Specify the name of an existing access list. This list is activated for the current user.

Advertising

Add this keyword to enable the presentation of advertising at preconfigured intervals while the user is browsing.

Syntax

ads-presentation=*`value`*

Where:

Parameter	**Description**
`value`	Set this to 1 to activate the display of advertising. Set to 0 to disable.

Bandwidth level

This keyword sets bandwidth level for a user's session. The actual data rate associated with a bandwidth level is defined on the **Network > Bandwidth control** page. See *Bandwidth levels on page 3-22*. To control the default bandwidth level for all users, see *Default user bandwidth level on page 15-51*.

Syntax

`bandwidth-level=`*`level`*

Where:

Parameter	**Description**
`level`	Specify one of the following the bandwidth levels for the user's session: VERY-HIGH HIGH NORMAL LOW

Data rate

This keyword sets the transmit and receive rates for a user's session. These rates are applied on a per-user basis providing direct control of a user's throughput in Kbps. Two keywords are available:

- max-input-rate: Controls the data rate at which traffic can be transferred from the user to the controller.
- max-output-rate: Controls the data rate at which traffic can be transferred from the controller to the user.

Note The settings for bandwidth level always take precedence over user data rates. This means if you set a data rate which exceeds the configured bandwidth level, the rate is capped at the bandwidth level.

Syntax

```
max-output-rate=rate
max-input-rate=rate
```

Where:

Parameter	Description
rate	Maximum transmit or receive speed in Kbps.

One-to-one NAT

Note This feature only applies to client traffic using IPSec or PPTP on the Internet port.

Add this keyword if the user requires a unique IP address when NAT is enabled on the controller. For more information, see *VPN one-to-one NAT on page 3-9* and *Default user one-to-one NAT on page 15-53*.

Syntax

```
one-to-one-nat=value
```

Where:

Parameter	Description
value	Set this to 1 to activate one-to-one NAT support.

Public IP address

Add this keyword if the user requires a public IP address that is visible on the external network connected to the controller Internet port. For more information using public IP addresses, see *Default user public IP address on page 15-54* and *Public IP address on page 3-10*.

Syntax

```
use-public-ip-subnet=value
```

Where:

Parameter	Description
value	Set this to 1 to activate assignment of a public IP address. Set to 0 to disable.

Quotas

These keywords let you define upload and download limits for each user. Limits can be defined in terms of packets or octets (bytes).

Syntax

```
max-input-packets=value
max-output-packets=value
max-input-octets=value
max-output-octets=value
max-total-octets=value
max-total-packets=value
```

Where:

Parameter	Description
value	For packets: 32-bit unsigned integer value. For octets: 64-bit unsigned integer value.

When a user session is terminated based on a quota, a new non-standard termination cause is used. The value for this termination cause is 0x8744.

The text value of for the termination cause is defined in the message.txt file under the token “stat-quota-exceeded”. The default value for this token is “Logged out. (Quota Exceeded.)”. This value can be displayed with the ASP function *GetAuthenticationErrorMessage() on page 15-91*.

A series of ASP functions are available that enable you to display quota information on the session page. See *Session quotas on page 15-85*.

Redirect URL

The redirect-url keyword is used to specify the target URL for redirection when using an access list with the REDIRECT action. Only one **redirect-url** value can be specified in a user RADIUS account. See *Redirect URL on page 15-59*.

SMTP redirection

The controller is able to provide SMTP email service on a per-user basis. This enables users to send e-mail while on the road without the restrictions imposed by most ISPs regarding the source address of outgoing mail. It works by intercepting the call to a user's e-mail server and redirecting it to an SMTP server that you configure. This setting overrides the setting of *Default user SMTP server on page 15-54*.

Note For mail redirection to work, the user's email server name must be publicly known. If the e-mail server name cannot be resolved, mail redirection fails.

Note If an access list definition is active in the controller profile that enables unauthenticated users to access their SMTP servers, the SMTP redirect feature will not work for these users.

Syntax

```
smtp-redirect=address[:port][,username,password]
```

Where:

Parameter	Description
address	Specify the IP address or domain name of the e-mail server which is used to send outgoing redirected mail.
port	Specify the port on the e-mail server to relay to. Range: 1 to 65535. Default: 25
username	Specify the username required to log on to the SMTP server. Maximum 32 characters. Only supported if the **Support authentication on SMTP proxy server** option is enabled on the **Public access > Access control** page. Works with SMTP servers that support PLAIN, CRAM-MD5, and no authentication.
password	Specify the password required to log on to the SMTP server. Maximum 32 characters. Only supported if the **Support authentication on SMTP proxy server** option is enabled on the **Public access > Access control** page. Works with SMTP servers that support PLAIN, CRAM-MD5, and no authentication.

Example 1: Proxy support on

```
smtp-redirect=smtp.mycompany.com,jimmy,letMEin
smtp-redirect=smtp.mycompany.com:8025,jimmy,letMEin
```

Example 2: Proxy support off

```
smtp-redirect=smtp.mycompany.com
smtp-redirect=smtp.mycompany.com:8025
```

Station polling

The controller continually polls authenticated client stations to ensure they are active. This feature is configured using the **Client polling** settings on the **Public access > Access control** page. If no response is received and the number of retries is reached, the client station is disconnected.

These keywords let you override the **Client polling** settings on a per-user basis.

Syntax

`polling-arp-interval=`*`interval`*

`polling-max-arp-count=`*`count`*

Where:

Parameter	**Description**
interval	Specify how long (in seconds) to wait between polls.
count	Specify how many polls a client station can fail to reply to before it is disconnected.

To disable polling, set both *interval* and *count* to 0.

The initial query is always done after the client station has been idle for 60 seconds. If there is no answer to this query, the settings for polling-arp-interval and polling-max-arp-count are used to control additional retries.

Custom public access interface Web pages

The following keywords let you define a custom welcome page and goodbye page on a per-user basis. These pages must be hosted on an external Web server.

- Welcome page: Users see this page after they are **logged in**. So, access to the Web server hosting this page must be granted to all authenticated users.
- Goodbye page: Users see this page after they are **logged out**. So, access to the Web server hosting this page must be granted to all unauthenticated users.

Syntax

welcome-*url=URL_of_page*[*placeholder*]

goodbye-url=URL_of_page[placeholder]

Where:

Parameter	Description
URL_of_page	Specify the URL of a Web page on an external Web server.
placeholder	Placeholder as defined in the following table.

Placeholders

By appending the following optional placeholders, you can pass important information to the Web server about the user. Server-side code can process this information to generate custom pages on-the-fly.

Placeholder	Description
%l	Returns the URL on the controller where user login information should be posted for authentication. This option is used with the remote login page feature. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
%n	Returns the NAS ID assigned to the controller. By default, this is the unit serial number. Not supported in local mode.
%s	Returns the RADIUS login name assigned to the controller. By default, this is the unit serial number.
%u	Returns the login name of the user.
%o	Returns the original URL requested by the user. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
%i	Returns the domain name assigned to the controller Internet port.
%p	Returns the IP port number on the controller where user login information should be posted for authentication.
%a	Returns the IP address of the controller Internet port.
%E	When the location-aware feature is enabled, returns the ESSID of the wireless AP with which the user is associated.
%P	When the location-aware feature is enabled, returns the wireless mode the user is using to communicate with the AP.
%G	When the location-aware feature is enabled, returns the group name of the wireless AP with which the user is associated.

Placeholder	Description
`%C`	When the location-aware feature is enabled, returns the Called-station-id content for the wireless AP with which the user is associated.
`%r`	Returns the string sent by the RADIUS server when an authentication request fails. The RADIUS server must be configured to support this feature. The information contained in the returned string depends on the configuration of the RADIUS server.
`%m`	Returns the MAC address of the client station that is being authenticated.
`%v`	Returns the VLAN assigned to the client station at the controller ingress (LAN port).

Colubris AV-Pair - Administrator attribute values

Administrator values let you define settings for administrator accounts.

Each Colubris AV-Pair value is specified using the following format: `<keyword>=<value>`

The following administrator value keyword is supported:

Administrative role

Use this AV-Pair value to identify the role of administrative accounts. See *Management tool on page 2-2*.

Syntax

`web-administrative-role=`*role*

Where:

Parameter	Description
`role`	Use one of the following values to identify the role of the account: ■ **Manager:** A manager is able to access all configuration pages and can change and save all configuration settings. ■ **Operator:** An operator is able to view all configuration pages, but is limited in the types of changes that can be made.

Public access interface ASP functions and variables

The public access interface Web pages use a number of ASP functions to perform specific tasks. These ASP functions are written in embedded Javascript, which is a limited version of Javascript running on the integrated Web server.

Also, a number of ASP variables are defined that can be used to store and retrieve configuration and user settings. There are two types of variables:

- **ASP variables:** The values of these variables must be loaded before they can be used by calling the appropriate ASP function. Values are only persistent per page. Therefore they must be loaded separately on each page before use.
- **Session variables:** Session variables are persistent across all public access pages.

Javascript syntax

The following syntax is used by embedded Javascript code.

	Syntax	Description
Equality operators	==	Equal to
	!=	Not equal to
	>	Greater than
	>=	Greater than or equal to
	<	Less than
	<=	Less than or equal to
Conditional operators	&&	Conditional And
	||	Conditional Or
Unary operator	!	Not (Inverts the value of a boolean value.)
String operator	+	Concatenates two strings.
Arithmetic operators	+	Addition.
	-	Subtraction.
	/	Division.
	*	Multiplication.
	( )	Priority of evaluation.
Control flow	if (*logical condition*) {} else {}	If then else statement.
	for(start; until; steps) { }	Looping.

Forms

The following forms can be used to gather information from a user and submit it to the public access interface for processing.

HtmlSubscriptionRequest

This form can be used create a user account and to execute a payment.

To complete certain form actions, you may be required to submit several parameters. These parameters do not all have to be submitted at the same time. The public access interface will combine the values from multiple POSTs and execute the required task once all required data has been submitted. This allows tasks that require many user inputs (creation of a new account, for example) to be spread out over multiple pages.

Before submitting, you should clear any variable which may still be present in the session store as follows:

- ClearSessionVar(subscription_plan)
- ClearSessionVar(payment_method)
- ClearSessionVar(password)
- ClearSessionVar(card_number)
- ClearSessionVar(card_expiration)
- ClearSessionVar(cart_id)

Fields

- **cancel:** Redirects the user to **cancel_url**.
- **cancel_url:** URL to which the user is redirected when the **cancel** field is specified.
- **card_expiration:** Credit Card expiration in the format **mm/yy**.
- **card_number:** Credit Card number.
- **confirm_password:** Password of the user account.
- **error_url:** URL to which the user is redirected if an error occurs.
- **password:** Password of the user account.
- **pay:** Include this field (with any value) to execute a payment.
- **payment_method:** Payment method must be **"**CreditCard**"**.
- **subscription_plan:** Name of the subscription plan.
- **success_url:** URL to which the user is redirected if no error occurs.
- **username:** Username of the user account.
- **valid_fields:** Specify the names of the fields that should be validated. Separate field names with a space. For example: valid_fields "username password confirm_password".

To create an account

Supply the following fields to create a new user account, or to reset an existing account:

- payment_method
- subscription_plan
- username
- password
- confirm_password
- valid_fields (listing all supplied fields) For example:
  valid_fields "payment_method subscription_plan username password confirm_password"

To execute a payment

Supply the following fields to execute a payment:

- payment_method
- subscription_plan
- username
- password
- confirmation_password
- card_expiration
- card_number
- pay
- valid_fields (listing all supplied fields) For example:
  valid_fields "payment_method subscription_plan username password confirm_password card_expiration card_number"

Note To review payment settings, omit the pay field.

HtmlLoginRequest

This form can be used to perform several login-related actions.

Fields

- **access_type:** Determines the type of action that will be executed:
  - **login:** The **username** and **password** are used to attempt an HTML login. If the login is successful, the user is redirected to the page specified by **success_url.** If the login fails, the user is redirected to the page specified by **error_url.**
  - **subscribe:** The user is redirected to the page specified by **subscription_url**.

  - **free_access:** A user account is created (with the user's MAC address as the username and password) and the user is logged into the public access interface. If the login is successful, the user is redirected to the page specified by **success_url.** If the login is fails, the user is redirected to the page specified by **error_url.**

- **error_url:** The URL to which the user is sent if the login fails. Applies to access_type = login or free_access.
- **original_url:** The URL that the user came from. Normally initialized using GetOriginalURL();
- **password:** Password to use for authentication. Applies to access_type = login.
- **subscription_url:** The URL to which the user is sent when access_type = subscribe.
- **success_url:** The URL to which the user is sent if the login is successful. Applies to access_type = login or free_access.
- **username:** Username to use for authentication. Applies to access_type = login.
- **valid_fields:** Name of the form fields to do validation upon.

HtmlLogout

This form performs a logout operation.

Field

- success_url: The URL to which the user is sent if the logout is successful.

Form errors

When the Web server validates a form, it builds a list of all fields that have validation errors. The following functions can be used to scan this list and retrieve error information for each field.

GetLastFormSubmitFirstField( )

Returns the name of the first field (as a string) that generated a validation error. If no error occurred for any fields in the form, an empty string is returned.

Example
var firstField = GetLastFormSubmitFirstField();

GetLastFormSubmitNextField(*field_name*)

Returns the name of the next field after the specified***field_name*** that generated an error. This enables you to move through the field error list one field at a time.

The field name is returned as a string. If no error occurred for any other fields in the form, an empty string is returned.

Example
var nextField = GetLastFormSubmitNextField("previousField");

LoadFormFieldError(*field_name*)

This function the following ASP variables with details about the errors caused by the specified***field_name***.

ASP variables

- **field_error:** Numeric error value.
  - 0 - No error found.
  - 1 - The field required a value but was empty.
  - 2 - The field contained a value which exceeds the maximum supported length.
  - 3 - The field contained a value which is invalid (only specific values were allowed).
- **field_error_details:** Additional information about the error. Will contain an empty string if not applicable. When **field_error** is set to 2, **field_error_details** will be equal to the maximum supported field length.

Example

```
LoadFormFieldError("field");
write(field_error);
write(field_error_details);
```

RADIUS

GetMsChapV2Failed( )

Displays the MS CHAP V2 error string received in the last RADIUS Reject or RADIUS Accept packet for the user. This function is only supported if you select MSCHAP V2 as the authentication scheme on the controller (**Controller >> Authentication > RADIUS profiles** page). The RADIUS server must also support this feature. For a list of possible return values see RFC 2759.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetRadiusNasId( )

Returns the NAS ID configured for RADIUS Profile on the controller. This can be used to identify the controller that authenticated a user. For an example of how this function is used, see GetNasAddress().

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetRadiusReplyMessage( )

Displays the reply message content received inside the last RADIUS Request or RADIUS Accept packet for the user. The RADIUS server must be configured to support this feature. The information contained in the returned string depends on the configuration of the RADIUS server.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetNasAddress( )

Returns the fully-qualified domain name of the controller as is specified in the currently loaded SSL certificate.

For example, in certain instances you may want users to register for an account before they log in. To accomplish this you could modify the Login page by adding a register button. This redirects the user's browser to a registration Web server where they can set up their account. (This page must be made accessible to non-authenticated users using the appropriate access list rule.)

To avoid having the user login once registration is complete, the registration Web server can send the user back to the controller using a special URL that automatically logs the user into the public access interface.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

Example
Assuming the registration server is 192.169.30.1, the register button code on the Login page might look something like this:

```
<FORM><INPUT
onclick="javascript:window.location='https://192.168.30.1/demo-php/
register.php?
NASip=<%GetNasAddress();%>&NASid=<%GetRadiusNasId();%>';"
type=button value="Click Here to Register">
</FORM>
```

The NAS ID and NAS address are required when the user is redirected back to the controller after registration. The code on the registration Web page would look something like this:

```
// Registering user information in the backend database
RegisterUser($username,
$firstname,
$lastname,
$company,
$title,
$phone,
$email,
$NASid,   // identifies the controller the user is connected to
$NASip
);

// set URL to redirect browser to
$targetURL = "location: https://
" . $NASip . ":8090/goform/HtmlLoginRequest?
username=" . $username . "&password=" . $password;
```

```
// When done
header($targetURL);
```

The target URL is built using the NAS IP and username and password. The form name is hard-coded.

Page URLs

GetFailRetryUrl( )

This feature has been deprecated.

Returns the URL of the next internal page to display as follows:

- Returns the Fail page URL if a login or logout request is currently pending.
- Returns the Transport page URL if the user is already logged in.

This function is designed to be used in conjunction with IsRequestPending().

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetLoginUrl( )

Returns the URL of the Login page.

This is not a normal return value, it cannot be assigned to an ASP variable, it is inserted directly into the HTML page.

GetOriginalUrl( )

Displays the URL the user tried to access before being redirected to the Login page.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetSessionUrl( )

Returns the URL of the Session page.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetWelcomeUrl( )

Returns the URL of the Welcome page.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

Session status and properties

All functions in this section do not provide a normal return value that can be assigned to an ASP variable. Instead, the return value is inserted directly into the HTML page.

Session time

GetSessionTime()

Returns session duration for the current user in minutes and seconds in the format: mm:ss.

ConvertSessionTime(unit)

Returns session duration for the current user in the specified unit. See *ConvertMaxSessionTime(unit) on page 15-83*.

TruncateSessionTime(unit)

Returns session duration for the current user truncated to the specified unit. See *TruncateMaxSessionTime(unit) on page 15-83*.

GetSessionTimeHMS()

Returns session duration for the current user in hours, minutes and seconds in the format: hh:mm:ss.

GetSessionRemainingTime()

Returns the amount of connection time remaining for the current user session in minutes and seconds in the format: mm:ss.

GetSessionRemainingTimeHMS()

Returns the amount of connection time remaining for the current user session in hours, minutes and seconds in the format: hh:mm:ss.

ConvertSessionRemainingTime(unit)

Returns the total amount of connection time remaining for the current user in the specified unit. See *ConvertMaxSessionTime(unit) on page 15-83*.

TruncateSessionRemainingTime(unit)

Returns the total amount of connection time remaining for the current user truncated to the specified unit. See *TruncateMaxSessionTime(unit) on page 15-83*.

GetMaxSessionTime()

Returns the total amount of connection time configured for the current user session in minutes and seconds in the format: mm:ss.

GetMaxSessionTimeHMS( )

Returns the total amount of connection time configured for the current user session in hours, minutes and seconds in the format: hh:mm:ss.

ConvertMaxSessionTime(unit)

Returns the total amount of connection time configured for the current user in the specified unit.

y	Years
d	Days
h	Hours
m	Minutes
s	Seconds

For example if the user account is configured for 5000 seconds, then:

- ConvertMaxSessionTime(“y”) returns 0, calculated as (5000 / (365*24 *60*60)).
- ConvertMaxSessionTime(“d”) returns 0, calculated as (5000 / (24*60*60)).
- ConvertMaxSessionTime(“h”) returns 1, calculated as (5000 / (60*60)).
- ConvertMaxSessionTime(“m”) returns 83, calculated as (5000 / 60).
- ConvertMaxSessionTime(“s”) returns 5000, calculated as (5000 / 1).

TruncateMaxSessionTime(unit)

Returns the total amount of connection time configured for the current user truncated to the specified unit.

y	Years
d	Days
h	Hours
m	Minutes
s	Seconds

For example if the user account is configured for 5000 seconds, then:

- TruncateSessionTime("y") returns 0.
- TruncateSessionTime("d") returns 0.
- TruncateSessionTime("h") returns 1.
- TruncateSessionTime("m") returns 23.
- TruncateSessionTime("s") returns 20.

Session input/output/totals

If you specify a value for the optional parameter **div**, then the return value is divided by **div**.

GetSessionInputPackets( )
GetSessionInputOctets(div)

Returns the number of packets/octets received by the current user session.

GetSessionOutputPackets( )
GetSessionOutputOctets(div)

Returns the number of packets/octets sent by the current user session.

GetSessionTotalPackets( )
GetSessionTotalOctets(div)

Returns the number of packets/octets sent and received by the current user session.

GetSessionMaxTotalPackets( )
GetSessionMaxTotalOctets(div)

Returns the maximum number of packets/octets that can be sent and received by the current user session.

GetSessionRemainingInputPackets( )
GetSessionRemainingInputOctets(div)

Returns the remaining number of packets/octets that can be received by the current user session.

GetSessionRemainingOutputPackets( )
GetSessionRemainingOutputOctets(div)

Returns the remaining number of packets/octets that can be sent by the current user session.

GetSessionRemainingTotalPackets( )
GetSessionRemainingTotalOctets(div)

Returns the remaining number of packets/octets that can be sent or received by the current user session.

GetSessionMaxInputPackets( )
GetSessionMaxInputOctets(div)

Returns the maximum number of packets/octets that can be received by the current user session.

GetSessionMaxOutputPackets( ) GetSessionMaxOutputOctets(div)

Returns the maximum number of packets/octets that can be sent by the current user session.

Session quotas

These functions let you retrieve the quota limits that are set for the current user session. If any of these limits are reached, the user is logged out. See *Quotas on page 15-70*.

If you specify a value for the optional parameter **div**, then the return value is the number of octets divided by **div**.

- Packets values are returned as a decimal string (10 characters) representing a 32-bit unsigned integer.
- Octet values are returned as a decimal string (20 characters) representing a 64-bit unsigned integer.

GetSessionRemainingInputPackets( ) GetSessionRemainingInputOctets(div)

Returns the number of incoming packets/octets the current user session can still receive.

GetSessionRemainingOutputPackets( ) GetSessionRemainingOutputOctets(div)

Returns the maximum number of outgoing packets/octets the current user session can still send.

GetMaxSessionInputPackets( ) GetMaxSessionInputOctets(div)

Returns the maximum number of incoming packets/octets the current user session can receive.

Returns the maximum number of incoming octets the current user session can receive.

GetMaxSessionOutputPackets( ) GetMaxSessionOutputOctets(div)

Returns the maximum number of outgoing packets/octets the current user session can send.

iPass support

iPassGetLoginUrl( )

Returns the iPass Login URL.

iPassGetAbortLoginUrl( )

Returns the iPass Abort Login URL.

iPassGetLogoffUrl( )

Returns the iPass Logout URL.

iPassGetRedirectResponseCode( )

Checks if the iPass authentication server is reachable and enabled. Returns one of the following values:

0	Authentication server is reachable and enabled.
105	The authentication server could not be reached or is unavailable.
255	The authentication server could not be reached due to an error on the controller (Internet port not up, for example).

iPassGetAccessProcedure( )

Returns the access procedure supported by the controller. The controller supports procedure version 1.0.

iPassGetLocationName( )

Returns the location ID defined on the **Public access > Access control** page.

iPassGetAccessLocation( )

Returns a value which can be used to determine the access point a user is connected to. This is useful when you are using one or more APs in addition to the controller.

- If a user logs into a AP, this function returns the MAC address of the AP's downstream port.
- If a user logs into the controller, this function returns the MAC address of the controller LAN port.

iPassGetLoginResponseCode( )

Returns one of the following values when a user attempts to login to iPass:

50	Login was successful.
100	Login failed. Access was rejected.
102	Login failed. Authentication server error or timeout.
201	Authentication is pending.
255	The authentication server could not be reached due to an error on the controller (Internet port not up, for example).

iPassGetLogoutResponseCode( )

Returns one of the following values when a user attempts to logout from iPass:

150	Logout was successful.
255	The authentication server could not be reached due to an error on the controller (Internet port not up, for example).

Web

GetWebFullURL("http" | "https")

This function returns the full URL (protocol, hostname and port) to the root of the Web server as either HTTP or HTTPS.

Example
var url = GetWebFullURL("http");

GetHTTPProtocol( )

Returns the protocol used when requesting the current Web page as a string. Possible values are:

- http
- https

Example
var protocol = GetHTTPProtocol();
write(protocol); /* will write either "http" or "https" depending on the URL you typed to view the page. */

Client information

LoadClientInformation( )

This function initializes a set of variables that provide information on the user that is requesting the current page.

ASP variables

- **client_username:** String containing the username of the user if known.
- **client_useraccount_index:** String that uniquely identifies the user's account.
- **client_ip_address:** String containing the IP address of the user that requested the page.
- **client_state:** The user's authentication state: **1** for authenticated, **0** otherwise If 0, all other variables will contain their last value, unless the user was never authenticated, in which case they will be blank.

- **client_session_time:** The user’s session time, indicating how many seconds have elapse since the user was first authenticated by the controller. Re-authentication will not affect the value unless the authentication was terminated.
- **client_session_idle_time:** Indicates how many seconds have elapsed since the controller first received traffic from this user that was inside the user's defined access-list destination(s).
- **client_session_transmitted_packets:** Number of packets the user has transmitted to destinations inside the user's defined access-list destination(s).
- **client_session_transmitted_bytes:** Number of bytes the user has transmitted to destinations inside the user's defined access-list destination(s).
- **client_session_received_packets:** Number of packets the user has received from sources inside the user's defined access-list destination(s).
- **client_session_received_bytes:** Number of bytes the user has received from sources inside the user's defined access-list destination(s).
- **client_subscription_plan_index:** The subscription plan index with which the user account is associated. A value of **0** indicates that the user account is not associated with a plan.
- **client_authentication_mode:** Indicates how the user was authenticated:

  0 - Unknown, authentication may be pending or the user is not authenticated.

  1 - Authenticated using the local user accounts.

  2 - Authenticated using a third-party RADIUS server.

  3 - Authenticated using Active Directory.
- **client_subscription_plan_name:** Name of the subscription plan assigned to the user. Additional information can be obtained using the function LoadSubscriptionPlanInformation().
- **client_subscription_plan_state:** User’s subscription plan state:

  0 - Plan is invalid, expired or no plan exists for that client.

  1 - Plan is valid.
- **client_ads_presentation:** User’s advertisement presentation state.

  0 - Advertisements are enabled for the user.

  1 - Advertisements are displayed for the user.
- **client_public_ip**: Indicates if the user’s IP address is public or private.

  0 - IP address is private.

  1 - IP address is public. For more information, see *Public IP address on page 3-10*.

- **client_public_ip_reserved:** Indicates if the public IP address is reserved or preferred.

  0 - Public IP is preferred.

  1 - Public IP is reserved.

  For more information, see *Public IP address on page 3-10*.

LoadClientAccountStatusInformation( )

This function initializes a set of variables that provide information on the current user.

ASP variables

- **client_account_status_is_online_time_exhausted**: Set to **1** if online time has been exhausted.
- **client_account_status_is_time_since_first_login_expired**: Set to **1** if time since first login has been exceeded its configured limit.
- **client_account_status_is_time_currently_outside_valid_period_of_day**: Set to **1** if the current time is outside the valid period for the account.
- **client_account_status_is_validity_period_not_begun**: Set to **1** if the validity period for the account has not yet begun.
- **client_account_status_is_validity_period_ended**: Set to **1** if the validity period for the account has ended.
- **client_account_status_is_input_octets_quota_exhausted**: Set to **1** if the download limit for the account has been exhausted.
- **client_account_status_is_output_octets_quota_exhausted**: Set to **1** if the upload limit for the account has been exhausted.
- **client_account_status_is_total_octets_quota_exhausted**: Set to **1** if the total traffic quota for the account has been exceeded.
- **client_account_status_first_login_time**: Time the user first logged in.
- **client_account_status_time_since_first_login**: Elapsed time since the user first logged in.
- **client_account_status_remaining_online_time**: Amount of online time remaining.
- **client_account_status_remaining_session_time**: Amount of time remaining for which the account is still valid.
- **client_account_status_expiration_time**: Date/time at which the account will expire. This is set by determining the first Validity period rule (*Defining subscription plans on page 10-35*) that will be reached, excluding the rules that apply to time limits during a day.
- **client_account_status_remaining_input_octets**: Amount of traffic the user can still download.

- **client_account_status_remaining_output_octets**: Amount of traffic the user can still upload.
- **client_account_status_remaining_total_octets**: Total amount of traffic the user can still upload or download.
- **client_account_status_active_sessions**: Number of sessions active on this account.

Subscription plan information

LoadSubscriptionPlanInformation(*subscription_plan*)

This function initializes a set of variables that provide information on the specified subscription plan.

ASP variables

- **subscription_plan_name:** Name of the plan.
- **subscription_plan_id:** ID which uniquely identifies each subscription plan.
- **subscription_plan_fee:** Subscription plan cost.
- **subscription_plan_tax:** Subscription plan tax. Calculated based on the subscription plan cost and the configured tax rate.
- **subscription_plan_total:** Total subscription plan charge.
- **subscription_plan_description:** Description of the plan.

GetFirstSubscriptionPlan( )

The function returns the first subscription plan name (as a string) configured on the controller for which billing is enabled.

Example

```
var plan;
for (plan = GetFirstSubscriptionPlan(); plan != ""; plan = GetNextSubscriptionPlan(plan)) {
LoadSubscriptionPlanInformation(plan);
}
```

GetNextSubscriptionPlan(*plan_name*)

Returns the next subscription plan name that follows the specified ***plan_name***. If ***plan_name*** is the last plan, an empty string is returned.

Example

```
var plan;
for (plan = GetFirstSubscriptionPlan(); plan != ""; plan = GetNextSubscriptionPlan(plan)) {
LoadSubscriptionPlanInformation(plan);
}
```

Other

AssignBillingRecordId( )

Use this function to reserve a billing record ID. If this function returns **0**, it means that the payment system has been halted. Any subscription-related activities should not be attempted until this function returns a non-zero value. See *Suspend payment system when log is full of queued records on page 14-42*).

Example

```
var billingRecordId = AssignBillingRecordId();
if (billingRecordId == 0) {
<p>The service is temporarily unavailable.Please try again later.</p>
}
```

ConditionalDisplay(*condition, state*)

This function is used to dynamically control execution of a block of code based on the value of a logical expression. An effective use for this function is to control blocks of display code, for certain features for example, that need to be turned on/off depending on user selections.

Parameters

- **Condition:** A logical embedded Javascript expression. If the expression is true, all content between the **Begin** and **End** function calls is executed.
- **State:** Indicates if this function marks the beginning or end of the block of code.
  - **Begin:** Marks the beginning of the code block.
  - **End:** Marks the end of the code block.

Example

```
<% ConditionalDisplay(client_state == 1, "begin"); %>
<p> Welcome to the wireless network.</p>
<% ConditionalDisplay(client_state == 1, "end"); %>
```

GetUserName( )

Returns the username for the current user.

GetAuthenticationErrorMessage( )

Reserved for use by **fail.asp** to display error messages for certain specific conditions. Do not use this function on other pages. Instead, use **LoadFormFieldError( )** or **GetSessionVar** with the variable **last_login_error.**

IncludeAsp(*filename*)

Pauses ASP processing in the current file and continue with the specified ASP **filename**.

Example

```
IncludeAsp("file.asp");
```

SetSessionRefreshInterval(sec)

Specifies the refresh interval for the session page in seconds.

write(*string*)

Writes the specified string to the browser.

Example

```
write("<p>You are connected.</p>");
```

LoadAccessInformation()

This function initializes a set of variables that provide information on the site access options configured on the **Controller >> Public access > Web content** page.

ASP variables

- **access_free:** Set to 1 if the **Free Access** option is enabled.
- **access_purchase:** Set to 1 if the **Allow creation of user accounts** option is enabled.

Example

```
LoadAccessInformation();
if (access_free) {
<p>Welcome to your free trial of the new high-speed wireless network service.</p>
}
```

LoadPaymentInformation()

This function initializes a set of variables that provide information on the current payment services configured on the **Controller >> Public access > Payment services** page.

ASP variables

- **payment_currency:** Contains the 3-letter code identifying the currency that will be used for all transactions.
- **payment_cc_gateway:** Returns a string that identifies the payment service that is configured. Either **authorize.net** or **worldpay**.

Example

```
LoadPaymentInformation();
if (payment_currency == "USD") {
 write(subscription_plan_fee + " $");
}
```

LoadWorldPayInformation()

This function initializes a set of variables that contain WorldPay-specific information.

ASP variables

- **worldpay_url:** String containing the configured WorldPay URL on the controller.
- **worldpay_installation_id:** String containing the configured WorldPay Installation ID on the controller.
- **worldpay_cart_id:** String containing a unique number for this order that represents a virtual cart in which items that are being bought are stored.

Example

```
LoadWorldPayInformation();
write(worldpay_url);
```

LoadTaxInformation( )

This function initializes a variable that provide information on the current tax setting configured on the **Controller >> Public access > Payment services** page.

ASP variable

- **tax_percent:** Tax rate that will be applied to all charges. The tax rate is configured on the controller.

Example

```
LoadTaxInformation();
write("Tax is " + tax_percent + "% here.");
```

Session information

The controller maintains a block of data, called a session, for each IP address that is connected to the public access interface. The session makes it possible to store and access data across more than one page in the public access interface.

Session variables are reset when:

- the ASP function ClearSessionVar() is called
- the user’s session is deleted or restarted

A session ends when 3 minutes passes without any user activity on the public access interface.

Session functions

GetSessionVar(*variable*)

Returns the value of the specified session variable.

ClearSessionVar(*variable*)

Clears the value of the specified session variable.

Session variables

The following session variables are provided:

- **last_login_error:** Contains the error number generated by the last login attempt. This is converted into the appropriate visual representation by the file **login_error_messages.asp**.

Value	Description
0 or ""	No error occurred.
1	A problem occurred that caused the current login process to stop before it completed. This is normally an issue related to an administrator changing the configuration which may cause a temporary failure.
2	The login was refused by the product or external authentication server.
3	The external authentication server was unreachable.
4	There is already another login from the user in progress, so this one has been stopped.
5	The user account username/password appear to be valid, however the account is invalid due to subscription plan usage being exceeded or validity limit being exceeded.
6	The user account username/password appear to be valid, however the associated account is administratively disabled.

- **username:** Contains the username a user submitted to login or define a subscription.
- **password:** Contains the password, as a sting of asterisks (***), a user submitted to login or define a subscription.
- **card_expiration:** Contains credit card expiration information in the form **mm/yy**.
- **card_number:** Contains the credit card number. The string contains all asterisks (*) with only the last four digits not hidden.
- **payment_method:** Contains the user's choice for payment method: Currently only supports the value: "CreditCard".
- **subscription_plan:** This variable hold the name of the subscription plan submitted in a subscription form.
- **cart_id:** Holds the cart ID for WorldPay payments. The cart ID is automatically generated and needs to be transmitted to the WorldPay Web site via a form. See the code in **payment.asp** for an example of how to do this.
- **authorize_net_reason:** Contains a text message indicating why the Authorize.Net credit card gateway refused a payment transaction.
- **authorize_net_transaction_id:** Contains the transaction ID that the Authorize.Net credit card gateway assigned to the transaction attempt. You can display this information to the user so that they can supply this information when calling for support.

- **last_subscription_error:** Contains the error number generated by the last subscription attempt. This is converted into the appropriate visual representation by the file **subscription_error_messages.asp**.

Value	Description
0 or ""	No error occurred.
1	A problem occurred that caused the current login process to stop before it completed. This is normally an issue related to an administrator changing the configuration which may cause a temporary failure.
2	The password and confirm password fields do not match.
3	The wrong password was supplied for the specified username.
4	An error occurred when creating the user account.
5	The subscription plan name is invalid.
6	The credit card payment failed.
7	The credit card payment succeeded, however an error occurred when activating the user account.
8	Reserved.
9	Reserved.
10	Same as #3, but indicates that user account creation is currently not allowed.

- **last_form_error:** Contains specific errors for each field in a form. To extract this information use the ASP functions described in under *Form errors on page 15-78*.

16

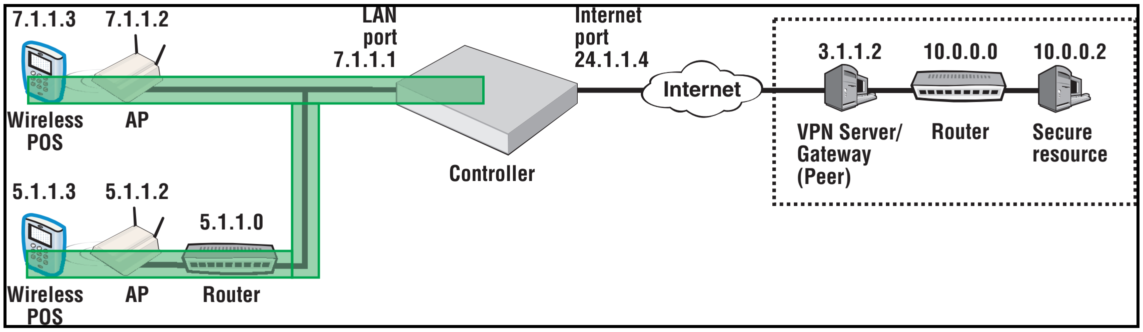
Working with VPNs

Contents

Overview

Virtual private networks (VPNs) create secure tunnels across non-secure infrastructure such as the Internet or publicly-accessible networks. The controller features virtual private network (VPN) capabilities that enable it to do the following:

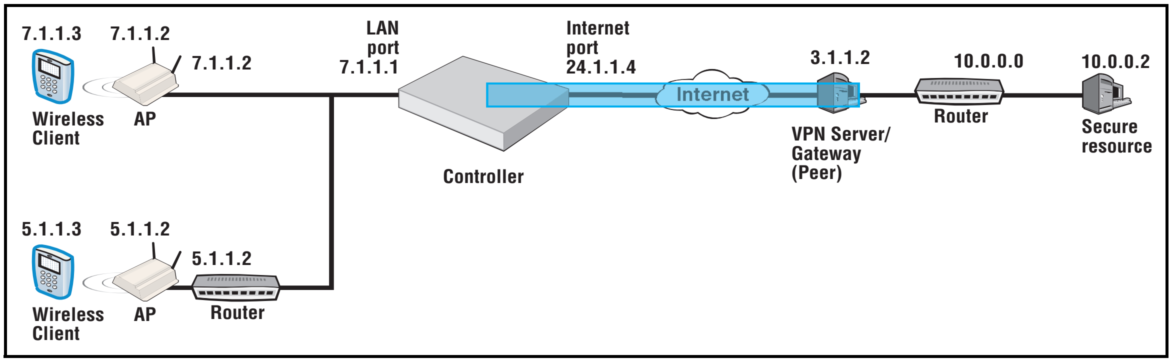
- Secure wireless client sessions with a VPN tunnel between wireless clients such as wireless point-of-sale (POS) terminals and the controller. IPSec, L2TP, and PPTP are all supported. (VPN tunnel represented in green.)



Note

For WPA-capable wireless clients, a better alternative to VPNs, is to extend WPA termination from the AP to the controller. See *Terminate WPA at the controller on page 5-24*.

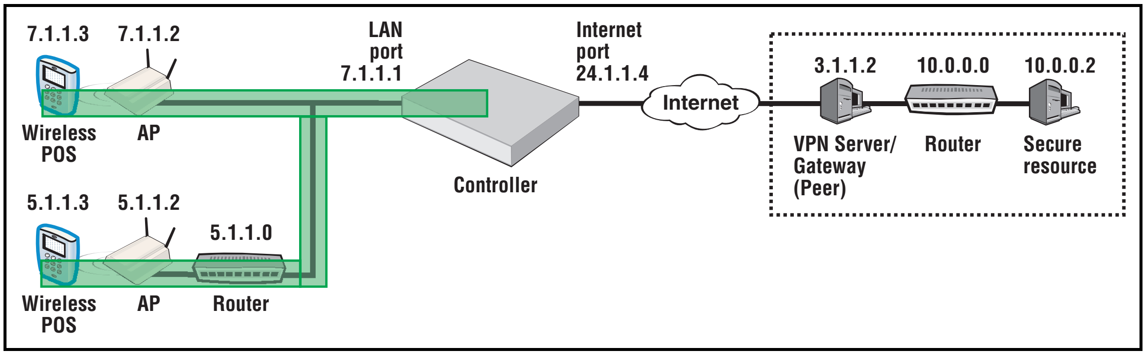
- Secure controller communications to VPN servers, including both management and client traffic. For example, the controller can securely contact a remote RADIUS server for user authentication. IPsec and PPTP are supported. (VPN tunnel represented in blue.)



Securing wireless client sessions with VPNs

Note The ability to secure wireless client sessions is intended for low-data-volume applications like that of wireless POS terminals.

To secure wireless client sessions, create a VPN tunnel from the wireless client to the controller. The sample topology seen earlier serves as an example for the sample configurations that follow. In this example, the controller LAN port has an IP address of 7.1.1.1, the APs are at 7.1.1.2 and 5.1.1.2, and the wireless POS are at 7.1.1.3 and 5.1.1.3.



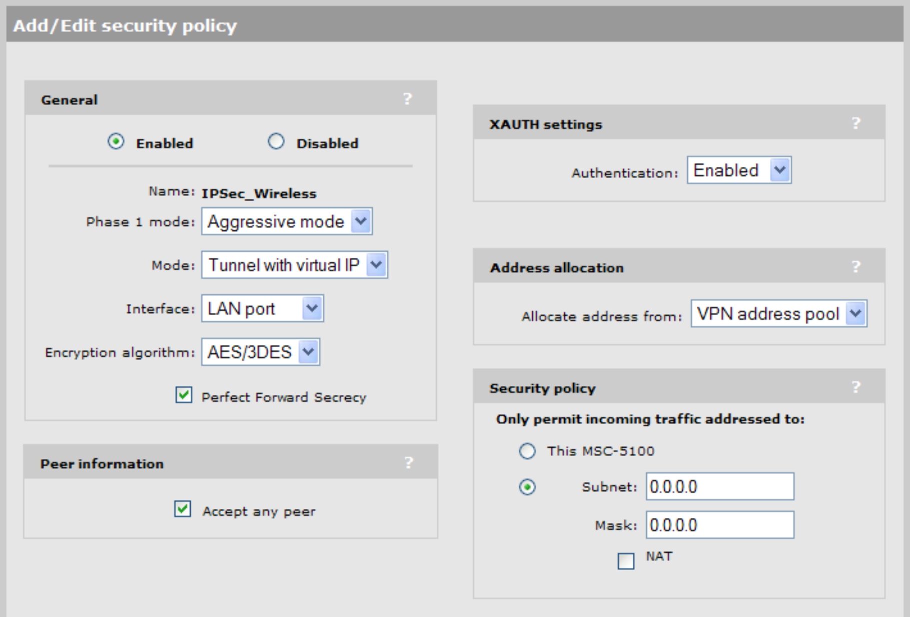
To use VPNs to secure wireless client sessions, configure an IPSec policy for this purpose, or configure the L2TP server or PPTP server.

Note Wireless clients are typically assigned IP addresses from the VPN address pool. Configure this first via **Controller >> Network > Address allocation > VPN address pool**. See *VPN address pool on page 16-5*.

Note Wireless clients require VPN software that is configured to work with your VPN configuration on the controller.

Configure an IPSec profile for wireless client VPN

1. On the page **Controller > VPN > IPSec** select **Add Policy**, and define a policy similar to this:



Add/Edit security policy

General

● Enabled ○ Disabled

Name: IPSec_Wireless

Phase 1 mode: Aggressive mode

Mode: Tunnel with virtual IP

Interface: LAN port

Encryption algorithm: AES/3DES

☑ Perfect Forward Secrecy

Peer information

☑ Accept any peer

XAUTH settings

Authentication: Enabled

Address allocation

Allocate address from: VPN address pool

Security policy

Only permit incoming traffic addressed to:

○ This MSC-5100

● Subnet: 0.0.0.0

Mask: 0.0.0.0

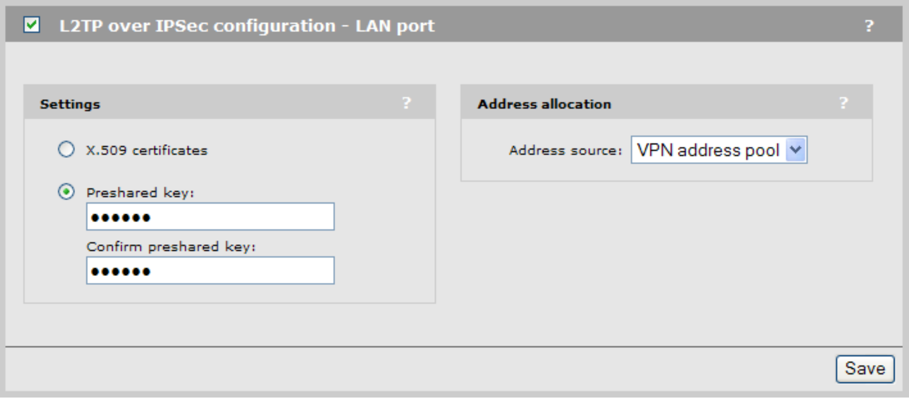
□ NAT

Note the selections made in the sample **Add/Edit security policy** page above. See the online help for option descriptions.

Option	Value to set	Notes
General	Enabled	
Name	User-defined	
Phase 1 mode	**Aggressive mode**	Aggressive mode requires that a group be configured. See *Local group list on page 16-11*.
Mode	**Tunnel with Virtual IP**	Allows IP addresses to be assigned to the wireless clients.
Interface	**LAN port**	
Encryption algorithm	Select as desired	
Perfect Forward Secrecy	Leave enabled	
Accept any peer	Enabled	Accepts any wireless client.
XAUTH > Authentication	Enabled	
Allocate address from	**VPN address pool**	First define address pool on **Network > Address allocation**.
Security policy	Subnet and Mask of **0.0.0.0**	A Subnet and Mask of 0.0.0.0. causes all wireless traffic between the client and the controller to be accepted.

Configure L2TP server for wireless client VPN

1. On the page **Controller >> VPN > L2TP server** enable **L2TP over IPSec configuration- LAN port**.



☑ L2TP over IPSec configuration - LAN port

Settings

○ X.509 certificates

● Preshared key: ••••••

Confirm preshared key: ••••••

Address allocation

Address source: VPN address pool

2. Either select X**.509 certificates** and install an X.509 security certificate (see *IPSec certificates on page 12-11*), or specify a **Preshared key**.

Note

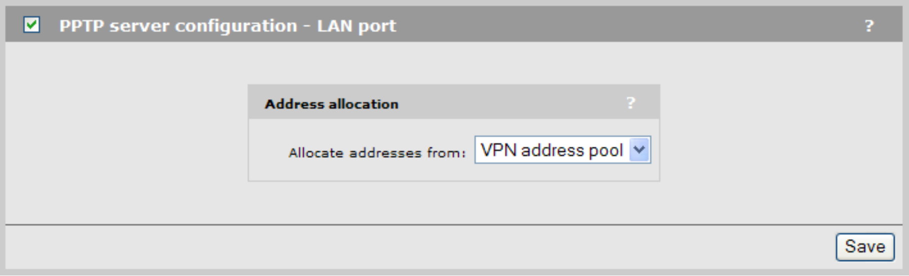
The VPN client running on the wireless device must also be configured with a matching X.509 certificate, or the **Preshared key** specified here.

3. Set **Address source** to **VPN address pool**.

   See the online help for option descriptions.

Configure PPTP server for wireless client VPN

1. On the page **Controller >> VPN > PPTP server** enable **PPTP server configuration - LAN port**.



☑ PPTP server configuration - LAN port

Address allocation

Allocate addresses from: VPN address pool

2. Set **Address source** to **VPN address pool**. See the online help for option descriptions.

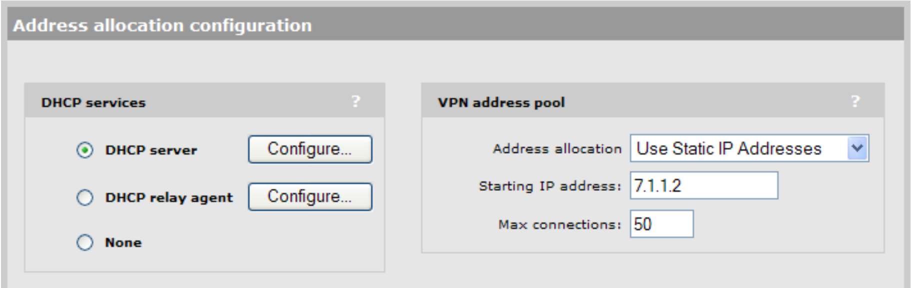
VPN address pool

When securing wireless client sessions with VPNs, it is typically necessary to provide an IP address to each client. To define a pool of addresses for this purpose, follow this procedure.

1. Select **Network > Address allocation**.

2. In **VPN address pool**, for **Address allocation** select either **Use static IP addresses** or **Use external DHCP server**.

   - For **Use static IP addresses**, define a sequential pool of addresses by specifying the **Starting IP address** and **Max connections**. For example a Starting IP address of 7.1.1.2 and a Max connections of 50, will yield a pool of IP addresses in the range 7.1.1.2 through 7.1.1.51.



Address allocation configuration

DHCP services

● DHCP server Configure...

○ DHCP relay agent Configure...

○ None

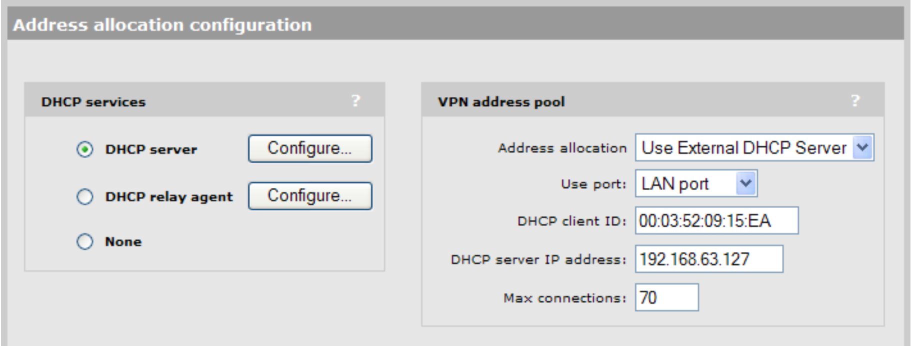
VPN address pool

Address allocation: Use Static IP Addresses

Starting IP address: 7.1.1.2

Max connections: 50

   - For **Use external DHCP server**, specify settings that correspond to your external DHCP server configuration. Set **Use port** to the controller port that will send out DHCP requests.



Address allocation configuration

DHCP services

● DHCP server Configure...

○ DHCP relay agent Configure...

○ None

VPN address pool

Address allocation: Use External DHCP Server

Use port: LAN port

DHCP client ID: 00:03:52:09:15:EA

DHCP server IP address: 192.168.63.127

Max connections: 70

3. Select **Save**.

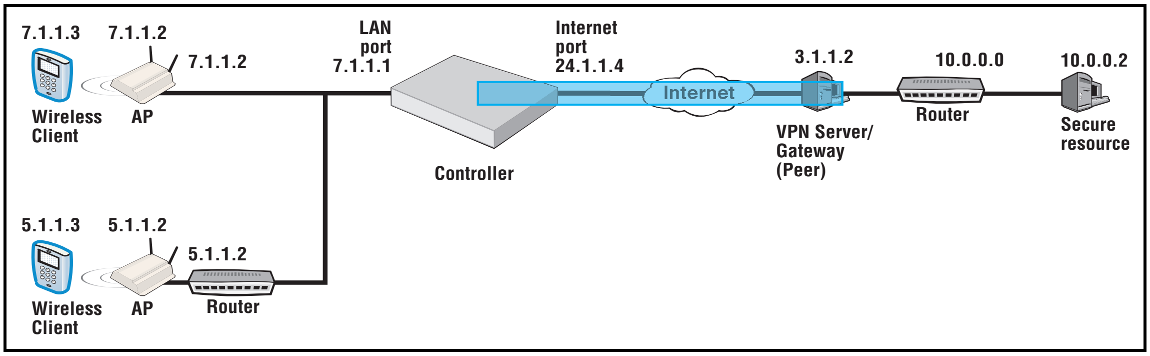
   See the online help for option descriptions.

Securing controller communications to remote VPN servers

To secure the communications between the controller and remote VPN servers, create a VPN tunnel from the controller to the remote VPN server.

The sample topology seen earlier serves as an example for the sample configurations that follow. In this example, the controller Internet port has an IP address of 21.1.14, the remote VPN server is at 3.1.1.2, and the secure resource is at 10.0.0.2.

Create a VPN tunnel like this either by configuring an IPSec policy or configuring the PPTP client.

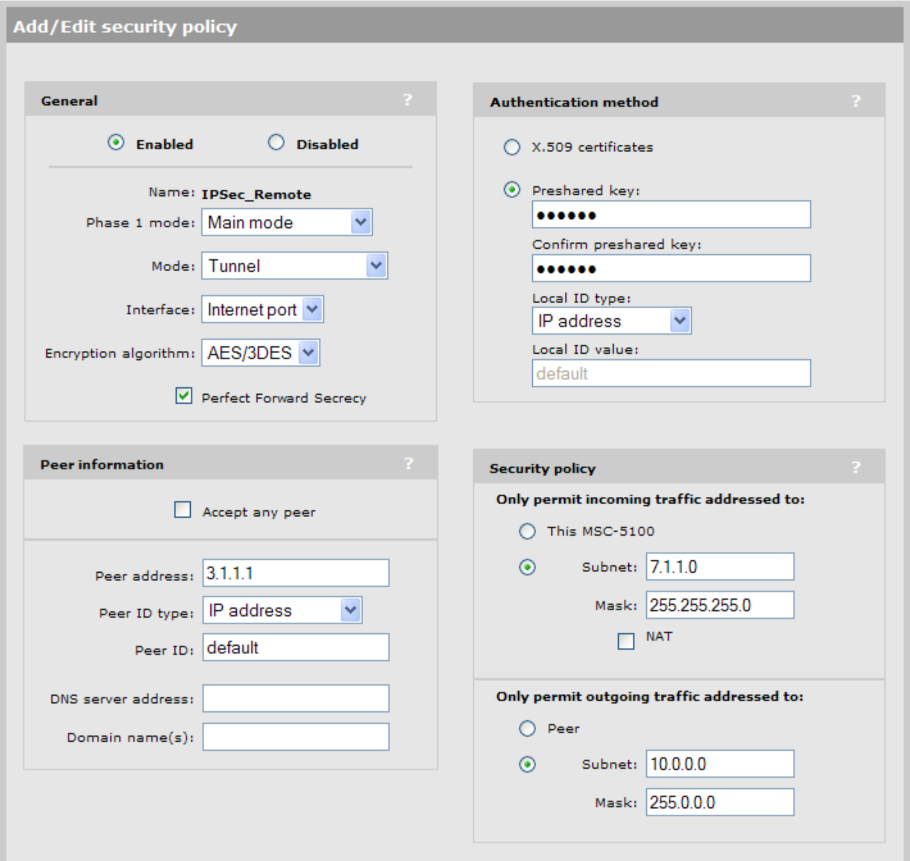


Caution

The VPN tunnel should not be used to transport user traffic. The tunnel should only be used to carry management traffic (RADIUS, SNMP, and management sessions). See *Keeping user traffic out of the VPN tunnel on page 16-10*.

Configure an IPSec policy for a remote VPN server

1. On the page **Controller >> VPN > IPSec** select **Add New Policy** and define a policy similar to this, substituting your own IP addresses:



Add/Edit security policy

General

● Enabled ○ Disabled

Name: IPSec_Remote
Phase 1 mode: Main mode
Mode: Tunnel
Interface: Internet port
Encryption algorithm: AES/3DES
☑ Perfect Forward Secrecy

Peer information

☐ Accept any peer

Peer address: 3.1.1.1
Peer ID type: IP address
Peer ID: default
DNS server address:
Domain name(s):

Authentication method

○ X.509 certificates
● Preshared key: ••••••
Confirm preshared key: ••••••
Local ID type: IP address
Local ID value: default

Security policy

Only permit incoming traffic addressed to:

○ This MSC-5100
● Subnet: 7.1.1.0
Mask: 255.255.255.0
☐ NAT

Only permit outgoing traffic addressed to:

○ Peer
● Subnet: 10.0.0.0
Mask: 255.0.0.0

Note the selections made in the sample **Add/Edit security policy** page above.

Option	Value to set	Notes
General	Enabled	
Name	user-defined	
Phase 1 mode	**Main mode**	
Mode	**Tunnel**	
Interface	**Internet port**	
Encryption algorithm	Select as desired	
Perfect Forward Secrecy	Leave enabled	
Accept any peer	Disabled	
Peer information	User-defined	Set according to VPN server needs. In this example, the VPN server address is 3.1.1.1.
Authentication method	User-defined	Set according to VPN server needs. Either the X.509 certificates or the Preshared key must match server configuration.
Security policy > Only permit incoming...	Identify the subnet	Identify the local subnet for which you wish to filter traffic, for example, 7.1.1.0. This must match the value defined in the policy on the peer (VPN server).
Only permit outgoing...	Identify the remote subnet	Identify the remote subnet for which you wish to filter traffic, for example, 10.0.0.0. This must match the value defined in the policy on the peer (VPN server).

See the online help for option descriptions.

See *Keeping user traffic out of the VPN tunnel on page 16-10*.

Configure PPTP client for a remote VPN server

Configure the PPTP client for the controller VPN client capability via the **Controller >> VPN > PPTP client** menu.

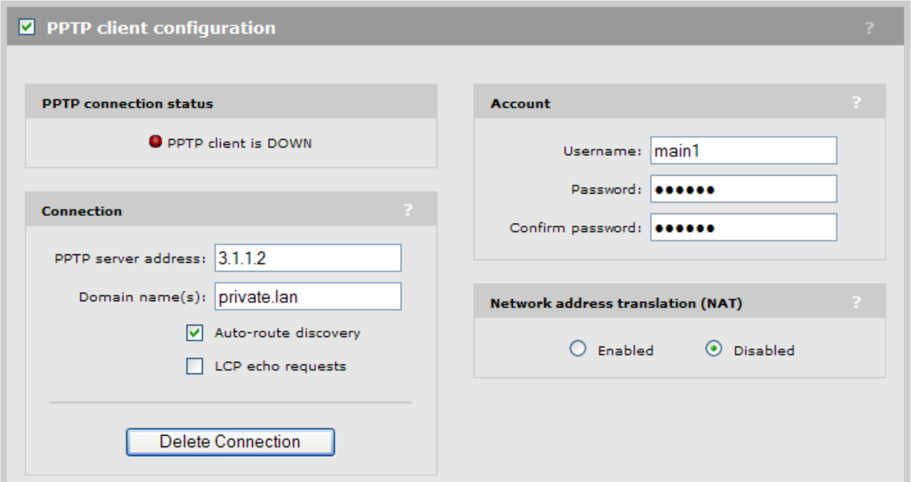
The PPTP client enables the controller to create a secure tunnel to any device that provides a PPTP server. All traffic sent though this tunnel is protected against eavesdropping by means of encryption.

Note

The PPTP tunnel should not be used to transport user traffic. To prevent user traffic from entering the tunnel, you must define access list definitions to DENY access to all subnets on the other side of the tunnel. The tunnel should be used to carry management traffic only (RADIUS, SNMP, management sessions). See *Keeping user traffic out of the VPN tunnel on page 16-10*.

Configuration

To view and configure the PPTP client, select **Controller >> VPN > PPTP client**. The PPTP client is disabled by default.



☑ PPTP client configuration

PPTP connection status

● PPTP client is DOWN

Connection

PPTP server address: 3.1.1.2

Domain name(s): private.lan

☑ Auto-route discovery

□ LCP echo requests

Account

Username: main1

Password: ●●●●●●

Confirm password: ●●●●●●

Network address translation (NAT)

○ Enabled ● Disabled

Connection

PPTP server address

Specify the domain name or IP address of the PPTP server the controller will connect to.

Domain name(s)

Specify the domain name(s) that are reachable through the tunnel. Put a space between each name as a separator. The controller routes all traffic addressed to this domain through the PPTP connection. If you do not want to enter a Domain name, enter **private.lan** instead.

Auto-route discovery

Enable this option if you want the controller to automatically discover and add routes to IP addresses on the other side of the PPTP tunnel. The addresses must be part of the specified domain. Routes are added only when an attempt is made to access the addresses.

LCP echo requests

Certain VPN servers may terminate your connection if it is idle. If you enable this option, the controller will send a packet from time to time to keep the connection alive.

Account

Username

Specify the username the controller will use to log on to the PPTP server. If you are logging on to a Windows XP domain, specify **domain_name\username**

Password / Confirm password

Specify the password the controller will use to log on to the PPTP server.

Network Address Translation (NAT)

If you enable NAT, it effectively hides the addresses of all local computers so that they are not visible on the other side of the PPTP connection.

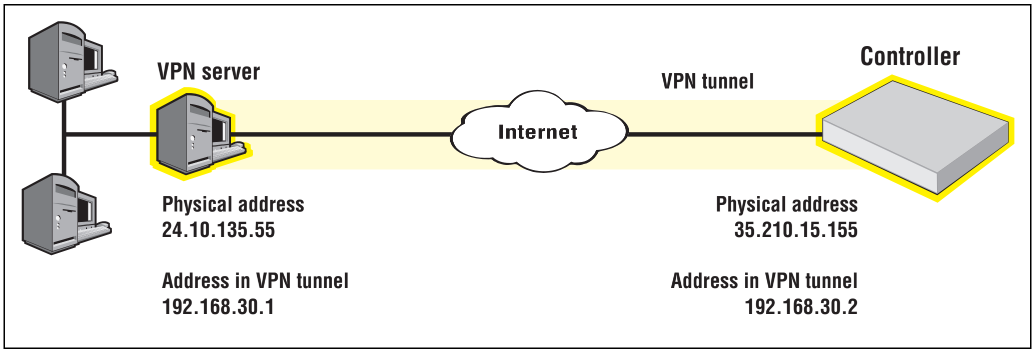
If you disable NAT, then the appropriate IP routes must be added to send traffic through the tunnel.

Keeping user traffic out of the VPN tunnel

Note The VPN tunnel should not be used to transport user traffic. The tunnel should only be used to carry management traffic (RADIUS, SNMP, and management sessions).

To prevent user traffic from entering the tunnel, you must define access list definitions to DENY access to all subnets on the other side of the tunnel.

Consider the following scenario:



To protect the VPN, add the following definitions to the site access list:

```
access-list=vpn,DENY,all,192.168.30.0/24,all
use-access-list=vpn
```

This definition applies to all users, whether they are authenticated or not. It blocks access to the VPN subnet for all traffic. For more information on using the access list feature, see *Access list on page 15-34*.

Additional IPSec configuration

The page **Controller >> VPN > IPSec** provides some additional configuration options and information. For information about IPsec certificates see *IPSec certificates on page 12-11*.

IPSec VLAN mapping

Use these settings to define how IPSec traffic is routed on the LAN and Internet ports. You can assign traffic to the untagged interface (no VLAN) or to any defined VLAN.

Local group list

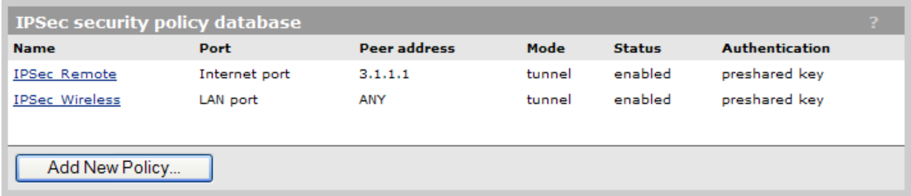
When using IPSec aggressive mode, groups can be used to authenticate IPSec connections from clients (peers). The client must supply the group name matching one of the groups defined here to establish a security association with the controller.

Create all needed groups, providing information as follows:

- Group name: Group names are case-sensitive and should be in the format user@FQDN.com or FQDN.com. For example, fred@mycompany.com or server99.mycompany.com.
- Password/Confirm password: Passwords must be at least six characters long and contain at least four different characters.

IPSec security policy database

The **IPSec security policy database** table shows all the IPSec security policies that are defined on the controller. A security policy defines the criteria that must be met for a peer to establish an IPSec security association (SA) with the controller.



IPSec security policy database

Name	Port	Peer address	Mode	Status	Authentication
IPSec Remote	Internet port	3.1.1.1	tunnel	enabled	preshared key
IPSec Wireless	LAN port	ANY	tunnel	enabled	preshared key

This information is provided:

- **Name**: Name assigned to the security policy.
- **Port**: Port assigned to the security policy.
- **Peer address**: Address of the peer which can establish an SA using this policy.
- **Mode**: Indicates the IPSec mode (tunnel or transport) supported by this policy.
- **Status**: Indicates whether the policy has been enabled. An SA can only be established when a policy is enabled.
- **Authentication**: Indicates the method used to authenticate peers.

17

LLDP

Contents

Overview

The IEEE 802.1AB Link Layer Discovery Protocol (LLDP) provides a standards-based method for network devices to discover each other and exchange information about their capabilities. An LLDP device advertises itself to adjacent (neighbor) devices by transmitting LLDP data packets on all ports on which outbound LLDP is enabled, and reading LLDP advertisements from neighbor devices on ports that are inbound LLDP-enabled. An LLDP enabled port receiving LLDP packets inbound from neighbor devices stores the packet data in a Neighbor database (MIB).

LLDP information is used by network management tools to create accurate physical network topologies by determining which devices are neighbors and through which ports they connect.

LLDP operates at layer 2 and requires an LLDP agent to be active on each network interface that will send and receive LLDP advertisements. LLDP advertisements can contain a variable number of TLV (type, length, value) information elements. Each TLV describes a single attribute of a device.

When an LLDP agent receives information from another device, it stores it locally in a special LLDP MIB (management information base). This information can then be queried by other devices via SNMP. For example, the HP ProCurve Manager software retrieves this information to build an overview of a network and all its components.

Note LLDP information is only sent/received on Ethernet links. LLDP information is not collected from wireless devices connected to an AP.

LLDP-MED

LLDP provides the base capabilities for network devices, but was not considered sufficient for IP telephony devices. As a result, in 2004, an initiative by ProCurve and was undertaken to enhance LLDP so that it could better support IP telephony devices. The development of LLDP-Medium Endpoint Discovery (LLDP-MED) (ANSI/TIA-1057/D6) extended the LLDP standard to support advanced features on the network edge for VoIP endpoint devices with specialized capabilities and LLDP-MED standards-based functionality. The extensions to LLDP include the specification of additional TLV (Type, Length, and Value) entries specifically for VoIP management. LLDP-MED benefits include:

- Plug-and-play provisioning for MED-capable, VoIP endpoint devices.
- Simplified, vendor-independent management enabling different IP telephony systems to interoperate on one network.
- Automatic deployment of convergence network policies that includes voice VLANs, Layer2/CoS priority, and Layer 3/QoS priority.
- Configurable endpoint location data to support the Emergency Call Service (ECS) such as Enhanced 911, 999 and 112.
- Detailed VoIP endpoint data inventory readable via SNMP from the switch.

- Power over Ethernet (PoE) status and troubleshooting support via SNMP.
- Support for IP telephony network troubleshooting of call quality issues via SNMP.

LLDP-MED endpoint devices are located at the network edge and communicate using the LLDP-MED framework. Any LLDP-MED endpoint device belongs to one of the following three classes:

- Class 1 (Generic Endpoint Devices): These devices offer the basic LLDP discovery services, network policy advertisement (VLAN ID, Layer 2/802.1p priority, and Layer 3/ DSCP priority), and PoE management. This class includes such devices as IP call controllers and communication-related servers.
- Class 2 (Media Endpoint Devices): These devices offer all Class 1 features plus media streaming capability, and include such devices as voice/media gateways, conference bridges, and media servers.
- Class 3 (Communication Devices): These devices are typically IP phones or end-user devices that otherwise support IP media and offer all Class 1 and Class 2 features, plus location identification and emergency 911 capability, Layer 2 switch support, and device information management.

Local mesh

LLDP is not supported over local mesh links when running in controlled mode.

In autonomous mode, each AP only sees the APs with which it has a local mesh link as neighbors.

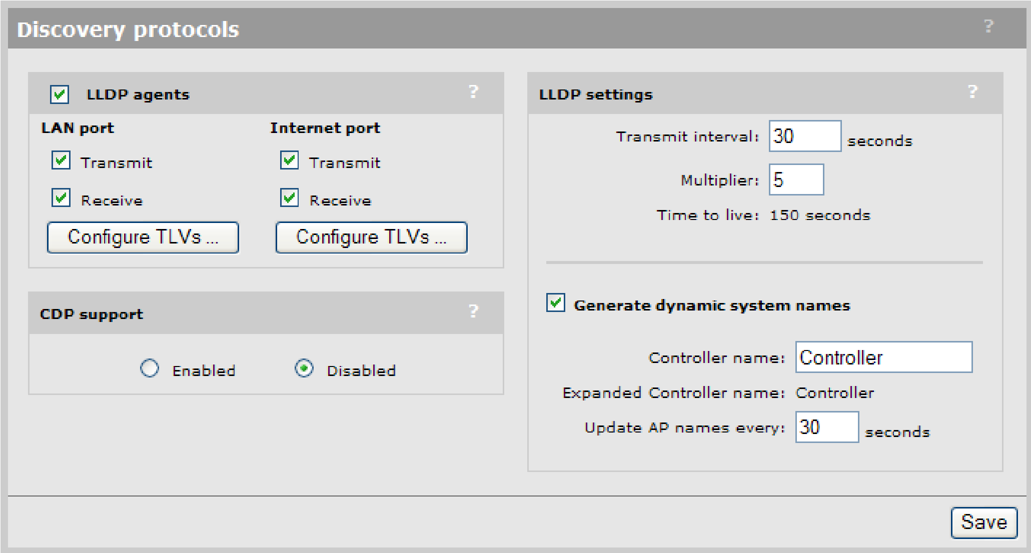
SNMP support

Support is provided for the following Physical Topology MIB (RFC 2922).

Note When operating in controlled mode the LLDP agents on controlled APs cannot be queried via SNMP. Instead, all LLDP information from the APs is stored in the controller’s MIBs.

Configuring LLDP on the controller

Controller settings are defined by selecting **Controller >> Network > Discovery protocols**.



Discovery protocols

☑ LLDP agents

LAN port
☑ Transmit
☑ Receive

Internet port
☑ Transmit
☑ Receive

CDP support
○ Enabled ● Disabled

LLDP settings
Transmit interval: 30 seconds
Multiplier: 5
Time to live: 150 seconds

☑ Generate dynamic system names
Controller name: Controller
Expanded Controller name: Controller
Update AP names every: 30 seconds

LLDP agents

Select this option to globally activate LLDP support on the controller.

LAN port / Internet port

For each port, select whether the agent will transmit and/or receive LLDP information. Select **Configure TLVs** to customize TLV support for each interface.

Transmit

Enable this option to have the agent transmit LLDP information to its neighbors.

Receive

Enable this option to have the agent accept LLDP information from its neighbors.

LLDP settings

Use these options to define global LLDP settings on the controller.

Transmit interval

Sets the interval (in seconds) at which local LLDP information is updated and TLVs are sent to neighboring network devices.

Multiplier

The value of **Multiplier** is multiplied by the **Transmit interval** to define the length of **Time to live.**

Time to live
Indicates the length of time that neighbors will consider LLDP information sent by this agent to be valid. **Time to live** is automatically calculated by multiplying **Transmit interval** by **Multiplier**.

Generate dynamic system names

When enabled, this feature replaces the system name with a dynamically generated value which you can define.

Controller name
Specify how the dynamically generated name will be created. You can use regular text in combination with placeholders to create the name. Placeholders are automatically expanded each time the name is regenerated.

If the placeholders cause the generated name to exceed 32 characters, it is truncated.

Placeholders

- **%RN:** System name of the neighboring device to which the port is connected, obtained via the System Name TLV. Since this is an optional TLV, if it is not available, the Chassis ID TLV is used instead.
- **%RP:** Port description of the port on the neighboring device to which the local port is connected, obtained via the Port Description TLV. Since this is an optional TLV, if it is not available, the Port ID TLV is used instead.
- **%SN:** Controller’s serial number.
- **%IP:** Controller’s IP address. An IP address can require up to 15 characters (nnn.nnn.nnn.nnn).

Note

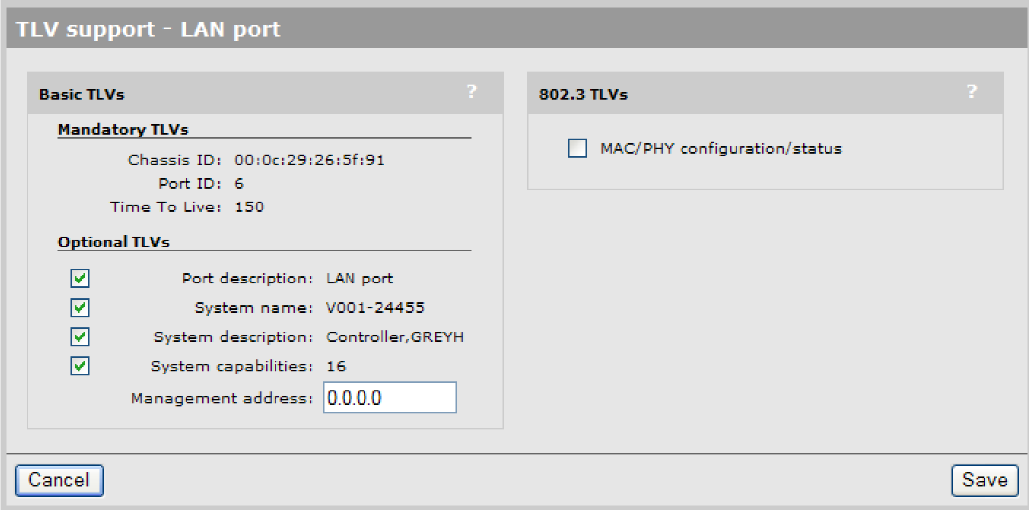
- When the LLDP agent is active on both the LAN port and the Internet port, the name generated on the LAN port is used for both interfaces.
- The dynamic name on the controller is only updated when a change is detected in the neighbor to which a port is connected.
- Once AP names are dynamically changed by this feature, there is no way to return to the old AP names.
- To define the suffix for APs, select **Controlled APs >> Configuration > LLDP**.

Expanded controller name
Shows the generated name with all placeholders expanded. To see the generated name you must select **Save**, wait about 10 seconds, and then select the **Refresh** button in your browser.

Update AP names every *nn* seconds
Specify the interval at which dynamic names for all controlled APs are updated.

TLV settings

To customize TLV settings, select **Configure TLVs** on the **Controller >> Network > Discovery protocols** page. The same TLV settings are available on both the LAN port and the Internet port.



Mandatory TLVs

Chassis ID: 00:0c:29:26:5f:91
Port ID: 6
Time To Live: 150

Optional TLVs

☑ Port description: LAN port
☑ System name: V001-24455
☑ System description: Controller,GREYH
☑ System capabilities: 16
Management address: 0.0.0.0

□ MAC/PHY configuration/status

Basic TLVs

The controller supports all mandatory and optional TLVs (type, length, value) information elements that are part of the basic management set.

Mandatory TLVs

The controller always sends these TLVs with the values as shown.

- **Chassis ID** (Type 1): The MAC address of the controller.
- **Port ID** (Type 2): The MAC address of the port on which the TLV will be transmitted.
- **Time to live** (Type 3): Defines the length of time that neighbors will consider LLDP information sent by this agent to be valid. Calculated by multiplying **Transmit interval** by the **Multiplier** (as defined on the **Discovery protocols** page).

Optional TLVs

Select the optional TLVs that you want to send with the values as shown.

- **Port description** (Type 4): A description of the port.
- **System name** (Type 5): Administrative name assigned to the device from which the TLV was transmitted. By default this is the SNMP system name. If the **Dynamic system name** option is enabled, the system name is replaced by the dynamically generated name. The controller can only have one system name. If both the LAN and Internet ports have active agents, then the name generated by the LAN port is used.
- **System description** (Type 6): Description of the system, comprised of the following information: hardware serial number, hardware revision number, and firmware version.

- **System capabilities** (Type 7): Indicates the primary function of the device. Set to:
  - **WLAN access point** for APs
  - **Router** for controllers.
- **Management IP address** (Type 8): The controller **always** sends a management IP address TLV containing the IP address of the port. This optional TLV lets you specify a secondary IP address on which the agent will respond to management requests. If set to 0.0.0.0, no secondary address is sent.

802.3 TLVs

The IEEE 802.3 organizationally specific TLV set is optional for all LLDP implementations. The controller supports a single optional TLV from the 802.3 definition.

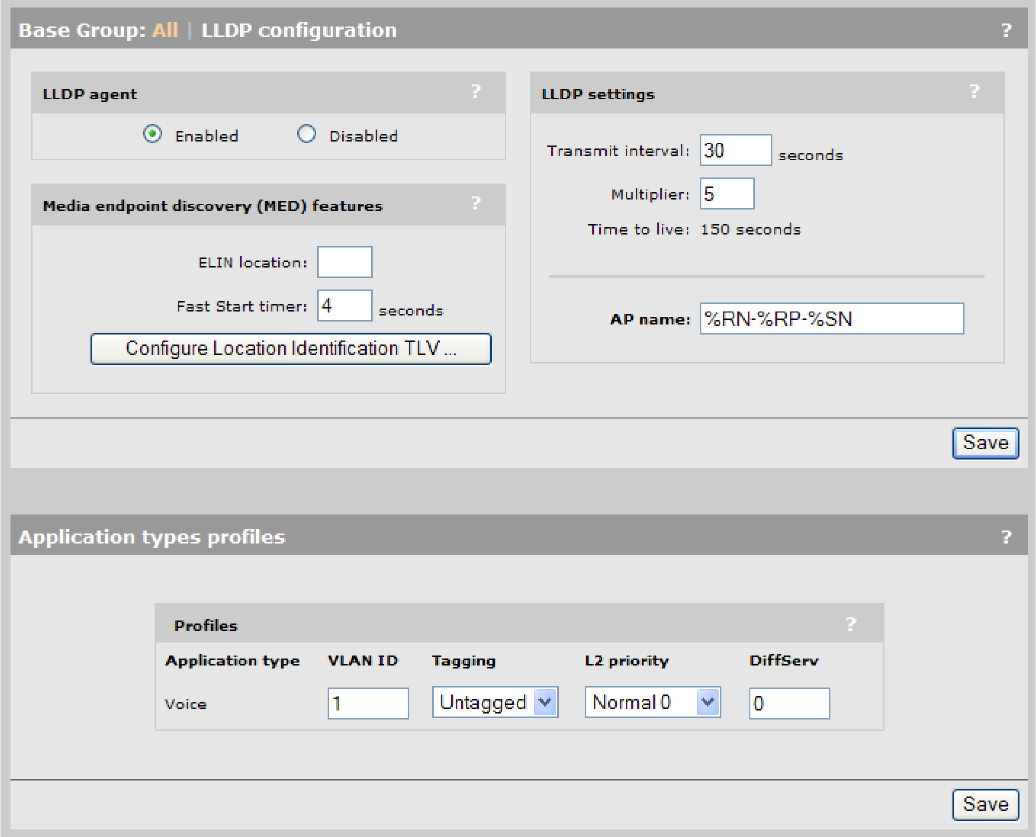
MAC/PHY configuration/status

This TLV provides the following information:

- Bit-rate and duplex capability
- Current duplex and bit-rating
- Whether these settings were the result of auto-negotiation during link initiation or manual override.

Configuring LLDP on an AP

AP settings are defined by selecting **Controlled APs >> Configuration > LLDP**.



Base Group: All | LLDP configuration

LLDP agent

● Enabled ○ Disabled

Media endpoint discovery (MED) features

ELIN location:

Fast Start timer: 4 seconds

LLDP settings

Transmit interval: 30 seconds

Multiplier: 5

Time to live: 150 seconds

AP name: %RN-%RP-%SN

Application types profiles

Profiles

Application type	VLAN ID	Tagging	L2 priority	DiffServ
Voice	1	Untagged	Normal 0	0

LLDP agent

Enable this option to activate LLDP support on the AP. When active, the agent will transmit and receive LLDP information.

When operating in controlled mode:

- The LLDP agent on an AP will not respond to SNMP requests. Therefore, local and remote MIB information is not available to external devices via the AP. Instead, this information can be retrieved from the controller.
- LLDP is not supported on local mesh links.

Supported TLVs

The LLDP agent on an AP supports the following Basic TLVs:

Mandatory TLVs

- Chassis ID (Type 1): The MAC address of the AP.
- Port ID (Type 2): The MAC address of port on which the TLV will be transmitted.

- Time to live (Type 3): Defines the length of time that neighbors will consider LLDP information sent by this agent to be valid. Calculated by multiplying **Transmit interval** by the **Multiplier**.

Optional TLVs

- Port description (Type 4): A description of the port.
- System name (Type 5): Administrative name assigned to the device from which the TLV was transmitted. By default this is the SNMP system name. If the **Dynamic system name** option is enabled, the system name is replaced by the dynamically generated name.
- System description (Type 6): Description of the system, comprised of the following information: operational mode, hardware type, hardware revision, and firmware version.
- System capabilities (Type 7): Indicates the primary function of the device. Set to: **WLAN access point.**

Media endpoint discovery (MED) features

The MED LLDP extensions specify two kinds of network devices: *network connectivity* and *endpoint*. Network connectivity devices connect endpoint devices to an IEEE 802-based LAN infrastructure. This means that HP access points and controllers are network connectivity devices. Endpoint devices are located at the network edge, and include devices such as IP phones, IP media servers, and IP communication controllers.

A network connectivity device does not send LLDP-MED TLVs on any port unless it detects an endpoint device connected to the port and receives LLDP-MED TLVs from the endpoint device.

The LLDP-MED TLVs supported by HP APs are as follows:

TLV name	Description
LLDP-MED Capabilities	Indicates the supported capabilities on the device by setting the appropriate bit to 1. ■ Bit 0: LLDP-MED Capabilities ■ Bit 1: Network Policy ■ Bit 2: Location Identification ■ Bit 3: Extended Power via MDI - PSE (only supported on the MSM317) ■ Bit 4: Extended Power via MDI - PD (not supported) ■ Bit 5: Inventory inventory ■ Bits 6-15: Reserved

TLV name	Description
Network Policy	The network policy TLV is a fixed length TLV that indicates a port VLAN type, VLAN identifier (VID), and both the Layer 2 and Layer 3 priorities associated with a specific set of application types.
Location Identification	Indicates the physical location of the device using the following form: ■ Emergency Call Services ELIN, as described for example by NENA TID 07-501.
Extended Power-via-MDI	Indicates the IEEE 802.1af (PoE) power related information on the device which includes: ■ Power type ■ Power source ■ Power priority ■ Power value
MAC/PHY Configuration/ Status	Indicates the following: ■ Bit-rate and duplex capability ■ Current duplex and bit-rating ■ Whether these settings were the result of auto-negotiation during link initiation or manual override

ELIN location
Emergency Call Services ELIN as described, for example, by NENA TID 07-501.

Fast Start timer
After an MED LLDPDU is received, this timer is started and the agent sends one MED LLDPDU to the MED device each second.

LLDP settings

Transmit interval
Sets the interval (in seconds) at which local LLDP information is updated and TLVs are sent to neighboring network devices.

Multiplier
The value of **Multiplier** is multiplied by the **Transmit interval** to define **Time to live.**

Time to live
Indicates the length of time that neighbors will consider LLDP information sent by this agent to be valid. **Time to live** is calculated by multiplying **Transmit interval** by **Multiplier**.

AP name
When the **Generate dynamic system names** option is enabled on the **Controllers >> Network > Discovery protocols** page, the system name of the AP will be replaced with a dynamically generated name that you define.

Specify how the dynamically generated name will be created. You can use regular text in combination with placeholders to create the name. Placeholders are automatically expanded each time the name is regenerated.

If the placeholders cause the generated name to exceed 32 characters, it is truncated.

Placeholders

- **%RN:** System name of the neighboring device to which the port is connected, obtained via the System Name TLV. Since this is an optional TLV, if it is not available, the Chassis ID TLV is used instead.
- **%RP:** Port description of the port on the neighboring device to which the local port is connected, obtained via the Port Description TLV. Since this is an optional TLV, if it is not available, the Port ID TLV is used instead.
- **%SN:** The AP serial number.
- **%IP:** The AP IP address. An IP address can require up to 15 characters (nnn.nnn.nnn.nnn).

Important
Once a system name is dynamically changed by this feature, there is no way to automatically return to the original system name.

Application type profiles

Application type profiles are used to define configuration settings which can be applied to the Application Type field in a Network Policy TLV on a MSM317 switch port.

The Network Policy TLV enables the MSM317 switch port to send configuration information to voice devices such as IP phones. To configure use of the Network Policy TLV, select **Controlled APs >> Configuration > Switch ports > {*switch-port*}**.

Application type

This release only supports the **Voice** application type.

VLAN ID

Specify a VLAN ID for this profile. This VLAN will be assigned to the switch port.

VLAN tagging

- Tagged: The VLAN is tagged.
- Untagged: The VLAN is untagged.

L2 priority

Select the layer 2 priority setting. This setting is used instead of the **Default traffic priority** set for the switch port. Supported settings are:

L2 priority	QoS queue
Low - 1 Low - 2	4
Normal - 0 Normal - 3	3
High - 4 High - 5	2
Very high - 7 Very high - 7	1

DiffServ

This value only applies if **VLAN tagging** is set to **Tagged**.

Specify a value for the Differentiated Services codepoint (DSCP) field in IPv4 and IPv6 packet headers (as defined in RFC2474). The codepoint is composed of the six most significant bits of the DS field.

DiffServ codepoint (DSCP) value	QoS queue
> 33	1
26 - 33	2
18 - 25	3
1 - 17	4
0	Disabled

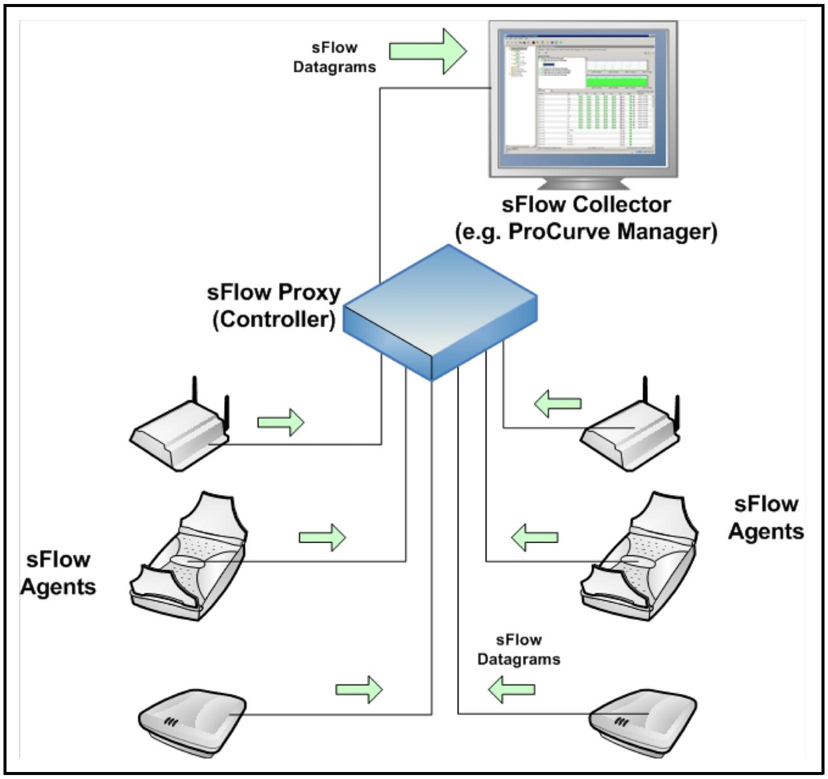
sFlow

Contents

Overview

sFlow sFlow is a technology for monitoring traffic in high speed switched or routed networks. The standard sFlow monitoring system is comprised of the following:

- An **sFlow Agent** that runs on a network device such as an AP, switch, or router. The agent uses sampling techniques to capture information about the data traffic flowing through the device and forwards this information to an sFlow collector.
- An **sFlow Collector** that receives monitoring information from sFlow agents. The collector stores this information so that a network administrator can analyze it.



sFlow proxy

In the case of the controller and its controlled APs, the sFlow monitoring system operates slightly differently. Instead of each AP sending information directly to a collector, the APs send their information to the controller, which acts as an sFlow proxy. The controller then forwards the information to one or more collectors.

The collectors are not aware of the APs, as all sFlow information is repackaged by the controller to indicate that it is the source device. Essentially, the interfaces on the APs appear as interfaces on the controller. When the controller detects that an AP is missing, it will answer SNMP SET and GET queries from collectors with an SNMP error message.

Note

- The controller does not generate any sFlow information of its own. The sFlow information is only generated by APs.
- The MSM317 only monitors ingress traffic on the Uplink and switch ports.

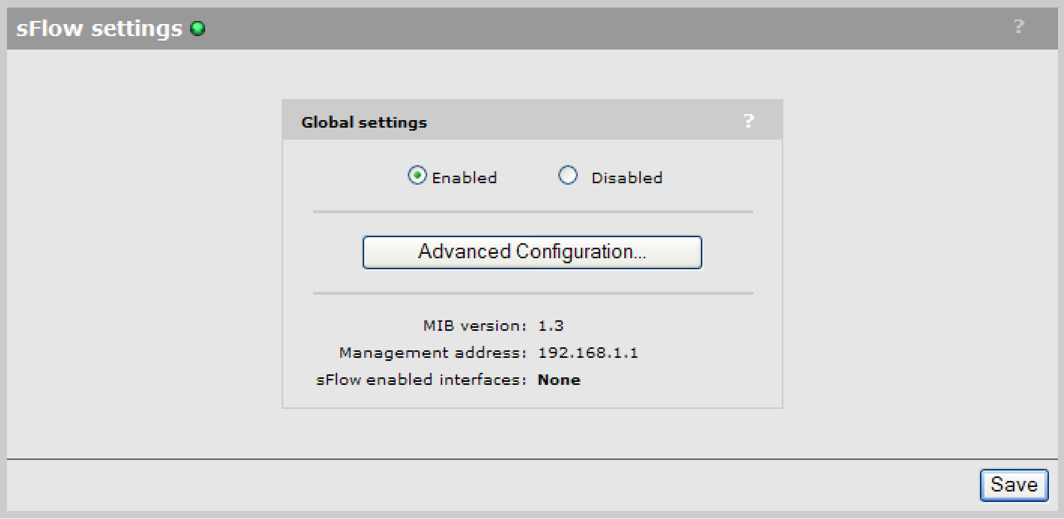
MIB support

The following MIBs are supported:

- sFlow-MIB base OID: 1.3.6.1.4.1.14706
- SNMP MIB2 System base OID: 1.3.6.1.2.1.1
- SNMP MIB2 Interfaces base OID: 1.3.6.1.2.1.2 Note: The ifType OID of the SNMP MIB2 Interfaces will have the value 71 (ieee802.11) for the wireless interfaces.
- SNMP MIB2 IPAddrTable base OID: 1.3.6.1.2.1.4.20
- SNMP MIB2 ifXTable base OID: 1.3.6.1.2.1.31.1.1.1
- SNMP MIB: HP-WLAN-SFLOW-EXTENSIONS-MIB base OID: 1.3.6.1.4.1.11.2.14.11.6.4.2

Configuring and activating sFlow

All sFlow configuration occurs via the controller management tool by selecting **Controller >> Tools > sFlow**.



sFlow settings

Global settings

● Enabled ○ Disabled

MIB version: 1.3
Management address: 192.168.1.1
sFlow enabled interfaces: **None**

Important Under normal conditions, sFlow settings on the controller will be configured by an sFlow collector operating elsewhere on the network. Therefore, in most cases all you need to do to support sFlow is select the **Enabled** option under **Global settings**.

Advanced users who want to fine tune their sFlow configuration, or who are using an sFlow collector in manual mode, can select **Advanced Configuration** to gain access to additional settings.

Manual configuration of sFlow will not work with PCM, and other collectors may require special configuration to operate in this manner.

Global settings

Enabled
Turns sFlow support on. Once enabled, sFlow agents will be activated on all controlled APs, and the agents will appear in the **Active sFlow agents** list. To see this list, select **Advanced Communication**.

Disabled
Turns sFlow support off.

Advanced communication
Select this button to define advanced sFlow configuration settings.

MIB version
Version number of the supported sFlow-MIB.

Management address
This is the IP address that a collector will use to configure sFlow. It is usually the LAN port IP address.

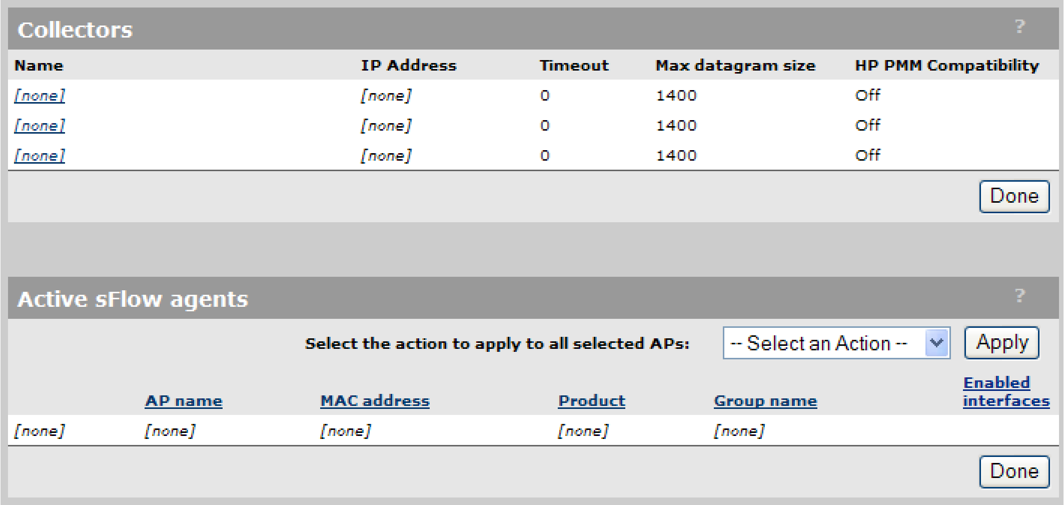
Note SNMP must be enabled on this port hosting the management address.

sFlow enabled interfaces
Displays the number of sFlow interfaces that are enabled.

To enable an interface, select **Advanced Configuration**.

Advanced sFlow configuration

This page provides access to all sFlow configuration settings, including those on controlled APs. (Configuration settings for the sFlow agents operating on an AP are also available by selecting the AP in the **Network Tree** and then selecting **Tools > sFlow**.)



Name	IP Address	Timeout	Max datagram size	HP PMM Compatibility
[none]	[none]	0	1400	Off
[none]	[none]	0	1400	Off
[none]	[none]	0	1400	Off

Select the action to apply to all selected APs: -- Select an Action --

	AP name	MAC address	Product	Group name	Enabled interfaces
[none]	[none]	[none]	[none]	[none]	

Once sFlow support is enabled, sFlow agents will be activated on all controlled APs, and the agents will appear in the **Active sFlow agents** list.

Collectors

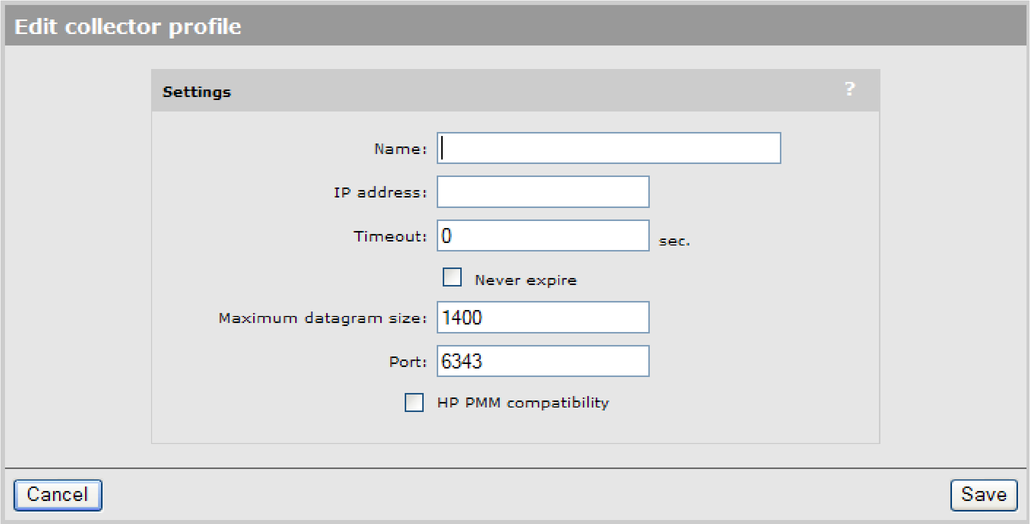
Up to three collectors can be configured. To configure a collector, select its name in the list. Once configured, collectors can be assigned to receive data from the sampling instances for any active sFlow agent.

The table lists the following information for each collector.

- **Name:** Name used to identify the collector.
- **IP address:** IP address of the collector. This is the address to which the controller will send sFlow data.
- **Timeout:** The time (in seconds) that the collector maintains ownership of a sampling instance.
- **Max datagram size:** The maximum number of data bytes that will be sent to the collector in a single sFlow datagram.
- **HP PMM compatibility:** When enabled, information not supported by HP PMM network management software is dropped from the sFlow data to conserve network bandwidth.

Collector configuration settings

A collector profile defines the settings that will be used to communicate with a collector.



Edit collector profile

Settings

Name:

IP address:

Timeout: 0 sec.

□ Never expire

Maximum datagram size: 1400

Port: 6343

□ HP PMM compatibility

Name

Friendly name used to identify the collector.

IP address

IP address of the collector.

Timeout

The time (in seconds) that the collector maintains ownership of a sampling instance.

- **Never expire:** Select this option to set the timeout to never expire.

Maximum datagram size

The maximum number of data bytes that will be sent to the collector in a single sample datagram.

Port

The UDP port on which sFlow data will be sent to the collector.

HP PMM compatibility

Enable this option to generate sFlow data in a format that is compatible with the HP PMM application. When enabled, information not supported by PMM is dropped from the sFlow data to conserve network bandwidth.

Active sFlow agents

Agents automatically appear in this table once sFlow support is enabled. An agent will appear for each controlled AP that is synchronized (green) under **Controlled APs** in the the **Network Tree**.

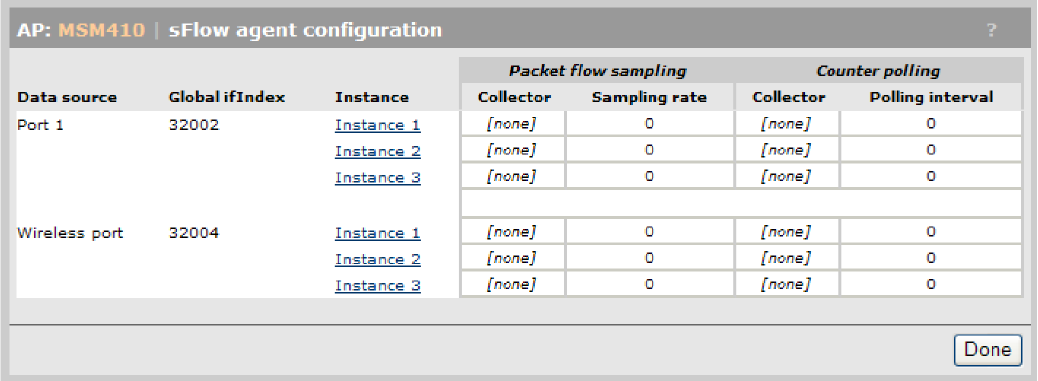
- To configure the agent on an AP, select its name in the list. See *sFlow agent settings*.
- To sort the list based on the values in a column, select the column title.

The table lists the following information for each agent.

- **AP name:** Name assigned to the AP. By default, this is its serial number.
- **MAC address:** MAC address assigned to the AP.
- **Product:** Product name of the AP.
- **Group name:** Name of the group to which the AP is assigned.

sFlow agent settings

This page displays all data sources that are available for sampling on an AP. Each data source can support up to three configurable sampling instances.



AP: MSM410 | sFlow agent configuration

			Packet flow sampling		Counter polling	
Data source	**Global ifIndex**	**Instance**	**Collector**	**Sampling rate**	**Collector**	**Polling interval**
Port 1	32002	Instance 1	[none]	0	[none]	0
		Instance 2	[none]	0	[none]	0
		Instance 3	[none]	0	[none]	0
Wireless port	32004	Instance 1	[none]	0	[none]	0
		Instance 2	[none]	0	[none]	0
		Instance 3	[none]	0	[none]	0

Data source

Name of a port on which the sFlow agent is active.

Global ifIndex

Each port on an AP is automatically assigned a unique number starting at 32001. This uniquely identifies the port across all ports on all controlled APs. The number is available to the collectors as an ifIndex value and can be retrieved using ifIndex-related MIB elements.

Instance

Each port can support up to three instances. Each instance defines a configurable sampling process. To configure an instance, select it.

Packet flow sampling

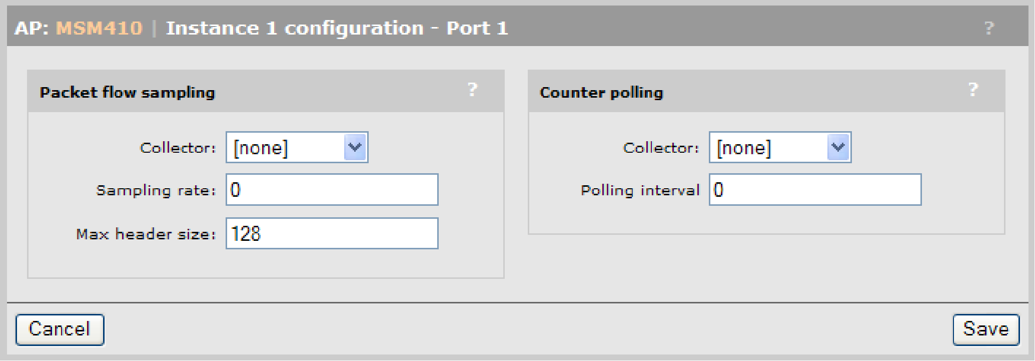
- Collector: Name of the collector to which packet sampling data will be sent.
- Sampling rate: Defines how often samples are taken.

Counter polling

- Collector: Name of the collector to which counter polling data will be sent.
- Polling interval: Defines how often samples are taken.

Instance configuration settings

Each instance can be customized as follows:



AP: MSM410 | Instance 1 configuration - Port 1

Packet flow sampling

Collector: [none]

Sampling rate: 0

Max header size: 128

Counter polling

Collector: [none]

Polling interval 0

Packet flow sampling

Packet flow sampling is executed by copying a specified amount of data from the header of packets and sending it to a collector for analysis.

Collector
Select the collector to which data will be sent.

Sampling rate
Specify the approximate number of packets between samples. For example, if set to 5, approximately every fifth packet will be sampled (There is some jitter introduced purposefully into the sample collection). A value of 0 disables sampling.

Max header size
Specify the maximum number of bytes to copy and forward from the header of the sampled packet.

Counter sampling

Counter sampling measurement are obtained by counting the number of packets and octets passing through the target interface between the defined polling interval.

Collector
Select the collector to which data will be sent.

Polling interval
Specify the amount of time (in seconds) between sending successive octet and packet counter values for this instance.

19

Working with autonomous APs

Contents

Key concepts

This chapter describes how to use the controller in conjunction with autonomous APs.

Tip

Most of this chapter applies to working with autonomous MSM APs. For third-party autonomous APs, see *Working with third-party autonomous APs on page 19-6*.

APs can operate in either controlled mode or autonomous mode. In controlled mode, the controller provides centralized management of APs. This is the preferred operation mode. See *Chapter 6: Working with controlled APs*.

However, in some other cases it is necessary to operate APs in autonomous mode, for example under the following circumstances:

- When an AP is used to create a static WDS (local mesh) link. Controlled mode does not support static local mesh links. It is strongly recommended that dynamic WDS (local mesh) links be used. They provide the same capabilities but with greater flexibility. Furthermore, local mesh is supported in controlled mode.
- An AP at software version 4.x or earlier is used. Controlled mode is available on APs at software version 5.x or higher. It is strongly recommended that controllers and autonomous APs be updated to the same software version, and preferably 5.x or higher. Controlled APs are automatically updated to the controller software version.

It is recommended that you operate most MSM APs in controlled mode, reserving autonomous mode only for APs that need features unique to autonomous mode. In autonomous mode, the following features are not available: Centralized management, wireless mobility, and WPA2 Opportunistic key caching.

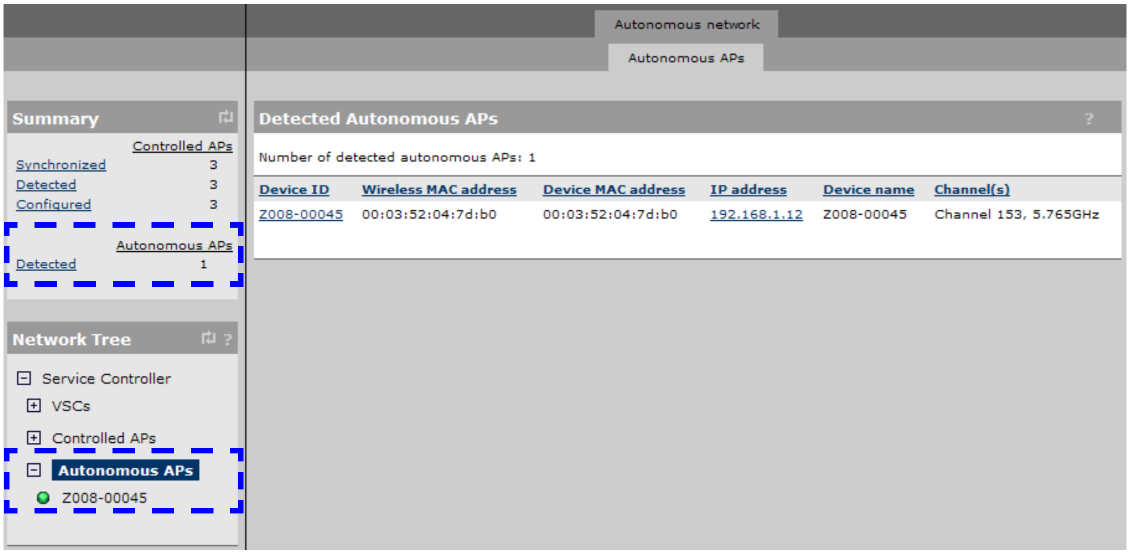
Autonomous AP detection

The controller automatically detects all autonomous APs that have their CDP discovery option enabled (default setting) and are installed on the same subnet as the controller.

To configure this CDP discovery, select **Network > CDP** on the AP management tool.

Viewing autonomous AP information

When the controller detects at least one autonomous AP, the **Summary** box and the **Network Tree** are updated to include autonomous AP information as follows:



	Controlled APs
Synchronized	3
Detected	3
Configured	3

	Autonomous APs
Detected	1

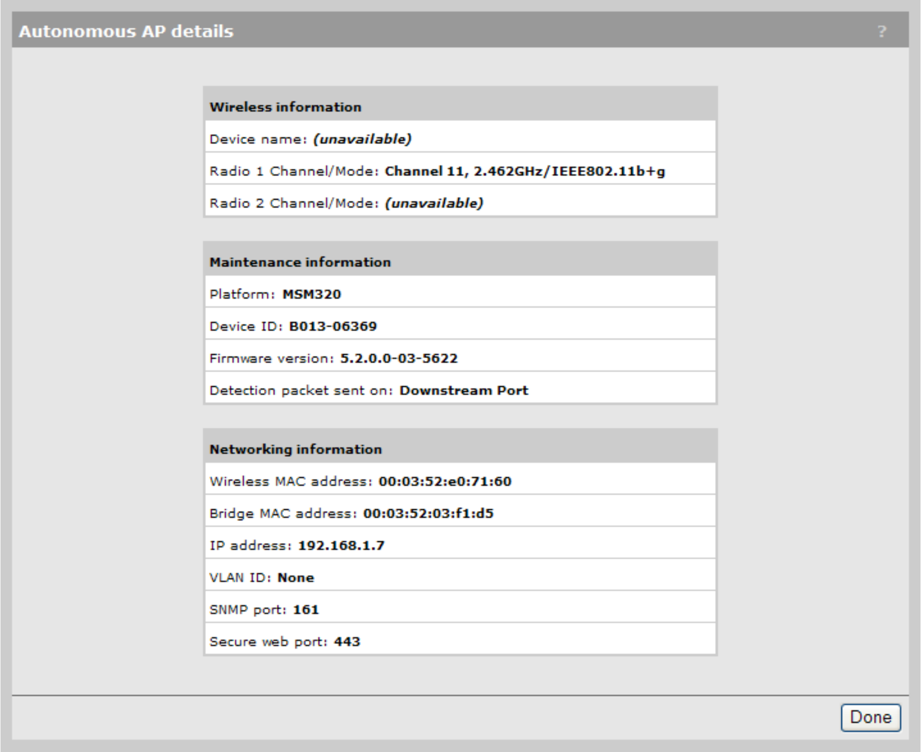
Detected Autonomous APs

Number of detected autonomous APs: 1

Device ID	Wireless MAC address	Device MAC address	IP address	Device name	Channel(s)
Z008-00045	00:03:52:04:7d:b0	00:03:52:04:7d:b0	192.168.1.12	Z008-00045	Channel 153, 5.765GHz

As shown in the above image, the **Summary** list includes a **Detected** link and count in the **Summary** list, and the **Network Tree** includes an **Autonomous APs** branch on **Controller**. These elements only appear when at least one autonomous APs has been detected. As shown, when Autonomous APs is selected, the list of **Detected Autonomous APs** list appears in the right pane.

Select a link in the **Device ID** column to display the **Autonomous APs details** like this:



Wireless information

Device name: ***(unavailable)***

Radio 1 Channel/Mode: **Channel 11, 2.462GHz/IEEE802.11b+g**

Radio 2 Channel/Mode: ***(unavailable)***

Maintenance information

Platform: **MSM320**

Device ID: **B013-06369**

Firmware version: **5.2.0.0-03-5622**

Detection packet sent on: **Downstream Port**

Networking information

Wireless MAC address: **00:03:52:e0:71:60**

Bridge MAC address: **00:03:52:03:f1:d5**

IP address: **192.168.1.7**

VLAN ID: **None**

SNMP port: **161**

Secure web port: **443**

You can also select the link in **IP address** column to launch the AP management tool. See the *MSM3xx/MSM4xx Management and Configuration Guide*.

Switching a controlled AP to autonomous mode

To switch a controlled AP to autonomous mode, select the AP in the **Default Group** branch of the Network Tree, and then in the right pane select **Maintenance > System** and select **Switch to Autonomous Mode**.

Note

The AP will restart and lose all configuration settings received from the controller, returning to its default configuration. You can then configure it via its management tool.

Configuring autonomous APs

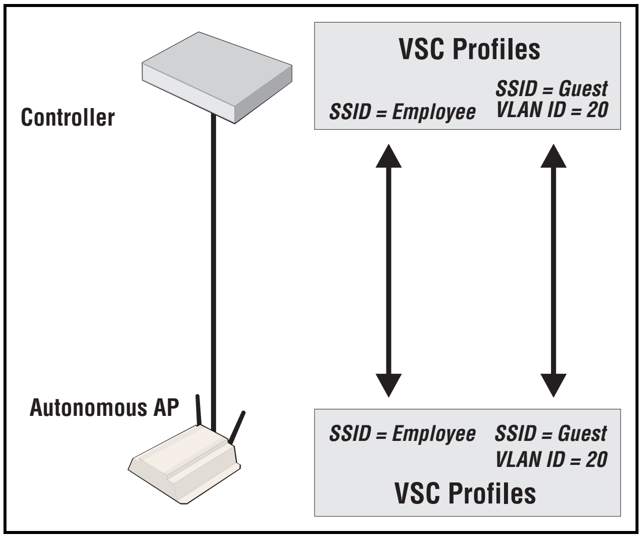
Autonomous APs must be configured via their own management tool. For convenience, you can launch an autonomous AP management tool from within the controller management tool by selecting the link in the IP address column of the Detected Autonomous APs page, providing network access is possible.

When connecting one or more autonomous APs to co-exist with a controller, some configuration issues must be addressed to ensure that data traffic and management traffic is able to flow between both devices.

If the management computer connects to the AP through the controller Internet port but the AP connects via the LAN port, static NAT mappings will be needed to be created to allow traffic to go through the controller firewall. See the *MSM3xx/MSM4xx Management and Configuration Guide*.

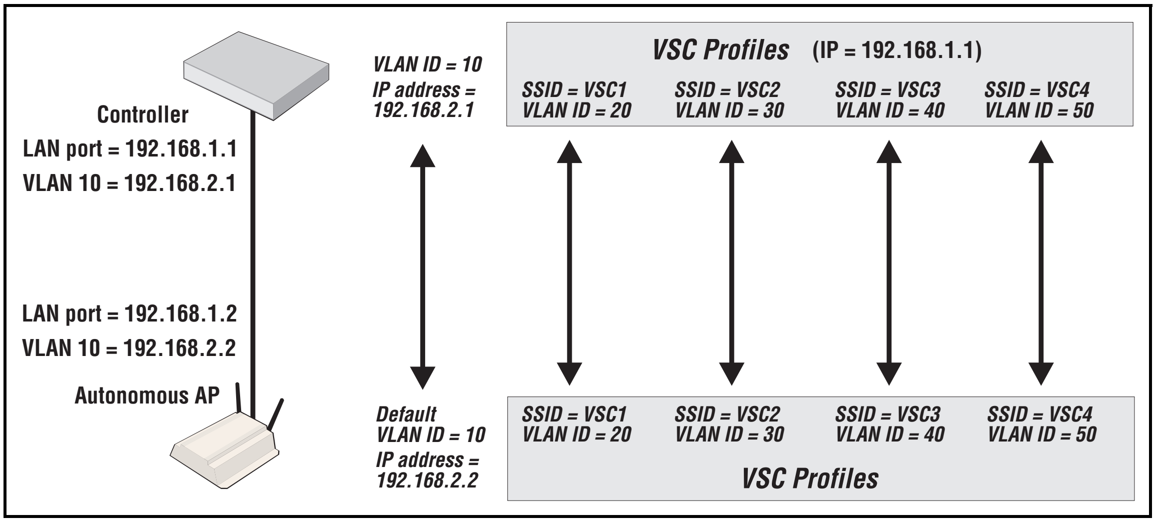
VSC definitions

Although the controller cannot configure autonomous APs, the APs can work with the controller to benefit from the advanced access control services a controller provides. To do this, use the autonomous AP management tool to configure VSCs that use the same SSID or VLAN as already configured on the controller. The matching VSC configuration is illustrated as follows:



Management with VLANs

When operating in a VLAN environment, management traffic can be carried on its own VLAN. Configure the VSC on both the autonomous AP and the controller as illustrated here:



In this example, the traffic for each wireless network is carried on its own VLAN. This leaves only management traffic from the autonomous AP on VLAN 10. A static IP is assigned on both ends to permit the two devices to communicate.

Working with third-party autonomous APs

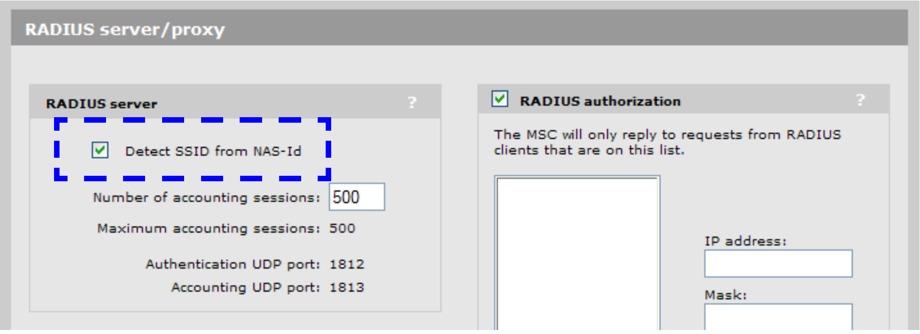
Third-party APs can be used with a controller with both access controlled and non-access controlled VSCs.

VSC selection

User traffic from third-party APs is mapped to a VSC on the controller in the same way as for MSM APs. See *Using multiple VSCs on page 5-36*. This means that traffic is assigned to the default VSC, unless it is on a VLAN, in which case it is assigned to the VSC with matching VLAN ingress definition.

Because the HP location-aware feature is not available on third-party APs, support for VSC selection using an SSID requires that the following additional configuration be performed:

- Configure the AP to send its SSID as the NAS ID in all **authentication and accounting** requests.
- Enable the **Detect SSID from NAS-Id** option on the **Controller >> Authentication > RADIUS server** page.



RADIUS server/proxy

RADIUS server

☑ Detect SSID from NAS-Id

Number of accounting sessions: 500

Maximum accounting sessions: 500

Authentication UDP port: 1812

Accounting UDP port: 1813

☑ RADIUS authorization

The MSC will only reply to requests from RADIUS clients that are on this list.

IP address:

Mask:

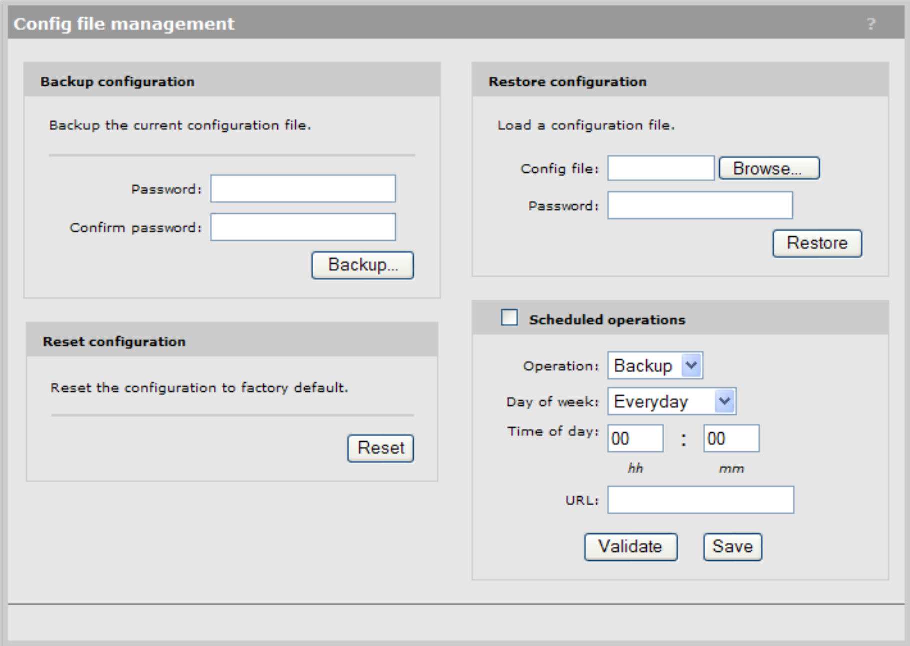
Maintenance

Contents

Config file management

The configuration file contains all the settings that customize the operation of the controller. You can save and restore the configuration file manually or automatically.

Select **Controller >> Maintenance > Config file management**.



Backup the current configuration file.

Load a configuration file.

Reset the configuration to factory default.

Operation: Backup

Day of week: Everyday

Time of day: 00 : 00

Manual configuration file management

The following options are available for manual configuration file management.

Backup configuration

This option enables you to backup your configuration settings so they can be easily restored in case of failure. This option is also used when you want to directly edit the configuration file.

Before you install new software, you should always make a backup of your current configuration. Select **Backup** to start the process. You will be prompted for the location to place the configuration file.

Configuration information is saved in the backup file as follows:

- **Certificates and private keys:** If you specify a password when saving the configuration file, certificates and private keys are encrypted with a key based on the password. If you do not specify a password, certificates and private keys are still encrypted, but with a default key that is identical on all APs.
- **Manager and operator username/password:** This information is not saved in the backup configuration file. This means that if you restore a configuration file, the current username and password on the AP are not overwritten.

- **All other configuration information:** All other configuration information is saved as plain text, allowing the settings to be viewed with a standard text editor.

Reset configuration

See *Appendix C: Resetting to factory defaults*.

Restore configuration

The **Restore configuration** option enables you to load a previously saved configuration file.

This option enables you to maintain several configuration files with different settings, which can be useful if you must frequently alter the configuration of the controller or if you are managing several controllers from a central site.

Use the following steps to restore a saved configuration file.

1. Select **Browse** and then locate the configuration file you want to restore.
2. Select **Restore** to upload it to the controller. If the configuration file is protected with a password, you must supply the password to restore the complete configuration. If you supply an invalid password, all settings are restored except for any certificates and private keys.

Note The controller automatically restarts when once the file has been loaded.

Scheduled operations

The **Scheduled operations** feature enables you to schedule unattended backups or restorations of the configuration file.

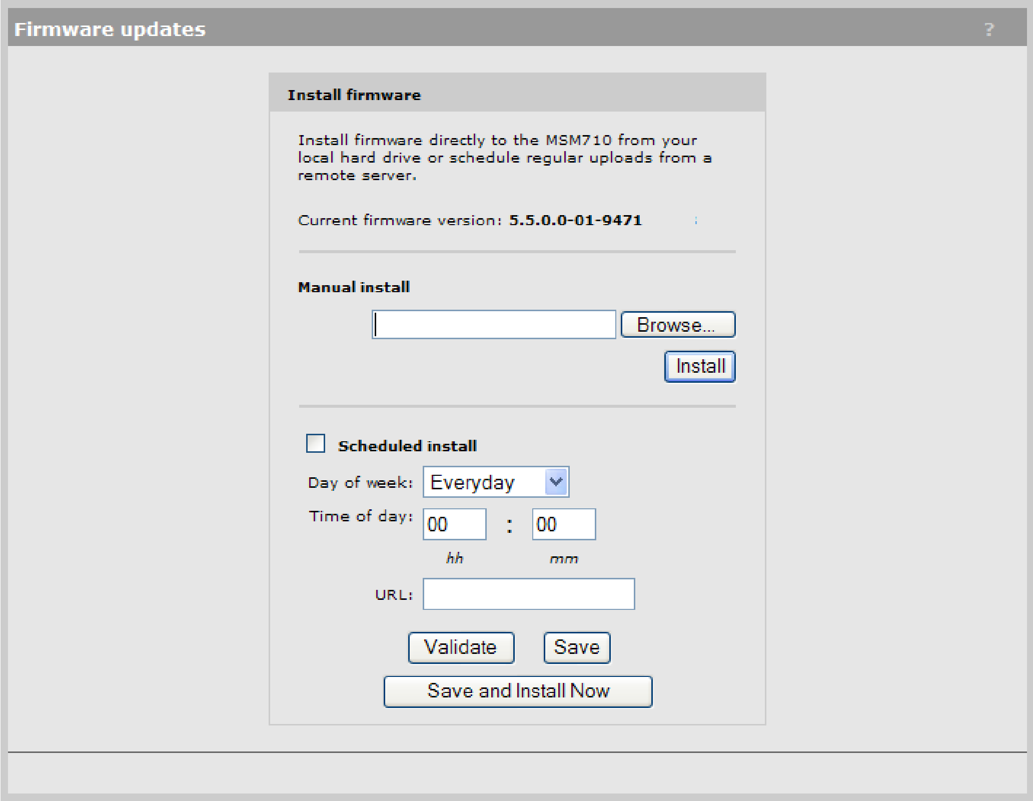
Use the following steps to schedule a backup or restoration of the configuration file.

1. Select **Controller >> Maintenance > Config file management.** The **Config file management** page opens.
2. Select the **Scheduled operations** checkbox.
3. For **Operation,** select **Backup** or **Restore**.
4. For **Day of week,** select **Everyday,** or select a specific day of the week on which to perform the backup or restoration.
5. For **Time of day,** specify the hour and minute on which to perform the backup or restoration. Use the format *hh mm,* where
    - *hh* ranges from 00 to 23
    - *mm* ranges from 00 to 59
6. For **URL,** specify the path that leads to the local or remote directory in which to save the configuration file or from which to load the configuration file. For example
    - **ftp://username:password@192.168.132.11/new.cfg**
    - **http://192.168.132.11/new.cfg**

7. Select **Validate** to test that the specified **URL** is correct.
8. Select **Save.**

Software updates

Controller software updates are managed by selecting **Controller >> Maintenance > Firmware updates.**



Install firmware directly to the MSM710 from your local hard drive or schedule regular uploads from a remote server.

Current firmware version: **5.5.0.0-01-9471**

□ **Scheduled install**

Day of week: Everyday

Time of day: 00 : 00

Caution

- Before updating be sure to check for update issues in the Release Notes.
- Even though configuration settings are preserved during software updates, it is recommended that you backup your configuration settings before updating.
- After updating the controller software, controlled APs are automatically updated to the same version that is installed on the controller. At the end of the update process, the controller and all controlled APs automatically restart, causing all users to be disconnected. Once the controller and APs resume operation, all users must reconnect. To minimize network disruption, use the scheduled install option to have updates performed outside of peak usage hours.

Performing an immediate software update

To update the controller software now, **Browse** to the software file (extension .cim) and then select **Install.**

Performing a scheduled software update

The controller can automatically retrieve and install software from a remote Web site identified by its URL.

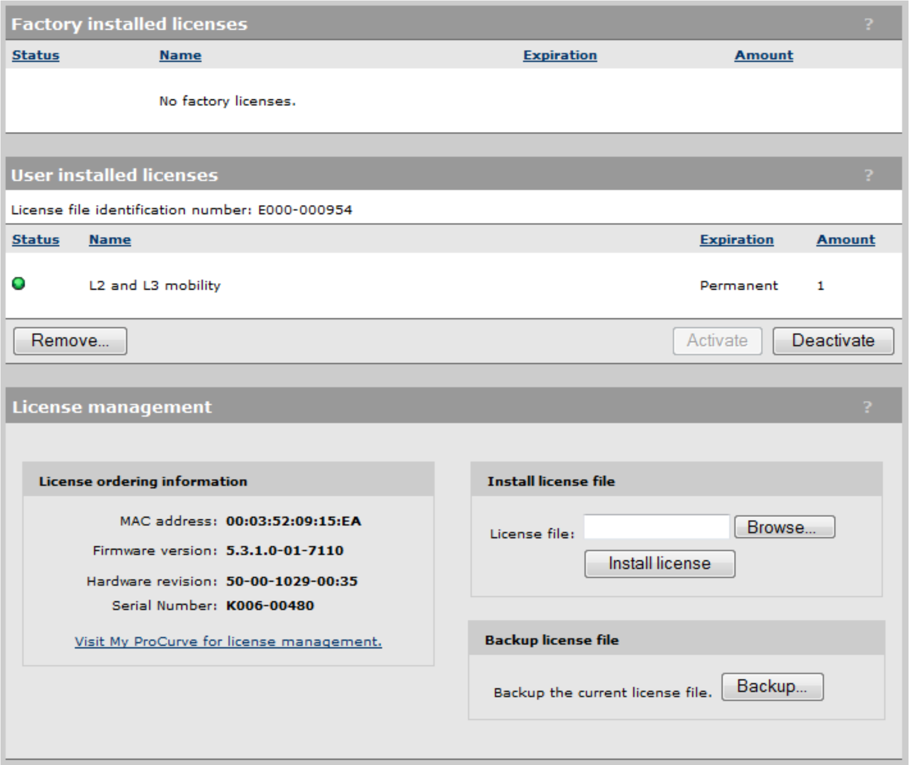
To schedule software installation, follow this procedure:

1. Enable **Scheduled install**.
2. For **Day of week,** select a specific day or **Everyday** and set **Time of day**.
3. For **URL**, specify an ftp or http address like this:
   - **ftp://username:password@192.168.132.11/newsoftware.cim**
   - **http://192.168.132.11/newsoftware.cim**
4. Select **Validate** to test that the specified **URL** is correct**.**
5. Select **Save,** or to commit the schedule and also update the software immediately, select **Save and Install Now**.

Note Before a scheduled software update is performed, only the first few bytes of the software file are downloaded to determine if the software is newer than the currently installed version. If it is not, the download stops and the software is not updated.

Licenses

Some controller features are optional, becoming active only when a license is installed. To view and manage licenses, select **Controller >> Maintenance > Licenses**.



Factory installed licenses

Status	Name	Expiration	Amount
	No factory licenses.		

User installed licenses

License file identification number: E000-000954

Status	Name	Expiration	Amount
●	L2 and L3 mobility	Permanent	1

License management

License ordering information

MAC address: **00:03:52:09:15:EA**

Firmware version: **5.3.1.0-01-7110**

Hardware revision: **50-00-1029-00:35**

Serial Number: **K006-00480**

Visit My ProCurve for license management.

Install license file

License file:

Backup license file

Backup the current license file.

Factory installed licenses

This table lists all licenses that were installed on the controller at the factory. These licenses are always active and cannot be removed or disabled.

User installed licenses

This table lists all user installed licenses. Work with these licenses as follows:

- Select **Deactivate** to temporarily deactivate all user installed licenses. Any features that depend on these licenses will become temporarily unavailable.
- Select **Activate** to re-activate user-installed licenses that have been deactivated.
- Select **Remove** to delete all user installed licenses. Before removing licenses, be sure to first backup the license file to your hard drive, by selecting **Backup**.

License management

Use these options to order, install, and backup license files.

- When you order a new feature license, you may be required to provide the information in the License ordering information box to your vendor.
- To install a license file, **Browse** to the file and then select **Install License**.
- Select **Backup** to save all user-defined licenses in a single file.

Once you receive your License Registration card for your purchased license, you will need the **MAC address** in the **License ordering information** box. See *Generating and installing a feature license*.

Factory reset considerations

After a controller has been reset to its factory defaults, factory-installed licenses are automatically re-activated, but user-installed licenses remain in a deactivated state until manually activated. This is done to ensure a true factory-default reset.

Generating and installing a feature license

When you purchase an optional feature license, a physical license registration card is shipped to you. License registration cards are not matched to your MSM7xx Controller until you go to the **My Networking** portal and generate a license file for a specific MSM7xx Controller.

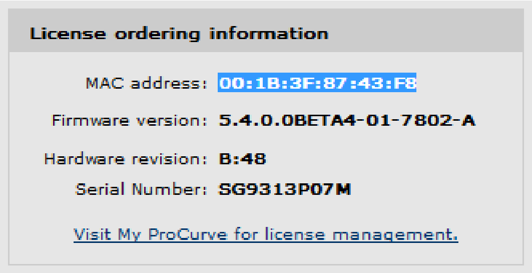
Once you receive your license registration card, follow this procedure to generate and install a feature license on your MSM7xx Controller.

Note When teaming is active, separate license files must be generated and individually installed on each controller that is a member of a team.

Generating a license

1. Go to www.hp.com/networking/mynetworking and sign in. New users must first create an account.
2. Select the **My Licenses** tab at the top of the page.
3. In the **Registration ID** field, type the **License Registration ID** found on your registration card. Type the ID exactly as shown, including the dashes. Select **Next**.

4. If you do not have the MAC address of your MSM7xx Controller already on file, open its management tool in a separate Web browser window, and select **Controller >> Maintenance > Licenses.** Under **License ordering information**, copy the **MAC address** onto your clipboard. For example:



License ordering information

MAC address: 00:1B:3F:87:43:F8

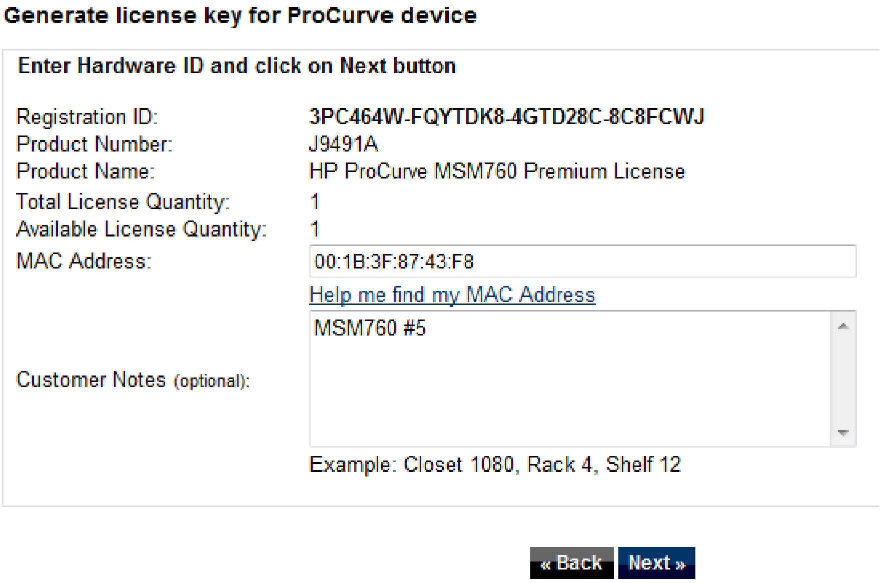
Firmware version: 5.4.0.0BETA4-01-7802-A

Hardware revision: B:48

Serial Number: SG9313P07M

Visit My ProCurve for license management.

5. Back on the My Networking portal Web page, paste or type the MAC address of your MSM7xx Controller in the **MAC Address** field. For example:



Generate license key for ProCurve device

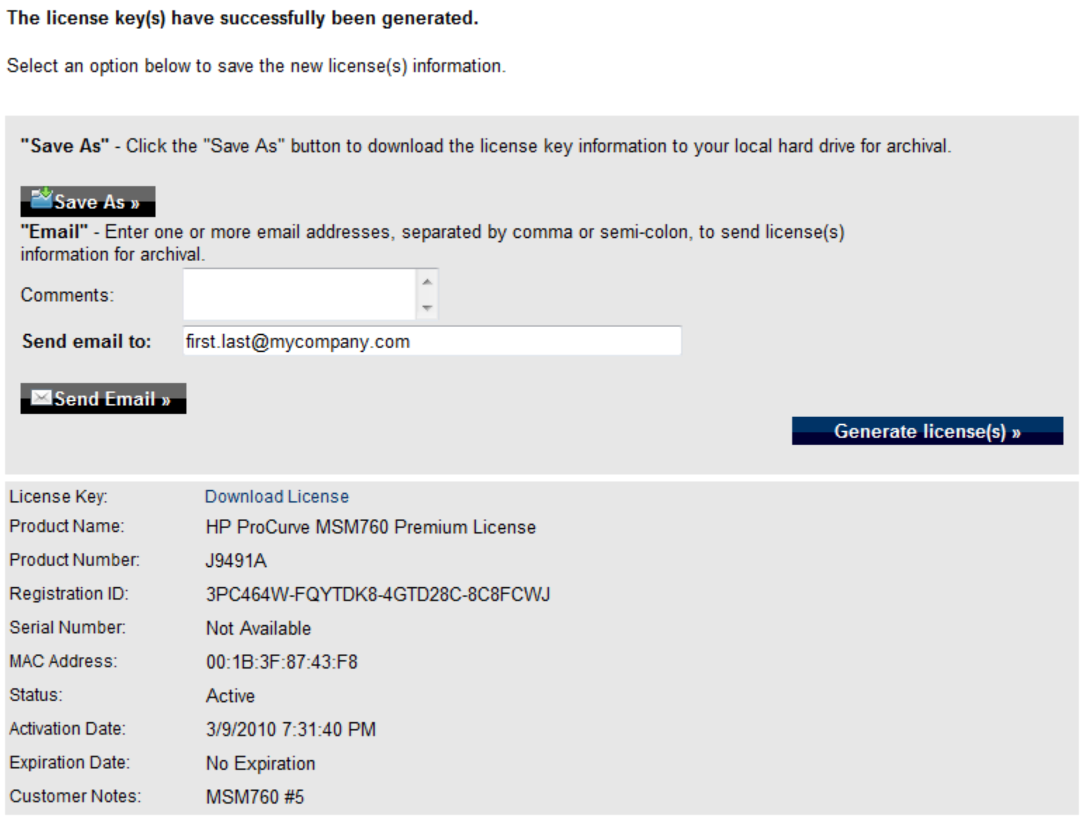
Enter Hardware ID and click on Next button

Registration ID:	3PC464W-FQYTDK8-4GTD28C-8C8FCWJ
Product Number:	J9491A
Product Name:	HP ProCurve MSM760 Premium License
Total License Quantity:	1
Available License Quantity:	1
MAC Address:	00:1B:3F:87:43:F8 Help me find my MAC Address
Customer Notes (optional):	MSM760 #5 Example: Closet 1080, Rack 4, Shelf 12

6. Optionally type a reminder for yourself in the **Customer Notes** field. Select **Next**.

7. Review and accept the License Agreement. Select **Next**.

The license key is generated and made available to you for saving or sending by email. For example:



The license key(s) have successfully been generated.

Select an option below to save the new license(s) information.

"Save As" - Click the "Save As" button to download the license key information to your local hard drive for archival.

"Email" - Enter one or more email addresses, separated by comma or semi-colon, to send license(s) information for archival.

Comments:

Send email to: first.last@mycompany.com

License Key:	Download License
Product Name:	HP ProCurve MSM760 Premium License
Product Number:	J9491A
Registration ID:	3PC464W-FQYTDK8-4GTD28C-8C8FCWJ
Serial Number:	Not Available
MAC Address:	00:1B:3F:87:43:F8
Status:	Active
Activation Date:	3/9/2010 7:31:40 PM
Expiration Date:	No Expiration
Customer Notes:	MSM760 #5

8. Use the **Save As** button to save the license key file on your system or use **Send Email** to send the license key file and information to an email address. The email will contain both the license file and the license key information displayed on this page.

9. When done, select **Generate license(s)** to return to the main licenses page.

Installing a license

If you are ready to install your new license on your MSM7xx Controller, go back to the MSM7xx Controller management tool and do the following:

1. Select **Controller >> Maintenance > Licenses.**

2. Under **Install license file**, select **Browse** and browse to your license file. Select the file and then select **Open**.

3. Select **Install license** to complete the license installation.

A

Safety and EMC regulatory statements

Contents

Safety Information

⚠ Documentation reference symbol. If the product is marked with this symbol, see the product documentation to get more information about the product.

WARNING A **WARNING** in the manual denotes a hazard that can cause injury or death.

Caution A Caution in the manual denotes a hazard that can damage equipment.

Do not proceed beyond a **WARNING** or Caution notice until you have understood the hazardous conditions and have taken appropriate steps.

Grounding

These are safety class I products and have protective earthing terminals. There must be an uninterruptible safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set. Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

For LAN cable grounding

- If your LAN covers an area served by more than one power distribution system, be sure their safety grounds are securely interconnected.
- LAN cables may occasionally be subject to hazardous transient voltages (such as lightning or disturbances in the electrical utilities power grid). Handle exposed metal components of the network with caution.

Servicing

There are no user-serviceable parts inside these products. Any servicing, adjustment, maintenance, or repair must be performed only by service-trained personnel.

These products do not have a power switch; they are powered on when the power cord is plugged in.

Informations concernant la sécurité

⚠ Symbole de référence à la documentation. Si le produit est marqué de ce symbole, reportez-vous à la documentation du produit afin d'obtenir des informations plus détaillées.

WARNING Dans la documentation, un **WARNING** indique un danger susceptible d'entraîner des dommages corporels ou la mort.

Caution — Un texte de mise en garde intitulé Caution indique un danger susceptible de causer des dommages à l'équipement.

Ne continuez pas au-delà d'une rubrique **WARNING** ou Caution avant d'avoir bien compris les conditions présentant un danger et pris les mesures appropriées.

Cet appareil est un produit de classe I et possède une borne de mise à la terre. La source d'alimentation principale doit être munie d'une prise de terre de sécurité installée aux bornes du câblage d'entrée, sur le cordon d'alimentation ou le cordon de raccordement fourni avec le produit. Lorsque cette protection semble avoir été endommagée, débrancher le cordon d'alimentation jusqu'à ce que la mise à la terre ait été réparée.

Mise à la terre du câble de réseau local:

- si votre réseau local s'étend sur une zone desservie par plus d'un système de distribution de puissance, assurez-vous que les prises de terre de sécurité soient convenablement interconnectées.
- Les câbles de réseaux locaux peuvent occasionnellement être soumis à des surtensions transitoires dangereuses (telles que la foudre ou des perturbations dans le réseau d'alimentation public). Manipulez les composants métalliques du réseau avec précautions.

Aucune pièce contenue à l'intérieur de ce produit ne peut être réparée par l'utilisateur. Tout dépannage, réglage, entretien ou réparation devra être confié exclusivement à un personnel qualifié.

Cet appareil ne comporte pas de commutateur principal ; la mise sous tension est effectuée par branchement du cordon d'alimentation.

Hinweise zur Sicherheit

⚠ — Symbol für Dokumentationsverweis. Wenn das Produkt mit diesem Symbol markiert ist, schlagen Sie bitte in der Produktdokumentation nach, um mehr Informationen über das Produkt zu erhalten.

WARNING — Eine **WARNING** in der Dokumentation symbolisiert eine Gefahr, die Verletzungen oder sogar Todesfälle verursachen kann.

Caution — Caution in der Dokumentation symbolisiert eine Gefahr, die dis Gerät beschädigen kann.

Fahren Sie nach dem Hinweis **WARNING** oder Caution erst fort, nachdem Sie den Gefahrenzustand verstanden und die entsprechenden Maßnahmen ergriffen haben.

Dies ist ein Gerät der Sicherheitsklasse I und verfügt über einen schützenden Erdungsterminal. Der Betrieb des Geräts erfordert eine ununterbrochene Sicherheitserdung von der Hauptstromquelle zu den Geräteingabeterminals, den Netzkabeln oder dem mit Strom belieferten Netzkabelsatz voraus. Sobald Grund zur Annahme besteht, daß der Schutz beeinträchtigt worden ist, das Netzkabel aus der Wandsteckdose herausziehen, bis die Erdung wiederhergestellt ist.

Für LAN-Kabelerdung:

- Wenn Ihr LAN ein Gebiet umfaßt, das von mehr als einem Stromverteilungssystem beliefert wird, müssen Sie sich vergewissern, daß die Sicherheitserdungen fest untereinander verbunden sind.
- LAN-Kabel können gelegentlich gefährlichen Übergangsspannungen ausgesetzt werden (beispielsweise durch Blitz oder Störungen in dem Starkstromnetz des Elektrizitätswerks). Bei der Handhabung exponierter Metallbestandteile des Netzwerkes Vorsicht walten lassen.

Dieses Gerät enthält innen keine durch den Benutzer zu wartenden Teile. Wartungs-, Anpassungs-, Instandhaltungs- oder Reparaturarbeiten dürfen nur von geschultem Bedienungspersonal durchgeführt werden.

Dieses Gerät hat keinen Netzschalter; es wird beim Anschließen des Netzkabels eingeschaltet.

Considerazioni sulla sicurezza

⚠ Simbolo di riferimento alla documentazione. Se il prodotto è contrassegnato da questo simbolo, fare riferimento alla documentazione sul prodotto per ulteriori informazioni su di esso.

WARNING La dicitura **WARNING**denota un pericolo che può causare lesioni o morte.

Caution La dicituraCaution denota un pericolo che può danneggiare le attrezzature.

Non procedere oltre un avviso di **WARNING** o di Cautionprima di aver compreso le condizioni di rischio e aver provveduto alle misure del caso.

Questo prodotto è omologato nella classe di sicurezza I ed ha un terminale protettivo di collegamento a terra. Dev'essere installato un collegamento a terra di sicurezza, non interrompibile che vada dalla fonte d'alimentazione principale ai terminali d'entrata, al cavo d'alimentazione oppure al set cavo d'alimentazione fornito con il prodotto. Ogniqualvolta vi sia probabilità di danneggiamento della protezione, disinserite il cavo d'alimentazione fino a quando il collegaento a terra non sia stato ripristinato.

Per la messa a terra dei cavi LAN:

- se la vostra LAN copre un'area servita da più di un sistema di distribuzione elettrica, accertatevi che i collegamenti a terra di sicurezza siano ben collegati fra loro;
- i cavi LAN possono occasionalmente andare soggetti a pericolose tensioni transitorie (ad esempio, provocate da lampi o disturbi nella griglia d'alimentazione della società elettrica); siate cauti nel toccare parti esposte in metallo della rete.

Nessun componente di questo prodotto può essere riparato dall'utente. Qualsiasi lavoro di riparazione, messa a punto, manutenzione o assistenza va effettuato esclusivamente da personale specializzato.

Questo apparato non possiede un commutatore principale; si mette scotto tensione all'inserirsi il cavo d'alimentazione.

Consideraciones sobre seguridad

⚠ Símbolo de referencia a la documentación. Si el producto va marcado con este símbolo, consultar la documentación del producto a fin de obtener mayor información sobre el producto.

WARNING Una **WARNING** en la documentación señala un riesgo que podría resultar en lesiones o la muerte.

Caution Una Caution en la documentación señala un riesgo que podría resultar en averías al equipo.

No proseguir después de un símbolo de **WARNING** o Caution hasta no haber entendido las condiciones peligrosas y haber tomado las medidas apropiadas.

Este aparato se enmarca dentro de la clase I de seguridad y se encuentra protegido por una borna de puesta a tierra. Es preciso que exista una puesta a tierra continua desde la toma de alimentación eléctrica hasta las bornas de los cables de entrada del aparato, el cable de alimentación o el juego de cable de alimentación suministrado. Si existe la probabilidad de que la protección a tierra haya sufrido desperfectos, desenchufar el cable de alimentación hasta haberse subsanado el problema.

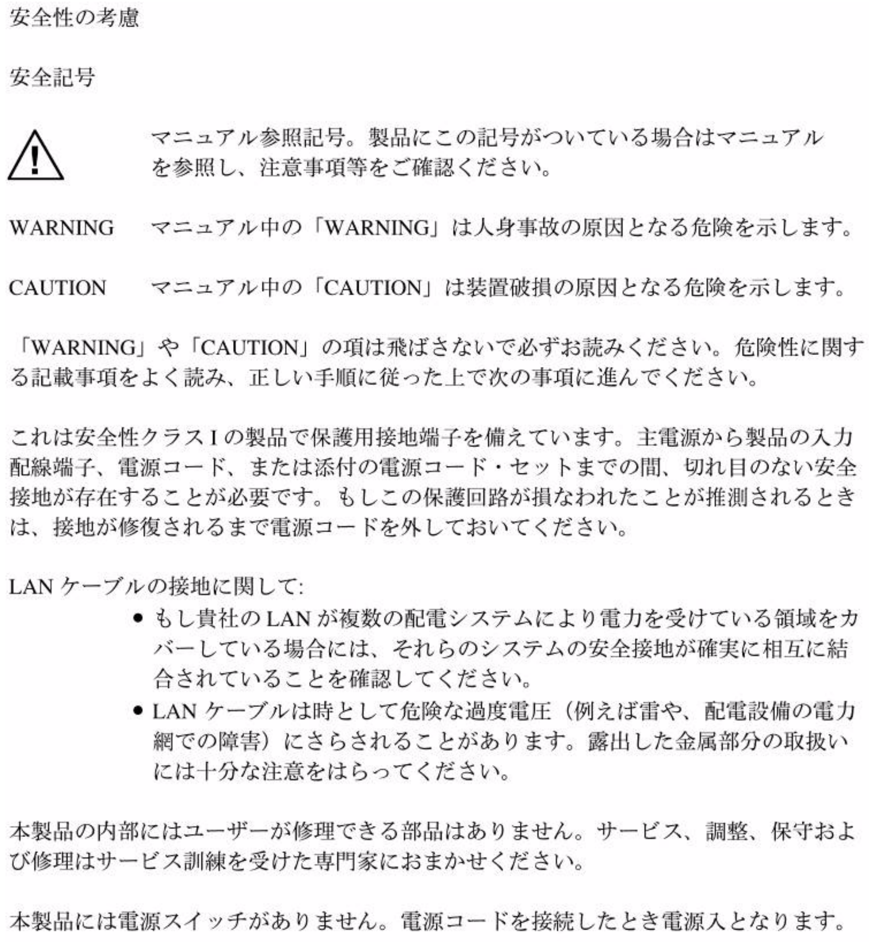
Puesta a tierra del cable de la red local (LAN):

- Si la LAN abarca un área cuyo suministro eléctrico proviene de más de una red de distribución de electricidad, cerciorarse de que las puestas a tierra estén conectadas entre sí de modo seguro.
- Es posible que los cables de la LAN se vean sometidos de vez en cuando a voltajes momentáneos que entrañen peligro (rayos o alteraciones en la red de energía eléctrica). Manejar con precaución los componentes de metal de la LAN que estén al descubierto.

Este aparato no contiene pieza alguna susceptible de reparación por parte del usuario. Todas las reparaciones, ajustes o servicio de mantenimiento debe realizarlos solamente el técnico.

Este producto no tiene interruptor de potencia; se activa cuando se enchufa el cable de alimentación.

Safety Information (Japan)



安全性の考慮

安全記号

⚠ マニュアル参照記号。製品にこの記号がついている場合はマニュアルを参照し、注意事項等をご確認ください。

WARNING　マニュアル中の「WARNING」は人身事故の原因となる危険を示します。

CAUTION　マニュアル中の「CAUTION」は装置破損の原因となる危険を示します。

「WARNING」や「CAUTION」の項は飛ばさないで必ずお読みください。危険性に関する記載事項をよく読み、正しい手順に従った上で次の事項に進んでください。

これは安全性クラスIの製品で保護用接地端子を備えています。主電源から製品の入力配線端子、電源コード、または添付の電源コード・セットまでの間、切れ目のない安全接地が存在することが必要です。もしこの保護回路が損なわれたことが推測されるときは、接地が修復されるまで電源コードを外しておいてください。

LANケーブルの接地に関して:

- もし貴社のLANが複数の配電システムにより電力を受けている領域をカバーしている場合には、それらのシステムの安全接地が確実に相互に結合されていることを確認してください。
- LANケーブルは時として危険な過度電圧（例えば雷や、配電設備の電力網での障害）にさらされることがあります。露出した金属部分の取扱いには十分な注意をはらってください。

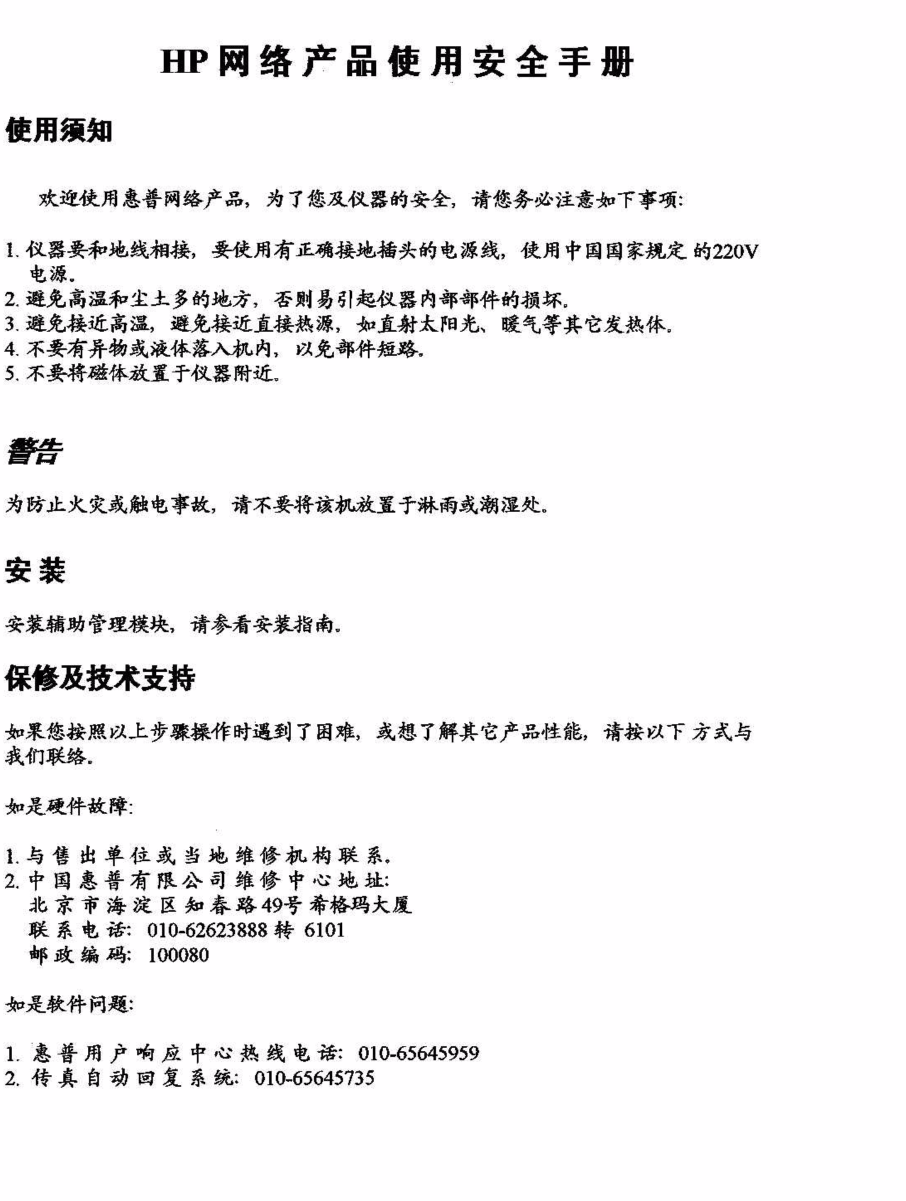
本製品の内部にはユーザーが修理できる部品はありません。サービス、調整、保守および修理はサービス訓練を受けた専門家におまかせください。

本製品には電源スイッチがありません。電源コードを接続したとき電源入となります。

Japan Power Cord Warning

製品には、同梱された電源コードをお使い下さい。
同梱された電源コードは、他の製品では使用出来ません。

Safety Information (China)



HP网络产品使用安全手册

使用须知

欢迎使用惠普网络产品，为了您及仪器的安全，请您务必注意如下事项:

1. 仪器要和地线相接，要使用有正确接地插头的电源线，使用中国国家规定 的220V
   电源。
2. 避免高温和尘土多的地方，否则易引起仪器内部部件的损坏。
3. 避免接近高温，避免接近直接热源，如直射太阳光、暖气等其它发热体。
4. 不要有异物或液体落入机内，以免部件短路。
5. 不要将磁体放置于仪器附近。

警告

为防止火灾或触电事故，请不要将该机放置于淋雨或潮湿处。

安装

安装辅助管理模块，请参看安装指南。

保修及技术支持

如果您按照以上步骤操作时遇到了困难，或想了解其它产品性能，请按以下 方式与我们联络。

如是硬件故障:

1. 与售出单位或当地维修机构联系。
2. 中国惠普有限公司维修中心地址:
   北京市海淀区知春路49号希格玛大厦
   联系电话: 010-62623888 转 6101
   邮政编码: 100080

如是软件问题:

1. 惠普用户响应中心热线电话: 010-65645959
2. 传真自动回复系统: 010-65645735

EMC Regulatory Statements

U.S.A.

FCC Class A (Applies to the MSM730/MSM750)
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications. Operation of this equipment in a residential area may cause interference in which case the user will be required to correct the interference at his own expense.

FCC Class B (Applies to the MSM710)
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. Theses limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver
- Connect the equipment into an outlet that is on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help."

CAUTION Any changes or modifications to this equipment not expressly approved by the

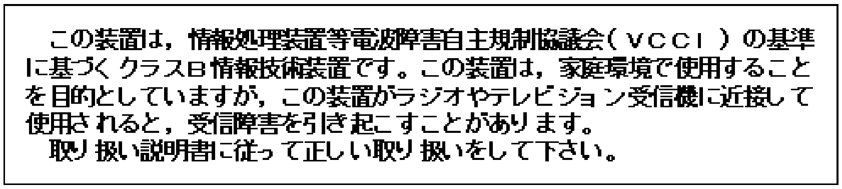
Hewlett-Packard Company may cause harmful interference and void the FCC authorization to operate this equipment."

Japan

VCCI Class A (Applies to the MSM730/MSM750)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

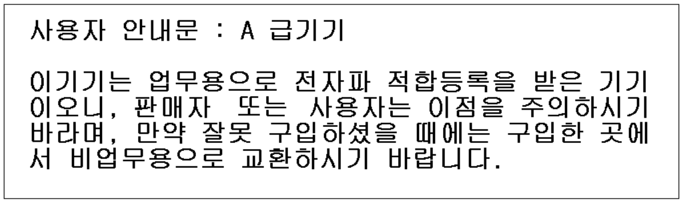
VCCI Class B (Applies to the MSM710)



　この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。
　取り扱い説明書に従って正しい取り扱いをして下さい。

Korea

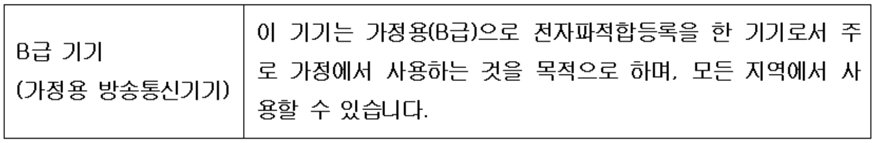
Class A (Applies to the MSM730/MSM750)



사용자 안내문 : A 급기기

이기기는 업무용으로 전자파 적합등록을 받은 기기이오니, 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

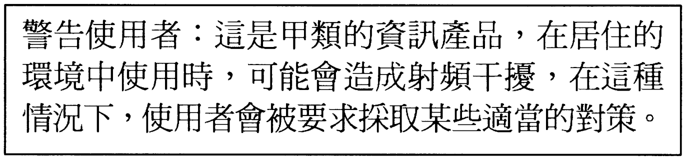
Class B (Applies to the MSM710)



B급 기기 (가정용 방송통신기기)	이 기기는 가정용(B급)으로 전자파적합등록을 한 기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.

Taiwan

Class A (Applies to the MSM730/MSM750)



警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Recycle Statements

Waste Electrical and Electronic Equipment (WEEE) Statements

Disposal of Waste Equipment by Users in Private Household in the European Union

This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

Likvidace zařízení soukromými domácími uživateli v Evropské unii

Tento symbol na produktu nebo balení označuje výrobek, který nesmí být vyhozen spolu s ostatním domácím odpadem. Povinností uživatele je předat takto označený odpad na předem určené sběrné místo pro recyklaci elektrických a elektronických zařízení. Okamžité třídění a recyklace odpadu pomůže uchovat přírodní prostředí a zajistí takový způsob recyklace, který ochrání zdraví a životní prostředí člověka. Další informace o možnostech odevzdání odpadu k recyklaci získáte na příslušném obecním nebo městském úřadě, od firmy zabývající se sběrem a svozem odpadu nebo v obchodě, kde jste produkt zakoupili.

Bortskaffelse af affald fra husstande i den Europæiske Union

Hvis produktet eller dets emballage er forsynet med dette symbol, angiver det, at produktet ikke må bortskaffes med andet almindeligt husholdningsaffald. I stedet er det dit ansvar at bortskaffe kasseret udstyr ved at aflevere det på den kommunale genbrugsstation, der forestår genvinding af kasseret elektrisk og elektronisk udstyr. Den centrale modtagelse og genvinding af kasseret udstyr i forbindelse med bortskaffelsen bidrager til bevarelse af naturlige ressourcer og sikrer, at udstyret genvindes på en måde, der beskytter både mennesker og miljø. Yderligere oplysninger om, hvor du kan aflevere kasseret udstyr til genvinding, kan du få hos kommunen, den lokale genbrugsstation eller i den butik, hvor du købte produktet.

Seadmete jäätmete kõrvaldamine eramajapidamistes Euroopa Liidus

See tootel või selle pakendil olev sümbol näitab, et kõnealust toodet ei tohi koos teiste majapidamisjäätmetega kõrvaldada. Teie kohus on oma seadmete jäätmed kõrvaldada, viies need elektri- ja elektroonikaseadmete jäätmete ringlussevõtmiseks selleks ettenähtud kogumispunkti. Seadmete jäätmete eraldi kogumine ja ringlussevõtmine kõrvaldamise ajal aitab kaitsta loodusvarasid ning tagada, et ringlussevõtmine toimub viisil, mis kaitseb inimeste tervist ning keskkonda. Lisateabe saamiseks selle kohta, kuhu oma seadmete jäätmed ringlussevõtmiseks viia, võtke palun ühendust oma kohaliku linnakantselei, majapidamisjäätmete kõrvaldamise teenistuse või kauplusega, kust Te toote ostsite.

Laitteiden hävittäminen kotitalouksissa Euroopan unionin alueella

Jos tuotteessa tai sen pakkauksessa on tämä merkki, tuotetta ei saa hävittää kotitalousjätteiden mukana. Tällöin hävitettävä laite on toimitettava sähkölaitteiden ja elektronisten laitteiden kierrätyspisteeseen. Hävitettävien laitteiden erillinen käsittely ja kierrätys auttavat säästämään luonnonvaroja ja varmistamaan, että laite kierrätetään tavalla, joka estää terveyshaitat ja suojelee luontoa. Lisätietoja paikoista, joihin hävitettävät laitteet voi toimittaa kierrätettäväksi, saa ottamalla yhteyttä jätehuoltoon tai liikkeeseen, josta tuote on ostettu.

Élimination des appareils mis au rebut par les ménages dans l'Union européenne

Le symbole apposé sur ce produit ou sur son emballage indique que ce produit ne doit pas être jeté avec les déchets ménagers ordinaires. Il est de votre responsabilité de mettre au rebut vos appareils en les déposant dans les centres de collecte publique désignés pour le recyclage des équipements électriques et électroniques. La collecte et le recyclage de vos appareils mis au rebut indépendamment du reste des déchets contribue à la préservation des ressources naturelles et garantit que ces appareils seront recyclés dans le respect de la santé humaine et de l'environnement. Pour obtenir plus d'informations sur les centres de collecte et de recyclage des appareils mis au rebut, veuillez contacter les autorités locales de votre région, les services de collecte des ordures ménagères ou le magasin dans lequel vous avez acheté ce produit.

Entsorgung von Altgeräten aus privaten Haushalten in der EU

Das Symbol auf dem Produkt oder seiner Verpackung weist darauf hin, dass das Produkt nicht über den normalen Hausmüll entsorgt werden darf. Benutzer sind verpflichtet, die Altgeräte an einer Rücknahmestelle für Elektro- und Elektronik-Altgeräte abzugeben. Die getrennte Sammlung und ordnungsgemäße Entsorgung Ihrer Altgeräte trägt zur Erhaltung der natürlichen Ressourcen bei und garantiert eine Wiederverwertung, die die Gesundheit des Menschen und die Umwelt schützt. Informationen dazu, wo Sie Rücknahmestellen für Ihre Altgeräte finden, erhalten Sie bei Ihrer Stadtverwaltung, den örtlichen Müllentsorgungsbetrieben oder im Geschäft, in dem Sie das Gerät erworben haben

Απόρριψη άχρηστου εξοπλισμού από χρήστες σε ιδιωτικά νοικοκυριά στην Ευρωπαϊκή Ένωση

Το σύμβολο αυτό στο προϊόν ή τη συσκευασία του υποδεικνύει ότι το συγκεκριμένο προϊόν δεν πρέπει να διατίθεται μαζί με τα άλλα οικιακά σας απορρίμματα. Αντίθετα, είναι δική σας ευθύνη να απορρίψετε τον άχρηστο εξοπλισμό σας παραδίδοντάς τον σε καθορισμένο σημείο συλλογής για την ανακύκλωση άχρηστου ηλεκτρικού και ηλεκτρονικού εξοπλισμού. Η ξεχωριστή συλλογή και ανακύκλωση του άχρηστου εξοπλισμού σας κατά την απόρριψη θα συμβάλει στη διατήρηση των φυσικών πόρων και θα διασφαλίσει ότι η ανακύκλωση γίνεται με τρόπο που προστατεύει την ανθρώπινη υγεία και το περιβάλλον. Για περισσότερες πληροφορίες σχετικά με το πού μπορείτε να παραδώσετε τον άχρηστο εξοπλισμό σας για ανακύκλωση, επικοινωνήστε με το αρμόδιο τοπικό γραφείο, την τοπική υπηρεσία διάθεσης οικιακών απορριμμάτων ή το κατάστημα όπου αγοράσατε το προϊόν.

Készülékek magánháztartásban történő selejtezése az Európai Unió területén

A készüléken, illetve a készülék csomagolásán látható azonos szimbólum annak jelzésére szolgál, hogy a készülék a selejtezés során az egyéb háztartási hulladéktól eltérő módon kezelendő. A vásárló a hulladékká vált készüléket köteles a kijelölt gyűjtőhelyre szállítani az elektromos és elektronikai készülékek újrahasznosítása céljából. A hulladékká vált készülékek selejtezéskori begyűjtése és újrahasznosítása hozzájárul a természeti erőforrások megőrzéséhez, valamint biztosítja a selejtezett termékek környezetre és emberi egészségre nézve biztonságos feldolgozását. A begyűjtés pontos helyéről bővebb tájékoztatást a lakhelye szerint illetékes önkormányzattól, az illetékes szemételtakarító vállalattól, illetve a terméket elárusító helyen kaphat.

Smaltimento delle apparecchiature da parte di privati nel territorio dell'Unione Europea

Questo simbolo presente sul prodotto o sulla sua confezione indica che il prodotto non può essere smaltito insieme ai rifiuti domestici. È responsabilità dell'utente smaltire le apparecchiature consegnandole presso un punto di raccolta designato al riciclo e allo smaltimento di apparecchiature elettriche ed elettroniche. La raccolta differenziata e il corretto riciclo delle apparecchiature da smaltire permette di proteggere la salute degli individui e l'ecosistema. Per ulteriori informazioni relative ai punti di raccolta delle apparecchiature, contattare l'ente locale per lo smaltimento dei rifiuti, oppure il negozio presso il quale è stato acquistato il prodotto.

Nolietotu iekārtu iznīcināšanas noteikumi lietotājiem Eiropas Savienības privātajās mājsaimniecībās

Šāds simbols uz izstrādājuma vai uz tā iesaiņojuma norāda, ka šo izstrādājumu nedrīkst izmest kopā ar citiem sadzīves atkritumiem. Jūs atbildat par to, lai nolietotās iekārtas tiktu nodotas speciāli iekārtotos punktos, kas paredzēti izmantoto elektrisko un elektronisko iekārtu savākšanai otrreizējai pārstrādei. Atsevišķa nolietoto iekārtu savākšana un otrreizējā pārstrāde palīdzēs saglabāt dabas resursus un garantēs, ka šīs iekārtas tiks otrreizēji pārstrādātas tādā veidā, lai pasargātu vidi un cilvēku veselību. Lai uzzinātu, kur nolietotās iekārtas var izmest otrreizējai pārstrādei, jāvēršas savas dzīves vietas pašvaldībā, sadzīves atkritumu savākšanas dienestā vai veikalā, kurā izstrādājums tika nopirkts.

Vartotojų iš privačių namų ūkių įrangos atliekų šalinimas Europos Sąjungoje

Šis simbolis ant gaminio arba jo pakuotės rodo, kad šio gaminio šalinti kartu su kitomis namų ūkio atliekomis negalima. Šalintinas įrangos atliekas privalote pristatyti į specialią surinkimo vietą elektros ir elektroninės įrangos atliekoms perdirbti. Atskirai surenkamos ir perdirbamos šalintinos įrangos atliekos padės saugoti gamtinius išteklius ir užtikrinti, kad jos bus perdirbtos tokiu būdu, kuris nekenkia žmonių sveikatai ir aplinkai. Jeigu norite sužinoti daugiau apie tai, kur galima pristatyti perdirbtinas įrangos atliekas, kreipkitės į savo seniūniją, namų ūkio atliekų šalinimo tarnybą arba parduotuvę, kurioje įsigijote gaminį.

Verwijdering van afgedankte apparatuur door privé-gebruikers in de Europese Unie

Dit symbool op het product of de verpakking geeft aan dat dit product niet mag worden gedeponeerd bij het normale huishoudelijke afval. U bent zelf verantwoordelijk voor het inleveren van uw afgedankte apparatuur bij een inzamelingspunt voor het recyclen van oude elektrische en elektronische apparatuur. Door uw oude apparatuur apart aan te bieden en te recyclen, kunnen natuurlijke bronnen worden behouden en kan het materiaal worden hergebruikt op een manier waarmee de volksgezondheid en het milieu worden beschermd. Neem contact op met uw gemeente, het afvalinzamelingsbedrijf of de winkel waar u het product hebt gekocht voor meer informatie over inzamelingspunten waar u oude apparatuur kunt aanbieden voor recycling.

Pozbywanie się zużytego sprzętu przez użytkowników w prywatnych gospodarstwach domowych w Unii Europejskiej

Ten symbol na produkcie lub jego opakowaniu oznacza, że produktu nie wolno wyrzucać do zwykłych pojemników na śmieci. Obowiązkiem użytkownika jest przekazanie zużytego sprzętu do wyznaczonego punktu zbiórki w celu recyklingu odpadów powstałych ze sprzętu elektrycznego i elektronicznego. Osobna zbiórka oraz recykling zużytego sprzętu pomogą w ochronie zasobów naturalnych i zapewnią ponowne wprowadzenie go do obiegu w sposób chroniący zdrowie człowieka i środowisko. Aby uzyskać więcej informacji o tym, gdzie można przekazać zużyty sprzęt do recyklingu, należy się skontaktować z urzędem miasta, zakładem gospodarki odpadami lub sklepem, w którym zakupiono produkt.

Descarte de Lixo Elétrico na Comunidade Européia

Este símbolo encontrado no produto ou na embalagem indica que o produto não deve ser descartado no lixo doméstico comum. É responsabilidade do cliente descartar o material usado (lixo elétrico), encaminhando-o para um ponto de coleta para reciclagem. A coleta e a reciclagem seletivas desse tipo de lixo ajudarão a conservar as reservas naturais; sendo assim, a reciclagem será feita de uma forma segura, protegendo o ambiente e a saúde das pessoas. Para obter mais informações sobre locais que reciclam esse tipo de material, entre em contato com o escritório da HP em sua cidade, com o serviço de coleta de lixo ou com a loja em que o produto foi adquirido.

Likvidácia vyradených zariadení v domácnostiach v Európskej únii

Symbol na výrobku alebo jeho balení označuje, že daný výrobok sa nesmie likvidovať s domovým odpadom. Povinnosťou spotrebiteľa je odovzdať vyradené zariadenie v zbernom mieste, ktoré je určené na recykláciu vyradených elektrických a elektronických zariadení. Separovaný zber a recyklácia vyradených zariadení prispieva k ochrane prírodných zdrojov a zabezpečuje, že recyklácia sa vykonáva spôsobom chrániacim ľudské zdravie a životné prostredie. Informácie o zberných miestach na recykláciu vyradených zariadení vám poskytne miestne zastupiteľstvo, spoločnosť zabezpečujúca odvoz domového odpadu alebo obchod, v ktorom ste si výrobok zakúpili.

Odstranjevanje odslužene opreme uporabnikov v zasebnih gospodinjstvih v Evropski uniji

Ta znak na izdelku ali njegovi embalaži pomeni, da izdelka ne smete odvreči med gospodinjske odpadke. Nasprotno, odsluženo opremo morate predati na zbirališče, pooblaščeno za recikliranje odslužene električne in elektronske opreme. Ločeno zbiranje in recikliranje odslužene opreme prispeva k ohranjanju naravnih virov in zagotavlja recikliranje te opreme na zdravju in okolju neškodljiv način. Za podrobnejše informacije o tem, kam lahko odpeljete odsluženo opremo na recikliranje, se obrnite na pristojni organ, komunalno službo ali trgovino, kjer ste izdelek kupili.

Eliminación de residuos de equipos eléctricos y electrónicos por parte de usuarios particulares en la Unión Europea

Este símbolo en el producto o en su envase indica que no debe eliminarse junto con los desperdicios generales de la casa. Es responsabilidad del usuario eliminar los residuos de este tipo depositándolos en un "punto limpio" para el reciclado de residuos eléctricos y electrónicos. La recogida y el reciclado selectivos de los residuos de aparatos eléctricos en el momento de su eliminación contribuirá a conservar los recursos naturales y a garantizar el reciclado de estos residuos de forma que se proteja el medio ambiente y la salud. Para obtener más información sobre los puntos de recogida de residuos eléctricos y electrónicos para reciclado, póngase en contacto con su ayuntamiento, con el servicio de eliminación de residuos domésticos o con el establecimiento en el que adquirió el producto.

Bortskaffande av avfallsprodukter från användare i privathushåll inom Europeiska Unionen

Om den här symbolen visas på produkten eller förpackningen betyder det att produkten inte får slängas på samma ställe som hushållssopor. I stället är det ditt ansvar att bortskaffa avfallet genom att överlämna det till ett uppsamlingsställe avsett för återvinning av avfall från elektriska och elektroniska produkter. Separat insamling och återvinning av avfallet hjälper till att spara på våra naturresurser och gör att avfallet återvinns på ett sätt som skyddar människors hälsa och miljön. Kontakta ditt lokala kommunkontor, din närmsta återvinningsstation för hushållsavfall eller affären där du köpte produkten för att få mer information om var du kan lämna ditt avfall för återvinning.

B

Console ports

Contents

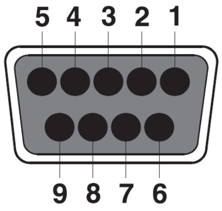
Overview

Console port and cable information for the MSM7xx controllers is provided as follows:

Product	**Information to use**
MSM710, MSM730, MSM750	Relevant section below
MSM760, MSM765zl	The provided Installation and Getting Started Guide.

MSM710 Console port

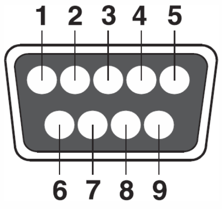
The MSM710 provides a DB-9 (female) Console (serial) port connector. The DB-9 connector (DCE) has pin assignments as follows:

Pin	Signal	Direction	Connector
1	DCD	→ to PC	 *DB-9 (female)*
2	RXD	→ to PC	
3	TXD	← from PC	
4	DTR	← from PC	
5	GND		
6	DSR	→ to PC	
7	RTS	← from PC	
8	CTS	→ to PC	
9	Unused		

To connect to a computer, use a standard (straight through) serial cable (male-to-female).

MSM730 Console port

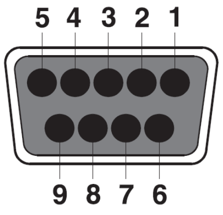
The MSM730 provides a DB-9 (male) Console (serial) port connector (DTE). The DB-9 connector has pin assignments as follows:

Pin	Signal	Direction	Connector
1	DCD	← from PC	 *DB-9 (male)*
2	RXD	← from PC	
3	TXD	→ to PC	
4	DTR	→ to PC	
5	GND		
6	DSR	← from PC	
7	RTS	→ to PC	
8	CTS	← from PC	
9	Unused		

To connect to a computer, use the supplied null-modem serial cable.

MSM750 Console port

The MSM750 provides an RJ-45 Console (serial) port connector. Connect the supplied RJ-45 to DB-9 (female) adapter. The DB-9 connector (DCE) has pin assignments as follows:

Pin	Signal	Direction	Connector
1	DCD	→ to PC	 *DB-9 (female)*
2	RXD	→ to PC	
3	TXD	← from PC	
4	DTR	← from PC	
5	GND		
6	DSR	→ to PC	
7	RTS	← from PC	
8	CTS	→ to PC	
9	Unused		

To connect to a computer, use a standard (straight through) serial cable (male-to-female).

Using the console port

The console port can be used to do the following:

- Reset the controller to factory default settings. For complete instructions, see *Using the Console (serial) port on page C-3*).
- Reset the manager username and password to factory default settings. For complete instructions, see *To reset manager credentials on a controller on page 2-6*.

C

Resetting to factory defaults

Contents

How it works

Depending on the controller model, there may be more than one way to reset the controller to its factory default settings. This appendix describes the methods available for each model type.

To reset only the manager username and password, see *To reset manager credentials on a controller on page 2-6*.

Caution Resetting a controller to factory defaults deletes all configuration settings, resets the manager username and password to “admin,” disables the DHCP server on the LAN port, sets the LAN port IP address to 192.168.1.1 (MSM765zl LAN port has no factory-default IP address), and sets the Internet port to operate as a DHCP client.

Note User-installed licenses are retained after a factory reset, but are deactivated. See *Factory reset considerations on page 20-7*.

Using the Reset button

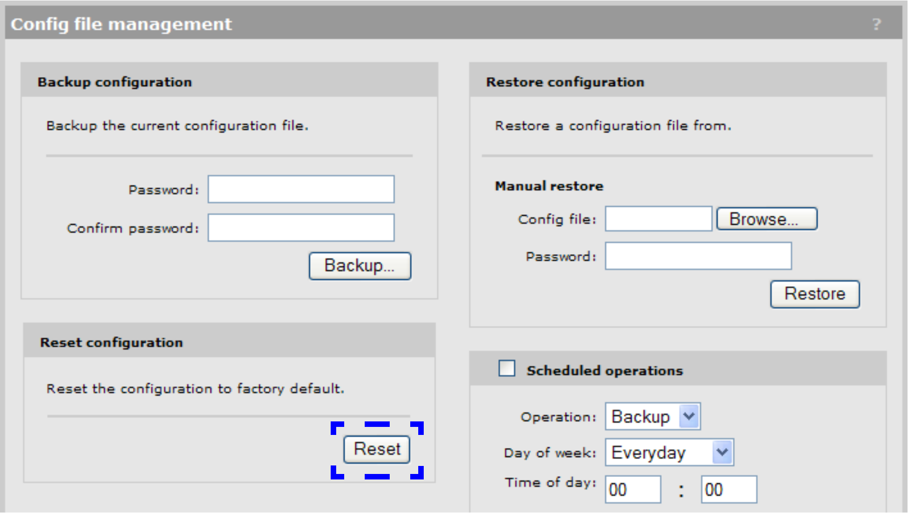
(MSM710 only.)

Using a tool such as a paper clip, press and hold the reset button (back of MSM710) for a few seconds until the front status lights blink three times.

Using the management tool

Supported on models: MSM710, MSM730, MSM750, MSM765zl, MSM760

1. Launch the management tool (default https://192.168.1.1).
2. Select **Controller >> Maintenance > Config file management**, and in section **Reset configuration**, select **Reset**.



Config file management

Backup configuration

Backup the current configuration file.

Password:

Confirm password:

Restore configuration

Restore a configuration file from.

Manual restore

Config file:

Password:

Reset configuration

Reset the configuration to factory default.

□ Scheduled operations

Operation: Backup

Day of week: Everyday

Time of day: 00 : 00

Using the Console (serial) port

Supported on models: MSM730, MSM750, MSM760

Note

It is recommended that you use the management tool as previously described to reset a controller to factory defaults. However, if you forgot the manager username or password, you can still force factory reset as described here:

1. Power off the controller.
2. Connect a serial cable to the controller console port as follows:
   - For the MSM730, and MSM750, see the relevant section in *Appendix B: Console ports*.
   - For the MSM760, see the *MSM760 Controllers Installation and Getting Started Guide.*
3. Configure a communications terminal program such as Microsoft Hyperterminal for Windows or Minicom for Linux as follows:
   - **Terminal**: VT-100 (ANSI)
   - **Speed**: Set speed according to the controller model:
     - For the MSM730 and MSM750, set speed to 115200 bps.
     - For the MSM760, set speed to 9600 bps.
   - **Data bits**: 8
   - **Stop bits**: 1
   - **Parity**: none
   - **Flow control**: none
4. Open an appropriately-configured terminal session.
5. Power on the controller. System boot messages appear.
6. **Do not press any keyboard keys**. Wait for the LILO prompt to appear. It looks like this:

```
LILO 22.1 boot:
```

Important

As soon as the LILO prompt appears, tap the keyboard space bar to prevent the automatic (non-factory-default) boot from continuing. You must tap the space bar or other key within four seconds of the prompt appearing.

7. At the LILO prompt, type the command `linux factory` and press **Enter**. The boot with factory defaults begins.

D

NOC authentication

Contents

Main benefits

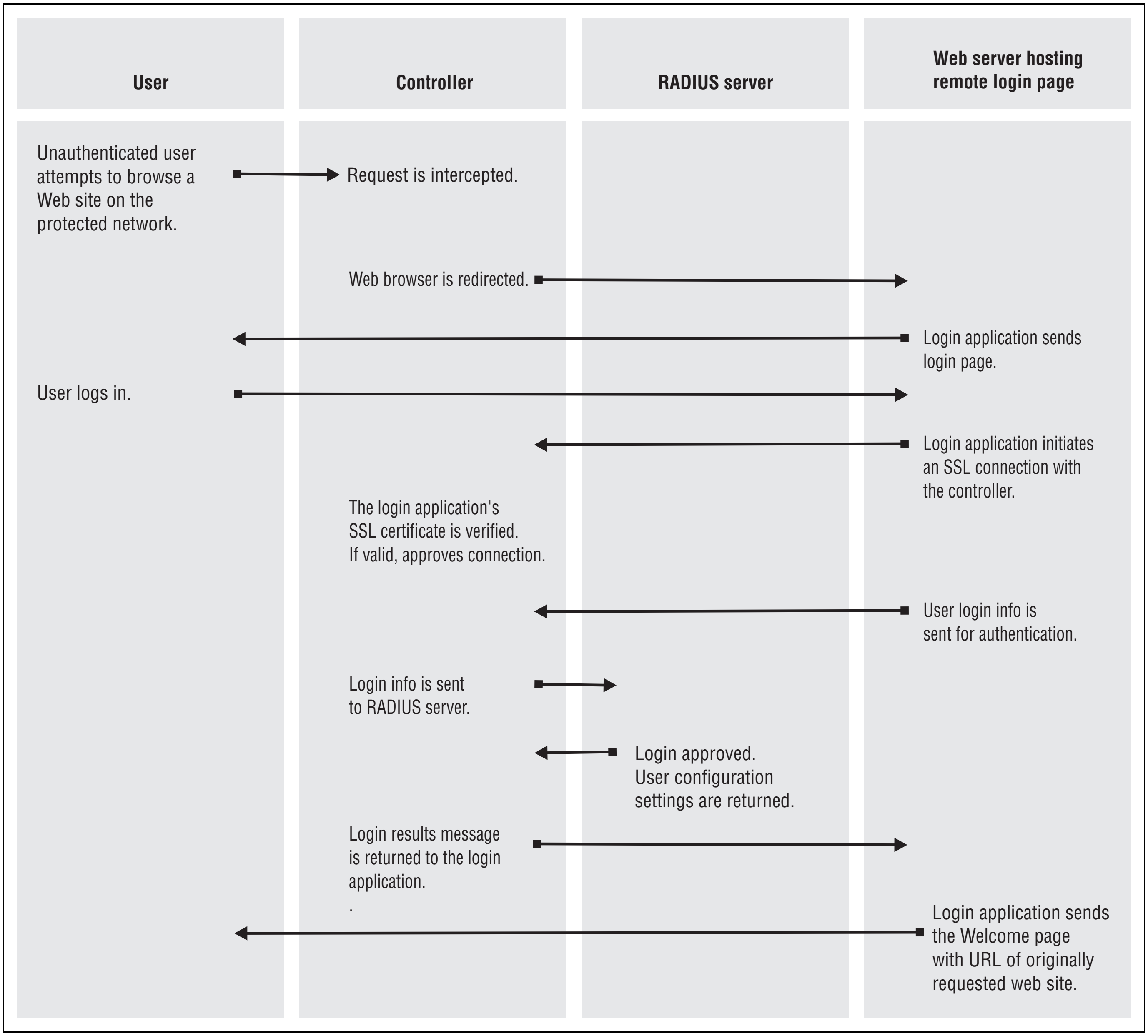
Using a remote login page with NOC (network operations center) authentication provides you with the following benefits:

- The login page is completely customizable. You are not bound by the limits imposed by loading a login page onto the controller.
- Users can login to the public access interface without exposing their Web browsers to the SSL certificate on the controller. This eliminates warning messages caused by having an SSL certificate on the controller that is not signed by a well-known certificate authority.
- If you want to support secure login with SSL, but have multiple controllers, using a remote login page means you only need to purchase a single SSL certificate signed by a well-known certificate authority, instead of one for each access point.

How it works

The NOC authentication feature provides a secure way of authenticating public access users, with strong mutual authentication between the login application on the Web server hosting the remote login page and the controller used for authenticating user logins. This occurs via the two Colubris-AVPair value strings (**ssl-noc-certificate** and **ssl-noc-ca-certificate**), which define the locations of two certificates. These certificates enable the controller to validate that the user login information does indeed come from a trusted application. For example, from a login application on the Web server.

The following diagram shows the sequence of events for a typical user session when using the NOC-based authentication feature.


User
Controller
RADIUS server
Web server hosting remote login page
Unauthenticated user attempts to browse a Web site on the protected network.
Request is intercepted.
Web browser is redirected.
Login application sends login page.
User logs in.
Login application initiates an SSL connection with the controller.
The login application's SSL certificate is verified. If valid, approves connection.
User login info is sent for authentication.
Login info is sent to RADIUS server.
Login approved. User configuration settings are returned.
Login results message is returned to the login application.
.
Login application sends the Welcome page with URL of originally requested web site.

Activating a remote login page with NOC authentication

To activate a remote login page, you must define several controller attributes. These attributes can be defined in the RADIUS account for the controller (if you are using a RADIUS server) or they can be locally configured.

The following table summarizes the Colubris-AVPair value strings for the remote login page with NOC authentication.

Item	Colubris-AVPair value string
External login	`login-url=`*`URL_of_the_page`* `[`*`placeholder`*`]` URL of the remote login page. Access to the Web server hosting this page must be granted to all unauthenticated users. Do this with an appropriate access list definition.
NOC certificate	`ssl-noc-certificate=`*`URL_of_the_Certificate`* Certificate issued to the application on the Web server that sends user info to the controller for authentication.
NOC CA certificate	`ssl-noc-ca-certificate=`*`URL_of_the_certificate`* Certificate of the certificate authority (CA) that issued the NOC certificate.
Custom SSL certificate	`ssl-certificate=`*`URL_of_the_certificate`* Custom certificate installed on the controller.

The following placeholders can be added to the login-url string.

Placeholder	Description
`%c`	Returns the IP address of the user's computer.
`%d`	Returns the WISPr location-ID. Supported for login-url only.
`%e`	Returns the WISPr location-Name. Supported for login-url only.
`%l`	Returns the URL on the controller where user login information should be posted for authentication. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
`%n`	Returns the NAS ID assigned to the controller. By default, this is the unit's serial number. Not supported in local mode.
`%s`	Returns the RADIUS login name assigned to the controller. By default, this is the unit's serial number. Not supported in local mode.

Placeholder	Description
%o	Returns the original URL requested by the user. By default, this value is URL encoded. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
%i	Returns the domain name assigned to the controller's Internet port.
%p	Returns the port number on the controller where user login information should be posted to for authentication.
%a	Returns the IP address of the controller's interface that is sending the authentication request.
%E	When the location-aware feature is enabled, returns the ESSID of the wireless access point the user is associated with.
%P	When the location-aware feature is enabled, returns the wireless mode ("ieee802.11a", "ieee802.11b", "ieee802.11g") the user is using to communicate with the access point.
%G	When the location-aware feature is enabled, returns the group name of the wireless access point the user is associated with.
%C	When the location-aware feature is enabled, returns the Called-station-id content for the wireless access point the user is associated with.
%r	Returns the string sent by the RADIUS server when an authentication request fails. The RADIUS server must be configured to support this feature. The information contained in the returned string depends on the configuration of the RADIUS server.
%m	Returns the MAC address of the wireless/wired client station that is being authenticated.
%v	Returns the VLAN assigned to the client station at the controller's ingress (LAN port).

Addressing security concerns

It is important that the connection between the login application and the controller be secure to protect the exchange of user authentication traffic. The following strategy provides for complete connection security.

Securing the remote login page

HTTPS can be used on the Web server to secure the login page. To avoid warning messages on the user's browser, the SSL certificate installed on the Web server should be signed by a well-known CA.

Authenticating with the login application

The connection between the login application and the controller is secured using SSL. When establishing the SSL connection with the controller, the login application must supply its SSL certificate. In a standard SSL setup, the controller uses the CA for this certificate to validate the certificate's identity and authenticate the login application.

However, the controller does not want to accept SSL connections from *just any* remote entity with a valid certificate. Rather, it only wants to accept connections from a specific entity: the login application.

To uniquely identify the login application, the *ssl-noc-certificate* attribute is defined in the RADIUS profile for the controller. This attribute contains the URL of the login application's SSL certificate. When the login application presents its SSL certificate, the controller retrieves *ssl-noc-certificate* and checks to make sure that they match.

For further authentication, a second attribute, *ssl-noc-ca-certificate*, is defined in the RADIUS profile for the controller. This attribute contains the URL of the public key of the certificate authority (CA) that signed the login application's SSL certificate. The controller uses the public key to determine if the login application's SSL certificate can be trusted.

Authenticating the controller

To identify itself, the controller uses the SSL certificate configured on the **Security > Certificate Stores** page or via the *ssl-certificate* attribute.

For added security, the login application could also check that this SSL certificate has been signed by the certificate authority for which the login application has the public key certificate. The default certificate installed on the controller is not signed by a well-known CA and cannot be used for this purpose. Instead, a new certificate must be installed on the controller. This certificate could be signed by a well-known certificate authority or your own CA.

NOC authentication list

Additional security is provided via the Security list on the **Public access > Web server** page. You use this list to define the set of remote IP addresses that the controller accepts authentication requests from. If a request is received from an address not in this list, it is discarded.

Setting up the certificates

This section presents an overview of the certificates you need to install to secure communication between the remote login page and the controller. For detailed discussion of the issues, see *Addressing security concerns on page D-5*.

Install certificates on the Web server

Install an SSL certificate and its matching CA certificate into a folder on the Web server hosting the remote login page. The login application and the controller access the certificates from this location.

The SSL certificate is used by the login application to secure communications with the controller.

Define attributes

Add the following attributes to the **Configured attributes** table on the **Public access > Attributes** page. (You can also define these attributes in the RADIUS profile for the controller if you are using a RADIUS server.) This enables it to retrieve the SSL and CA certificates from the Web server:

`ssl-noc-certificate=`*`URL_of_the_Certificate`* Certificate issued to the application on the Web server that sends user info to the controller for authentication.
`ssl-noc-ca-certificate=`*`URL_of_the_certificate`* Certificate of the certificate authority (CA) that issued the NOC certificate.
`ssl-certificate=`*`URL_of_the_certificate`* Custom certificate installed on the controller.

Install a certificate on controller

Note This step is optional, but recommended.

Install an SSL certificate on the controller to replace its default SSL certificate. This certificate is used to secure communications between the controller and the login application on the Web server.

If you do not change the default certificate on the controller, the login application may not be able to validate the controller certificate when establishing the SSL connection. The reason for this is because the default certificate is self-signed and is not trusted by any well-known CA.

This can be done by adding an additional attribute to the **Configured attributes** table on the **Public access > Attributes** page. (You can also define this attribute in the RADIUS profile for the controller if you are using a RADIUS server.).

```
ssl-certificate=URL_of_the_certificate
```

Authenticating users

After a user has supplied login information on the remote login page, the login application must submit an authentication request containing the user's login name, password, and IP address to the controller by establishing an SSL session to the following URL:

```
https://controller_ip:8090/goform/HtmlNocLoginRequest
?username=username&password=password&ipaddr=user_ip
```

Where:

Parameter	Description
`controller_ip`	Defines the IP address of the controller or you could use a domain name if you have defined one using the hosts file on the Web server. (By default, the secure Web server on the controller operates on port 8090. This can be changed on the **Management > Management Tool** page if required.) The controller requires that the contents of the Host HTTP header match the actual domain name/IP address and port the controller is operating on: Host: controller_domain_name:secure_web_server_port_number or Host: controller_IP_address:secure_web_server_port_number This is usually the case unless the controller is behind a device that provides network address translation (NAT). In this situation, the login application must manually forge the Host HTTP header. The easiest way to do this is to define `login-url` with the `%i` and `%p` placeholders. This returns the domain name of the controller and the port number of its secure Web server. The login application can then construct the appropriate Host HTTP header.
`username`	Username supplied by the user.
`password`	Password supplied by the user.
`user_ip`	IP address of the user's computer.

Example 1

Assume that the controller is not behind a NATing device, and that its IP address is 192.168.4.2. The subject DN in its SSL certificates is www.noc-cn3.com.

The Host HTTP header should be set to one of:

- Host: www.noc-cn3.com:8090
- Host: 192.168.4.2:8090

Example 2

Assume that the controller is behind a NATting device. The device has the address 192.168.30.173, and the controller has the address 192.168.4.2. A NAT mapping is defined on the NATting device that redirects traffic received on port 8090 to 192.168.4.2:8090.

The login application must send its requests to 192.168.30.173, which results in a HTTP Host header that contains one of the following:

- Host: natting.device.com:8090
- Host: 192.168.30.173:8090

When this request is forwarded to the controller, it is rejected. To solve the problem, the login application must forge the host HTTP header. This is easily done by plugging in the values returned by the %i, %a, and %p placeholders. For example:

Host: %i:%p
or
Host: %a,%p

The controller sends the username and password to the RADIUS server to authenticate the user. If authentication is successful, the user’s IP address is used to grant wireless network access to the user’s computer.

The controller returns a positive or negative answer for the user login, along with the relevant URLs that may be needed by the login application in order to redirect the user to either a Welcome page or a Login error page located on the Web server. This information is returned as standard HTML. The login application must parse this information to retrieve the response. All possible responses are described in the following section.

Returned values

The following examples show the information returned for various authentication conditions.

NOC authentication mode is not enabled

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_DISABLED
</HTML>
```

The controller did not receive the login application’s SSL certificate

The login application did not send its certificate. Therefore, the request was rejected.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_CANNOT_GET_PEER_CERT
</HTML>
```

Certificate mismatch

The login application sent an SSL certificate that does not match the one defined by ssl-noc-certificate in the RADIUS profile for the controller.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_CANNOT_GET_PEER_CERT
</HTML>
```

Certificate not valid yet

The login application sent an SSL certificate that matches the one defined by ssl-noc-certificate in the RADIUS profile for the controller. However, the certificate that was sent is not yet valid.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_CERT_NOT_YET_VALID
</HTML>
```

Certificate not valid anymore

The login application sent an SSL certificate that matches the one defined by ssl-noc-certificate in the RADIUS profile for the controller. However, the certificate that was sent is not valid anymore.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_CERT_EXPIRED
</HTML>
```

Certificate not signed by proper CA

The login application sent a valid SSL certificate that matches the one defined by ssl-noc-certificate in the RADIUS profile for the controller. However, the certificate is not signed by the CA defined by noc-ca-certificate in the RADIUS profile for the controller.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_CERT_NOT_SIGNED_BY_AUTHORIZED_CA
</HTML>
```

Missing username and/or password

The user’s username or password was not supplied.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_MISSING_USERNAME_OR_PASSWORD
</HTML>
```

The specified IP address is already logged in

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_LOGGED_IN
</HTML>
```

Authentication was successful

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_SUCCESS
NOC_INFO_WELCOME_URL=<welcome url>
NOC_INFO_SESSION_URL=<session url>
</HTML>
```

Authentication failed

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_ERR_MESSAGE=<error message>
NOC_INFO_LOGIN_ERR_URL =<login error url>
</HTML>
```

Logout succeeded

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_SUCCESS
</HTML>
```

Logout failed

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=<error message>
</HTML>
```

Examples of returned HTML code

The following examples show the actual HTML code returned file for various authentication conditions.

User was successfully authenticated by the RADIUS server

```
<HTML>
status=success
welcome-url=https://206.162.167.226:8888/cebit-php/
welcome.php?site=www.noc-
controller.com&user=user00&wantedurl=&nasipaddress=&nasid=L003-00069
session-url=http://192.168.1.1:8080/session.asp
</HTML>
```

User’s IP address is already in use by an active session

```
<HTML>
status=already-logged-in
</HTML>
```

User authentication was refused by the RADIUS server

This could be due to an unknown username, or invalid username or password.

```
<HTML>
status=failure
external-err-msg=Your login was refused.
login-err-url=https://206.162.167.226:8888/cebit-php/login-
error.php?site=john-cn3000&user=user12&nasipaddress=
</HTML>
```

User could not be authenticated

The controller could not contact a RADIUS server.

```
<HTML>
status=failure
external-err-msg=You cannot be logged in at this time. Please try again
later.
login-err-url=https://206.162.167.226:8888/cebit-php/login-
error.php?site=john
-cn3000&user=user12&nasipaddress=
</HTML>
```

Simple NOC authentication example

This is a simple example showing how to use the NOC authentication feature.

1. Retrieve the Public Access Examples zip file at www.hp.com/networking/public-access-examples.
2. Create the following folder on your Web sever: **newlogin.**
3. Copy these files from the Public Access Examples zip file into the **newlogin** folder:
   - login.html
   - transport.html
   - session.html
   - fail.html
   - logo.gif
4. Customize **login.html** to accept username and password information from users and then send it to the controller. You could use code similar to the following PHP example to send login information back to the controller for authentication:

   ```
   https://controller_ip:8090/goform/HtmlNocLoginRequest
   ?username=username&password=password&ipaddress=user_ip
   ```

   The variable `loginurl` contains the URL on the controller where user information is sent for authentication.
5. Start the management tool.

6. Select **Public access** > **Web server**.
7. Enable the **NOC-based authentication** feature.
8. Under **Security** add the IP address of the Web server to the **Allowed Addresses** box.
9. Under **Active interfaces** make sure that the interface on which the request will be received is enabled.
10. Select **Save**.
11. Add the following entries to the **Configured attributes** table on the **Public access > Attributes** page. (You can also define these attributes in the RADIUS profile for the controller if you are using a RADIUS server.)

    `login-url=`*URL_of_page_on_remote_server*

    `access-list=loginserver,ACCEPT,tcp,`*web_server_IP_address*`,443`

    `ssl-noc-certificate=`*URL_of_the_certificate*

    `ssl-noc-ca-certificate=`*URL_of_the_certificate*

    `transport-page=`*web_server_URL*`/newlogin/transport.html`

    `session-page=`*web_server_URL*`/newlogin/session.html`

    `fail-page=`*web_server_URL*`/newlogin/fail.html`

    `logo=`*web_server_URL*`/newlogin/logo.gif`

    `use-access-list=loginserver`

Forcing user logouts

Users can be logged out by calling the following URL:

```
https://controller_ip:8090/goform/HtmlNocLogoutRequest
?ipaddress=user_ip
```

Note This request must come from the login application (or another other application that is using the same SSL certificate).

The controller returns a positive or negative answer for the user logout as standard HTML. The login application must parse this information to retrieve the response.

Logout success

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_SUCCESS
</HTML>
```

Logout failure

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=<error message>
</HTML>
```

These definitions are contained in **noc.h**.

E

DHCP servers and Colubris vendor classes

Contents

Overview

This section shows you how to configure the following DHCP servers to use the vendor-specific class:

- *Windows Server 2003 configuration on page E-2.*
- *ISC DHCP server configuration on page E-7.*

A vendor class allows certain devices to request specific information from a Dynamic Host Configuration Protocol server. Specifically, the HP ProCurve vendor class enables you to define a list of available controllers to which APs operating in controlled mode can connect.

When DHCP clients send the Colubris *vendor class identifier* in a DHCP request, a properly configured DHCP server returns the Colubris-specific options defined on the server. These values are returned as DHCP option 43 (vendor-specific information) and can be interpreted only by a HP ProCurve device.

Windows Server 2003 configuration

This section describes how to configure a Windows 2003 DHCP server to use the HP ProCurve vendor class.

The following procedure assumes that you have a Windows 2003 Server that has a DHCP server configured and running.

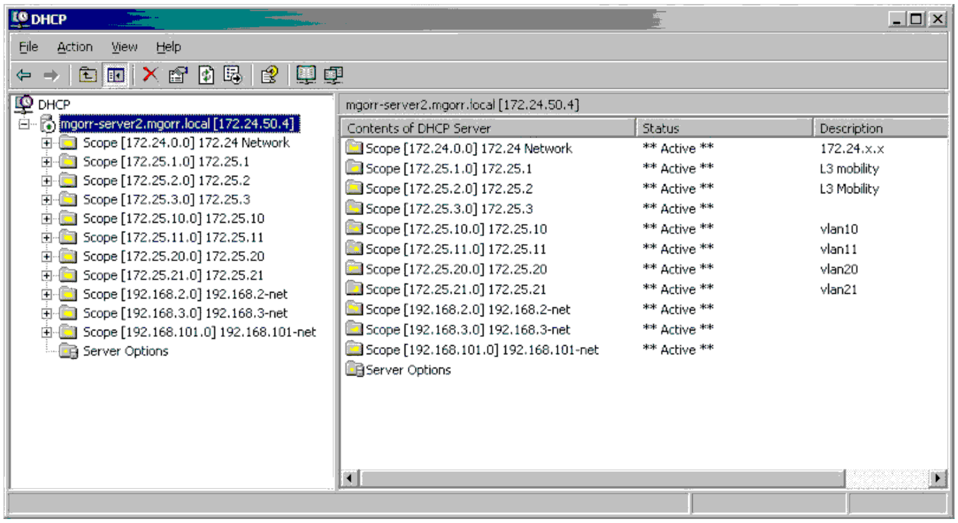
For more information see “Configuring Options and Classes on Windows Server” at

http://technet2.microsoft.com/WindowsServer/en/Library/d55609a5-2a1c-4f3f-ba8f-42b21828dc201033.mspx

Creating the vendor class

Use the following steps to create the Colubris vendor class on the DHCP server.

1. Select **Start > Settings > Control Panel > Administrative Tools > DHCP.** The **DHCP** administration page opens.

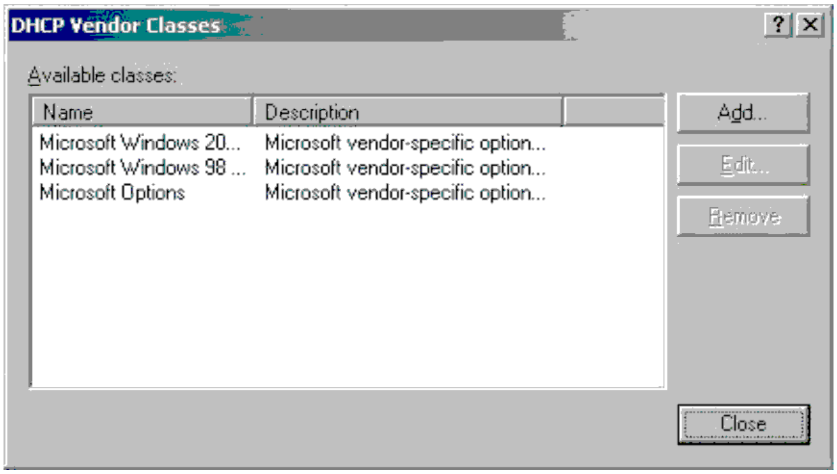


DHCP
mgorr-server2.mgorr.local [172.24.50.4]
Scope [172.24.0.0] 172.24 Network
Scope [172.25.1.0] 172.25.1
Scope [172.25.2.0] 172.25.2
Scope [172.25.3.0] 172.25.3
Scope [172.25.10.0] 172.25.10
Scope [172.25.11.0] 172.25.11
Scope [172.25.20.0] 172.25.20
Scope [172.25.21.0] 172.25.21
Scope [192.168.2.0] 192.168.2-net
Scope [192.168.3.0] 192.168.3-net
Scope [192.168.101.0] 192.168.101-net
Server Options

mgorr-server2.mgorr.local [172.24.50.4]

Contents of DHCP Server	Status	Description
Scope [172.24.0.0] 172.24 Network	** Active **	172.24.x.x
Scope [172.25.1.0] 172.25.1	** Active **	L3 mobility
Scope [172.25.2.0] 172.25.2	** Active **	L3 Mobility
Scope [172.25.3.0] 172.25.3	** Active **	
Scope [172.25.10.0] 172.25.10	** Active **	vlan10
Scope [172.25.11.0] 172.25.11	** Active **	vlan11
Scope [172.25.20.0] 172.25.20	** Active **	vlan20
Scope [172.25.21.0] 172.25.21	** Active **	vlan21
Scope [192.168.2.0] 192.168.2-net	** Active **	
Scope [192.168.3.0] 192.168.3-net	** Active **	
Scope [192.168.101.0] 192.168.101-net	** Active **	
Server Options		

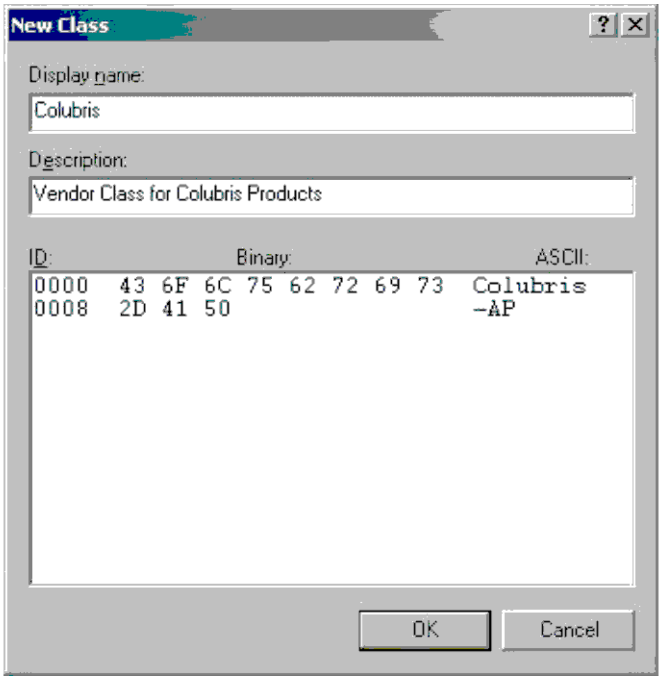
2. On the **DHCP** administration page in the navigation pane at left, select the name of the DHCP server to manage, and then select **Action > Define Vendor Classes.** The **DHCP Vendor Classes** page opens. Several default Microsoft vendor classes are preconfigured.



Available classes:

Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...

3. On the **DHCP Vendor Classes** page, select **Add.** The **New Class** page opens.



Display name: Colubris

Description: Vendor Class for Colubris Products

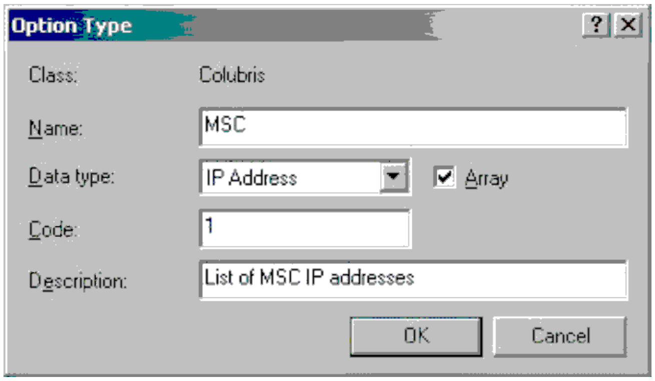
```
ID:             Binary:                  ASCII:
0000   43 6F 6C 75 62 72 69 73   Colubris
0008   2D 41 50                  -AP
```

4. On the **New Class** page
   - Under **Display name,** specify **Colubris.**
   - Under **Description,** specify any desired descriptive information for this vendor class.
   - Select under **ASCII** and specify **Colubris-AP.**
   - Select **OK.**
5. The **New Class** page closes, and you return to the **DHCP Vendor Classes** page. To close the **DHCP Vendor Classes** page and return to the **DHCP** administration page, select **Close.**

Defining vendor class options

Use the following steps to define Colubris vendor class options on the DHCP server.

1. On the **DHCP** administration page, select **Action > Set Predefined Options.** From the **Option class** drop-down menu, select **Colubris,** and then select **Add.** The **Option Type** page opens.



Class: Colubris

Name: MSC

Data type: IP Address ☑ Array

Code: 1

Description: List of MSC IP addresses

2. On the **Option Type** page,
   - Under **Name,** specify **MSC** (for MSM controllers).
   - Under **Data type,** select **IP Address** and enable the **Array** checkbox.
   - Under **Code,** specify **1.**
   - Under **Description,** specify **List of MSC IP addresses** (for MSM controller IP addresses).
3. Select **OK** to close the **Option Type** page, and then select **OK** again to return to the **DHCP** administration page.

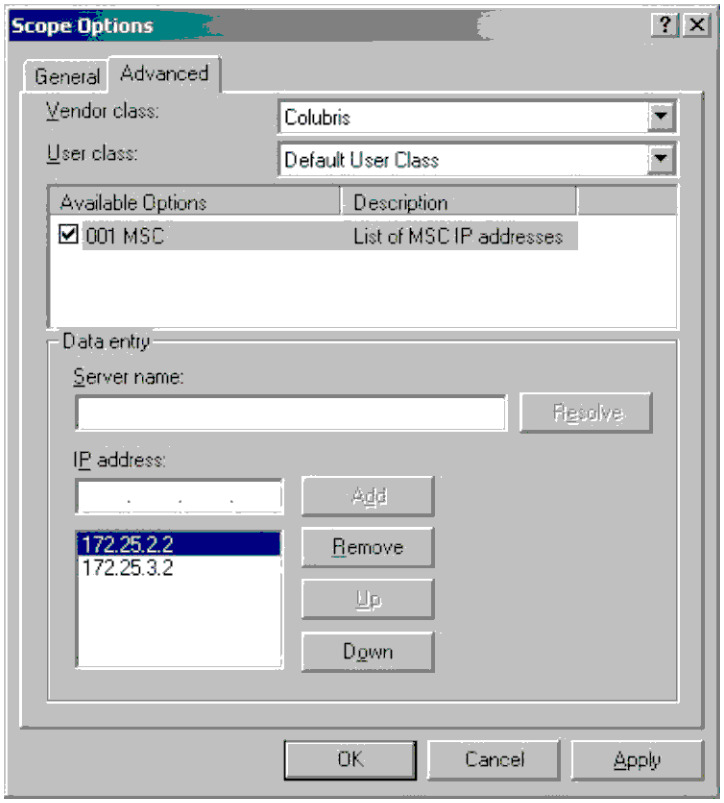
Applying the vendor class

After you define the Colubris vendor class and its options, you can apply the class to specific Scopes or to the entire DHCP server. You must define the Colubris vendor class for every Scope from which an AP can get an address.

Use the following steps to add the Colubris vendor-specific option to one **Scope** on the DHCP server.

1. On the **DHCP** administration page, in the navigation pane, open the folder that corresponds to the desired **Scope**.

2. Right-click **Scope Options,** and from the resulting menu select **Configure Options.** The **Scope Options** page opens. Select the **Advanced** tab.



Vendor class: Colubris

User class: Default User Class

Available Options	Description
☑ 001 MSC	List of MSC IP addresses

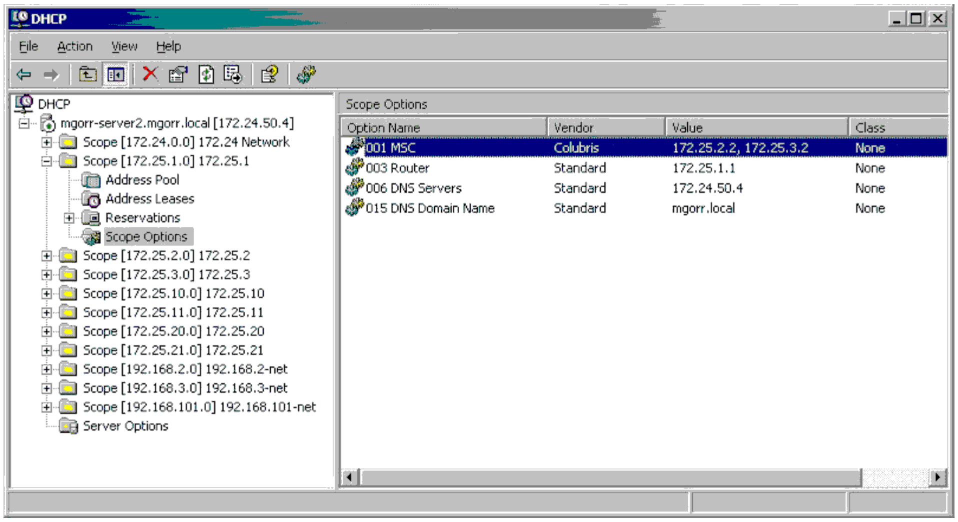
IP address:

172.25.2.2
172.25.3.2

3. On the **Advanced** tab, configure the following:

- From the **Vendor class** drop-down menu, select **Colubris.**
- Under **Available options,** enable the **001 MSC** checkbox.
- Under **IP address,** specify the IP address of the primary controller in your network and select **Add.** Continue to build a list by specifying the IP addresses of all controllers in your network, in descending order of importance.
- Select **OK**.

4. The controller IP addresses now appear on the DHCP administration page under **Scope Options.** When an AP requests an IP address, these addresses are returned in a DHCP Ack message as option 43.



DHCP
mgorr-server2.mgorr.local [172.24.50.4]
Scope [172.24.0.0] 172.24 Network
Scope [172.25.1.0] 172.25.1
Address Pool
Address Leases
Reservations
Scope Options
Scope [172.25.2.0] 172.25.2
Scope [172.25.3.0] 172.25.3
Scope [172.25.10.0] 172.25.10
Scope [172.25.11.0] 172.25.11
Scope [172.25.20.0] 172.25.20
Scope [172.25.21.0] 172.25.21
Scope [192.168.2.0] 192.168.2-net
Scope [192.168.3.0] 192.168.3-net
Scope [192.168.101.0] 192.168.101-net
Server Options

Scope Options

Option Name	Vendor	Value	Class
001 MSC	Colubris	172.25.2.2, 172.25.3.2	None
003 Router	Standard	172.25.1.1	None
006 DNS Servers	Standard	172.24.50.4	None
015 DNS Domain Name	Standard	mgorr.local	None

Note For information on solving problems, see *Troubleshooting on page E-9*.

ISC DHCP server configuration

This section shows you how to configure a Linux machine running an Internet Systems Consortium (ISC) DHCP server to use the Colubris Networks vendor class. The procedure assumes that you have a Linux or Unix server that is running the ISC DHCP server.

You configure the ISC DHCP server by editing its configuration file; specifically, the main configuration file, */etc/dhcpd.conf*.

Following is a simple example of the */etc/dhcpd.conf* configuration file:

```
# dhcpd.conf
ddns-update-style ad-hoc;
option domain-name "colubris.com";
option domain-name-servers 172.25.1.3;
default-lease-time 3600;

subnet 172.25.1.0 netmask 255.255.255.0 {
        range 172.25.1.100 172.25.1.150;
        option routers 172.25.1.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.1.255;

}
subnet 172.25.2.0 netmask 255.255.255.0 {
        range 172.25.2.100 172.25.2.150;
        option routers 172.25.2.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.2.255;
}
```

This sample file defines some general options to apply to all clients, as well as two DHCP Scopes—172.25.1.x and 172.25.2.x. You must add lines to the *dhcpd.conf* file to define the following for the ISC server:

- What the Colubris vendor class identifier looks like
- What to return to the client when it sees that identifier.

The following explains the changes that you must make to this sample file and the function of each added line.

- Create an option space called **Colubris** and define a variable called **msc-address** within the space by adding the following lines.

  ```
  option space Colubris;

  option Colubris.msc-address code 1 = array of ip-address;
  ```

- Tell the server what to do when the client sends the vendor class identifier **Colubris-AP** by adding the following lines. In this case you want the server to return the options defined in the Colubris space that was created in the first step. Using the **vendor-option-space** command tells the server to return these values using DHCP option 43.

  ```
  if option vendor-class-identifier =  "Colubris-AP" {

          vendor-option-space Colubris;

  }
  ```

- Specify the controller IP addresses to return to the client by adding the following lines, where **172.25.2.2** and **172.25.3.2** are the specific IP addresses that you want returned. You can define this option globally or in one or more Scopes. You must define this option on all subnets from which an AP can potentially get an IP address. In this example only clients on the 172.25.1.x subnet get this option.

  ```
  option Colubris.msc-address 172.25.2.2, 172.25.3.2;
  ```

Following is a revised sample configuration file that contains these additions, which appear in bold:

```
# dhcpd.conf
ddns-update-style ad-hoc;
option domain-name "colubris.com";
option domain-name-servers 172.25.1.3;
default-lease-time 3600;

option space Colubris;
option Colubris.msc-address code 1 = array of ip-address;

if option vendor-class-identifier =  "Colubris-AP" {
        vendor-option-space Colubris;
}


subnet 172.25.1.0 netmask 255.255.255.0 {
        range 172.25.1.100 172.25.1.150;
        option routers 172.25.1.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.1.255;
        option Colubris.msc-address 172.25.2.2, 172.25.3.2;
```

```
}

subnet 172.25.2.0 netmask 255.255.255.0 {
        range 172.25.2.100 172.25.2.150;
        option routers 172.25.2.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.2.255;
}
```

Troubleshooting

This section shows an Ethereal trace of a DHCP transaction, with the frames edited for readability. Four frames must be exchanged between the client and the server:

1. Client sends a `DHCP-Discover.`
2. Server sends a `DHCP-Offer.`
3. Client sends a `DHCP-Request.`
4. Server sends a `DHCP-Ack.`

The client sends its vendor class identifier in the `DHCP-Request` frame. The DHCP field of Frame 3 is expanded below.

The server sends the controller addresses encapsulated as option 43 in the `DHCP-Ack` frame. Unfortunately, the only way to decode these values is to look at the hexadecimal data. In this case the server returned the following 10 bytes:

```
2b 0a 01 08 ac 19 02  02 ac 19 03 02
```

which can be decoded as shown in the following table.

Segment	Value	Meaning
2b	43	DHCP option 43
0a	10	Field is 10 bytes long
01	01	Colubris option code 1 as defined in the DHCP server
08	08	Option code 1 is 8 bytes long
ac 19 02 02	172.25.2.2	Controller IP addresses to return to the client
ac 19 03 02	172.25.3.2	

```
Frame 1 - DHCP-Discover

Frame 1 (346 bytes on wire, 346 bytes captured)
Ethernet II, Src: Colubris_01:5f:05 (00:03:52:01:5f:05), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
```

```
Frame 2 - DHCP-Offer

Frame 2 (346 bytes on wire, 346 bytes captured)
Ethernet II, Src: Cisco_23:0e:80 (00:0d:bc:23:0e:80), Dst: Colubris_01:5f:05
(00:03:52:01:5f:05)
802.1Q Virtual LAN
Internet Protocol, Src: 172.25.1.1 (172.25.1.1), Dst: 172.25.1.201 (172.25.1.201)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol

Frame 3 - DHCP-Request

Frame 3 (346 bytes on wire, 346 bytes captured)
Ethernet II, Src: Colubris_01:5f:05 (00:03:52:01:5f:05), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4262bc18
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Colubris_01:5f:05 (00:03:52:01:5f:05)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Request
    Option 54: Server Identifier = 172.24.50.4
    Option 50: Requested IP Address = 172.25.1.201
    Option 60: Vendor class identifier = "Colubris-AP"
    Option 12: Host Name = "R054-00118"
    Option 55: Parameter Request List
    End Option
    Padding


Frame 4 - DHCP-Ack

Frame 4 (358 bytes on wire, 358 bytes captured)
Ethernet II, Src: Cisco_23:0e:80 (00:0d:bc:23:0e:80), Dst: Colubris_01:5f:05
(00:03:52:01:5f:05)
802.1Q Virtual LAN
Internet Protocol, Src: 172.25.1.1 (172.25.1.1), Dst: 172.25.1.201 (172.25.1.201)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4262bc18
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 172.25.1.201 (172.25.1.201)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 172.25.1.1 (172.25.1.1)
    Client MAC address: Colubris_01:5f:05 (00:03:52:01:5f:05)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP ACK
    Option 58: Renewal Time Value = 12 hours
    Option 59: Rebinding Time Value = 21 hours
    Option 51: IP Address Lease Time = 1 day
    Option 54: Server Identifier = 172.24.50.4
    Option 1: Subnet Mask = 255.255.255.0
    Option 3: Router = 172.25.1.1
    Option 15: Domain Name = "mgorr.local"
    Option 6: Domain Name Server = 172.24.50.4
    Option 43: Vendor-Specific Information (10 bytes)
    End Option

0000  00 03 52 01 5f 05 00 0d bc 23 0e 80 81 00 00 65   ..R._....#.....e
0010  08 00 45 00 01 54 81 68 00 00 ff 11 de 33 ac 19   ..E..T.h.....3..
0020  01 01 ac 19 01 c9 00 43 00 44 01 40 68 ec 02 01   .......C.D.@h...
0030  06 00 42 62 bc 18 00 00 00 00 00 00 00 00 ac 19   ..Bb............
0040  01 c9 00 00 00 00 ac 19 01 01 00 03 52 01 5f 05   ............R._.
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0110  00 00 00 00 00 00 00 00 00 00 63 82 53 63 35 01   ..........c.Sc5.
0120  05 3a 04 00 00 a8 c0 3b 04 00 01 27 50 33 04 00   .:.....;...'P3..
0130  01 51 80 36 04 ac 18 32 04 01 04 ff ff ff 00 03   .Q.6...2........
0140  04 ac 19 01 01 0f 0c 6d 67 6f 72 72 2e 6c 6f 63   .......mgorr.loc
0150  61 6c 00 06 04 ac 18 32 04 2b 0a 01 08 ac 19 02   al.....2.+......
0160  02 ac 19 03 02 ff                                 ......
```

Technology for better business outcomes

To learn more, visit www.hp.com/networking

January 2011

Manual Part Number
5998-1136