HP MSM3xx / MSM4xx Access Points

Management and Configuration Guide

HP MSM3xx / MSM4xx Access Points

Management and Configuration Guide

Publication Number
5998-1147
May 2011

Applicable Products
See *Products covered on page 1-2*.

Trademark Credits
Windows NT®, Windows®, and MS Windows® are US registered trademarks of Microsoft Corporation.

sFlow

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
Before installing and operating this product, please read *Safety information on page 1-10*.

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

Contents

1 Introduction

2 Management

A Console ports

B Regulatory information

C Connecting external antennas

D Resetting to factory defaults

1

Introduction

Contents

About this guide

This guide explains how to install, configure, and operate HP MSM3xx/MSM4xx Access Points in autonomous mode. Basic information on operating in controlled mode is also provided. For detailed controlled-mode instructions, see the *MSM7xx Controllers Management and Configuration Guide*.

Products covered

This guide provides autonomous-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
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

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 or MSM AP	Refers to any HP MSM3xx or MSM4xx Access Point.
Controller	Refers to any HP MSM7xx Controller, including both Access Controller and Mobility Controller variants.

Conventions

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.

Management tool

This guide uses specific syntax when directing you to interact with the management tool user interface. Refer to the following image for identification of key user-interface elements and then the table below for example directions:

Example directions in this guide	What to do in the user interface
Select **Wireless > Local Mesh**.	On the main menu select **Wireless** and then select **Local mesh** on the sub-menu.
For **Password** specify **secret22**.	In the field **Password** enter the text **secret22** exactly as shown.

Ports

If the AP you are configuring only has a single port, this manual refers to it as Port 1. Ignore references to Port 2.

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.

New in this release

The following new features and enhancements have been added in release 5.5:

New feature or enhancement	For information see...
New access points	This release supports the following new 802.11n dual-radio access points: E-MSM430, E-MSM460, and E-MSM466. For for more information on these APs, see: ■ *E-MSM430, E-MSM460, and E-MSM466 802.11n Access Points Quickstart* ■ *Radio configuration on page 3-8* ■ *802.11n MIMO antennas for the E-MSM466 on page C-2*
Broadcast filtering	*Broadcast filtering on page 4-10*
Band steering	*Band steering on page 4-10*
Beamforming	*Tx beamforming on page 3-28*
Transmission protection	*Tx protection on page 3-29*
Identify RADIUS server by host name	*Primary/Secondary RADIUS server on page 6-5*
LEAP support	This release supports LEAP (with WEP, TKIP, or WPA2 keys) when using an external RADIUS server to validate user login credentials. Support is automatic. No configuration is required.

Introducing the MSM3xx/4xx Access Points

The HP MSM APs bring intelligence to the network edge, providing scalable, seamless wireless access anywhere, anytime. They dispense multiple network services, enforce robust security and deliver high performance client access, unlike *thin* or *lite* access points. An integral component of HP Multi-Service Mobility solutions, MSM APs support a plug-and-play automatic configuration and ongoing central control by HP MSM Mobility and Access Controllers for the highest degree of configurability and ease of management.

Key features

Wireless

- Single-, dual-, and tri-radios
- 802.11n and 802.11a/b/g
- Per-radio software-selectable configuration of the 2.4 GHz and 5 GHz frequency bands
- Plenum-rated or NEMA-rated enclosures for indoor and outdoor wireless coverage
- Self-healing, self-optimizing local mesh extends network availability to areas without an Ethernet infrastructure
- 802.3af Power over Ethernet or external power cord

Management

- Centrally controlled, configured and updated with a Mobility or Access Controller
- Auto-selection of RF channel and transmit power
- Per-client event log of association, security, and DHCP activities for easy diagnosis
- Packet capture on a VSC or LAN interface
- In autonomous mode, SNMP, CLI, and Web-based management interfaces for integration with HP Mobility Manager or third-party, standards-based network management systems
- LLDP support, providing the ability to discover and exchange information with other network devices

Security

- Enforcement of client authorization based on user credentials (802.1X/EAP), hardware identifiers (MAC address, WEP key), and HTML login
- Hardware-assisted encryption using WPA2/AES (IEEE 802.11i), WPA/RC4 and/or WEP
- Dedicated RF sensor and dedicated client access eliminate time-slicing on the MSM325 and MSM335.
- Layer-2 client isolation per VSC
- 802.1X supplicant for connection to a secure switch port
- Block access based on client station MAC addresses

- Wireless Network Design Process
- Protocol filtering per VSC to deny unwanted traffic
- IP filtering per-user and per-VSC to forward traffic to a pre-defined location
- Management communication through SSH/SSL, IPsec, and digital certificates
- Cable-lock compatible for physical security on the MSM335, MSM410, MSM422, E-MSM430, E-MSM460, and E-MSM466
- Controlled-mode security to prevent data from being recovered from stolen APs

Controlled mode versus autonomous mode

MSM APs can operate in one of two modes: controlled mode (default) or autonomous mode.

Note

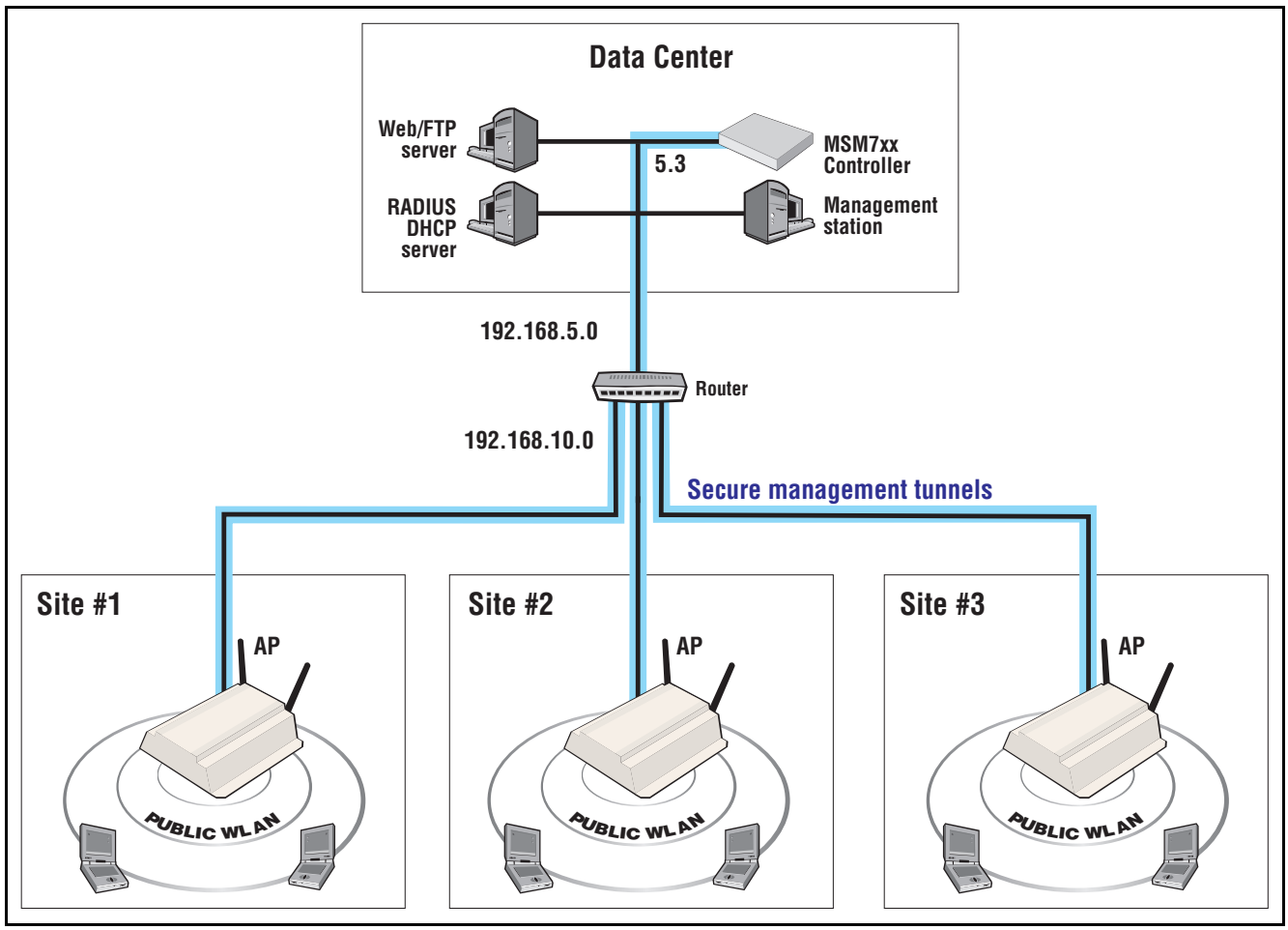
This guide explains how to install, configure, and operate HP MSM3xx/MSM4xx Access Points in autonomous mode. For detailed controlled-mode instructions, see the *MSM7xx Controllers Management and Configuration Guide*.

Controlled mode

When operating in controlled mode, APs are managed by an MSM7xx Controller (controller). On startup, the AP must establish a management tunnel with a controller before it becomes fully operational. Discovery of the controller is automatic if default settings are used on the AP and the controller, and both devices are on the same subnet.

The controller manages the AP and provides all configuration settings, making it easy to enforce consistent security and QoS policies, and automate AP configuration to minimize deployment and operation costs.

The following example shows multiple APs installed to offer public access networking at several different physical locations. A single controller is used to manage the devices and control access to the wireless network.

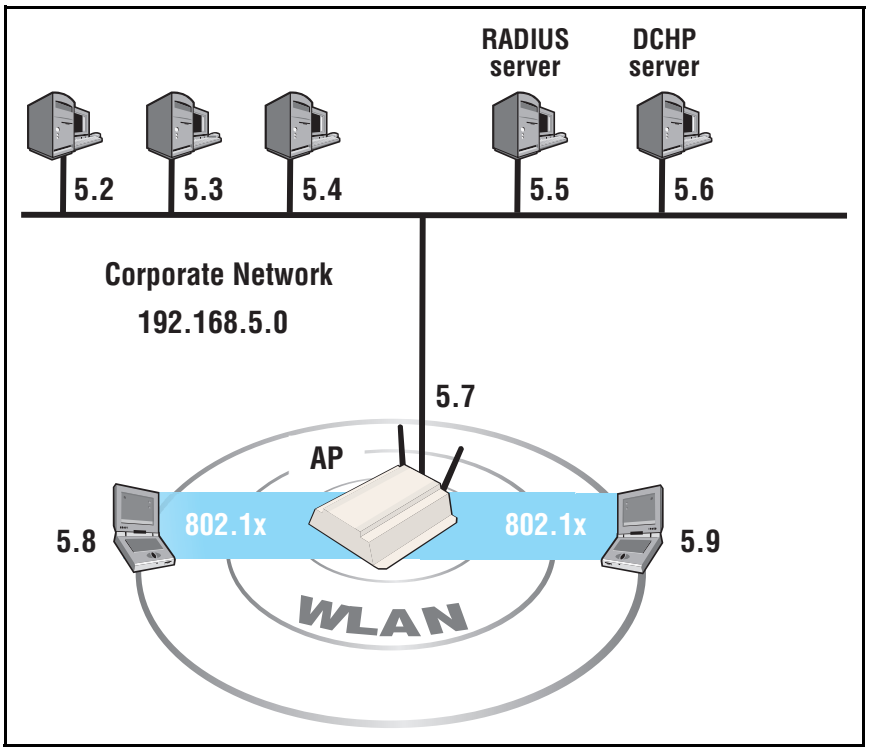


Autonomous mode

When operating in autonomous mode, APs are managed individually using their integrated management tool. This mode is suited to small scale deployments that can benefit from easy integration of wireless services into an existing network infrastructure.

Autonomous APs do not provide the benefits of centralized management and monitoring.

An autonomous AP can be used to create a wireless extension to an existing network and provide intelligent data-forwarding that maintains the security of the network. For example:



In this scenario an AP is installed on an existing corporate network to provide wireless networking services for employees. Since the AP functions as a DHCP client and all its ports are bridged, it simply creates a wireless extension to the existing network.

Security for the wireless network is provided using 802.1X. The AP uses the existing RADIUS server on the corporate network to validate employee logins.

If you deploy more than one AP, the APs can be:

- Interconnected using a backbone LAN.
- Linked with other APs through a local mesh link.

Summary

The operational differences between the two modes are summarized in the following table.

Feature/function	Controlled mode AP	Autonomous mode AP
Reset AP to factory default settings	AP remains in controlled mode.	AP changes from autonomous to controlled mode.
Network connection (Ethernet)	Supported on Port 1 only.	Supported on Port 1 and Port 2 (if available).
Centralized configuration/ software management	Fully automated using the management tool on a controller. Allows APs to be configured individually or in groups.	New configuration/software can be downloaded from a central location at a preset day and time.
Configuration changes	Performed using the management tool on a controller. Multiple APs can be updated at the same time.	Performed locally using each the management tool on each AP.
Remote configuration and management	Automatic establishment of a secure tunnel to protect management and control traffic.	Via secure HTTPS browser session.
Local mesh groups (wireless links)	Dynamic links.	Dynamic and static links.
Wireless mobility support using Mobility Traffic Manager	Supported (with the appropriate license).	Not supported.
Centralized access control	Supported.	Not supported.
LLDP	Supported.	Supported.
sFlow sflow	Supported.	Not supported.
STP	Disabled by default.	Enabled by default.

Safety information

Warning

Professional Installation Required

Prior to installing or using an AP, 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.

Surge protection and grounding: If you plan on connecting an outdoor antenna to the AP, make sure that proper lightning surge protection and grounding precautions are taken according to local electrical code. Failure to do so may result in personal injury, fire, equipment damage, or a voided warranty. The HP hardware warranty provides no protection against damage caused by static discharge or a lightning strike.

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 AP 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 AP and all interconnected 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 MSM APs. 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 AP management tool **Login** page.
Network topology map, including the addresses assigned to all relevant devices.	Your network administrator.

Getting started

Get started with your AP by following the directions in the relevant Quickstart or section of the MSM3xx / MSM4xx APs Installation and Getting Started Guide. Then:

- If operating in autonomous mode, continue with the next chapter in this guide.
- If operating in controlled mode, see *Working with controlled APs* in the *MSM7xx Controllers Management and Configuration Guide*.

Online documentation

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

2

Management

Contents

Management tool

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

The computer used to connect to the management tool must:

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

Starting the management tool

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

`https://AP_IP_address`

Factory default APs use address 192.168.1.1.

About passwords

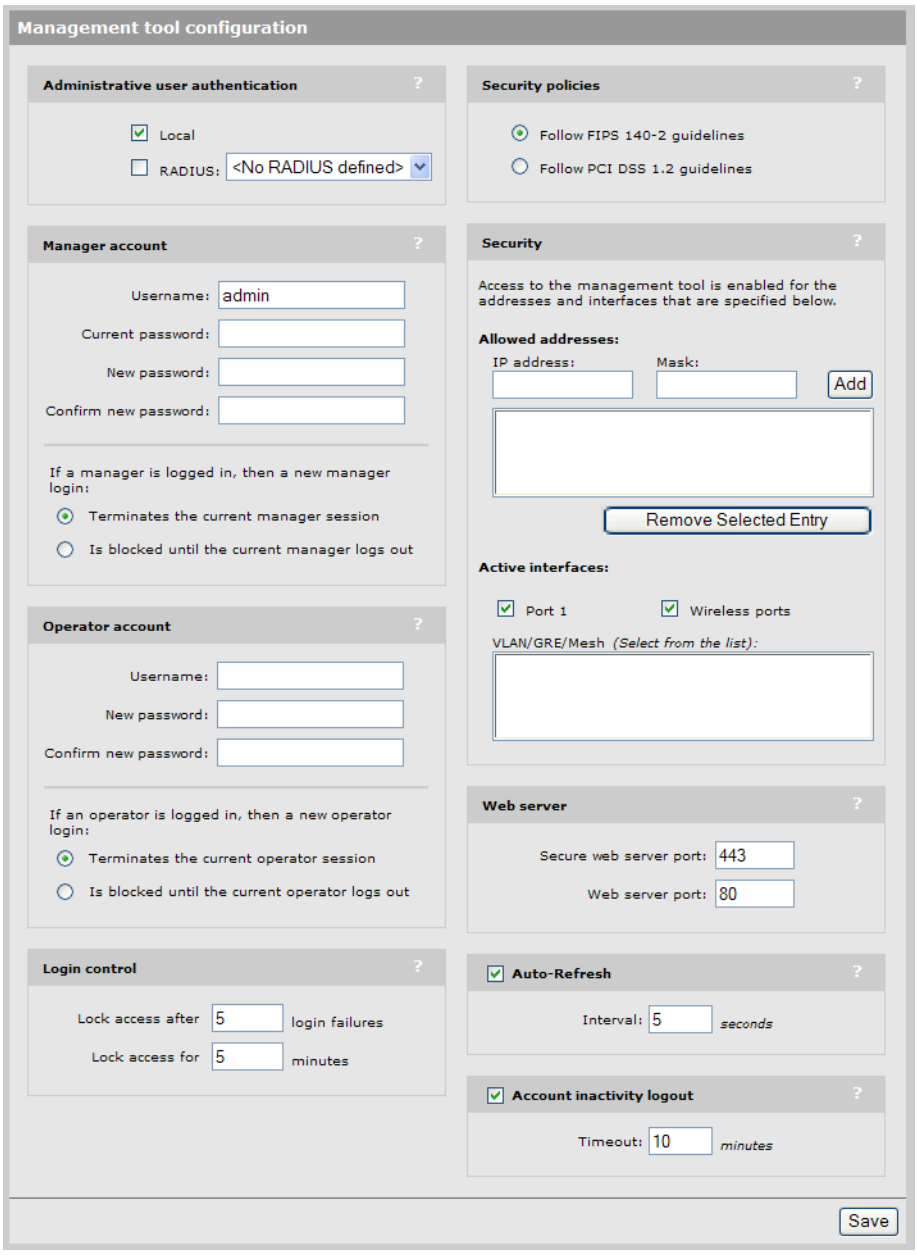
The default username and password is **admin**. New passwords must be 6 to 16 printable ASCII characters in length with at least 4 different characters. Passwords are case sensitive. Space characters and double quotes (") cannot be used. Passwords must also conform to the selected security policy as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

For information on starting the management tool for the first time, see the relevant document as described in *Getting started on page 1-11*.

A security certificate warning is displayed the first time that you connect to the management tool. This is normal. Select whatever option is needed in your Web browser to continue to the management tool. The default certificate provided with the AP 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 6-17*.

Customizing management tool settings

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



Administrative user authentication

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

- **Local account settings:** A single manager and operator account can be configured locally under **Manager account** and **Operator account** on this page.

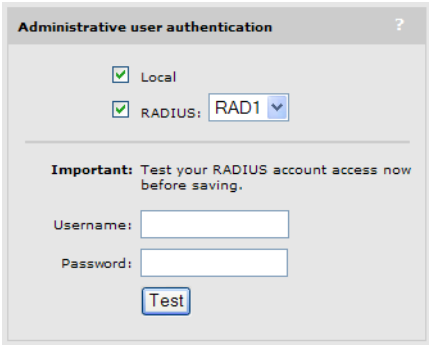
- **RADIUS server:** Using a RADIUS server enables you to have multiple accounts, each with a unique login name and password. Identify accounts using the vendor specific attribute **web-administrative-role**. See *Configuring administrative accounts on a RADIUS server on page 6-11*. To use a RADIUS server, you must define a RADIUS profile on the **Authentication > RADIUS profiles** page.

If both options are enabled, the local account is always checked first.

Authenticating administrative credentials using an external RADIUS server

Configure RADIUS authentication as follows:

1. Define an account for the manager or operator on the RADIUS server. Specify the appropriate value for the vendor specific attribute **web-administrative-role.** See *Configuring administrative accounts on a RADIUS server on page 6-11***.**
2. On the AP, create a RADIUS profile that will connect the AP to the RADIUS server. See *Configuring a RADIUS client profile on the AP on page 6-2*.
3. Under **Administrative user authentication**, enable RADIUS and select the RADIUS profile you created. In this example, the profile is called **RAD1**.



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.

Caution

If you forget the manager password, the only way to access the management tool is to reset the AP to factory default settings. See *Resetting to factory defaults on page D-1*.

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.

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:
  - Passwords must be at least six characters long.
  - 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:
  - Passwords must be at least seven characters long.
  - 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.

Security

The management tool is protected by the following security features:

- **Allowed IP address:** 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:
  - Port 1
  - Port 2 (on products that have a second Ethernet port)
  - Wireless port
  - VPN
  - VLAN/GRE/Mesh

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

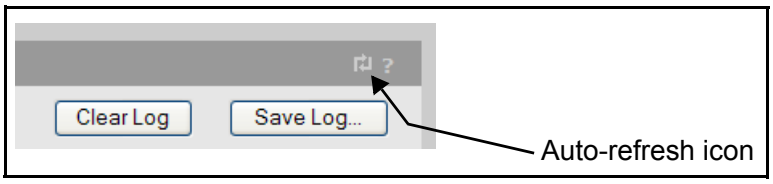
Web server

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 AP 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 6-17*.
- **Web server port**: Specify a port number for the AP 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 AP 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.



Web inactivity logout

When this option is enabled, a manager will automatically be logged out if their session is idle for the specified number of minutes.

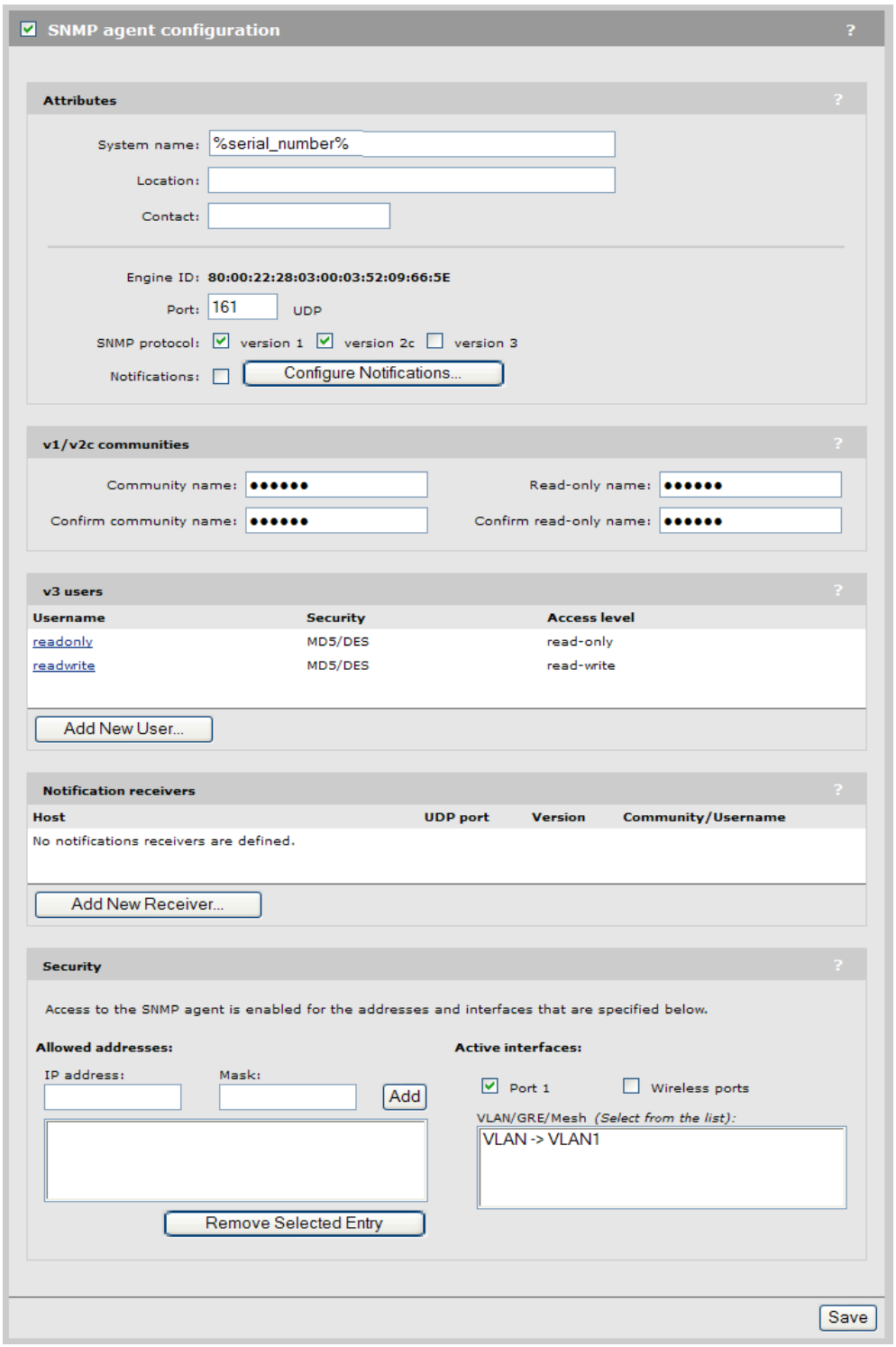
SNMP

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

The AP supports SNMP v1/v2c/v3 and both MIB II and HP-specific MIB attributes via the HP Enterprise MIB.

Configuring SNMP settings

Select **Management > SNMP** to open the **SNMP agent configuration** page. By default, the SNMP agent is enabled (**SNMP agent configuration** in title bar is checked). If you disable the agent, the AP will not respond to SNMP requests.



Attributes

System name
Specify a name to identify the AP. By default, this is set to the placeholder **%serial number%**, which is automatically replaced with the serial number of the AP.

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

Contact
Contact information for the AP.

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

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

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

The AP supports the following MIB II notifications:

- coldStart
- linkUp
- linkDown
- authenticationFailure

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

v1/v2c 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 AP. By default, this is set to **private**.

Read-only name
This is the password that controls read-only access to SNMP agent. A network management program must supply this name when attempting to get SNMP information from the AP. 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 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 AP will send notifications.

UDP port
The port on which the AP 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.

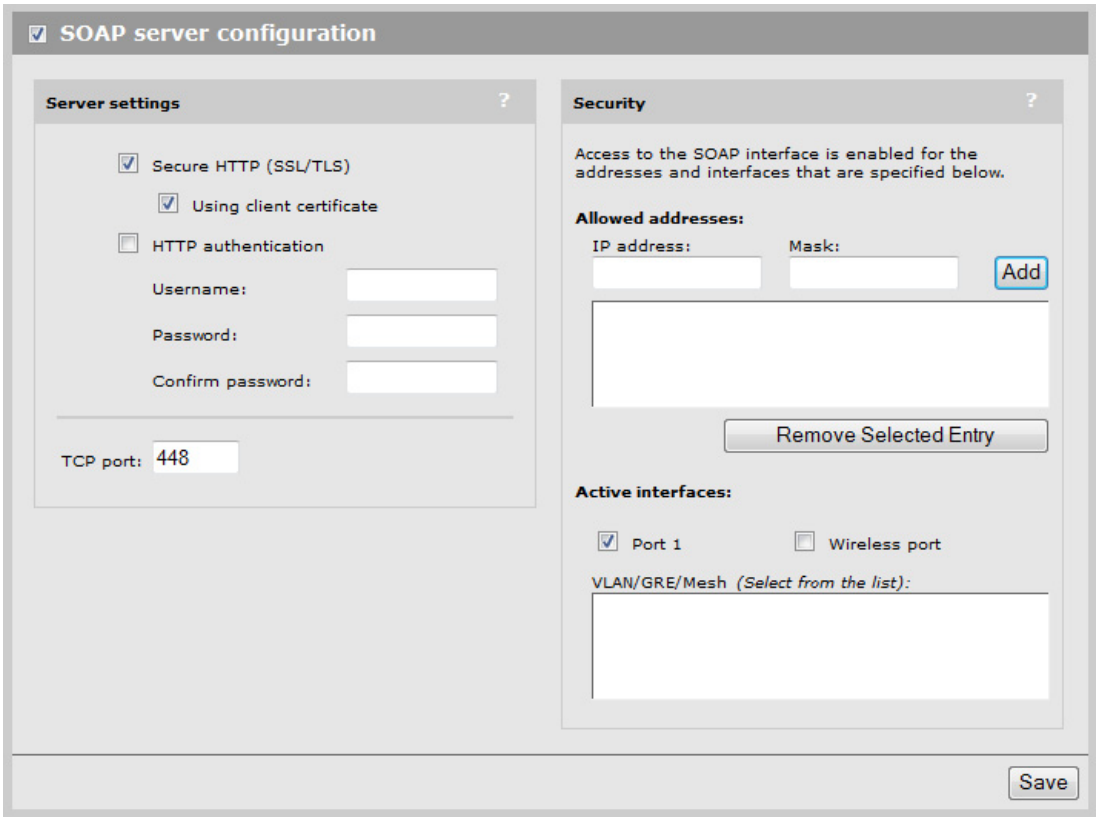
SOAP

The AP 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 **Management > SOAP** to open the **SOAP server configuration** page. By default, the SOAP server is enabled.



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 a 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 a X.509 client certificate is mandatory for SOAP clients.
- The SOAP server is configured to trust all client certificates signed by the default Colubris SOAP CA installed on the AP.
- 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 *Managing certificates on page 6-12*.)

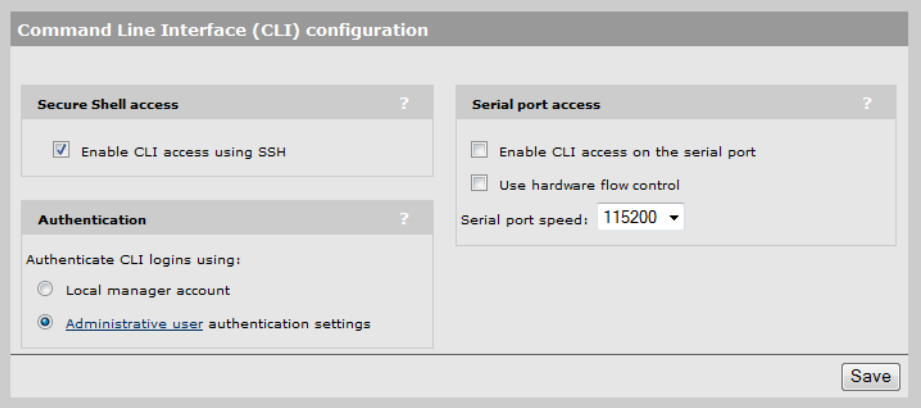
CLI

The AP provides a command line interface (CLI) that can be used to perform configuration and management tasks via the serial port or an IP connection on any of the AP interfaces.

A maximum of three concurrent CLI sessions are supported regardless of the connection type. For information on using the CLI, see the *CLI Reference Guide*.

Configuring CLI support

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



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

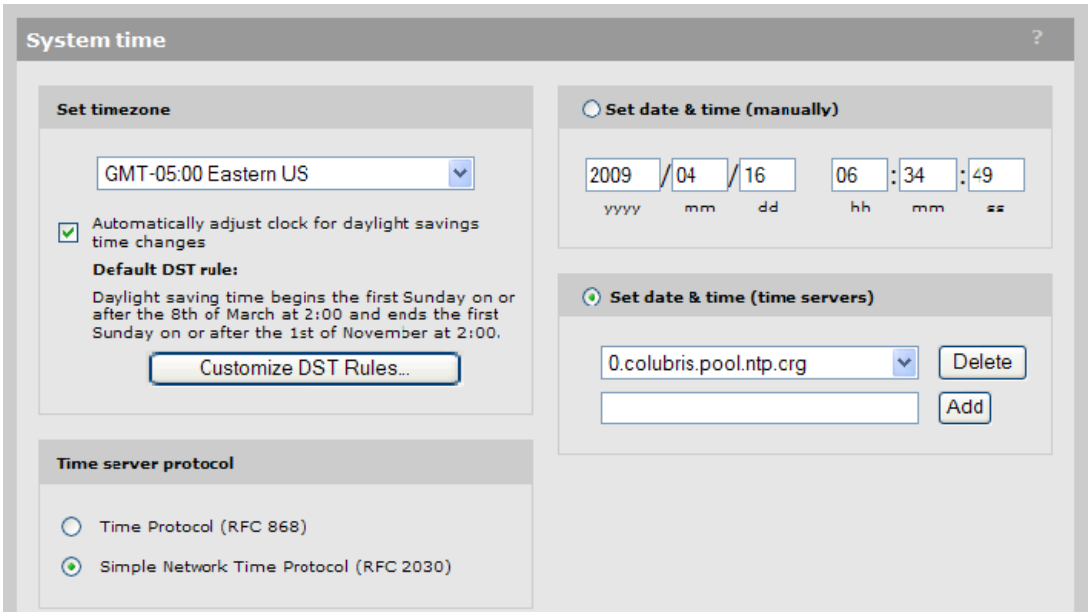
The login username and password use the same settings (**Local** and/or **RADIUS**) as defined for the manager account under **Administrative user authentication**.

Serial port access

On APs with serial (console) ports, you can opt to provide CLI access via the serial port. You can also use hardware flow control and set the speed for CLI access via the serial port.

System time

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



1. Set **timezone & DST** as appropriate.
2. Set **Time server protocol**, to **Simple Network Time Protocol**.
3. Select **Set date & time (time servers)** and then select the desired time server. **Add** other servers if desired. The AP contacts the first server in the list. If the server does not reply, the AP tries the next server and so on.

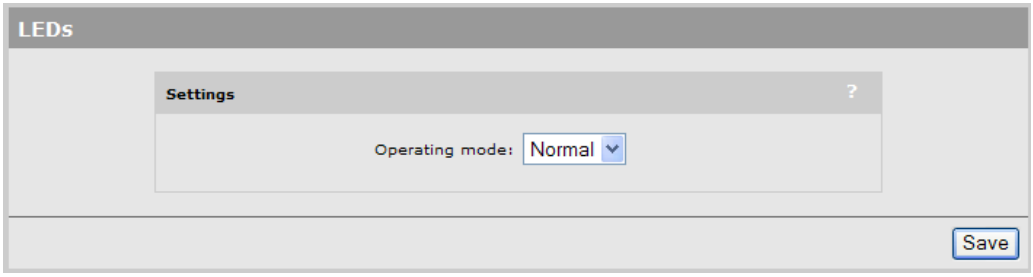
4. Select **Set date & time (time servers)** and then select the desired time server. **Add** other servers if desired. The AP contacts the first server in the list. If the server does not reply, the AP tries the next server and so on. By default, the list contains two ntp vendor zone pools that are reserved for HP networking devices. By using these pools, you will get better service and keep from overloading the standard ntp.org server. For more information visit: www.pool.ntp.org.
5. Select **Save** and verify that the date and time is updated accurately. A working Internet connection on Port 1 is required.

Note

If access to the Internet is not available to the AP, you can temporarily set the time manually with the **Set date & time (manually)** option. However, It is important to configure a reliable time server on the AP. Correct time is particularly important when a service controller is used. Synchronization and certificate problems can occur if the time is not accurate.

LEDs

Select **Management > LEDs** to control operation of the status lights on the AP after the AP has successfully started up and become fully operational.



Until fully operational, status lights follow their normal behavior. This allows potential error conditions to be diagnosed.

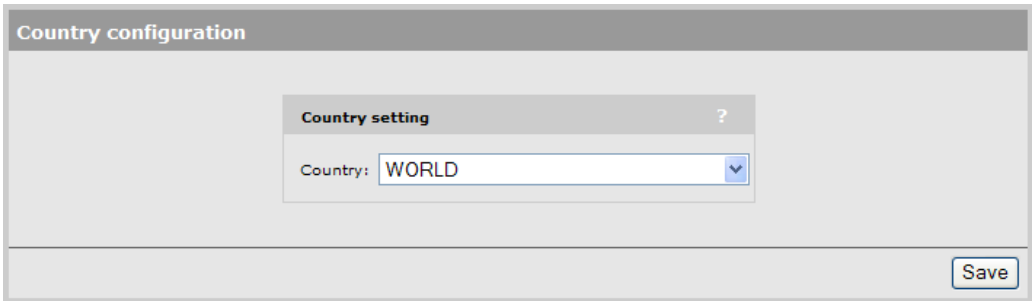
The following settings are available:

- **Normal**: All status lights on the AP operate normally.
- **Quiet**: All status lights on the AP are turned off once the AP is fully operational.
- **Awake**: The power light flashes once per minute once the AP is fully operational.

Country

Select **Management > Country** to open the **Country** page. This page enables you to configure the country in which the controller operates.

Note The Country page is not available on APs delivered with a fixed country setting.



Set the country in which the AP will operate. This enables the AP to properly customize the list of operating frequencies (channels) that you can configure on the **Wireless > Radio(s)** page. Only frequencies that conform to the regulations in your area will be available.

Caution Incorrectly entering the country code 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.

3

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 3-32*) 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 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 3-8*. To set the regulatory domain, see *Country on page 2-16*.

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 3-31*.

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 3-8*.

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

- Select **Wireless > Neighborhood** to view detailed information about all wireless APs operating in the immediate area so that you can effectively set the operating frequencies This wireless neighborhood feature also makes it easy for you to find rogue APs. See *Wireless neighborhood on page 3-32*.

- Select **Status > Wireless** to view detailed information about packets sent and received, transmission errors, and other low-level events.
- Select **Status > Client data rate matrix** 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 4-9*.

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

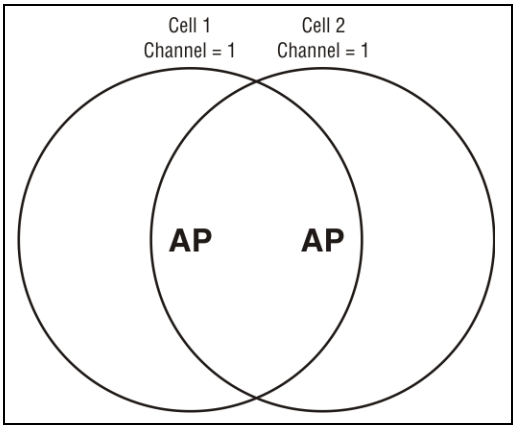
Overlapping wireless cells occur when two or more APs are operating within transmission range of each other. This may be under your control, (for example, when you use several cells to cover a large location), or out of your control (for example, when your neighbors set up their own wireless networks). 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 **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 **Wireless > 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 by selecting **Management > Country.** This means that the number of non-overlapping channels available to you varies by geographical location.

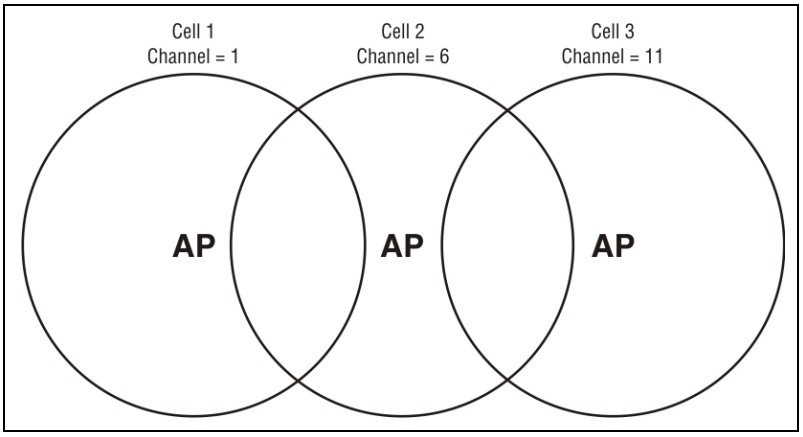
The following table shows the number of channels that are available in North America, Japan, and Europe.

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).

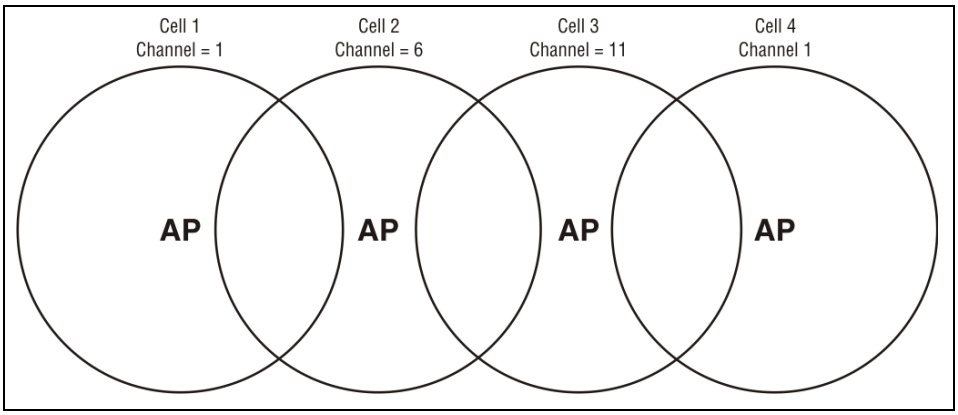
North America	Japan	Europe
■ cell 1 on channel 1	■ cell 1 on channel 1	■ cell 1 on channel 1
■ cell 2 on channel 6	■ cell 2 on channel 7	■ cell 2 on channel 7
■ cell 3 on channel 11	■ cell 3 on channel 14	■ cell 3 on channel 13

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



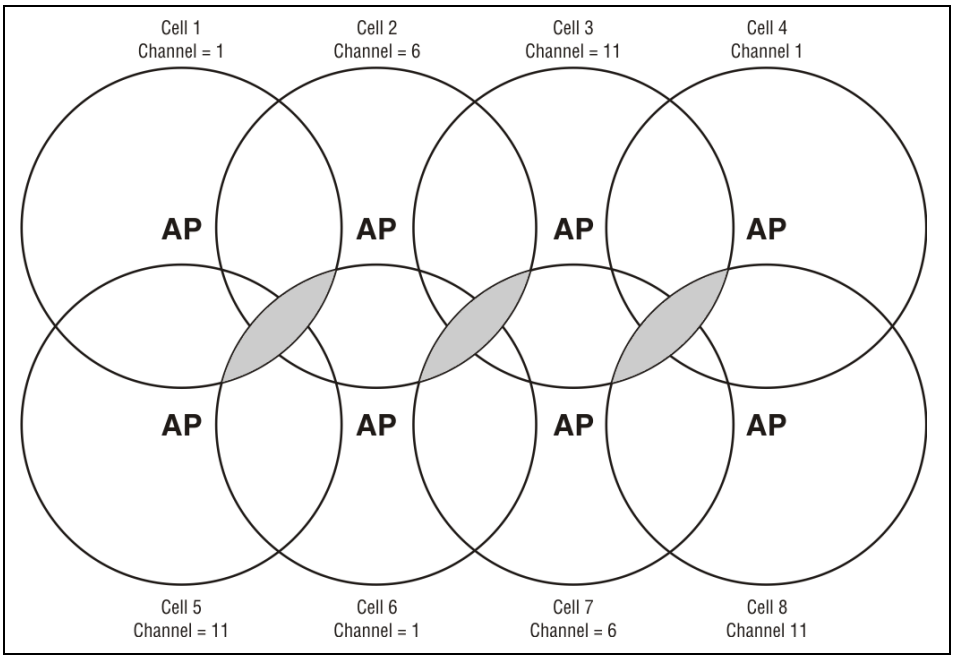
Reducing transmission delays by using different operating frequencies in North America.

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 **Wireless > Radio(s)** 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 APs. For information see *Transmit power control on page 3-31*.

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 3-29*) to allow network administrators greater flexibility over their deployments.

Note

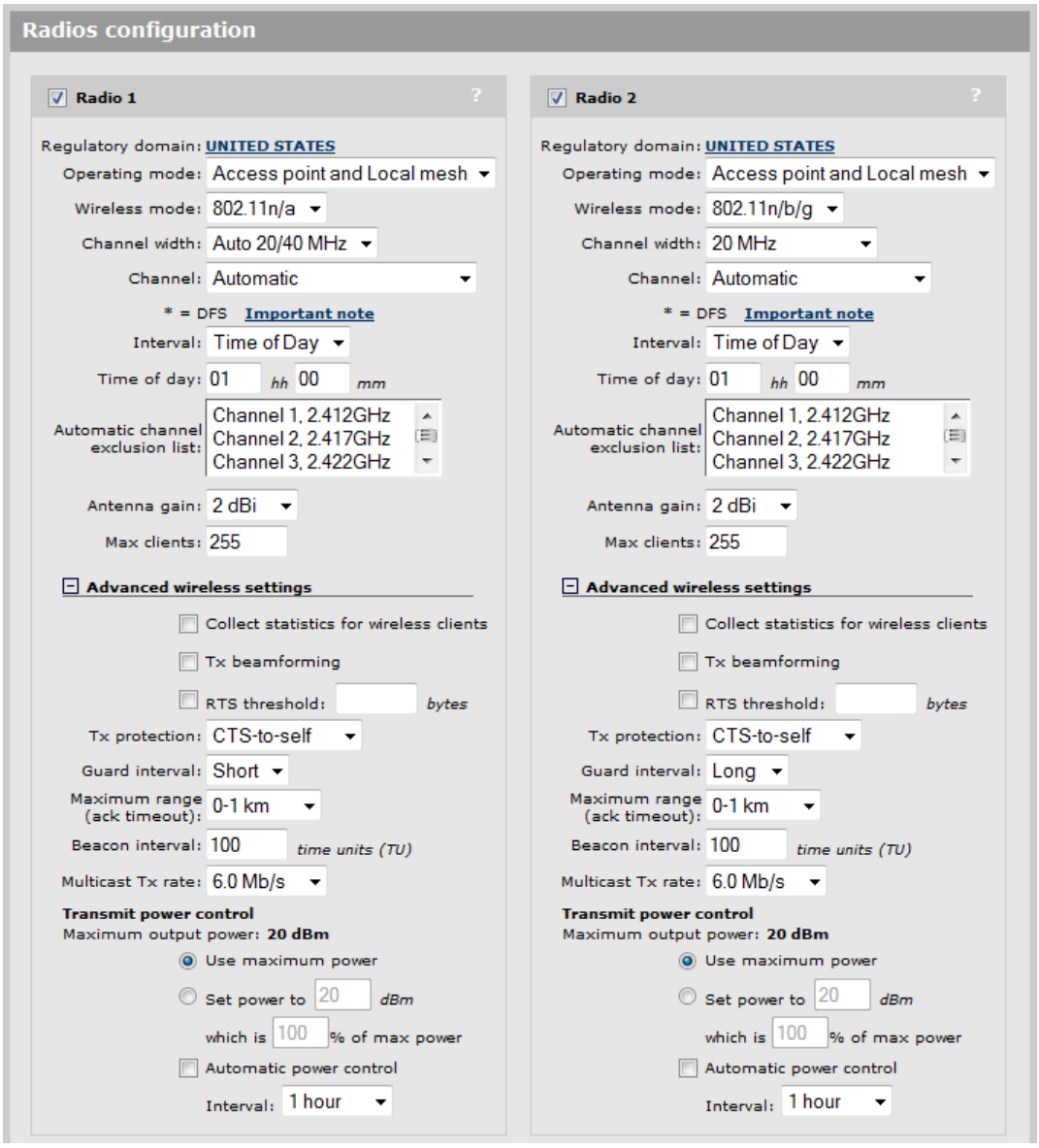
802.11n clients can only achieve maximum throughput when legacy clients are not present on the same radio.

Radio configuration

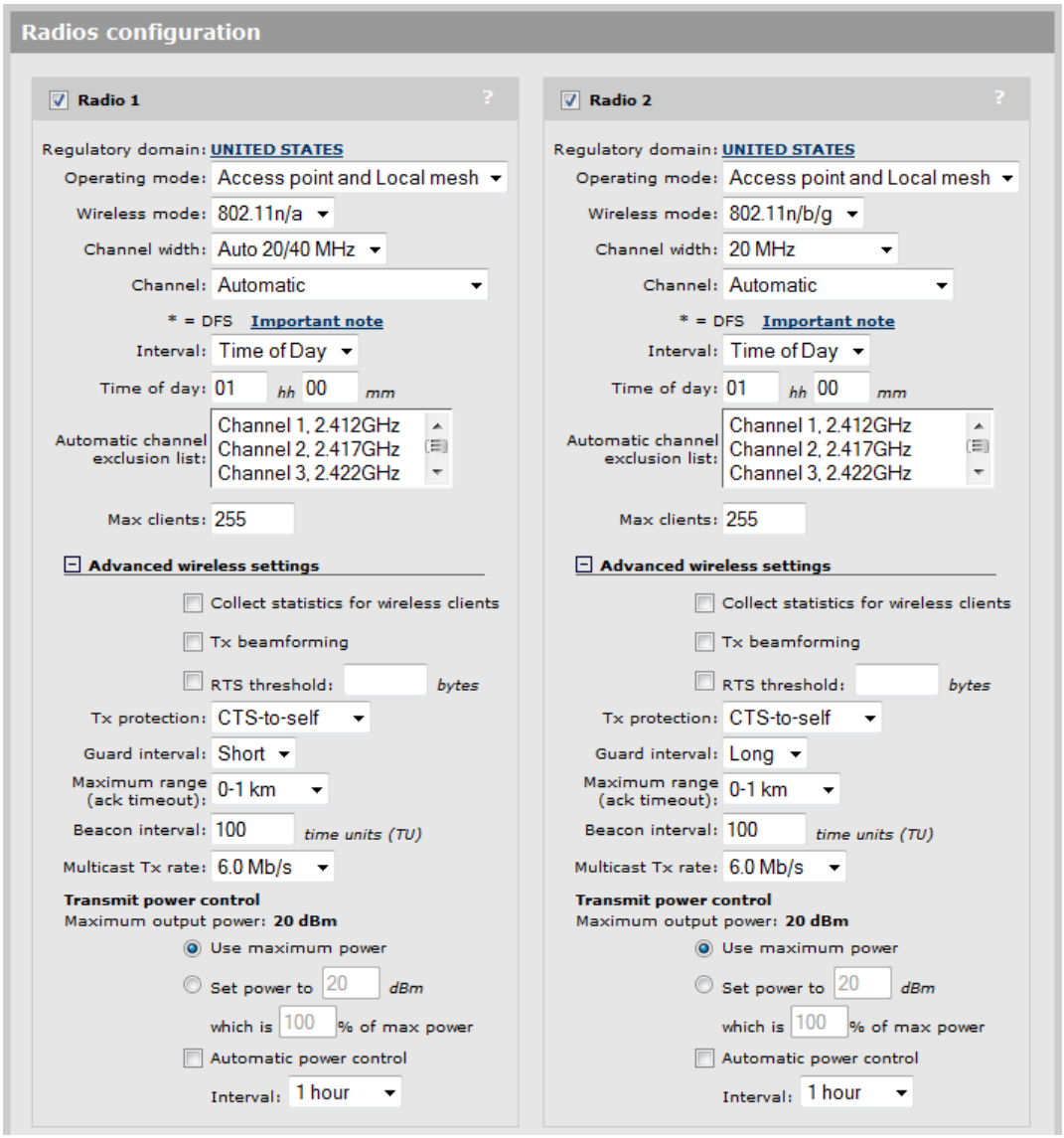
To define configuration settings for a radio, select **Wireless > Radio(s)**. This opens the Radio(s) configuration page. The contents of this page will vary depending on the product. The following screen shots show the Radio(s) configuration page for each AP type.

(For all screen shots: **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.)

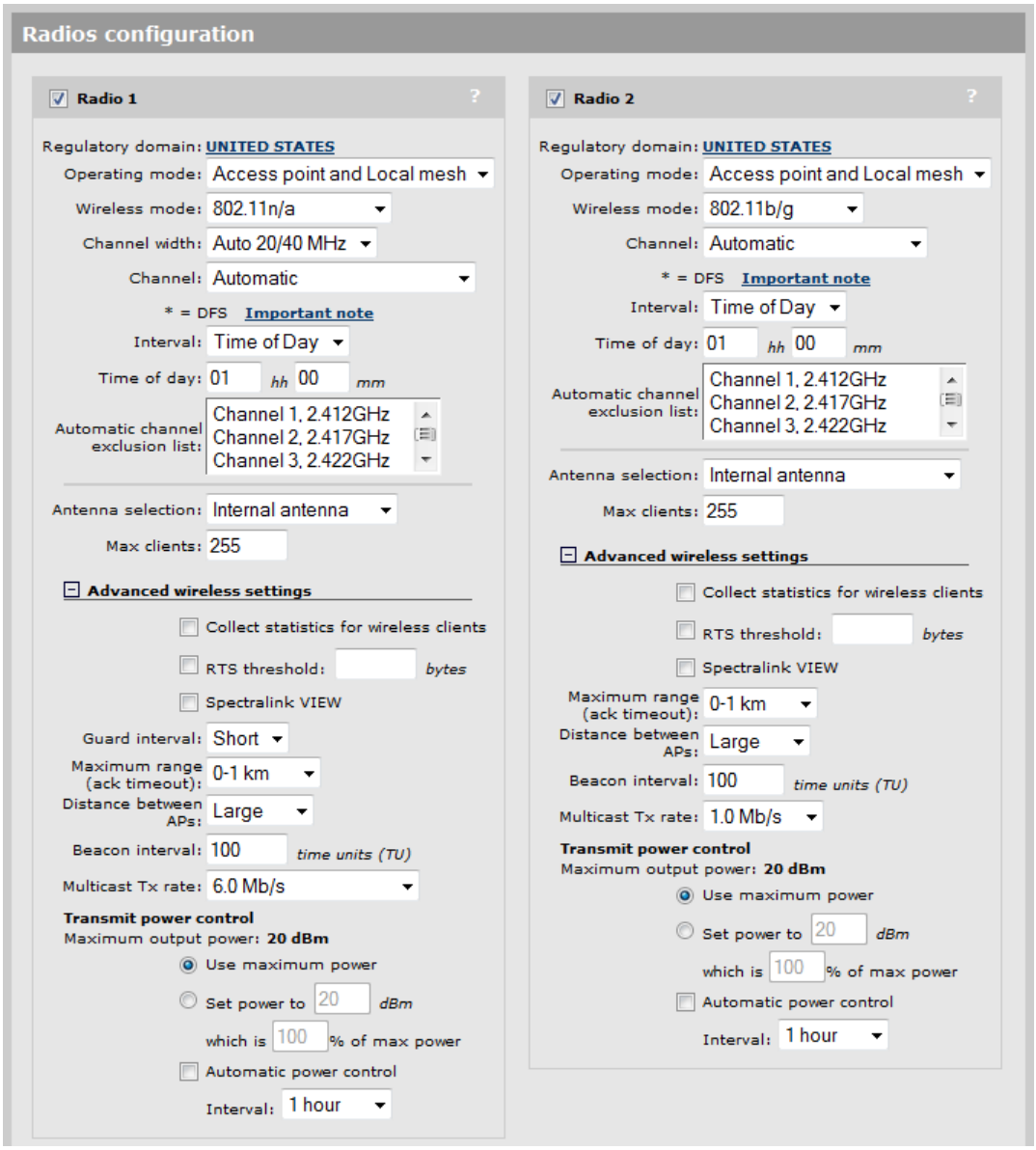
E-MSM466



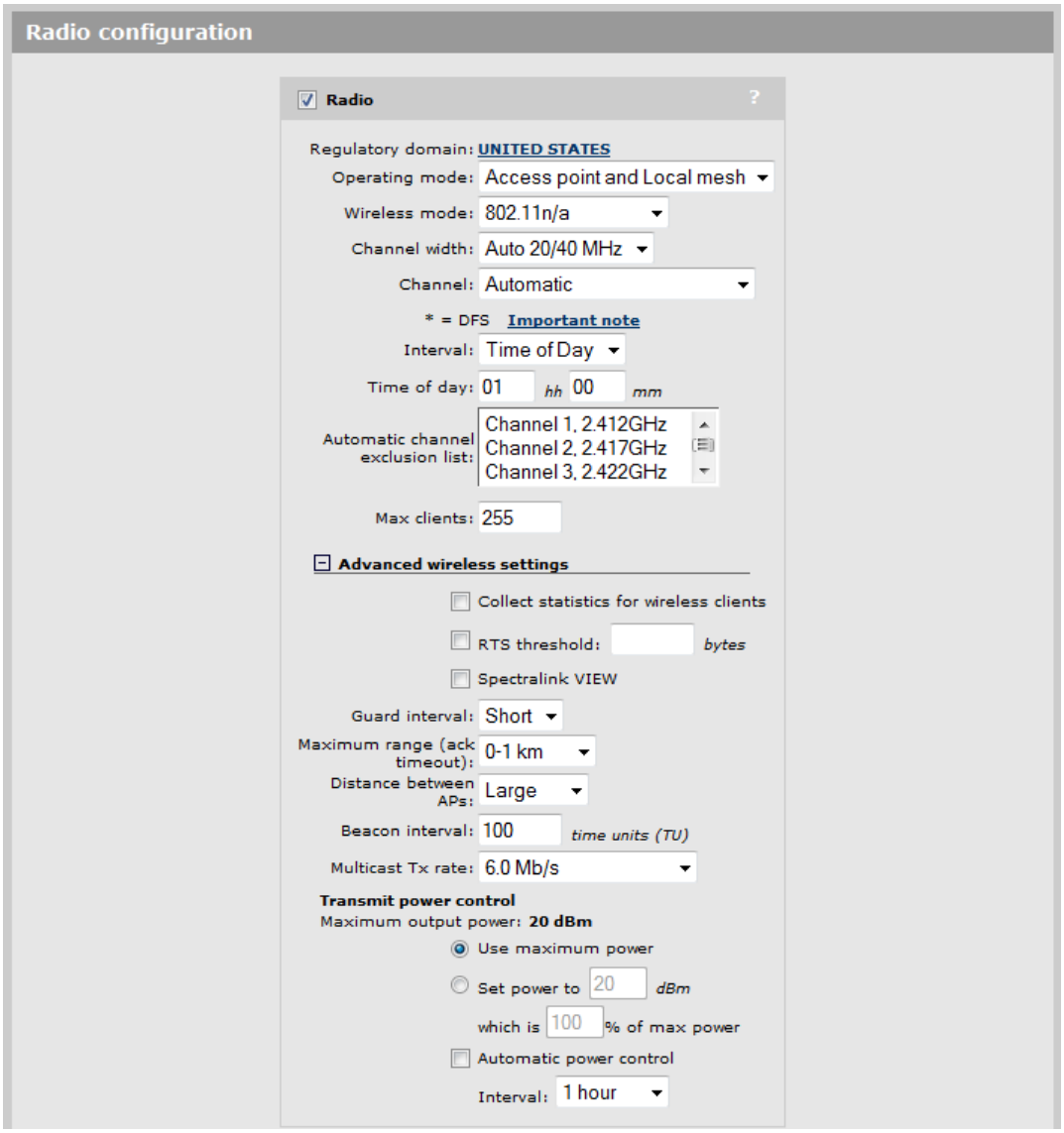
E-MSM460 and E-MSM430



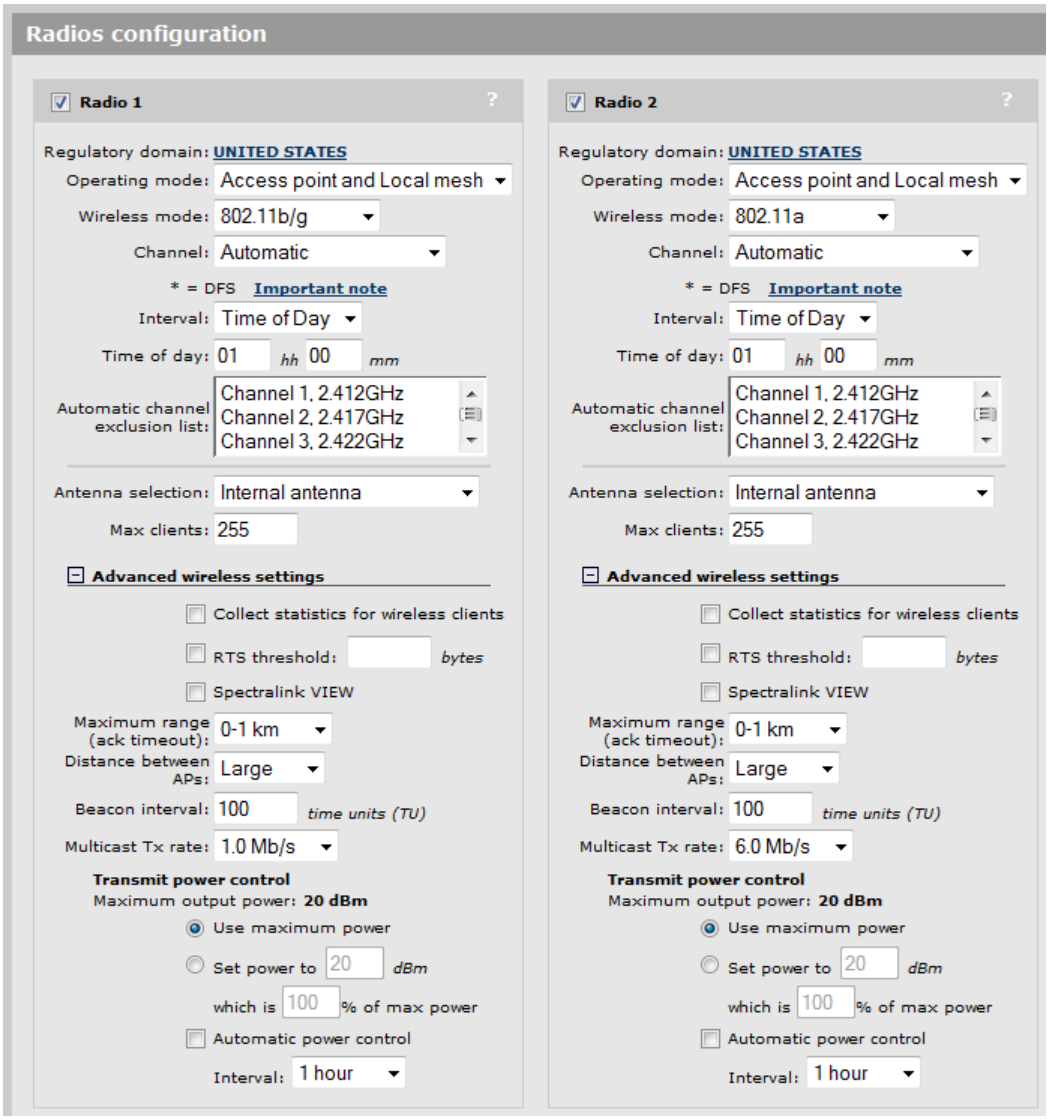
MSM422


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

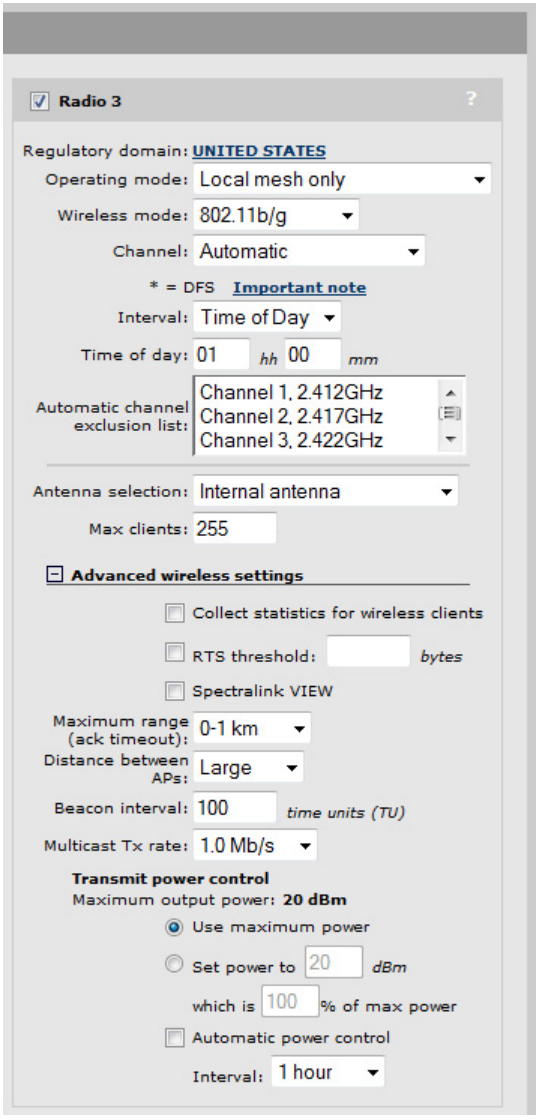
MSM410


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

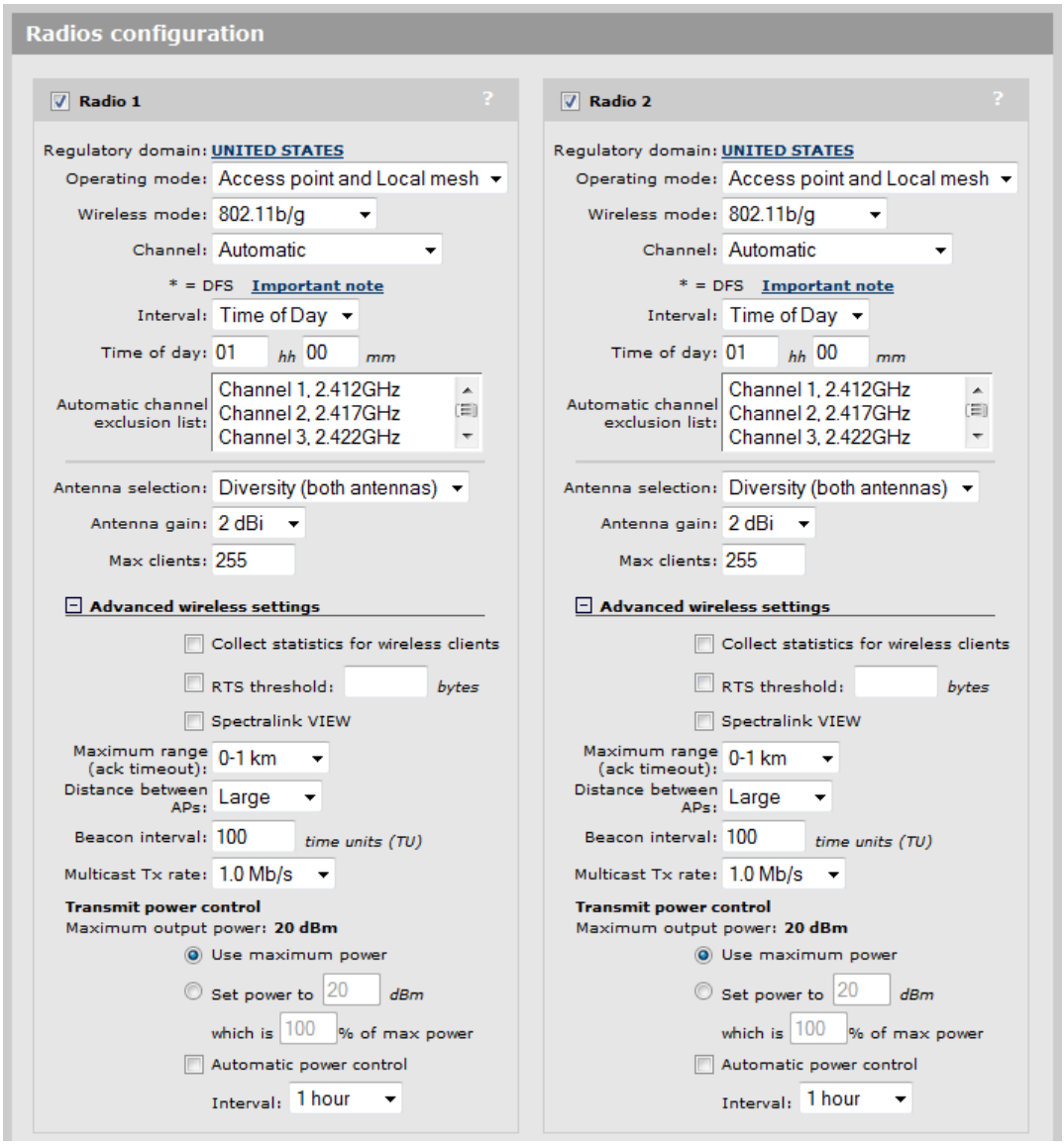
MSM335 (radio 1 and 2)



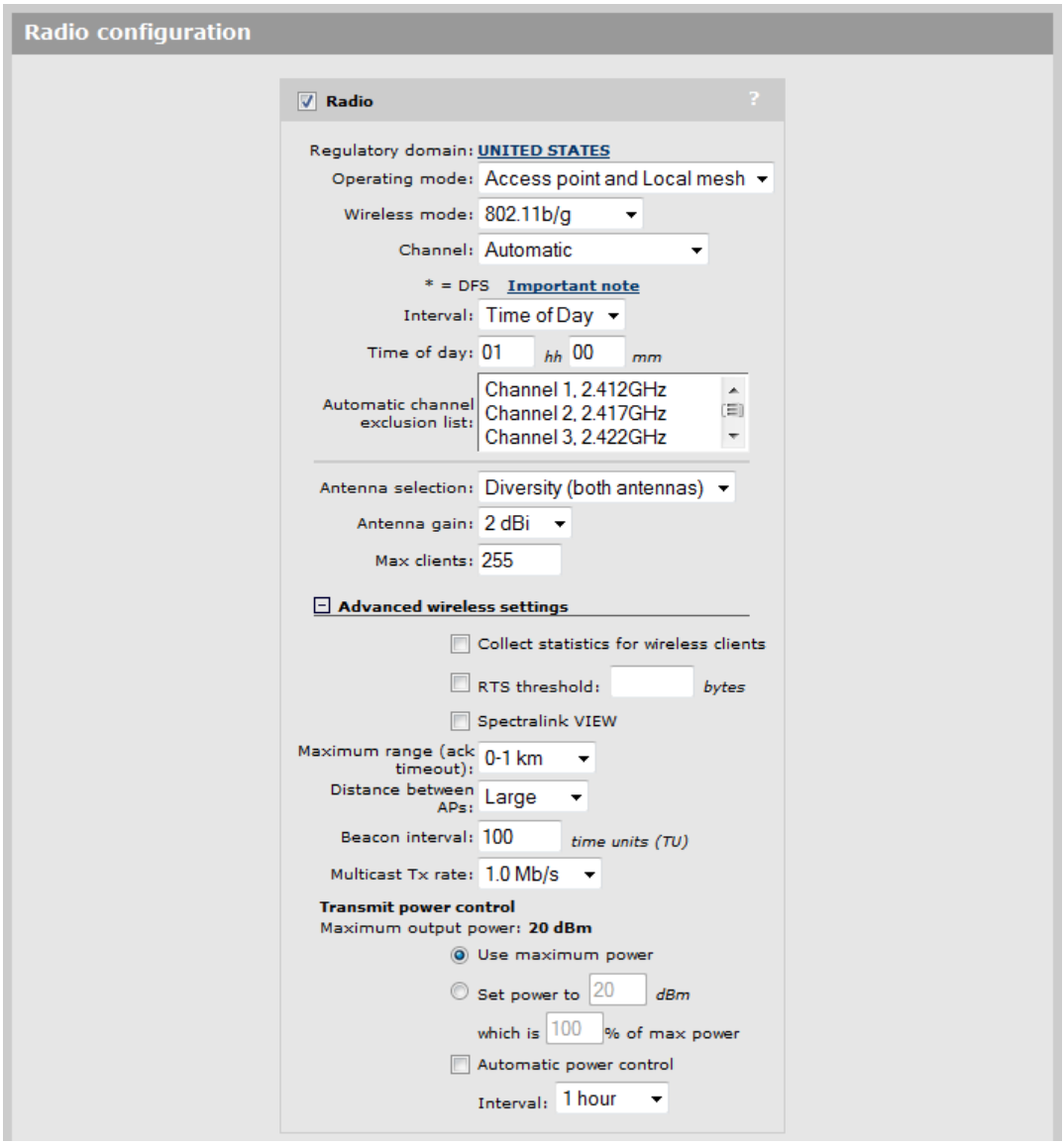
MSM335 (radio 3)



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

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 *Country on page 2-16*.

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 **Wireless > Neighborhood**. This mode also enables 802.11 traffic to be traced using the **Tools > Network trace** feature.
- **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 8-5*.

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	✔	✔	✔	✔	✔
MSM335 (Radio 1 + 2)	✔	✔	✔	✔	✔
MSM335 (Radio 3)	×	×	✔	✔	✔
MSM410	✔	✔	✔	✔	×
MSM422	✔	✔	✔	✔	×

Product	Access point and Local mesh	Access point only	Local mesh only	Monitor	Sensor
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 *Country on page 2-16*.

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, MSM320, MSM335, MSM410, MSM422

These products support the following wireless modes.

802.11n (5 GHz)

Supported on	MSM410, MSM422 (radio 1)
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	MSM410, MSM422 (radio 1)
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, 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, 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, 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, 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, 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 thoughput 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 3-31*.

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 3-32* 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 3-4*.

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. 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 *Appendix C: Connecting external antennas*.

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 3-31*.
- 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 MIB:

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 **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 from the AP 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 from the AP are protected by first sending a Request To Send (RTS) frame to the intended recipient and then waiting for a Clear to Send (CTS) frame to be sent back. 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 data may 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**
> 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.
>
> For a list of supported antennas, see the *Accessories* section for your AP at www.hp.com/networking/support (for **Product Brand**, select **ProCurve)**. For specific power limits according to your regulatory domain, consult the *Antenna Power-Level Settings Guide* also available at the same address.
>
> 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

You can use the wireless neighborhood feature to conduct a site survey to discover the operating frequencies of other APs in your area for site planning purposes.

It can also be used to flag discovered APs as either *authorized APs* or *rogue APs*. This is useful for monitoring the installation of wireless access points in your company's work areas to ensure that new APs (which could be a security risk if improperly configured) are not deployed without your knowledge.

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.

Background scanning

(MSM310, MSM320, MSM335, MSM410, MSM422 only)

For any other radio configuration, scanning is controlled by the settings on the **Network > Wireless neighborhood** page. To enable scanning, select the **Repeat scanning every xx seconds** checkbox and set a value. Scanning is performed for all the channels in the currently selected radio **Operating mode**. One channel is scanned during each scan interval. By default, the scan interval is set to 600 seconds. This is done to minimize the impact on radio throughput.

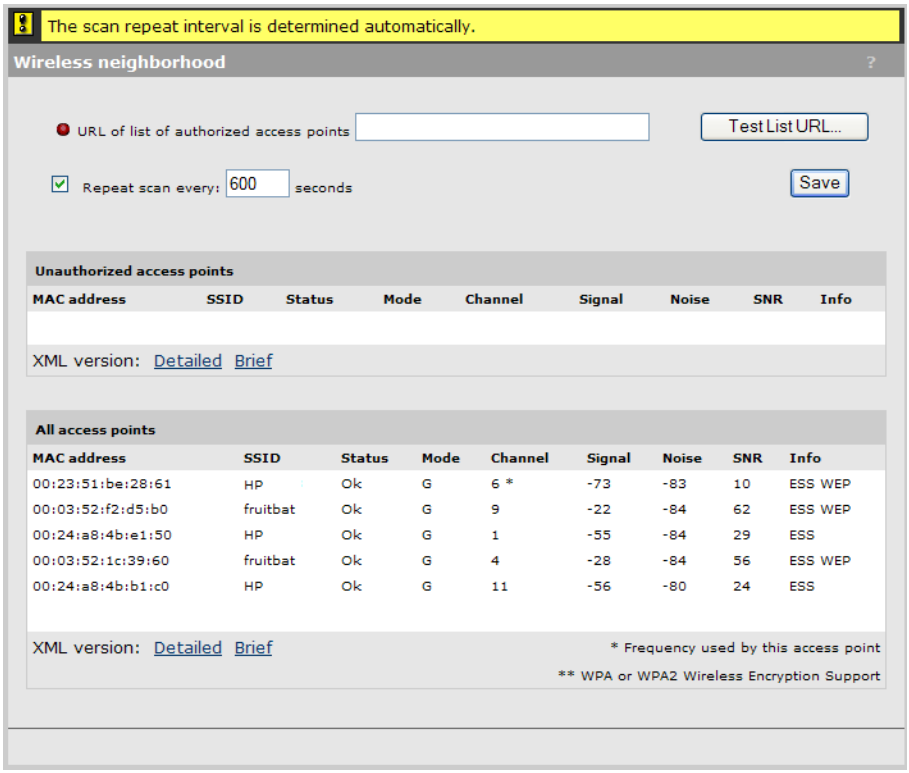
Use this method to continuously view APs operating in your area while minimizing the effect on throughput.

Note

- Scanning is temporarily disabled when a trace is active (**Tools > Network trace** page).
- To obtain the best possible wireless performance (such as needed for voice applications), scanning should be disabled.

Viewing scan results

To view the results of the latest scan, open the **Wireless > Neighborhood** page. For example:



To update scanning results, select the refresh button in your browser.

Identifying unauthorized APs

When an AP is discovered during a scan, its MAC address is compared against the list of authorized APs (which you must define). If the scanned AP does not appear in the list of authorized APs, it is displayed in the Unauthorized access points list.

Creating the list of authorized APs

The list of authorized APs must be defined in an external file in XML format. Each entry in the file comprises two items: MAC address and SSID. Each entry should appear on a new line. The easiest way to create this file is to wait for a scan to complete, then open the list of all APs in **Brief** format. Edit this list so that it contains only authorized APs and save it. Then specify the address of this file under **List of authorized access points.**

You must edit the **Brief** list file to remove extra text that appears before and after each MAC address. For example, if the brief list appears as follows:

```
<?xml version='1.0'?> <simple-ap-list> # MAC SSID 00:03:52:07:f5:11
"AP_1"
00:03:52:07:f5:23 "AP_2"
00:03:52:07:f5:12 "AP_3"
</simple-ap-list>
```

Reformat the list to appear as follows:

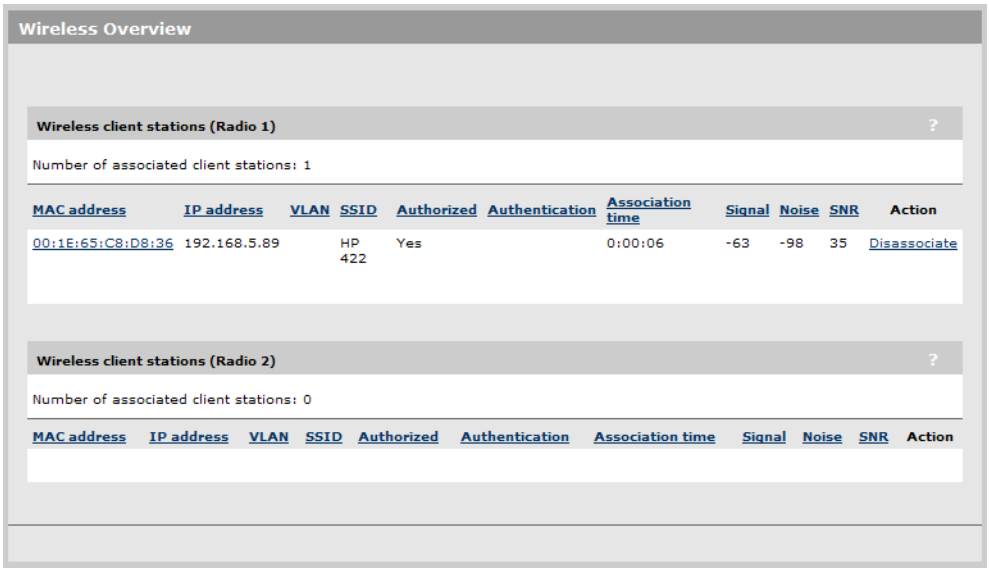
```
00:03:52:07:f5:11 "AP_1"
00:03:52:07:f5:23 "AP_2"
00:03:52:07:f5:12 "AP_3"
```

Viewing wireless information

The AP provides several pages where you can view information related to wireless operations.

Viewing all wireless clients

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



This page lists all wireless clients associated with all VSCs.

MAC Address

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

IP address

IP address assigned to the client station.

VLAN

VLAN assigned to the client station.

SSID

SSID to which the client station is associated.

Authorized

- Yes: Client station has the right to transmit/receive traffic.
- No: Indicates that the client station can only transmit/receive 802.1X packets.
- Filtered: Indicates that traffic is blocked by a MAC filter.

Authentication

Indicates how the station was authenticated 802.1X and/or MAC. If a station successfully authenticates with both 802.1X and MAC, only the 802.1X indication is shown.

Association time

Indicates how long the client station has been associated with the AP.

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.

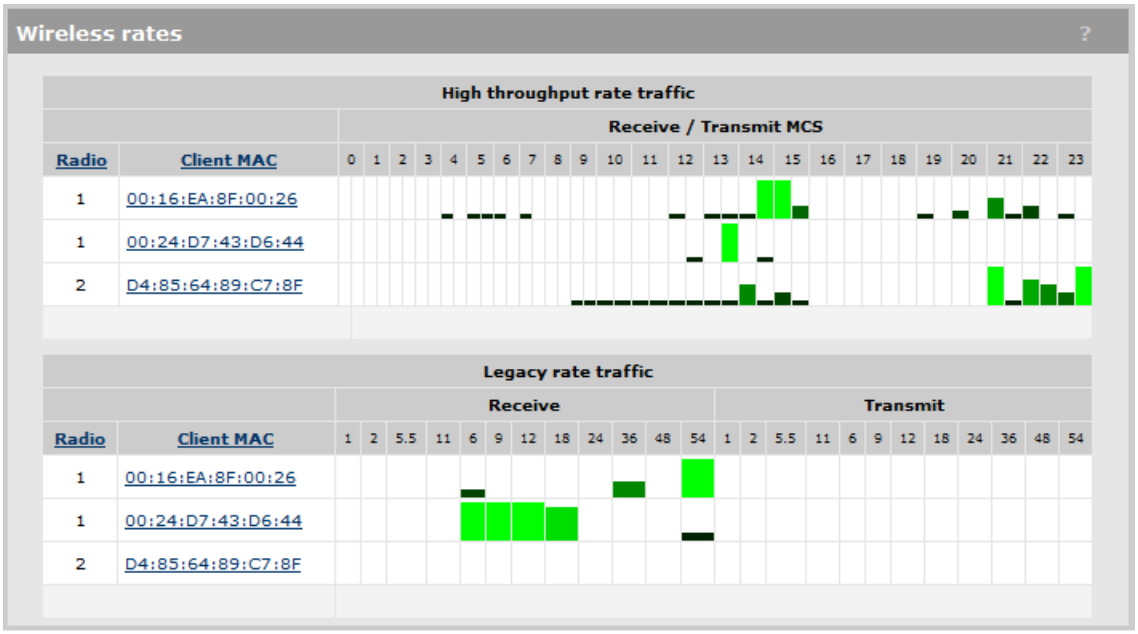
In most environments, SNR is a good indicator for the quality of the radio link between the client stations and the AP. A higher SNR value means a better quality radio link.

Action

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

Viewing wireless client data rates

To view information on the data rates used by all wireless client stations currently connected to the AP, select **Status > Client data rate matrix**.



High throughput (HT) rate traffic

Displays information for users connected via any 802.11n mode. Rates are shown for each supported MCS (modulation coding scheme). The size of the bar indicates the amount of traffic sent or received at each MCS.

MCS	Data rates in Mbps			
	Channel width / Guard interval			
	20 MHz/ 800 ns	20 MHz/ 400 ns	40 MHz/ 800 ns	40 MHz/ 400 ns
0	6.50	7.20	13.50	15.00
1	13.00	14.4	47.00	30.00
2	19.50	21.70	40.50	45.00
3	26.00	28.90	54.00	60.00
4	39.00	43.30	81.00	90.00
5	52.00	57.80	108.00	120.00
6	58.50	65.00	121.50	135.00
7	65.00	72.20	135.00	150.00
8	13.00	14.40	27.00	30.00

MCS	Data rates in Mbps			
	Channel width / Guard interval			
	20 MHz/ 800 ns	20 MHz/ 400 ns	40 MHz/ 800 ns	40 MHz/ 400 ns
9	26.00	28.90	54.00	60.00
10	39.00	43.30	81.00	90.00
11	52.00	57.80	108.00	120.00
12	78.00	86.70	162.00	180.00
13	104.00	115.6	216.00	240.00
14	117.00	130.00	243.00	270.00
15	130.00	144.40	270.00	300.00
16	130.00	144.40	270.00	300.00
17	130.00	144.40	270.00	300.00
18	130.00	144.40	270.00	300.00
19	130.00	144.40	270.00	300.00
20	130.00	144.40	270.00	300.00
21	130.00	144.40	270.00	300.00
22	130.00	144.40	270.00	300.00
23	195.00	216.60	405.00	600.00

- MHz = megahertz
- ns = nanoseconds
- Supported rates vary depending on the wireless operating mode.

Legacy rate traffic

Displays information for users connected via any 802.11 a/b/g mode. The size of the bar indicates the amount of traffic sent or received at each rate.

Wireless access points

To view wireless information for the AP, select **Status > Wireless**.

The information you see will vary depending on the AP. For example, this is the status page on an MSM422.

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

(Only on the E-MSM430, E-MSM460, E-MSM466)

- **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.

4

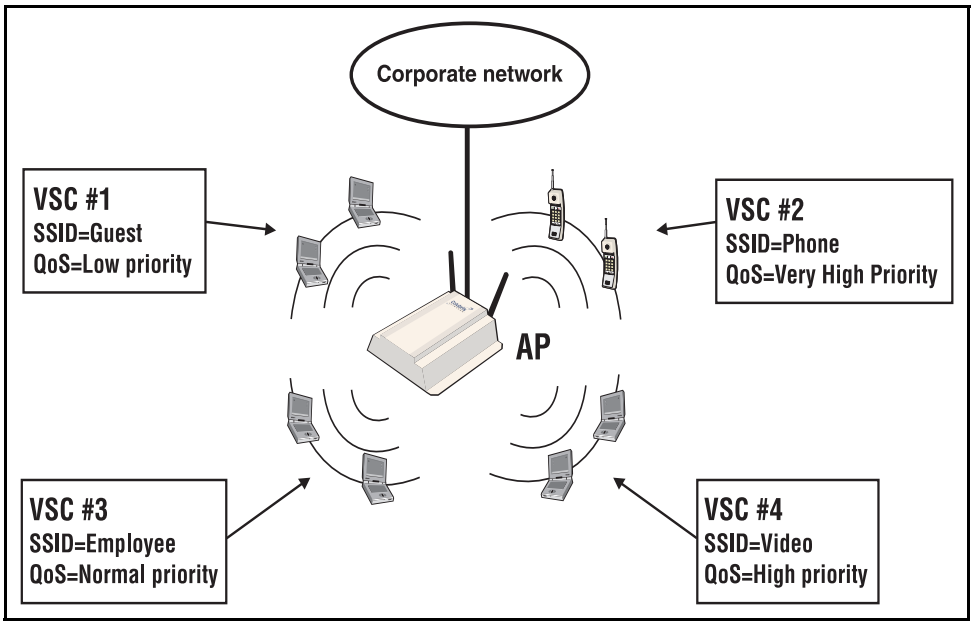
Working with VSCs

Contents

Key concepts

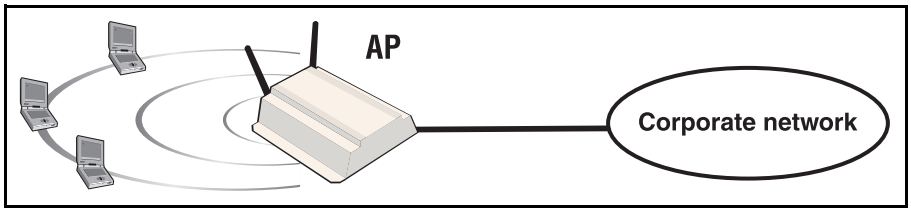
A VSC (virtual service community) is a collection of configuration settings that define key operating characteristics of an AP. In most cases, a VSC is used to define the characteristics of a wireless network.

Multiple VSC definitions can be created to enable support for different types of users. For example, in the following scenario, four VSCs are used. Each VSC is configured with a different wireless network name (SSID), and the quality of service (QoS) feature is used to set the priority of user traffic.



Stand-alone deployment

An autonomous AP can be deployed as a stand-alone device to provide wireless networking support for an existing wired network. The AP essentially creates a wireless extension to the existing wired network, bridging wireless users onto the wired backbone.



User authentication

The AP can validate user login credentials using a third-party RADIUS server. The following authentication types are supported: WPA / WPA2, 802.1X, and MAC.

WPA / WPA2 and 802.1X authentication

Full support is provided for users with WPA / WPA2 client software, and 802.1X client software that uses the following:

- EAP-TLS: Extensible Authentication Protocol Transport Layer Security.
- EAP-TTLS: Extensible Authentication Protocol Tunnelled Transport Layer Security.
- PEAP: Protected Extensible Authentication Protocol.

Note

For security reasons, use of 802.1X without enabling dynamic WEP encryption is not recommended.

MAC-based authentication

Devices can be authenticated based on their MAC address. This is useful for authenticating devices that do not have a web browser (cash registers, for example). As soon as the device MAC address appears on the network, the AP attempts to authenticate it.

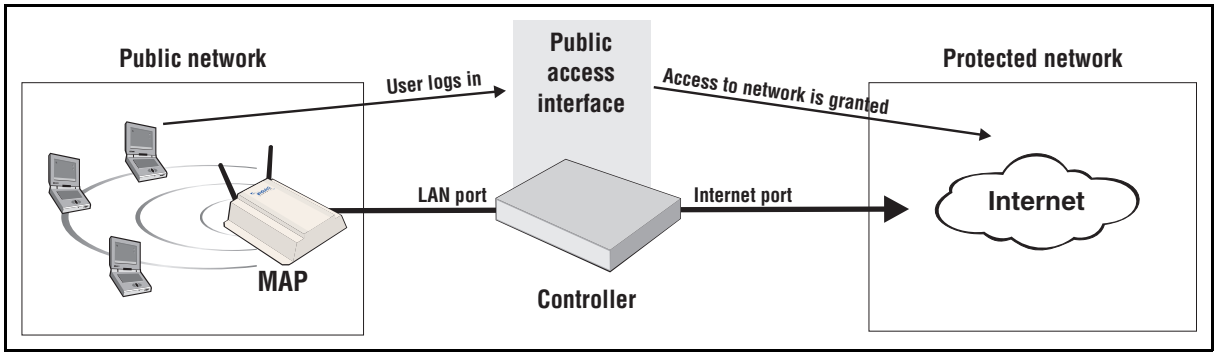
Using more than one authentication type in a VSC

For added flexibility, you can enable both the 802.1X and VSC-based MAC authentication at the same time. MAC authentication always takes place first. If it fails, 802.1X is then attempted.

Deployment with a controller

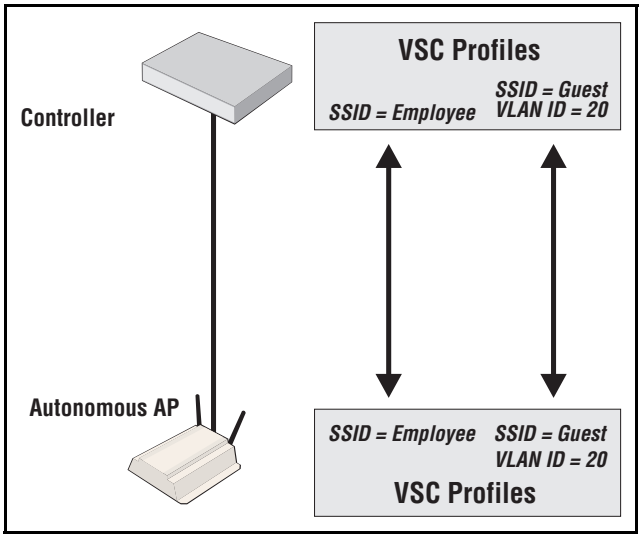
Autonomous APs can also be used with a controller to create a public access network infrastructure. In this type of deployment, all VSCs are access-controlled, which means that the AP forwards all wireless user traffic to the controller which handles user authentication and access control.

To reach protected network resources, wireless users must successfully authenticate with the public access interface that is provided by the controller.



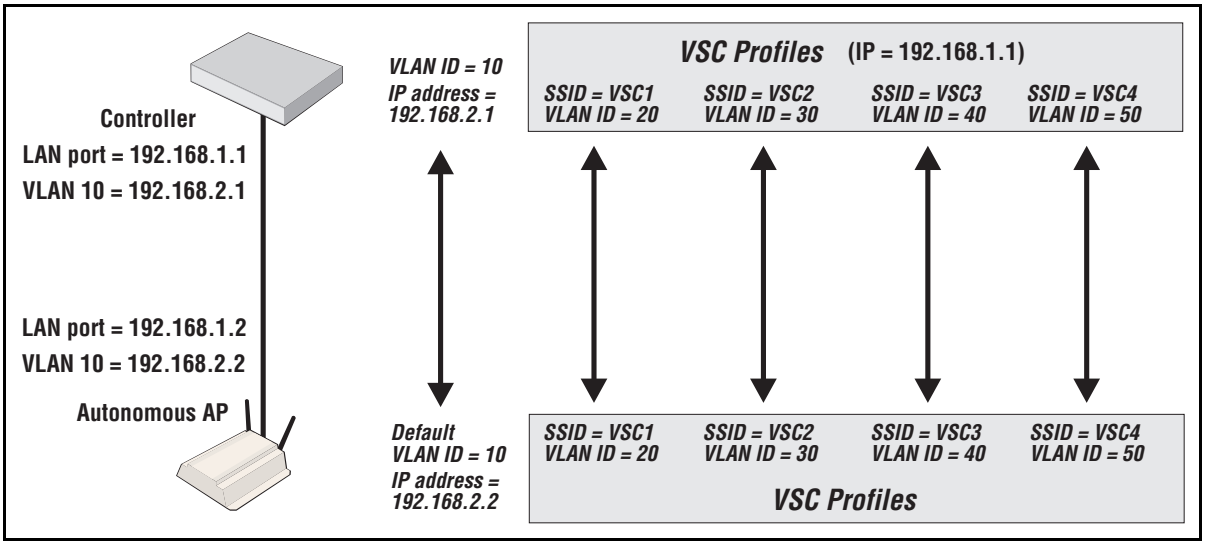
The following authentication types are supported on the controller: WPA / WPA2, 802.1X, MAC, HTML. For more information on controller authentication features, see the *MSM7xx Controllers Management and Configuration Guide*.

In this type of installation, VSC definitions on both the AP and controller must match so that traffic from wireless users connected to the AP can be sent to the controller for handling. For example, if two VSCs are being used, they could be configured as follows:



Management with VLANs

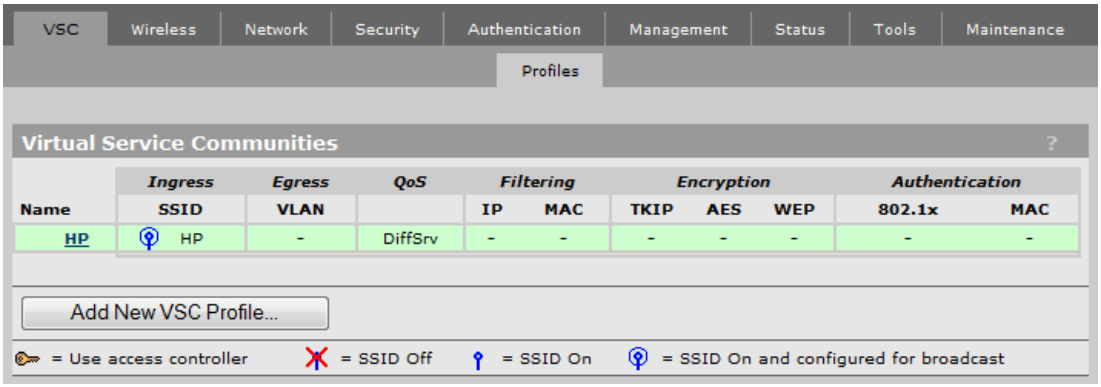
When operating in a VLAN environment, management traffic can be carried on its own VLAN. Configure the VSC on both the autonomous AP and the controller as illustrated.



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.

Viewing and editing VSC profiles

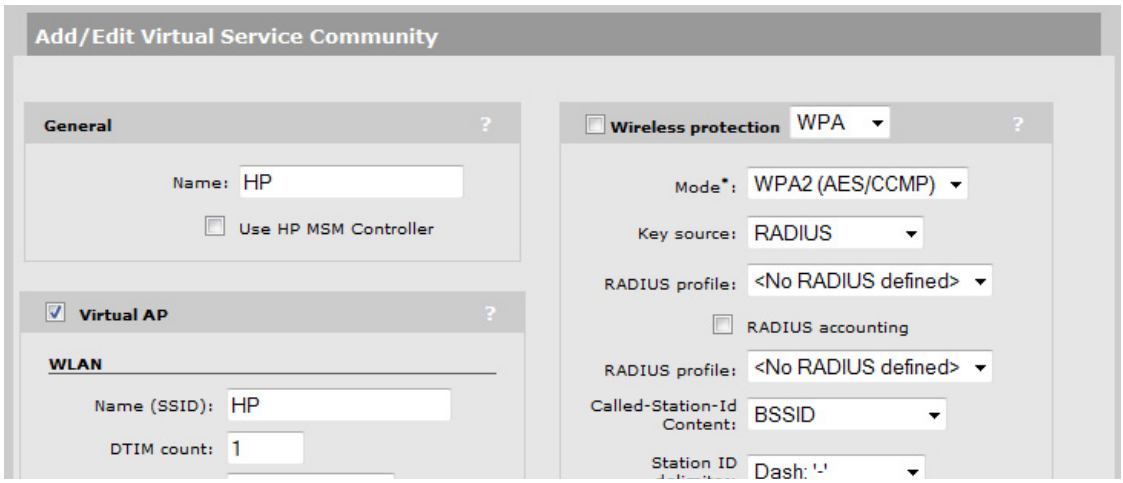
Select **VSC** on the main menu to open the VSC page. This page lists all defined VSC profiles and enables you to add new ones.



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

- To edit an existing profile, select its **Name**.
- To add a new profile, select **Add New VSC Profile**.

In either case, the **Add/Edit Virtual Service Community** page opens providing all VSC profile options.

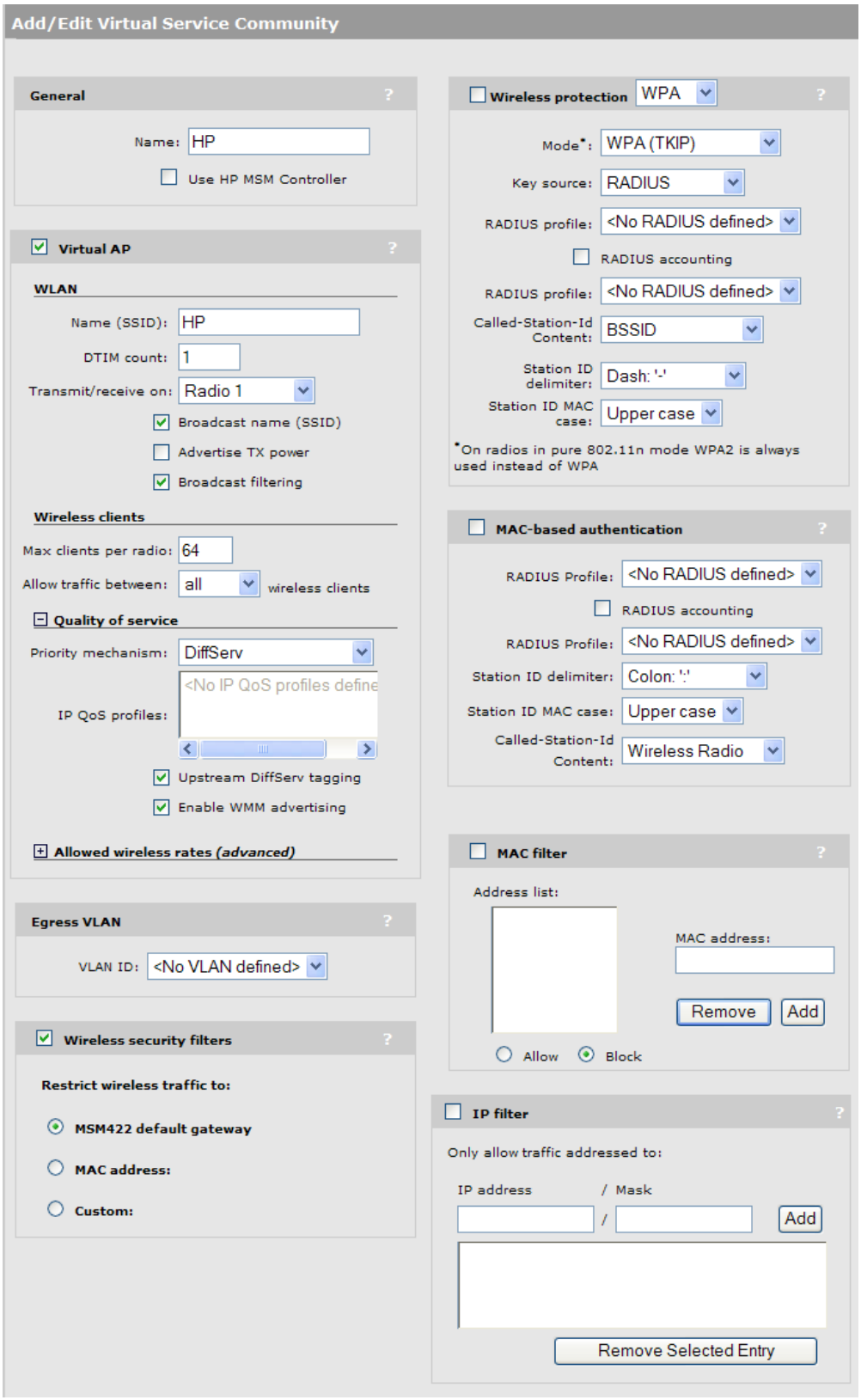


The following sections provide an overview of each VSC option and how it is used. For complete descriptions of individual parameters see the online help in the management tool.

VSC configuration options

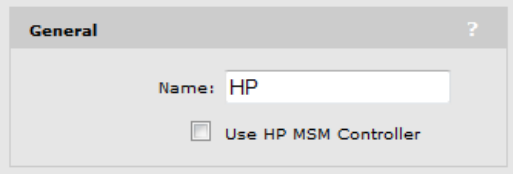
This section provides an overview of all the configuration options available for a VSC. It will give you a good idea on how the features can be used.

The following screen capture shows the configuration of the default VSC profile. The description that follow describe how to configure each parameter.



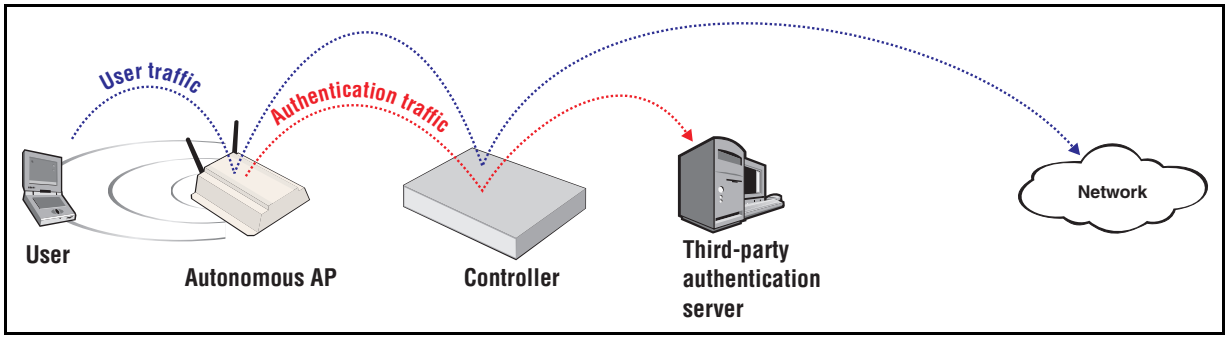
General

Availability of certain VSC features and their functionality are dependent on the setting of the **Use HP MSM Controller** in the **General** box. This option determines how authentication and access control are handled by the VSC.



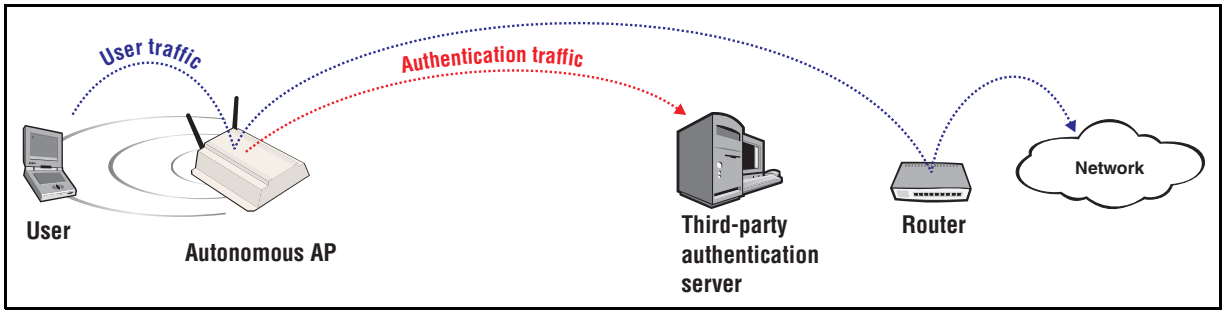
If *Use HP MSM Controller* option is enabled

This creates an **access-controlled VSC**, which means that the AP must be used in conjunction with a controller because the VSC is automatically configured to forward all user traffic to the controller for authentication (**Wireless protection** and **MAC-based authentication** options are forced to use the controller as the RADIUS server). Also, once authenticated, user traffic is restricted by the **Wireless security filters** option. Only traffic addressed to the controller is permitted. (These filters can be disabled if required.)



If *Use HP MSM Controller* option is disabled

This creates a **non-access-controlled VSC**, which allows the AP to operate independent of a controller and manage user authentication itself using the services of a third-party RADIUS server. Once authenticated, user traffic is restricted to the default gateway assigned to the AP by the **Wireless security filters** option. (These filters can be disabled or re-configured if required.)



Note: When access control is disabled, user traffic sent by the AP must bypass the controller, otherwise it will be interpreted and processed.

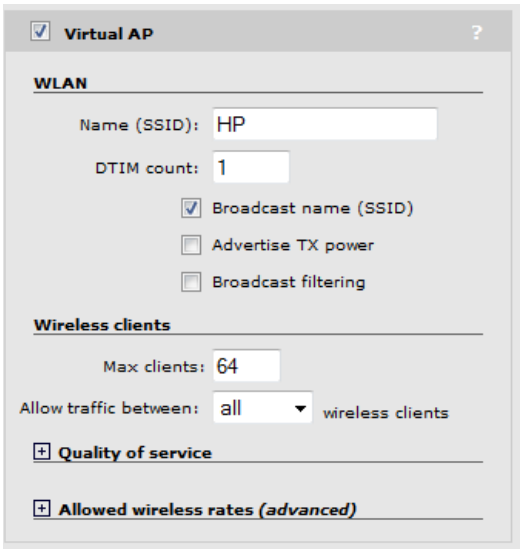
The following table shows how VSC configuration options are affected by setting the **Use HP MSM controller** option.

VSC option	The *Use HP MSM controller* option is ...	
	Enabled	**Disabled**
Virtual AP	Available.	Available.
Egress VLAN	Available.	Available.
Wireless security filters	Available, but wireless traffic is restricted to the controller.	Available, but wireless traffic is restricted to the default gateway. Can be changed.
Wireless protection	Available, but user authentication must be performed by the controller.	Available. User authentication can be performed by any external RADIUS server.
MAC-based authentication	Available, but user authentication must be performed by the controller.	Available. User authentication can be performed by any external RADIUS server.
Location-aware	Available.	Not available.
Wireless MAC filter	Available.	Available.
Wireless IP filter	Available.	Available.

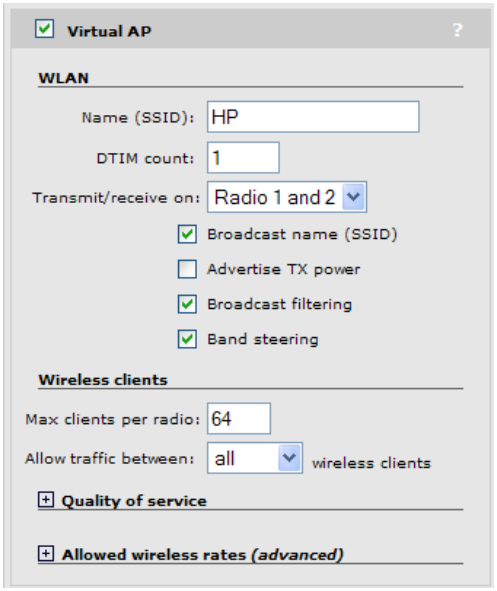
Virtual AP

These settings define the characteristics of the wireless network created by the VSC, including its name, the number of clients supported, and quality of service settings. This box is split into four sections: WLAN, Wireless clients, Quality of service, and Allowed wireless rates.

APs with a single radio

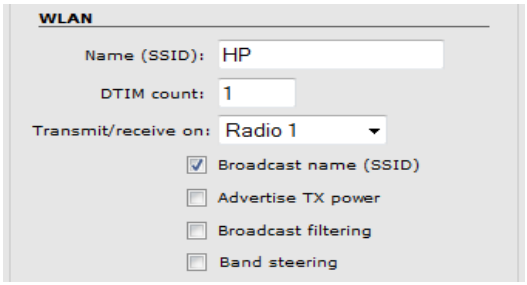


APs with dual radios



WLAN

Use these settings to define the characteristics of the wireless network.



Name (SSID)

Specify a name to uniquely identify the wireless network associated with this VSC. Each client computer that wants to connect to this VSC must use this name. The name is case-sensitive.

DTIM count

Defines the DTIM period in the beacon. Client stations use the DTIM to wake up from low-power mode to receive multicast traffic.

The device transmits 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.

Transmit/receive on

Select the radio on which this VSC will transmit and receive.

Broadcast name (SSID)

When enabled, the AP will broadcast its 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, the AP will broadcast its 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

Supported on: MSM422, E-MSM430, E-MSM460, E-MSM466

Band steering is used to help solve dense client issues. When band steering is enabled, the AP attempts 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.

The 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.

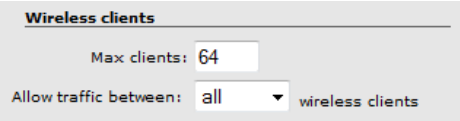
- Once a client is associated at 5 GHz, the AP will not respond to any 2.4 GHz probes from the client as long as the client's signal strength at 5 GHz is greater than -80 dBm (decibel milliwatt). If the client's signal strength falls below -80 dBm, then the AP will respond to 2.4 GHz probes from the client without delay.

Note

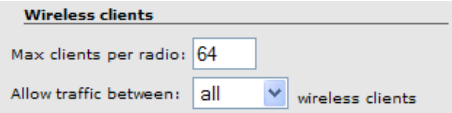
- To support band steering, one radio must be configured for 2.4 GHz operation and the other for 5 GHz operation.
- Band steering is temporarily suspended when the radio configured for 5 GHz operation reaches its maximum number of supported clients.

Wireless clients

APs with a single radio



APs with dual radios



Max 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 dual radio products the limit applies separately on each radio.

Allow traffic between wireless clients

Use this option to control how users that are connected to the same VSC can communicate with each other. The following settings are available:

- **No:** Blocks all user-to-user communication.
- **802.1X:** Only authenticated 802.1X users can communicate.
- **All:** All authenticated and unauthenticated users can communicate. Default setting.
- **IPV6:** Only authenticated users using IP version 6 can communicate.

Configuring communication between different VSCs

Communication between users connected to different VSCs can only occur if the same VLANs are assigned in the **VSC egress mapping** option for both VSCs.

For example, to support traffic between authenticated users on two different VSCs, the **Authenticated** option under **VSC egress mapping** must be set to the same VLAN on both VSCs.

In addition, the following rules govern how traffic is exchanged:

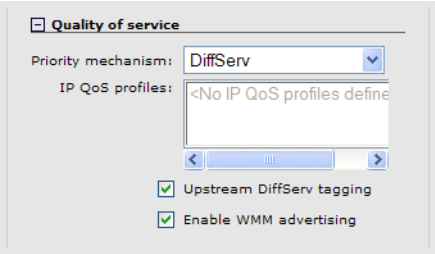
- Unicast traffic exchanged between VSCs on the ***same*** radio is controlled by the setting of the receiver's VSC.
- Unicast traffic exchanged between VSCs on ***different*** radios is controlled by the setting of the sender's VSC.
- Multicast traffic exchanged between VSCs is always controlled by the setting of the sender's VSC.

Generally, most users 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 users on the two VSCs, or between users on VSC1. However, all users on VSC2 can communicate with each other.
- If VSC1 is set to **802.1X** and VSC2 set to **All**, only 802.1X users can communicate between the two VSCs.

Quality of service

The quality of service (QoS) feature provides a number of different mechanisms to prioritize wireless traffic sent to wireless client stations. For detailed information, see *Quality of service (QoS) on page 4-23*.

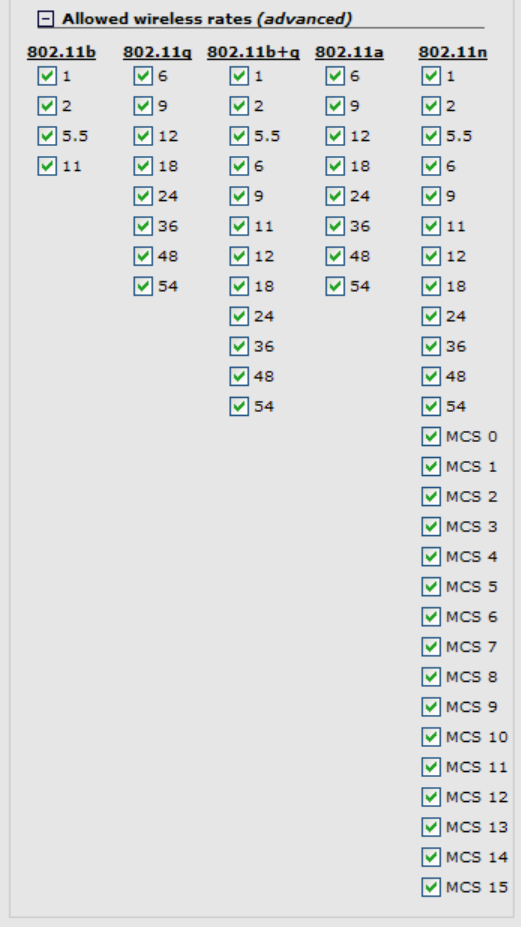


Allowed wireless rates

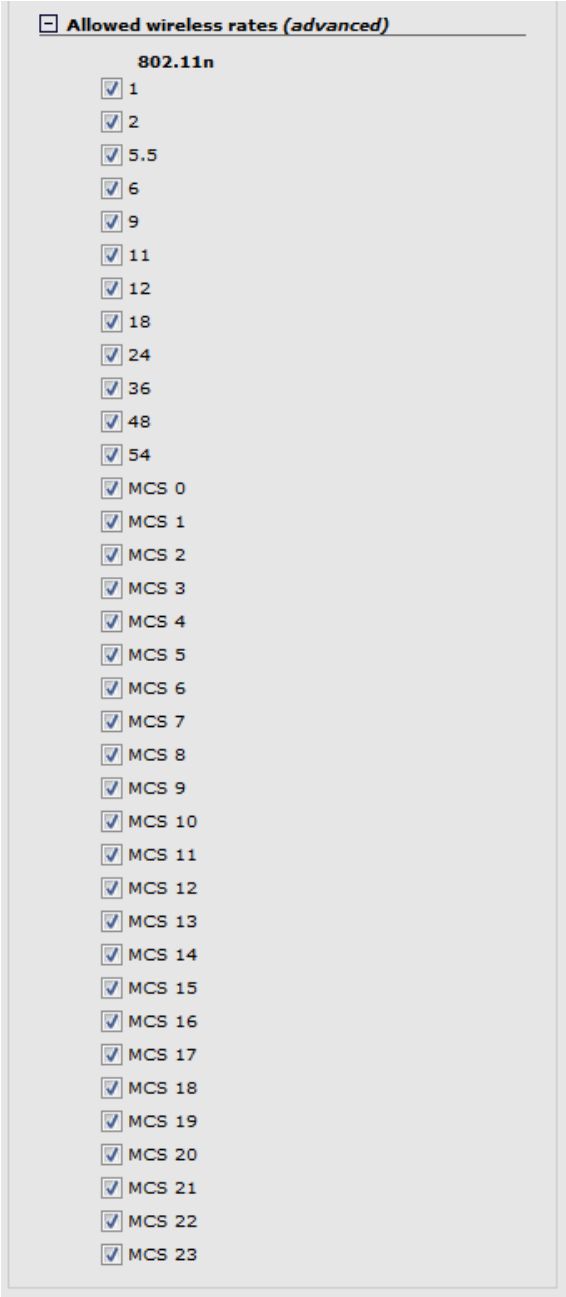
Select the wireless transmission speeds (in Mbps) that this VSC will support for each wireless mode. Clients will only be able to connect at the rates that you select. If a client does not support the selected rate and mode, it will not be able to connect to this VSC.

The following examples are from the MSM410 and MSM422 and the E-MSM430, E-MSM460, and E-MSM466.

MSM410, MSM422 (radio 1), E-MSM430



E-MSM460 and E-MSM466



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 the 802.11n

802.11n supports legacy rates (1 to 54), and high-throughput (HT) rates MCS 0 to MSC 23.

- **MCS 0 to MCS 15** are supported by the MSM410, MSM422 (radio 1), E-MSM430, E-MSM460, and E-MSM466.
- **MCS 16 to MCS 23** are supported by the E-MSM460 and E-MSM466.

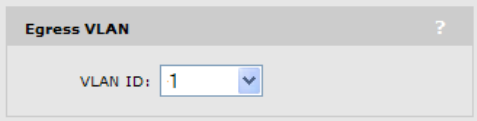
You must always enable at least one legacy rate for 802.11n.

Notes on the E-MSM430, E-MSM460, and E-MSM466

On these products, the wireless rates shown apply to all wireless modes supported on both radios, which are 802.11n/a/b/g. If you remove a rate, it is removed for all wireless modes.

Egress VLAN

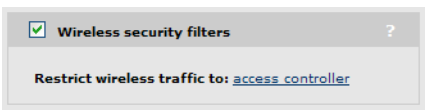
Sets the VLAN to which this profile forwards traffic. If you do not select a VLAN, traffic is sent untagged. VLAN s can also be assigned using other methods, some of which may override the Egress VLAN. See *VLAN support on page 5-5* for details.



Wireless security filters

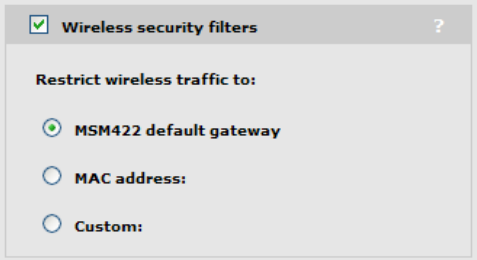
APs feature an intelligent bridge that can apply security filters to safeguard the flow of wireless traffic. These filters limit both incoming and outgoing traffic as defined below and force the AP to exchange traffic with a specific upstream device.

- If **Use HP MSM Controller** is enabled under **General**, the AP will only forward user traffic that is addressed to the access controller (MSM7xx Controller) defined on the **Security > Access controller** page. All other traffic is blocked. Make sure that the access controller is set as the default gateway for all wireless users. If not, user traffic will be blocked by the AP. The default wireless security filters are in effect.



Select the **access controller** link to open the **Security > Access controller** page where you can configure access controller options.

- If **Use HP MSM Controller** is disabled under **General**, then you can manually configure the security filters as required using the following options.



  - ***AP-name* default gateway:** The AP will only forward user traffic that is addressed to default gateway assigned on the **Network > Ports** page (via DHCP, PPPoE, or static addressing options).
  - **MAC address:** The AP will only forward user traffic that is addressed to the upstream device with the specified MAC address. Make sure that this device is set as the default gateway for all wireless users. If not, user traffic will be blocked by the AP.
  - **Custom:** Lets you define custom inbound and outbound security filters. 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-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

    - %a : MAC address of the controller.
    - %b : MAC address of the bridge.
    - %g : MAC address of the default gateway assigned to the AP.
    - %w : MAC address of AP wireless port.

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 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.

Wireless protection

Three types of wireless protection are offered: WPA, 802.1X, 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-MSM466, E-MSM460, and E-MSM430

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

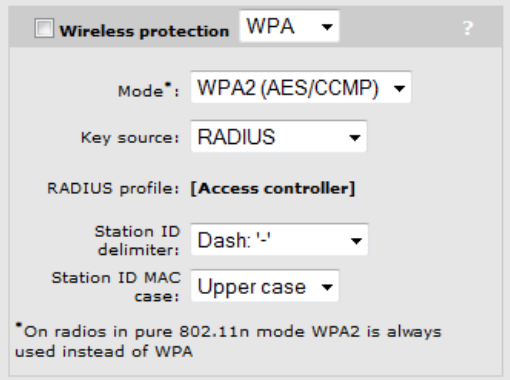
This option enables support for users with WPA / WPA2 client software. Support is provided for:

- **WPA (TKIP)**: WPA with TKIP encryption. (Not supported on the E-MSM466, E-MSM460, E-MSM430.)
- **WPA2 (AES/CCMP)**: WPA2 (802.11i) with CCMP encryption. If all your clients are WPA2, select this option for the maximum possible security.
- **WPA or WPA2**: Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time. Some legacy WPA clients may not work if this mode is selected. This mode is slightly less secure than using the pure WPA2 mode.

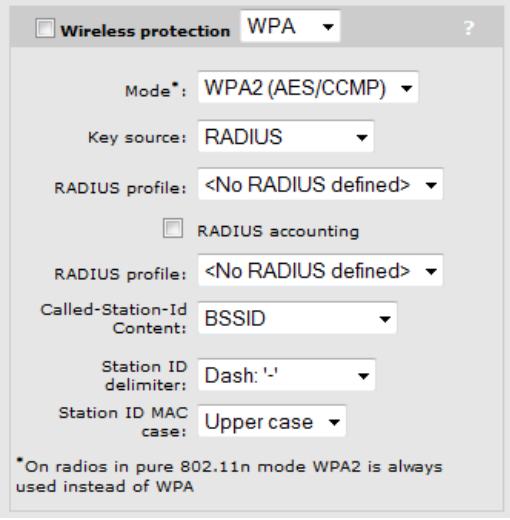
Authentication must occur via an external device (unless preshared keys are used). If **Use HP MSM controller** is enabled under **General**, this must be an HP MSM Controller, otherwise a third-party RADIUS server can be used.

WPA options supported when the *Use HP MSM controller feature* is ...

Enabled



Disabled



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

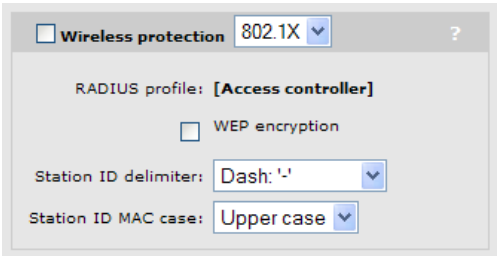
802.1X

This option enables support for users with 802.1X client software that use any of the following authentication methods: EAP-TLS, EAP-TTLS, and EAP-PEAP. Additionally, when an external RADIUS server is used, support for EAP-SIM, EAP-AKA, EAP-FAST, and EAP-GTC is also provided. Check your external RADIUS server for supported authentication methods.

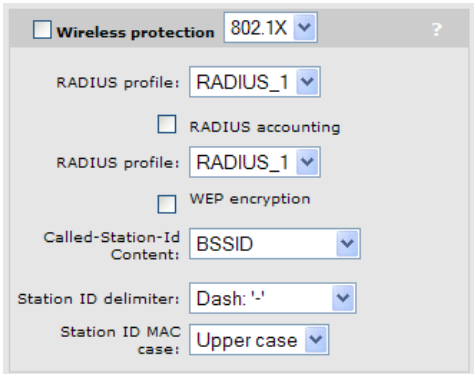
Authentication must occur via an external device. If **Use HP MSM controller** is enabled (under **General**), this must be an HP MSM Controller. Otherwise a third-party RADIUS server can be used.

802.1X options supported when the *Use HP MSM controller* option is ...

Enabled



Disabled



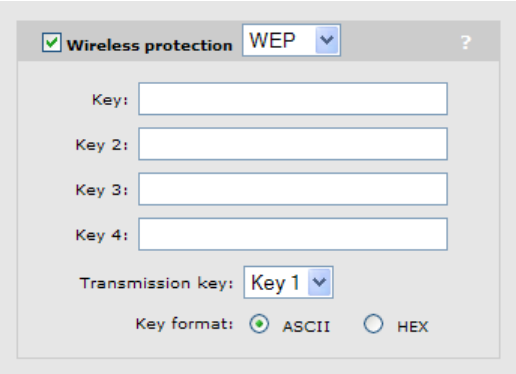
For a complete description of all options see the online help.

Note

For security reasons, using 802.1X without enabling at least WEP encryption is not recommended.

WEP

This option provides support for users needing WEP encryption.



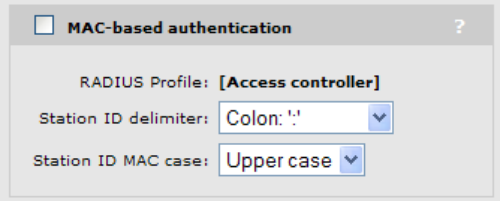
For a complete description of all options see the online help.

MAC-based authentication

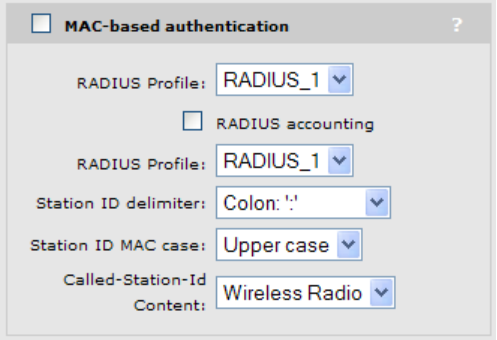
This option enables wireless users to be authenticated by their MAC addresses. Authentication must occur via an external device. If **Use HP MSM Controller** is enabled under **General**, this must be an HP MSM Controller. Otherwise a third-party RADIUS server can be used.

MAC-based authentication options supported when the *Use HP MSM Controller* option is ...

Enabled



Disabled

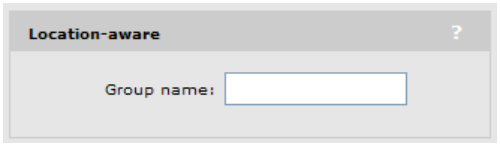


For a complete description of all options, see the online help.

Location-aware

This feature 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 only available when **Use HP MSM controller** is enabled under **General**.

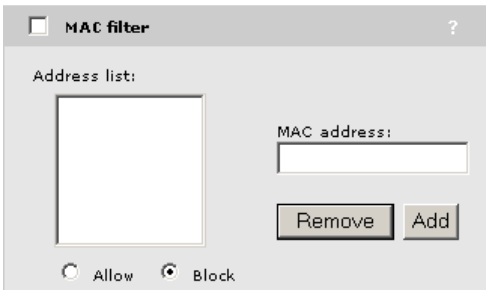
For each user login, location-aware sends the PHY Type, SSID, and VLAN to the controller. It also includes the specified **Group name**.



MAC filter

When enabled, this option enables you to control access to the AP based on the MAC address of client stations. You can either block access or allow access, depending on your requirements. Up to 64 MAC addresses are supported per VSC.

When both this option and the MAC-based authentication options are enabled, the following applies: if a user's MAC address does not appear in the MAC filtering list then MAC-based authentication takes place for that user.



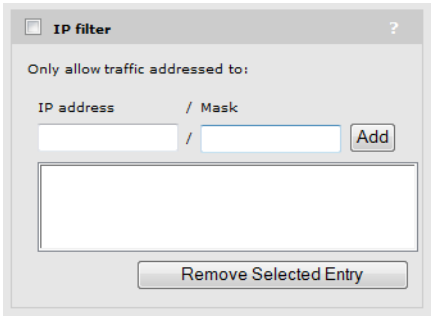
Specify the MAC address as six pairs of hexadecimal digits separated by colons; for example, 00:00:00:0a:0f:01.

Filter behavior:

- Allow: Only client stations whose MAC addresses appear in the MAC address list can connect to the wireless network.
- Block: All client stations whose MAC addresses appear in the MAC address list are blocked from accessing the wireless network.

IP filter

The IP filter enables you to block wireless-to-wired LAN traffic on this VSC based on its destination address.



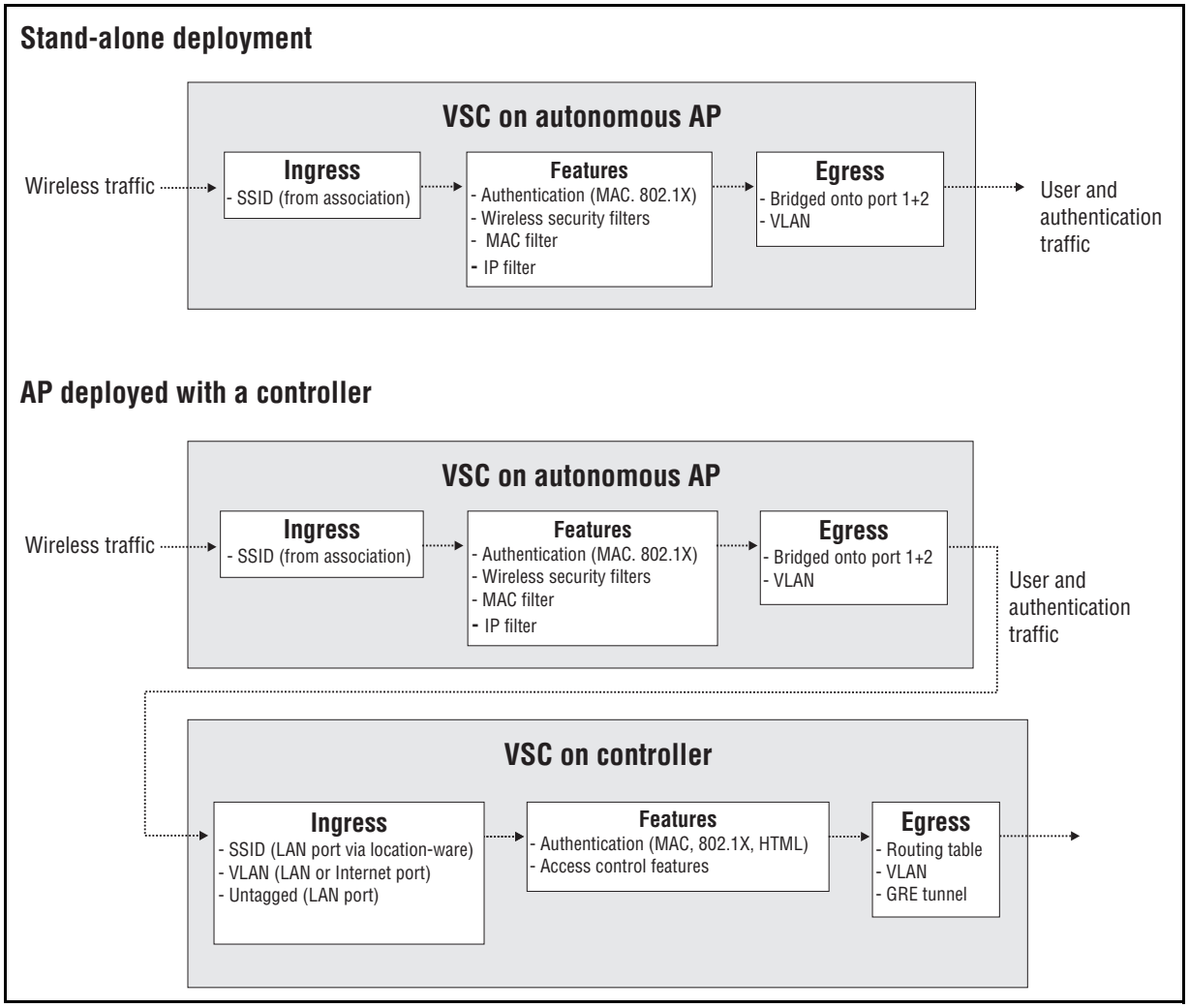
Specify the list of destination IP addresses for which traffic will be accepted. All other traffic will be blocked. Up to 64 IP addresses are supported.

The IP filter does not block the following:

- DNS queries (i.e., TCP/UDP traffic on port 53)
- DHCP requests/responses

VSC data flow

Each VSC provides a number of configurable options. The following diagrams illustrate how traffic from wireless users is handled by VSC definitions on an AP and controller, and shows the options that apply on each device.



stand-alone deployment

VSC on autonomous AP

Ingress

The AP only handles wireless traffic. The SSID is the name of the wireless network with which the user associates.

Features

- **Authentication:** Authentication can be either 802.1X or MAC. To validate user credentials the AP makes use of an external RADIUS server, which can be the controller or a third-party device. For more information, see *Stand-alone deployment on page 4-2*
- **Wireless security filters:** Enables the AP to block traffic unless it is addressed to a specific device (like the controller). For more information, see *Wireless security filters on page 4-14*.
- **MAC filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses. For more information, see *MAC filter on page 4-19*.
- **IP filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user IP addresses. For more information, see *IP filter on page 4-20*.

Egress

- **Bridge onto port 1+2:** Unless a centralized mode tunnel has been established, user and authentication traffic is bridged onto ports 1 and 2 (if available).
- **VLAN:** All traffic on port 1 or 2 (if available) can be assigned to a VLAN.

AP deployed with a controller

Ingress

The AP only handles wireless traffic. The SSID is the name of the wireless network that the user associates with.

Features

- **Authentication:** Authentication can either 802.1X or MAC. To validate user credentials the AP makes use of the controller. For more information, see the chapter on *User authentication* in the *MSM7xx Controllers Management and Configuration Guide*.
- **Wireless security filters:** Enables the AP to block traffic unless it is addressed to a specific device (like the controller). For more information, see *Wireless security filters on page 4-14*.
- **MAC filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses. For more information, see *MAC filter on page 4-19*.
- **IP filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user IP addresses. For more information, see *IP filter on page 4-20*.

Egress

- **Bridge onto port 1+2:** User and authentication traffic is bridged onto ports 1 and 2 (if available).
- **VLAN:** All traffic on port 1 or 2 (if available) can be assigned to a VLAN.

VSC on controller

For more information on controller configuration, see the *MSM7xx Controllers Management and Configuration Guide*.

Ingress

- **SSID (LAN port):** SSID is retrieved using the location-ware function client runs on AP.
- **VLAN (LAN or Internet port):** Traffic with a VLAN ID is handled by the VSC with a matching VLAN definition.
- **Untagged (LAN port):** Untagged traffic on the LAN port may originate from wired users, or APs operating in autonomous mode (HP or third-party).

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 a third-party authentication server (Active Directory or RADIUS).
- **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.

Egress

The controller enables user traffic to be forwarded to different output interfaces, which include the routing table, VLAN ID, or IP GRE tunnel.

Quality of service (QoS)

The quality of service (QoS) feature provides a number of different mechanisms to prioritize wireless traffic sent to wireless client stations. This is useful when the AP handles wireless traffic from multiple devices (or multiple applications on a single device), that have different data flow requirements.

QoS can be enabled on a VSC (see *Quality of service on page 4-12*) or on a local mesh link (see *Quality of service on page 7-6*).

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 queues 3 and 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	0,2
4	1,3

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	Very-based Very High
2	Very-based High
3	Very-based Normal
4	Very-based Low

Differentiated Services (DiffServ)

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.

Upstream DiffServ tagging

Enable this option to have the M111 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 the AP and then forwarded onto the wired network by the AP.

Mechanism	**INCOMING TRAFFIC** Wireless traffic sent from client stations to the AP	**OUTGOING TRAFFIC** Traffic sent by the AP to the network		
		L2 marking	**L3 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			
TOS	TOS			
VSC-based	WMM Non-WMM	802.1p (requires an egress VLAN to be defined for the VSC)		
IP QoS	WMM			

Downstream traffic marking

This table describes the marking applied to traffic received from the wired network by the AP and then sent to connected wireless client stations.

Mechanism	**INCOMING TRAFFIC** Traffic received from wired network	**OUTGOING TRAFFIC** Wireless traffic sent from AP 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.)

5

Network configuration

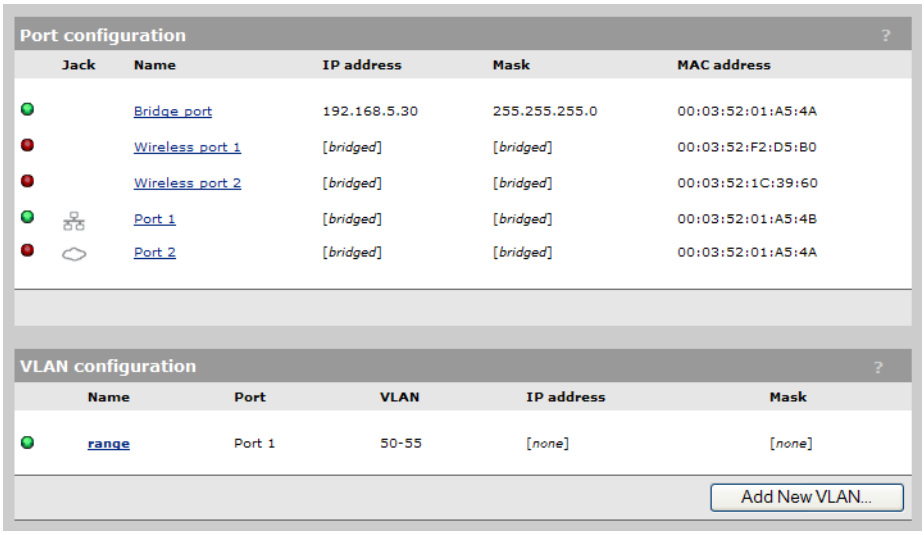
Contents

Port configuration

The **Port configuration** page displays summary information about all logical and physical ports and VLANs. Open this page by selecting **Network > Ports**.

Note

If the AP you are configuring only has a single port, this manual refers to it as Port 1. Ignore references to Port 2.

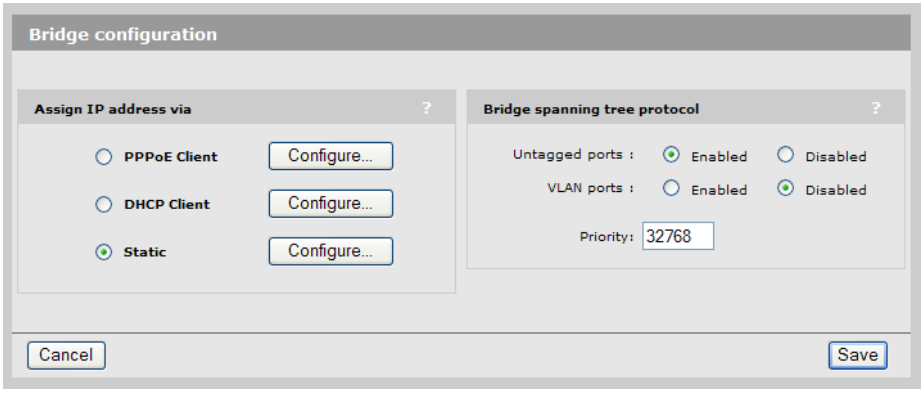


Port configuration information

- **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, is disabled, or is disconnected.
- **Jack**: Physical interface to which a logical port is assigned.
- **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.

Bridge port configuration

All ports (Ethernet and wireless) on the AP are bridged. Therefore, common settings are configured using the bridge port (which is a logical port). To verify, and possibly adjust bridge port configuration, select **Network > Ports** > **Bridge port**.



Assign IP address via

The bridge port supports the following addressing options:

- PPPoE client
- DHCP client (default setting)
- Static

By default, the bridge port operates as a DHCP client. Select the addressing option that is required by your network administrator and then select **Configure**. See the online help for descriptions of all configuration options.

Bridge spanning tree protocol

When this option is enabled, the AP uses the Spanning-Tree Protocol to prevent undesirable loops from occurring in the network that may result in decreased throughput.

Spanning tree can be enabled for untagged ports and/or VLAN ports.

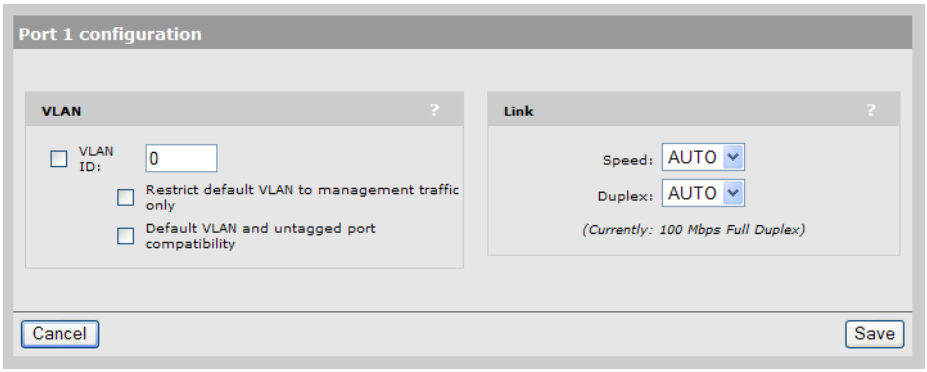
When VLAN support is enabled, it applies to VLANs defined on the **Network > Ports** page only. It does not apply to the management VLAN defined in the VLAN box on the **Network > Ports > [Port 1 | Port 2]** page.

Priority

Sets the priority of the AP within the spanning tree network. Generally, the bridge with lowest priority is designated as the root bridge of the spanning tree.

Port configuration

To verify and possibly adjust port configuration, select **Network > Ports > [Port 1 | Port 2]**. Configuration options for both ports are the same.



VLAN

Allows you to define a default VLAN on the port.

VLAN ID

Defines the default VLAN ID for this port. All outgoing traffic that does not have a VLAN already assigned to it is sent on this VLAN.

Note

Do not assign this same VLAN ID to users dynamically via RADIUS. If you do, traffic for these users will be blocked.

Restrict default VLAN to management traffic only

The default VLAN can be restricted to carry management traffic only. Management traffic includes:

- All traffic that is exchanged with the controller (login authentication requests/replies)
- All traffic that is exchanged with external RADIUS servers
- HTTPS sessions established by managers and operators of the management tool
- Incoming and outgoing SNMP traffic
- DNS requests and replies.

Default VLAN and untagged port compatibility

When this option is enabled, any traffic being sent on the default VLAN is also sent untagged on this port.

Link

Speed

- Auto: Lets the AP automatically set port speed based on the type of equipment it is connected to.
- 10: Forces the port to operate at 10 mbps.
- 100: Forces the port to operate at 100 mbps.
- 1000: Forces the port to operate at 1000 mbps.

Duplex

- Auto: Lets the AP automatically set duplex mode based on the type of equipment it is connected to
- Full: Forces the port to operate in full duplex mode.
- Half: Forces the port to operate in half duplex mode.

Wireless port configuration

See *Radio configuration on page 3-8*.

VLAN support

The AP provides a robust and flexible virtual local area network (VLAN) implementation that supports a wide variety of scenarios.

For example, VLANs can be used to isolate management from user traffic, or to route traffic over a local mesh connection.

You can map user traffic to a VLAN for each virtual service community (VSC) or on a per-user basis by setting the appropriate RADIUS attributes in a user's account.

Up to 80 VLAN definitions can be created. VLAN ranges are supported enabling a single definition to span a range of VLAN IDs.

The following AP features can be supported on a VLAN:

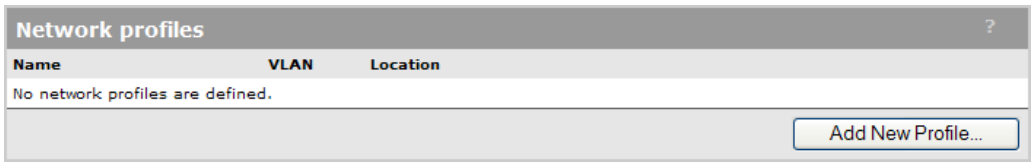
- Management tool access
- SNMP access
- SOAP access

Defining a VLAN

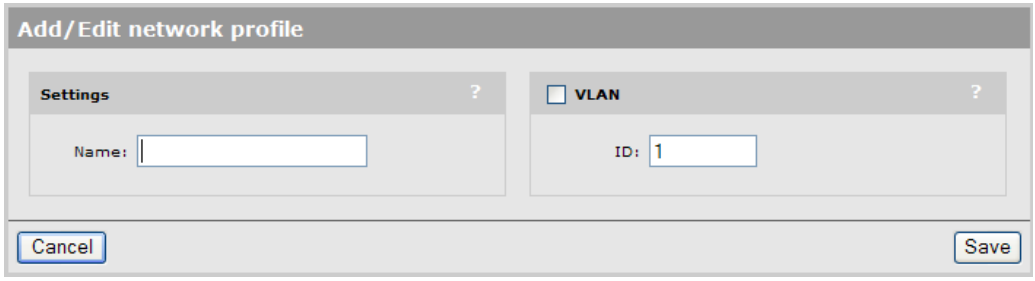
To create a new VLAN definition, first you must define a network profile with the required VLAN ID. Next, you use the profile to assign a VLAN to a port.

Creating a network profile

1. Select **Network > Network profiles.** By default the list is empty.



2. Select **Add New Profile**.



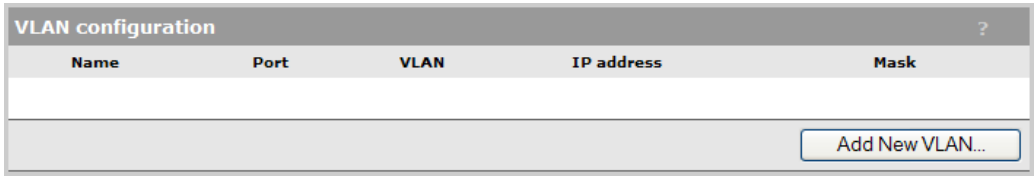
3. Under **Settings**, specify a **Name** to identify the profile.
4. Select **VLAN**, and then set **ID** to the VLAN ID you want to assign. You can also define a range of VLANs in the form *X*-*Y*, where *X* and *Y* can be 1 to 4094. For example: 50-60.

   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. Ranges are useful when you need to support many different VLANs on the same port when assigning per-user VLANs using RADIUS attributes.
5. Select **Save**. The definition is added to the Network profiles page.

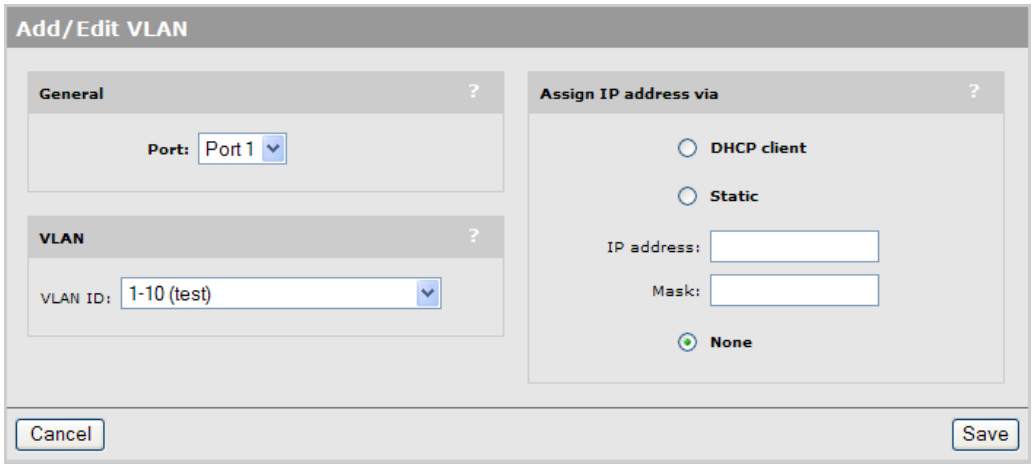
Assigning a VLAN to a port

Define a VLAN on an Ethernet port as follows:

1. Select **Network > Ports**. By default, no VLANs are defined.



2. Select **Add New VLAN.** The **Add/Edit VLAN** page opens.



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. 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. Use this when you define a VLAN range.
6. Select **Save**.

Defining an egress VLAN for a VSC

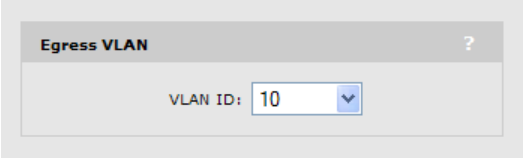
You can map egress traffic on each VSC to its own VLAN. Wireless clients that connect to a VSC with VLAN support are bridged to the appropriate VLAN. Address allocation and security measures are the responsibility of the target network to which the VLAN connects.

Note

You cannot assign the same VLAN ID to the default VLAN and to a VLAN that is mapped to a VSC egress.

1. Select **Network > VSC**. Select an existing VSC to edit it or select **Add New VSC Profile**.

2. Under **Egress VLAN**, select an **VLAN ID**. To be included in the drop-down list, the VLAN must be defined on the **Network > Ports** page and not be assigned to a VLAN range.



3. Select **Save**.

Configuring a default VLAN

You can configure port 1 (or port 2) with a default VLAN setting so that any outgoing traffic that is not tagged with a VLAN ID receives the default VLAN ID.

You can restrict this default VLAN to carry management traffic only, which includes the following:

- All traffic that is exchanged with the controller (login authentication requests/replies)
- All traffic that is exchanged with external RADIUS servers
- HTTPS sessions established by managers and operators of the management tool
- Incoming and outgoing SNMP traffic
- DNS requests and replies.

To assign a default VLAN, see *Port configuration on page 5-4*.

Assigning VLANs to individual users

You can assign a VLAN to an individual user by setting the attributes **Tunnel-Medium-Type**, **Tunnel-Private-Group-ID**, and **Tunnel-Type** in the user's RADIUS account. Restrictions are as follows:

- A user cannot be assigned to a VLAN that is set as the default VLAN on port 1 or port 2.
- A user can only be assigned to a VLAN that is defined on the **Network >Ports** page.
- Only applicable to clients using WPA or 802.1X. (Not applicable to MAC authentication.)

Note

A VLAN that is assigned to a user overrides a VLAN assigned by a VSC or by the default VLAN.

For more information see *Configuring user accounts on a RADIUS server on page 6-5*.

VLAN bridging

If you assign a VLAN ID to more than one interface, the VLAN is bridged across the interfaces.

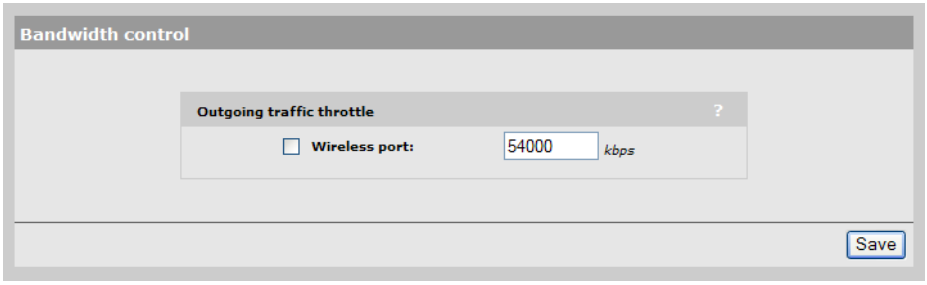
For example, if you create the VLANs shown in the following table, all VLAN traffic with ID 50 is bridged across all three interfaces. If you create a VSC and assign the egress VLAN to any of these VLANs, output from the VSC can be sent to any interface.

VLAN name	VLAN ID	Assigned to
Bridge_1	50	Port 1
Bridge_2	50	Port 2
Bridge_3	50	Local mesh 1

Bandwidth control

The AP incorporates a bandwidth management feature that provides control of outgoing user traffic on the wireless ports.

To configure Bandwidth control, select **Network > Bandwidth control.**

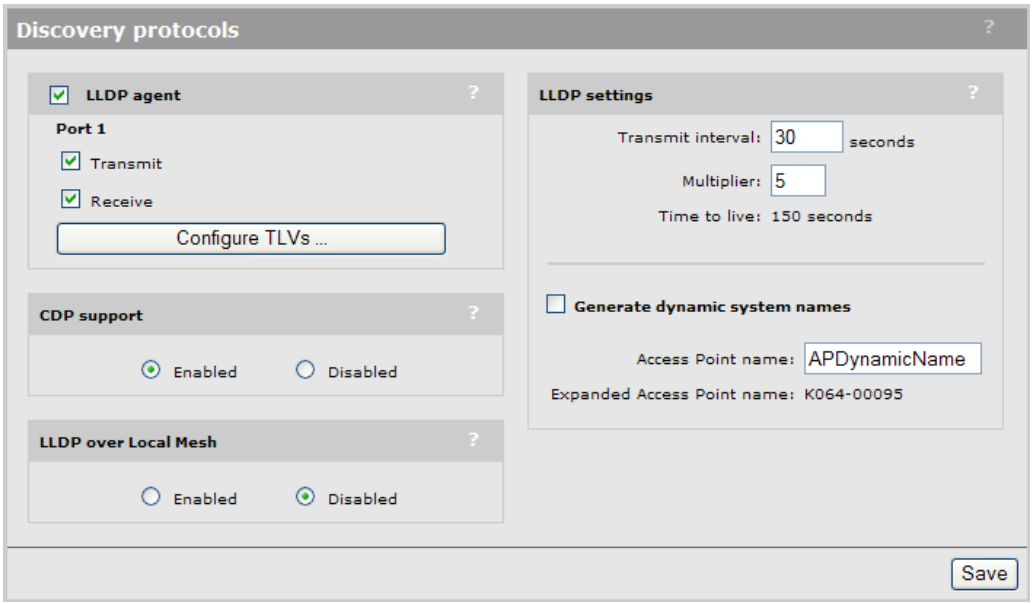


- If outgoing traffic arrives at the rate defined by the specified bandwidth limit (or less), it is processed without delay.
- If outgoing traffic arrives at a rate that is greater than the defined bandwidth limit, it causes the AP to throttle the traffic. If the traffic rate is over-limit for just a short burst, the data will be queued and forwarded without loss. If the traffic rate is over-limit for a sustained period, the AP will drop data to bring the rate down to the bandwidth limit that is set.

For example, if you set bandwidth control to 5000 kbps, the maximum rate at which traffic can be sent to wireless client stations is 5000 kbps.

Discovery protocols

Select **Network > Discovery protocols** to configure LLDP and CDP options. Both protocols provide a mechanism for devices on a network to exchange information with their neighbors.



CDP

The AP can be configured to transmit CDP (Cisco Discovery Protocol) information on all ports. This information is used to advertise AP information to third-party devices, such as CDP-aware switches.

When installed with a controller, the controller uses CDP information sent by autonomous APs to collect information about these APs for display in its management tool.

To enable CDP transmission, select **Network > Discovery protocols.**

LLDP

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.

Support is provided for the following MIBs:

- Physical topology MIB (RFC 2922)
- Entity MIB version 2 (RFC 2737)
- Interfaces MIB (RFC 2863)

Note

LLDP information is only sent/received on Ethernet links. LLDP information is not collected from wireless devices connected to an AP. However, LLDP can function across a local mesh link and will show the AP on the other side of the link as a neighbor.

LLDP agent

Select this option to enable the LLDP agent on port 1. Select **Configure TLVs** to customize TLV support.

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 over local mesh

Enables support for LLDP on any active local mesh links. APs on the other side of a local mesh link will be shown as neighbors when this feature is active.

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 containing the following information:

- 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.
- 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.
- Controller name suffix (if specified). Up to 16 characters can be appended to the name. To define the suffix for APs, select **Configuration > LLDP**.

To create the system name, the items are concatenated using a hyphen as separator. For example:

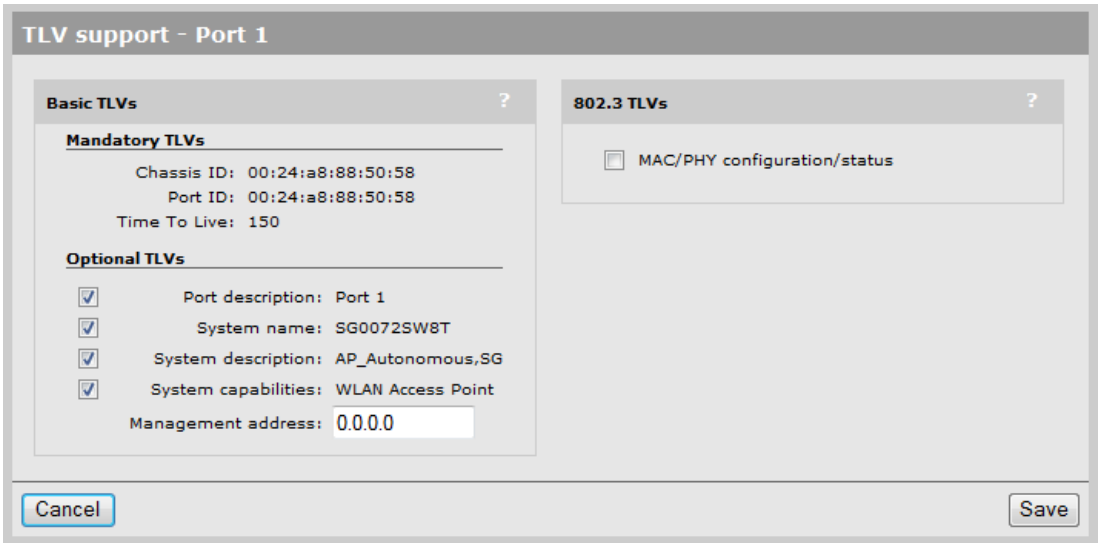
systemname-portid-suffix

Note

Once AP names are dynamically changed by this feature, there is no way to return to the old AP names.

TLV settings

To customize TLV settings, select **Configure TLVs** on the **Network > Discovery protocols** page.



Basic TLVs

The AP supports all mandatory and optional TLVs (type, length, value) information elements that are part of the basic management set.

Mandatory TLVs
The AP always sends these TLVs with the values as shown.

- **Chassis ID** (Type 1): The MAC address of the AP.
- **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: 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** for APs
  - **Router** for controllers.
- **Management IP address** (Type 8): Specify the IP address on which the agent will respond to management requests.

802.3 TLVs

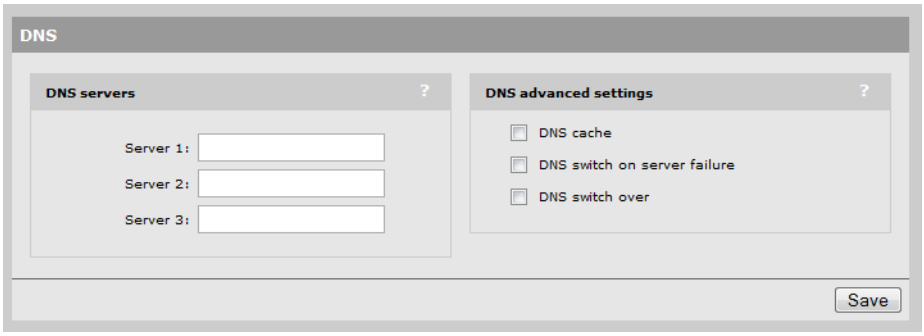
The IEEE 802.3 organizationally specific TLV set is optional for all LLDP implementations. The AP supports a single optional TLV from the 802.3 definition.

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.

DNS

The AP provides several options to customize DNS handling. To configure these options, select **Network > DNS.**



DNS servers

- **Server 1**: Specify the IP address of the primary DNS server for the AP to use.
- **Server 2**: Specify the IP address of the secondary DNS server for the AP to use.
- **Server 3**: Specify the IP address of the tertiary DNS server for the AP 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 AP restarts

DNS switch on server failure

This setting controls how the AP switches between the primary and secondary DNS servers.

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

DNS switch over

This setting controls how the AP switches back to the primary DNS server after it has switched to the secondary DNS server because the primary was unavailable.

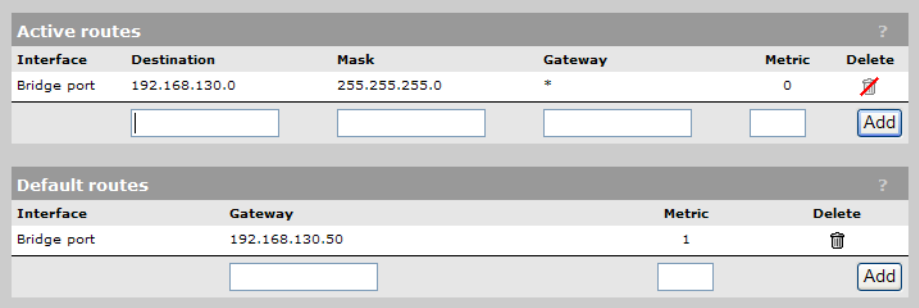
- When enabled, the AP switches back to the primary server after it becomes available again.
- When disabled, the AP switches back to the primary server only if the secondary server becomes unavailable.

IP routes

All wireless traffic on the AP is bridged to the egress interface on the VSC with which it is associated. Therefore, IP routes cannot be applied to user traffic. However, IP routes can be used to ensure that the management traffic generated by the AP is sent to the correct destination. For example, if two VSCs are defined, each with authentication assigned to a different RADIUS server operating on a different subnet and VLAN, routing table entries may be required to ensure proper communication with the RADIUS servers.

Configuration

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



Active routes

This table shows all active routes on the AP. 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 AP 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 AP automatically determines the interface to be used based on the **Gateway** address.
- **Destination**: Traffic addressed to this IP address 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 AP 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 AP chooses the one with the lower metric.
- **Delete:** Select the garbage can icon to delete a route. If the icon has a red line through it, then the route cannot be deleted.

Default routes

The **Default routes** table shows all default routes on the AP. 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 AP automatically determines the interface to be used based on the **Gateway** address.
- **Gateway**: IP address of the gateway to which the AP forwards routed traffic (known as the next hop).

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

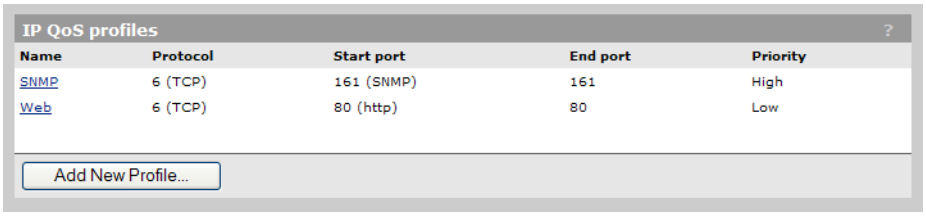
- **Metric**: Priority of a route. If two routes exist for a destination address, the AP chooses the one with the lower metric.
- **Delete:** Select the garbage can icon to delete a route. If the icon has a red line through it, then the route cannot be deleted.

IP QoS

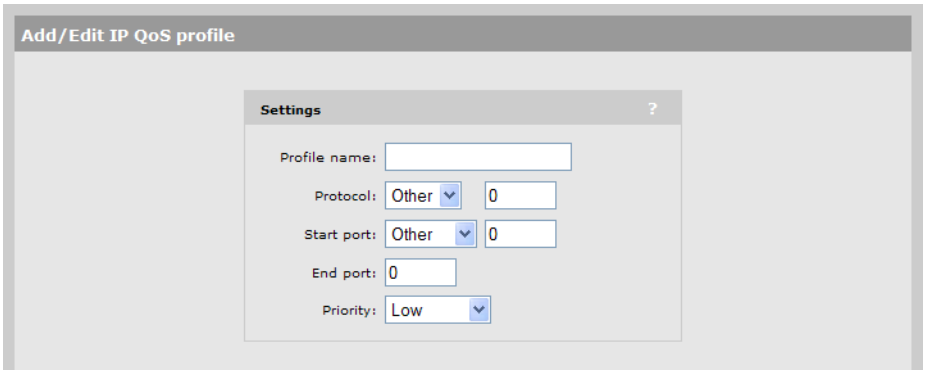
You configure IP quality of service (QoS) by creating IP QoS profiles that you can then associate with a VSC (*Quality of service (QoS) on page 4-23*) or with local mesh profiles (*Quality of service on page 7-6*). You can configure up to 32 IP QoS profiles on the AP. You can associate up to 10 IP QoS profiles to a VSC.

Configuration

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



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



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 at http://www.iana.org.
- **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.

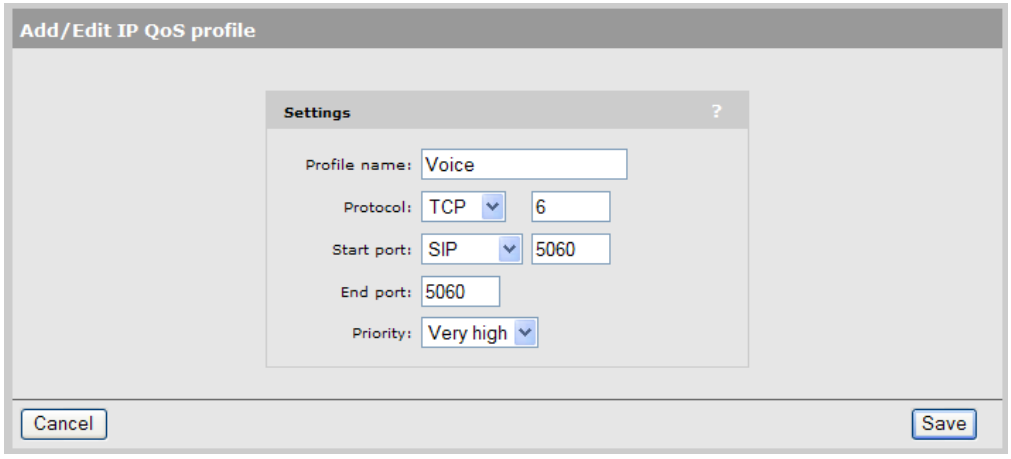
Example

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 **Add/Edit IP QoS Profile** page opens.



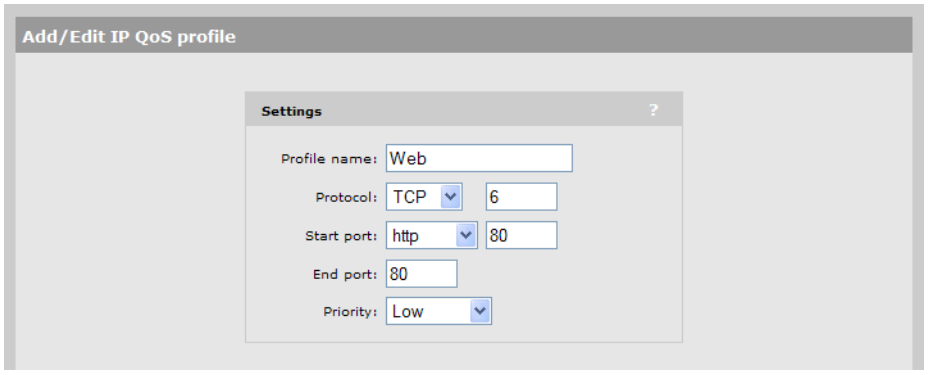
2. For **Profile name,** specify **Voice.**
3. Set **Protocol** to **TCP.**
4. Set **Start port** to **SIP. Start port** and **End port** are automatically populated with the correct value: **5060.**
5. Set **Priority** to **Very High.**
6. Select **Save.**

Note

You could also create another profile using the same parameters but with **Protocol** set to **UDP** in order to handle any kind of SIP traffic.

7. On the **IP QoS Profile** page select **Add New Profile.**
8. Set **Profile name** to **Web.**
9. Set **Protocol** to **TCP.**
10. Set **Start port** to **http. Start port** and **End port** are automatically populated with the common HTTP port: **80.**

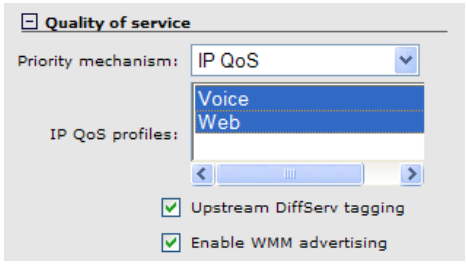
11. Set **Priority** to **Low.**



12. Select **Save.**

Assign the profiles to a VSC

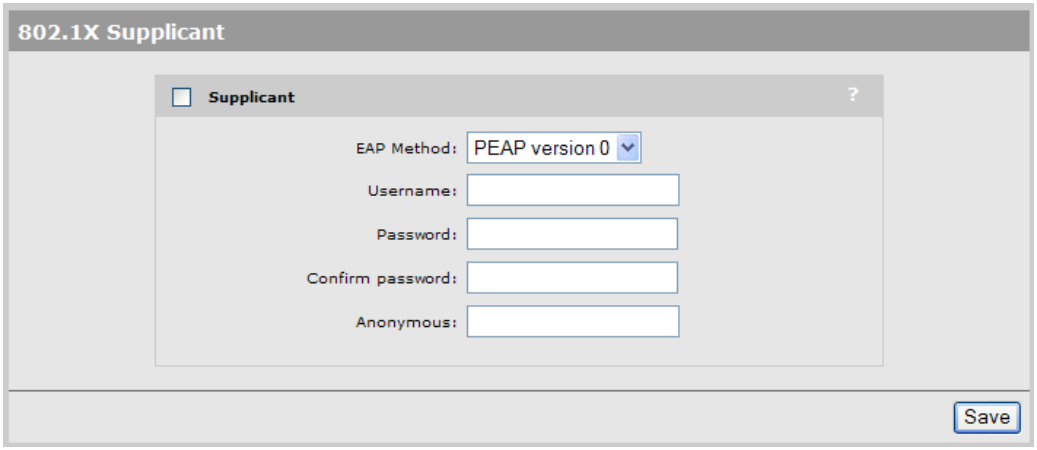
1. Select VSC on the main menu and then select one of the VSC profiles in the **Name** column. Scroll down to the **Quality of service** section under **Virtual AP** .



2. Set **Priority mechanism** to **IP QoS.**
3. For **IP QoS profiles**, hold down the Ctrl key and then select **Voice** and **Web**.
4. Select **Save.**

802.1X supplicant

The 802.1X supplicant can be used when the AP is connected to a secure switch port that requires 802.1X authentication. To configure the 802.1X supplicant, select **Network > 802.1X supplicant.**



Important

- If this option is enabled and the AP is connected to a unsecured switch port, 802.1X is ignored.
- The AP always performs 802.1X authentication without VLAN tagging. 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.
- VLAN attributes received in the RADIUS access accept are not provided to other applications running on the AP.
- The AP sends the EAPOL start and waits for the Request Identity. On a time-out, the AP will perform a single retry. On a second time-out, the 802.1X supplicant will become idle. The switch is responsible for restarting the IEEE 802.1X authentication by sending an EAP Request Identity.

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.

6

Security

Contents

Using an external RADIUS server

The AP can use one or more external RADIUS servers to perform a number of authentication and configuration tasks, including the tasks shown in the table below.

Task	For more information see
Validating administrator login credentials.	*Authenticating administrative credentials using an external RADIUS server on page 2-4*.
Validating user login credentials for WPA, 802.1X, or MAC-based authentication types on non-access-controlled VSCs.	*Wireless protection on page 4-16*. *MAC-based authentication on page 4-19*.
Retrieving RADIUS attributes on a per-user basis on non-access-controlled VSCs.	*Configuring user accounts on a RADIUS server on page 6-5*.
Storing accounting information for each user on non-access-controlled VSCs.	Accounting support is enabled under *Wireless protection on page 4-16* or *MAC-based authentication on page 4-19*.

Note

- On VSCs that have the **Use HP MSM controller** option enabled (creating an access-controlled VSC), see the *MSM7xx Controllers Management and Configuration Guide* for details on how user authentication is configured.
- When a VSC has the **Use HP MSM controller** option disabled (creating a non-access-controlled VSC), an external RADIUS server can be used to validate user credentials for WPA, 802.1X, or MAC-based authentication as described in this section.

Configuring a RADIUS client profile on the AP

The AP enables you to define up to 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 AP.

For backup redundancy, each profile supports a primary and secondary server.

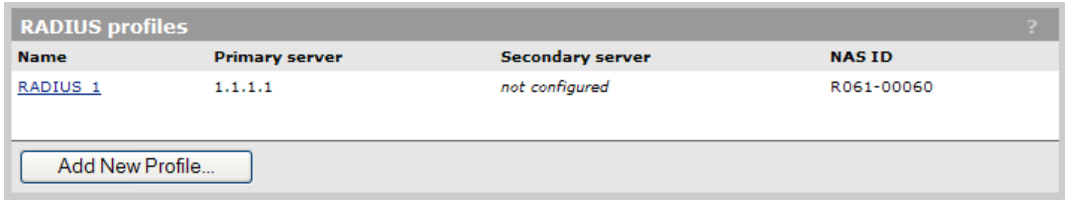
The AP can function with any RADIUS server that supports RFC 2865 and RFC 2866. Authentication occurs via authentication types such as: EAP-MD5, CHAP, MSCHAP v1/v2, LEAP, PAP, EAP-TLS, EAP-TTLS, EAP-PEAP. EAP-SIM, EAP-AKA, EAP-FAST, and EAP-GTC.

Note

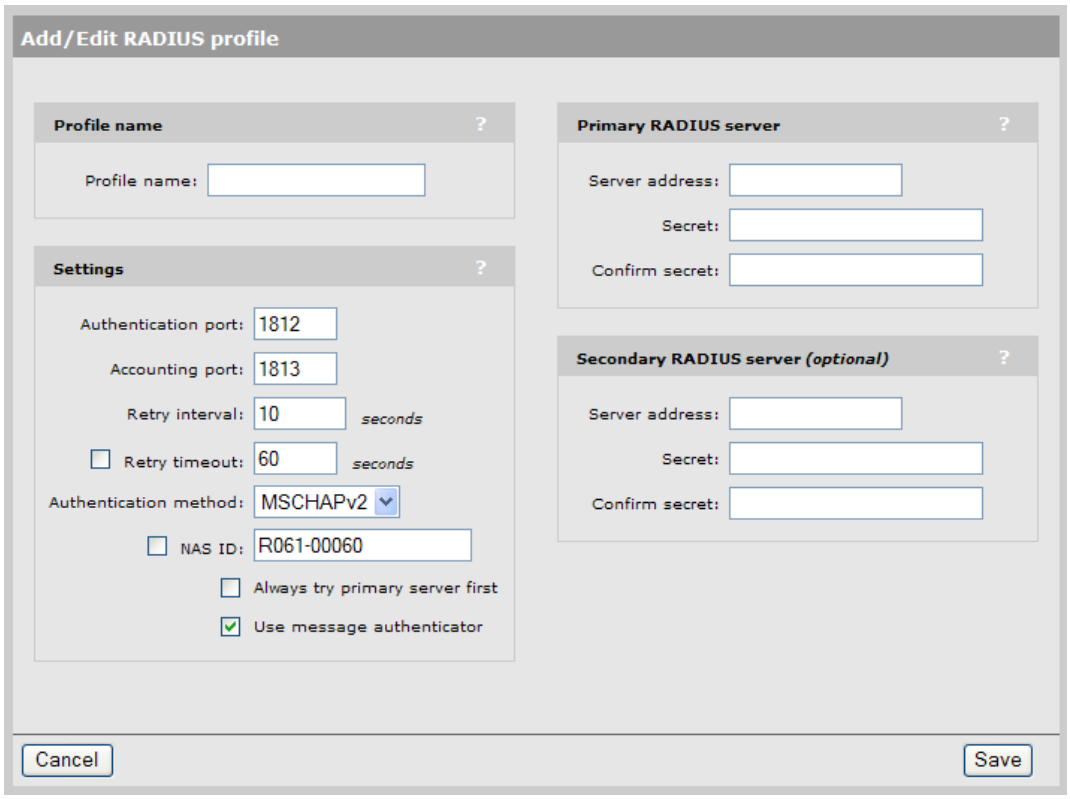
If you change a RADIUS profile to connect to a different server while users are active, all RADIUS traffic for active user sessions is immediately sent to the new server.

To define a RADIUS profile

1. Select **Authentication > RADIUS profiles.** The RADIUS profiles page opens.



2. Select **Add New Profile.** The Add/Edit RADIUS Profile page opens.



3. Configure the profile settings as described in the following section.
4. Select **Save**.

Configuration settings

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 RADIUS server waits before access and accounting requests time out. If the server does not receive a reply within this interval, the AP 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 access to the management tool
  - MAC-based authentication of devices.

  You can determine the maximum number of retries as follows:

  - MAC-based 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 AP 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 AP 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, MSCHAP V1, and CHAP are less secure protocols.

- **NAS ID:** Specify the identifier for the network access server that you want to use for the AP. By default the serial number of the AP is used. The AP 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 AP to contact the primary server first.

  Otherwise, the AP 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 AP sends the first RADIUS access request to the secondary RADIUS server.

  If the secondary RADIUS server does not reply, the AP retransmits the RADIUS access request to the primary RADIUS server. When two servers are configures, the AP always alternates between the two.

- **Use message authenticator:** When enabled, causes the RADIUS Message-Authenticator attribute to be included in all RADIUS access requests sent by the AP.

  Note: This option has no effect on IEEE802dot1x authentication requests. These requests always include the RADIUS Message-Authenticator attribute.

Primary/Secondary RADIUS server

- **Server address:** IP address or fully-qualified domain name of the primary RADIUS server.
- **Secret/Confirm secret:** Specify the password for the AP 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.

Configuring user accounts on a RADIUS server

When a non-access-controlled VSC is set to use WPA, 802.1X, or MAC-based authentication, a RADIUS server must be used to authenticate user logins. You must create an account for each user on the RADIUS sever with the appropriate username and password.

The AP provides support for a number of standard RADIUS user attributes, including those for authentication and accounting. Refer to your RADIUS documentation for more information on how to use these attributes.

Access Request attributes

This table lists all attributes supported in Access Request packets for each authentication type.

Attribute	Admin login	802.1X	MAC	Format
Acct-Session-Id	×	✔	✔	32-bit unsigned integer
Called-Station-Id	×	✔	✔	Called-Station-Id
Calling-Station-Id	×	✔	✔	Calling-Station-Id
EAP-Message	✔	✔	×	EAP-Message
Framed-MTU	✔	✔	×	Framed-MTU
Message-Authenticator	✔	✔	✔	Message-Authenticator
NAS-Identifier	✔	✔	✔	NAS-Identifier
NAS-Ip-Address	×	✔	✔	NAS-Ip-Address
NAS-Port	✔	✔	✔	NAS-Port
NAS-Port-Type	✔	✔	✔	NAS-Port-Type
Service-Type	✔	✔	✔	Service-Type
State	✔	✔	×	State
User-Name	✔	✔	✔	User-Name
User-Password	×	×	✔	User-Password
Vendor-specific (Colubris) SSID	×	×	✔	Colubris-AVPair (SSID)

Descriptions

- **Acct-Session-Id** (32-bit unsigned integer): A unique accounting ID used to make it easy to match up records in a log file.
- **Called-Station-Id** (string): BSSID of the VSC used by a wireless client, or the MAC address of the LAN port used by a wired client. By default, the MAC address is sent in IEEE format. For example: 00-02-03-5E-32-1A. The format can be changed under **Wireless protection** on the **VSC > Profiles** page.
- **Calling-Station-Id** (string): The MAC address of the 802.1X client station. By default, the MAC address is sent in IEEE format. For example: 00-02-03-5E-32-1A. The format can be changed under **Wireless protection** on the **VSC > Profiles** page.
- **Framed-MTU** (32-bit unsigned integer): Hard-coded value of 1496.
- **Message-Authenticator** (string): As defined in RFC 2869. Always present even when not doing an EAP authentication. Length = 16 bytes.
- **NAS-Identifier** (string): The NAS ID set on the **Security > RADIUS** page for the RADIUS profile being used.
- **NAS-Ip-Address** (32-bit unsigned integer): The IP address of the port the AP is using to communicate with the RADIUS server.
- **NAS-Port** (32-bit unsigned integer): A virtual port number starting at 1. Assigned by the AP.
- **NAS-Port-Type** (32-bit unsigned integer): Always set to 19, which represents WIRELESS_802_11.
- **Service-Type** (32-bit unsigned integer): Set to LOGIN_USER.
- **State** (string): As defined in RFC 2865.
- **User-Name** (string): The username assigned to the user. Or if MAC-authentication is enabled, the MAC address of the wireless client station.

The following attributes are mutually exclusive depending on the RADIUS authentication method.

- **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. Or, if MAC-authentication is enabled, this attribute contains the MAC address of the wireless client station.
- **EAP-Message** (string): As defined in RFC 2869. Only present when the authentication method for the RADIUS profile is set to EAP-MD5.
- **Vendor-specific (Colubris-AVPair SSID)**: SSID that the customer is associated with.

  The Colubris-AVPair 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>`

Access Accept attributes

This table lists all attributes supported in Access Accept packets for each authentication type.

Attribute	Admin login	802.1X	MAC
Acct-Interim-Interval	×	✔	✔
Class	×	✔	✔
EAP-Message	✔	✔	×
Idle-Timeout	×	✔	×
MS-MPPE-Recv-Key	×	✔	×
MS-MPPE-Send-Key	×	✔	×
Session-TImeout	×	✔	✔
Termination-Action	×	✔	✔
Tunnel-Medium-Type	×	✔	×
Tunnel-Private-Group-ID	×	✔	×
Tunnel-Type	×	✔	×
Vendor-specific (Microsoft) MS-MPPE-Recv-Key MS-MPPE-Send-Key	 × ×	 ✔ ✔	 × ×

Descriptions

- **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.
- **Class** (string): As defined in RFC 2865.
- **EAP-Message** (string): 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.
- **Session-Timeout** (32-bit unsigned integer): Maximum time a session can be active. After this interval:
  - 802.1X clients are automatically re-authenticated.

- MAC clients are blocked and must de-associate and then re-associate to start a new MAC authentication cycle.

- **Termination-Action**: As defined by RFC 2865. If set to 1:
  - Customer traffic is not allowed during the 802.1X re-authentication.
  - When receiving traffic from a MAC client, the AP starts a new authentication cycle automatically and the client does not need to re-associate.
- **Tunnel-Medium-Type**: Used only when assigning a specific VLAN number to a customer. In this case it must be set to 802.
- **Tunnel-Private-Group-ID**: Used only when assigning a specific VLAN number to a customer. In this case it must be set to the VLAN ID.
- **Tunnel-Type**: Used only when assigning a specific VLAN number to a customer. In this case it must be set to VLAN.
- **Vendor-specific (Microsoft)**
  - **MS-MPPE-Recv-Key**: As defined by RFC 3078.
  - **MS-MPPE-Send-Key**: As defined by RFC 3078.

Access Reject attributes

Access Reject RADIUS attributes are not supported.

Access Challenge attributes

This table lists all attributes supported in Access Challenge packets for each authentication type.

Attribute	Admin login	802.1X	MAC
EAP-Message	×	✔	×
Message-Authenticator	×	✔	×
State	×	✔	×

Descriptions

- **EAP-Message** (string): As defined in RFC 2869.
- **Message-Authenticator** (string): As defined in RFC 2869. Always present even when not doing an EAP authentication. length = 16 bytes.
- **State** (string): As defined in RFC 2865.

Accounting Request attributes

This table lists all attributes supported in Accounting Request packets for each authentication type.

Attribute	802.1X	MAC
Acct-Input-Gigawords	✔	×
Acct-Input-Octets	✔	×
Acct-Input-Packets	✔	×
Acct-Output-Gigawords	✔	×
Acct-Output-Octets	✔	×
Acct-Output-Packets	✔	×
Acct-Session-Id	✔	✔
Acct-Session-Time	✔	✔
Acct-Status-Type	✔	✔
Acct-Terminate-Cause	✔	×
Called-Station-Id	✔	✔
Calling-Station-Id	✔	✔
Class	✔	✔
Framed-IP-Address	✔	×
Framed-MTU	✔	×
NAS-Identifier	✔	✔
NAS-Port	✔	✔
NAS-Port-Type	✔	✔
User-Name	✔	✔
Vendor-specific (HP/Colubris) SSID	✔	✔

Descriptions

- **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): Number of packets 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): Number of packets sent by the user. Only present when Acct-Status-Type is Interim-Update or Stop.
- **Acct-Session-Id** (32-bit unsigned integer): Random value generated by the AP.
- **Acct-Session-Time** (32-bit unsigned integer): Number of seconds since this session was authenticated.
- **Acct-Status-Type** (32-bit unsigned integer): Supported values are Accounting-Start (1), Accounting-Stop (2), and Accounting-On (7) and Accounting-Off (8).

  Acct-Terminate-Cause (32-bit unsigned integer): Termination cause for the session. Only present when Acct-Status-Type is Stop. Supported causes are: Idle-Timeout, Lost-Carrier, Session-Timeout, and User-Request. See RFC 2866 for details.
- **Called-Station-Id** (string):
  - **802.1X**: BSSID of the VSC. By default, the value address is sent in IEEE format. For example: 00-02-03-5E-32-1A. The format can be changed in the **Wireless protection** section of the **VSC > Profiles** page.
  - **MAC**: MAC Address of the radio (**Network > Ports** page). By default, the MAC address is sent in IEEE format. For example: 00-02-03-5E-32-1A. The format can be changed in the **Wireless protection** section of the **VSC > Profiles** page.
- **Calling-Station-Id** (string): The MAC address of the wireless client station in IEEE format. By default, the MAC address is sent in IEEE format. For example: 00-02-03-5E-32-1A. The format can be changed in the **Wireless protection** section of the **VSC > Profiles** page.
- **Class** (string): As defined in RFC 2865. Multiple instances are supported.
- **Framed-IP-Address** (32-bit unsigned integer): IP Address as configured on the client station (if known by the AP).
- **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 IEEE802.1X authentication.
- **NAS-Identifier** (string): The NAS ID set on the **Security > RADIUS** page for the profile being used.
- **NAS-Port** (32-bit unsigned integer): A virtual port number starting at 1. Assigned by the AP.
- **NAS-Port-Type** (32-bit unsigned integer): Always set to 19, which represents WIRELESS_802_11.
- **User-Name** (string): The RADIUS username provided by the 802.1X client.

- **Vendor-specific (Colubris-AVPair SSID)**: SSID that the customer is associated with.

  The HP Colubris-AVPair 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>`

Configuring administrative accounts on a RADIUS server

This section presents all RADIUS attributes that are supported for administrator (manager/operator) accounts.

Note Only Access Request packets are supported for administrative accounts. Access Accept, Access Reject, Access Challenge, Accounting Request, and Accounting Response requests are not supported.

Access Request attributes

The following are supported Access Request RADIUS attributes.

- **User-Name** (string): The username assigned to the user or a device when using MAC authentication.
- **NAS-Identifier** (string): The NAS ID set on the **Security > RADIUS** page for the profile being used.
- **Service-Type** (32-bit unsigned integer): As defined in RFC 2865. Set as follows:
  - Web Admin is SERVICE_TYPE_ADMINISTRATIVE
- **Framed-MTU** (32-bit unsigned integer): Hard-coded value of 1496.
- **MSCHAP-Challenge** (string): As defined in RFC 2433. Only present when the authentication scheme on the **Security > RADIUS** page is set to MSCHAPv1 or MSCHAPv2. Length = 8 bytes.
- **MSCHAP-Response** (string): As defined in RFC 2433. Only present when the authentication scheme on the **Security > RADIUS** page is set to MSCHAPv1. Length = 49 bytes.
- **Vendor-specific (Colubris-AVPair Administrative role)**: Administrative role assigned to the user, either manager or operator.

  The Colubris-AVPair 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>`

The following keyword and value is supported for administrative accounts:

`web-administrative-role=`*role*

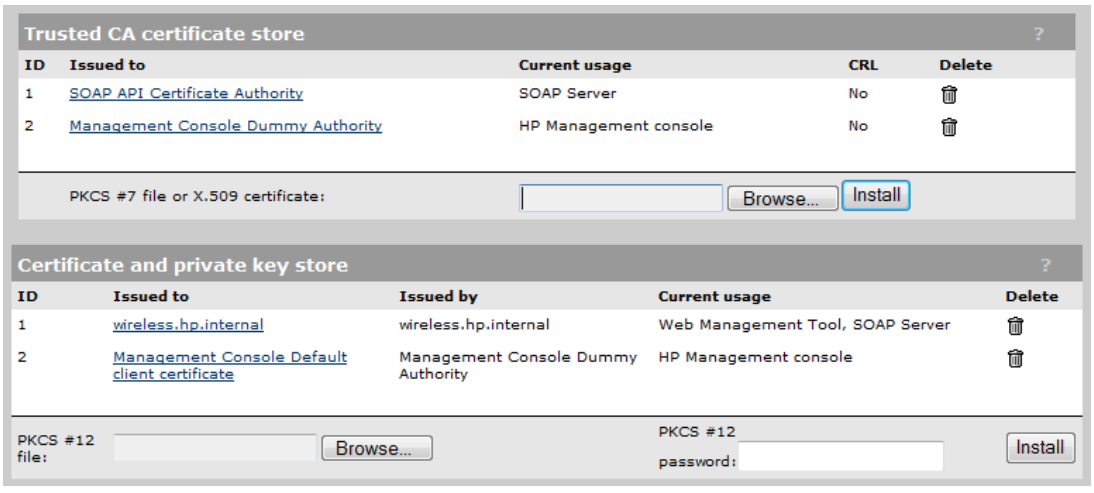
Where:

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.

Managing certificates

Digital certificates are electronic documents that are used to validate the end parties or entities involved in data transfer. These certificates are normally associated with X.509 public key certificates and are used to bind a public key to a recognized party for a specific time period.

The certificate store provides a repository for managing all certificates. To view the certificate stores, select **Security > Certificate stores**.



Trusted CA certificate store

This list displays all CA certificates installed on the AP. The AP uses the CA certificates to validate the certificates supplied by peers during authentication. Multiple CA certificates can be installed to support validation of peers with certificates issued by different CAs.

The AP uses the CA certificates to validate certificates supplied by:

- Managers accessing the AP management tool
- SOAP clients communicating with the AP SOAP server

The following information is displayed 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.

Content and file format	Items carried in the file	Description
X.509 certificate in PKCS #7 file	One X.509 certificate	Popular format with Microsoft products.
X.509 certificate in PEM file	One or more X.509 certificate	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 AP checks the certificate supplied by a SOAP client to ensure that it is issued by a trusted certificate authority (CA).
- **Management Console Dummy Authority:** Used when the management tool communicates with HP PCM/PMM software.

Certificate and private key store

Caution

For security reasons, you should replace the default certificate with your own.

This list displays all certificates installed on the AP. The AP uses these certificates and private keys to authenticate itself to peers.

The following information is displayed 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.

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 name in the certificate is automatically assigned as the domain name of the AP.

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.local:** Default certificate used by the management tool, SOAP server, and HTML-based authentication.
- **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 AP using SSL, the AP sends only its own SSL 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 AP. Consequently, the web browser issues security warnings.

To avoid this problem, install an SSL certificate on the AP only if it is directly signed by the root certificate authority or if you have appended all certificates that make up the chain.

Consequently, the web browser issues security warnings.

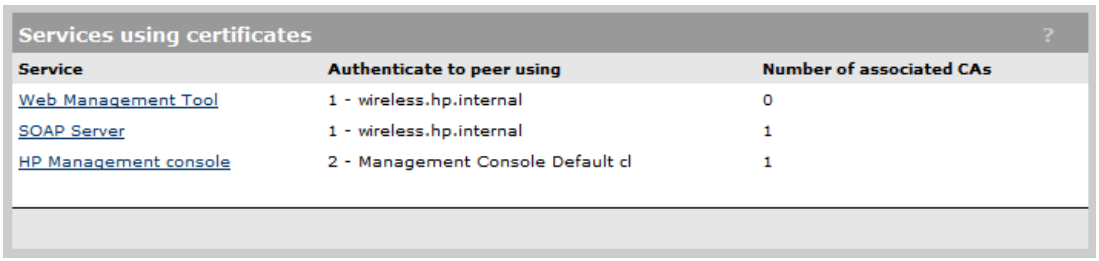
To avoid this problem, make sure that you install the entire certificate chain when you install a new certificate on the AP.

Note

If you enable the **Notifications** option on the **Management > SNMP** page and then select **Configure Notifications** and enable the **Certificate about to expire** notification under **Maintenance,** an SNMP notification is sent to let you know when the AP SSL certificate is about to expire.

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:



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

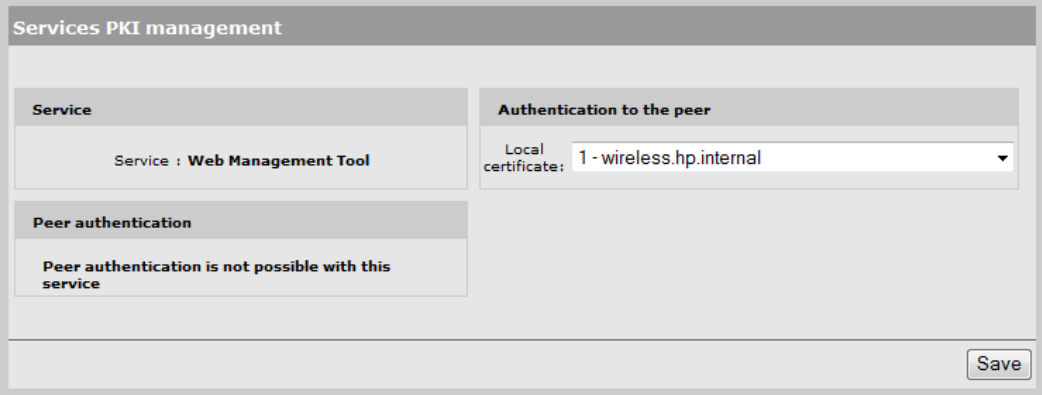
Name of the certificate and private key. The AP is able to prove that it has the private key corresponding to the public key in the certificate. This is what establishes the AP as a legitimate user of the certificate.

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:



Under **Authentication to the peer**, select a new **Local certificate** and then select **Save**.

About certificate warnings

When you connect the management tool, certificate warnings occur because the default certificate installed on the AP 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 AP.

To continue to work with the management tool without installing a certificate, select the option that allows you to continue to the Website.

To eliminate these warnings you can do one of the following:

- Obtain a registered X.509 (SSL) certificate from a recognized certificate authority and install it on the AP. This is the best solution, since it ensures that your certificate can be validated by any web browser. A number of companies offer this service for a nominal charge. These include: Thawte, Verisign, and Entrust.
- Become a private certificate authority (CA) and issue your own certificate: You can become your own CA. and create as many certificates as you require. However, since your CA will not be included in the internal list of trusted CAs maintained by most browsers, users will get a security alert until they add your CA to their browser.

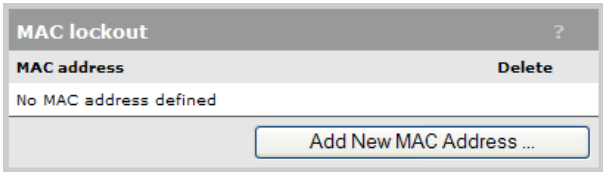
MAC lockout

This feature lets you block traffic from client stations based on their MAC address. MAC lockout applies to client stations connected to:

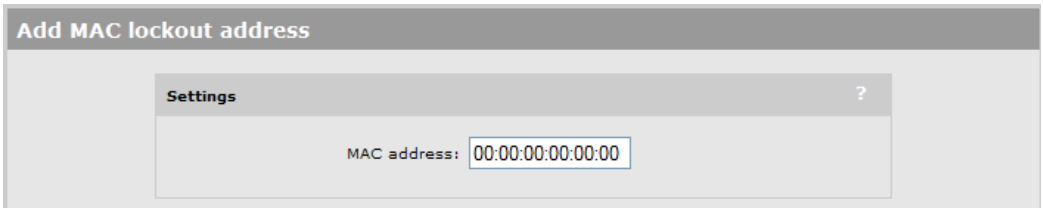
- Wireless ports
- Wired ports (including switch ports)
- Local mesh ports

Adding a MAC lockout address

1. Select **Security > MAC lockout**.



2. Select **Add New MAC Address**.



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**.

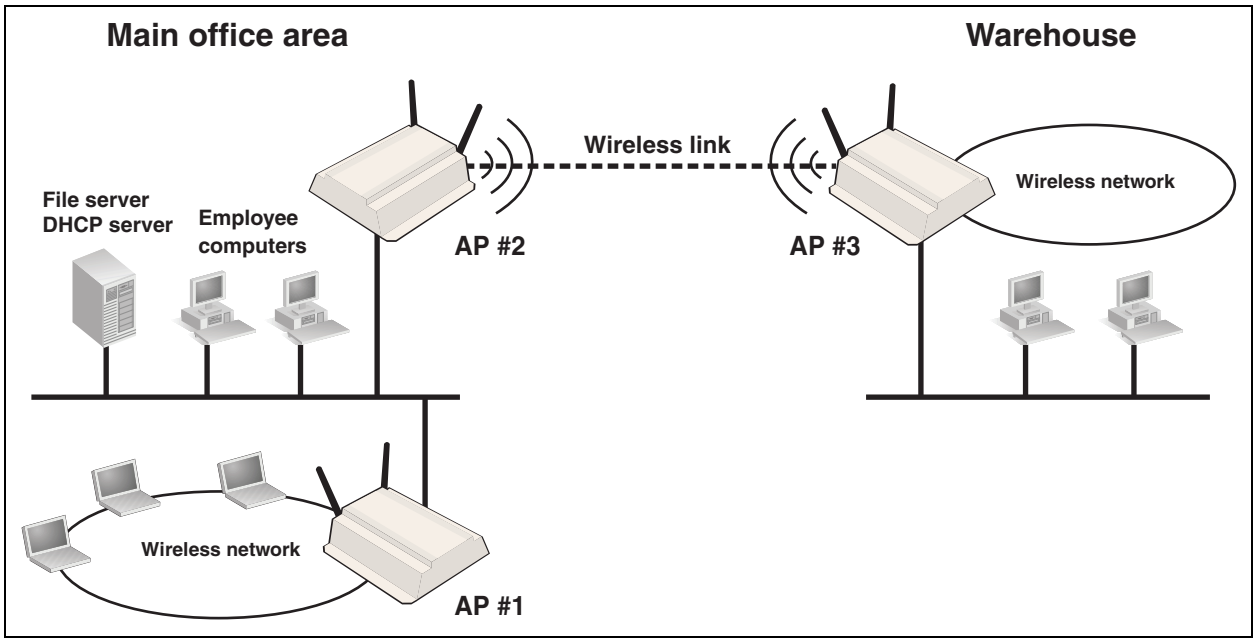
7

Local mesh

Contents

Introduction

The local mesh feature enables you to create wireless links between one or more APs. These links create a wireless bridge that interconnects the networks connected to the Ethernet port on each AP. For example, AP #2 and AP #3 use the local mesh feature to create a wireless link between the main office network and a small network in a warehouse.



Local mesh links provide an effective solution for extending network coverage in situations where it is impractical or expensive to run cabling.

Key local mesh features include:

- **Automatic link establishment:** Nodes automatically establish wireless links to create a fully-connected network. A dynamic network identifier (local mesh ID) restricts connectivity to local mesh nodes, enabling distinct local meshes 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

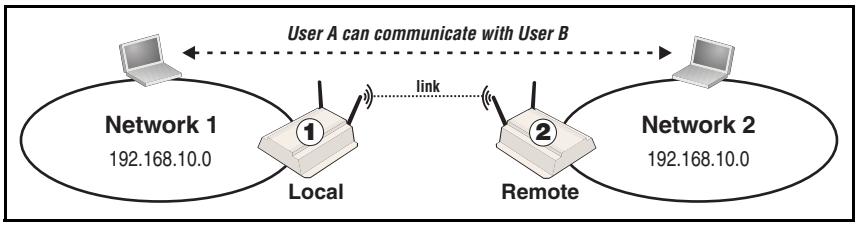
Depending on the radio regulations of some countries, DFS channels are only available on the 802.11aband, which is the preferred band for local mesh backhaul. If more than one node detects radar simultaneously and must switch channels, each node does not necessarily switch to the same channel, and the 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 7-6*.

Local mesh link types

Two types of local mesh links are supported: static and dynamic.

Static local mesh links

Static local mesh links can be used to create a fixed wireless connection between two APs, creating a wireless bridge between the networks connected to the two APs. For example, in the following scenario, a static wireless link is created between AP 1 and AP 2. Each AP is connected to a separate physical network, but both networks are on the same IP subnet (192.168.5.0). Traffic is bridged across the wireless link, allowing User A to communicate with User B.



Terminology

The following terms are used in this guide when discussing the static local mesh feature.

Term	Definition
Local	The AP that you are currently configuring to support a static link.
Remote	The AP that to which the static link will connect.
Link	The wireless connection between a local and remote AP.

Configuration guidelines

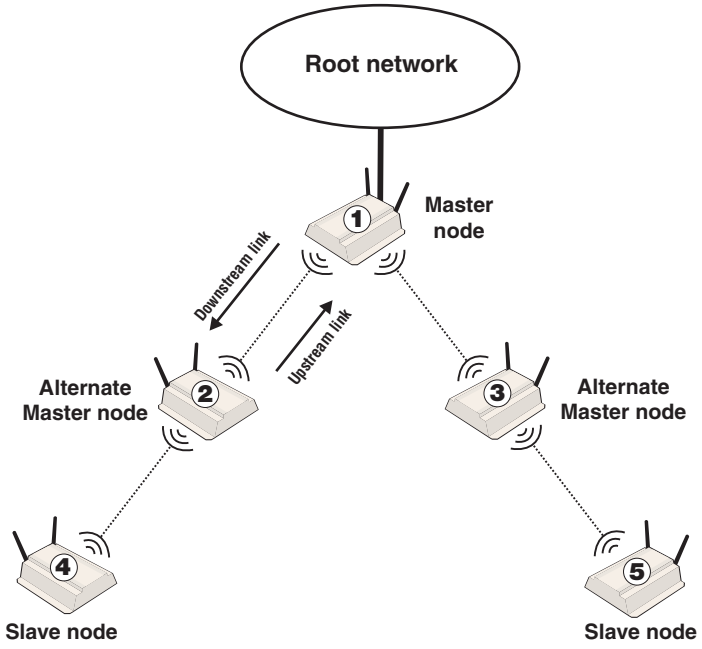
The following guidelines apply when you create a static local mesh link between two or more APs:

- All radios used to establish the link must be set to the same operating frequency and channel. This means that on the **Wireless > Radio** page under **Channel,** you cannot select **Automatic.**

- All APs must be on the same subnet, and each AP must have a unique IP address.
- If AES/CCMP security is enabled, the same key must be defined on all APs.
- Only one static wireless link can be defined between any two APs.

Dynamic local mesh links

The dynamic local mesh feature enables an AP to automatically find and connect with other APs to automatically create wireless links. When multiple APs are properly configured, they can automatically combine to create a mesh topology that is self-configuring and self-healing. For example, in the following scenario, a dynamic local mesh is composed of five APs. When the APs are started, they automatically establish the connections to build the mesh based on their role (master, alternate master, slave). If AP 2 fails, AP 4 automatically switches its connection to AP 3.



Traffic is bridged across the wireless links, allowing users connected to any AP to reach the root network.

Terminology

The following illustration and table define terms that are used in this guide when discussing the dynamic 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.

Term	Definition
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.

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 waits 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.

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:

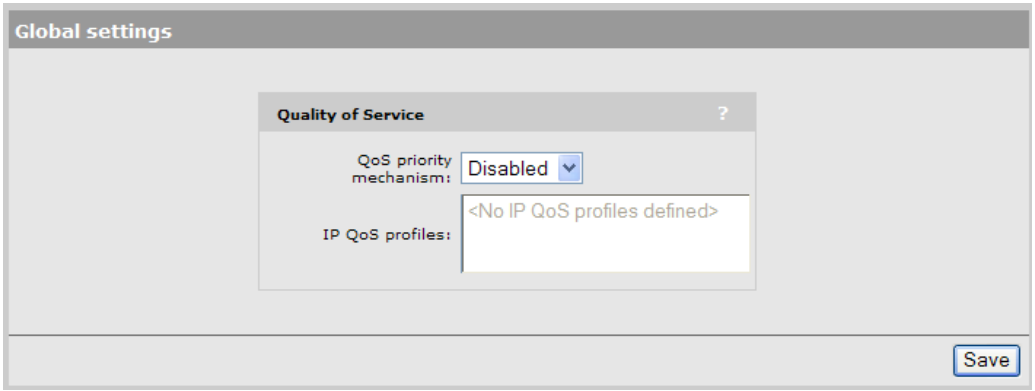
- Configure the radios on all nodes to use the same fixed channel.
- Configure the radios for automatic channel selection. In this case the master selects the least noisy channel. Slaves and alternate masters scan channels until they find the master, then tune to the master channel and link with the master.

Configuration guidelines

- You can configure a total of six local mesh profiles on each node.
- Each dynamic local mesh profile (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.

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.



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).

Radio configuration

Simultaneous AP and local mesh support (single radio)

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.

A more effective way to handle this is to use a multi-radio AP. This allows one radio to be dedicated to wireless users and another to local mesh links. Each radio can be configured optimally according to its application.

Simultaneous AP and local mesh support (dual radios)

Two radios can be enabled at the same time on a local mesh profile. This enables the node to search for a master (or alternate master) on both radios. Once a master is found and the link is established on one radio, the other is used to create downstream links. This greatly improves throughput over single-radio deployments.

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.

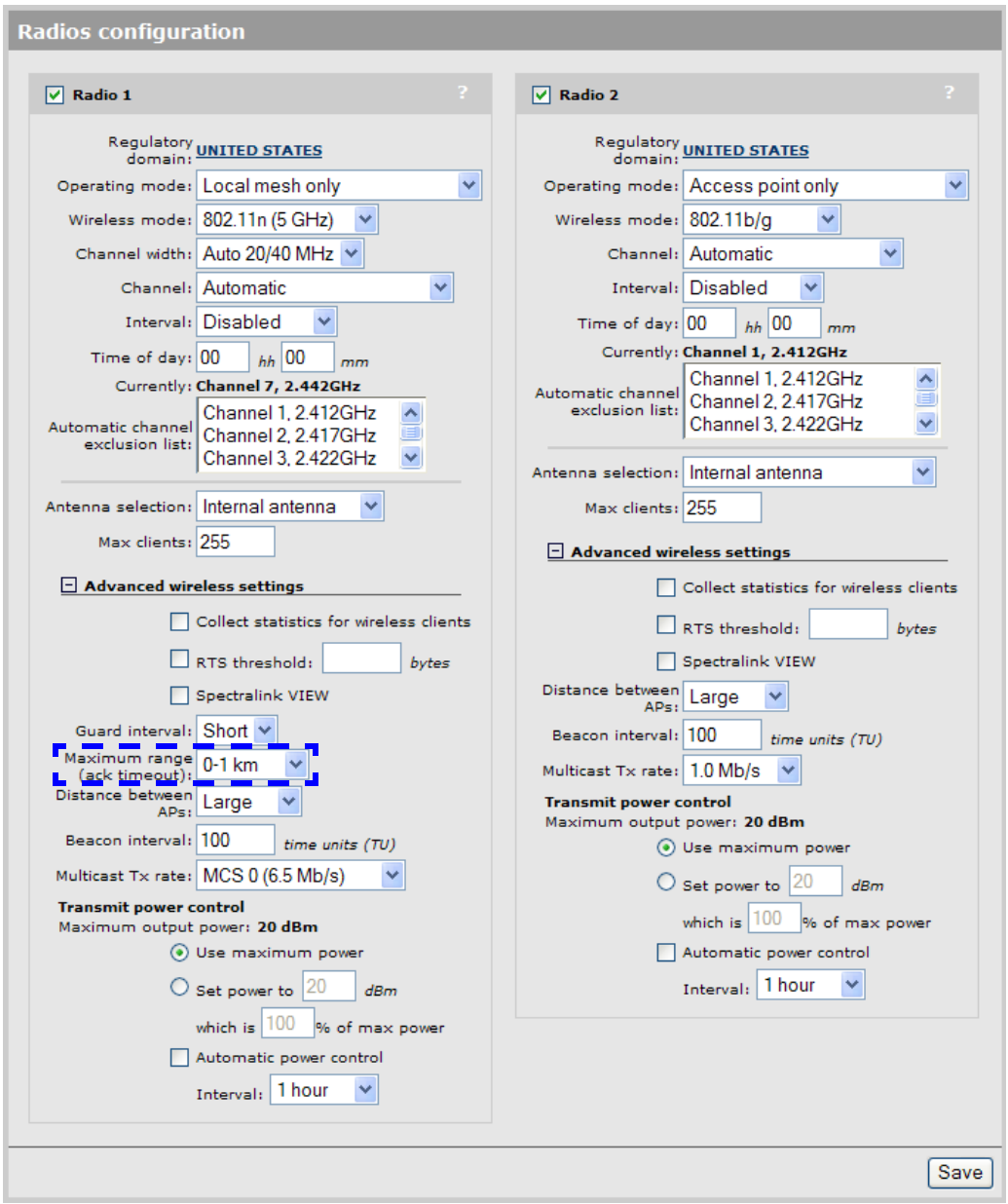
The main limitations in using the 5 GHz band are:

- 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.

Maximum range (ack timeout)

This is a global setting that is configurable on the **Radio** page when the **Operating mode** is set to **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.)



LLDP

Support can be enabled for LLDP on local mesh links (see *LLDP over local mesh on page 5-11*). When this feature is active, APs on the other side of a local mesh link are shown as neighbors.

Note LLDP is not supported over local mesh links on APs operating in controlled mode.

Local mesh profiles

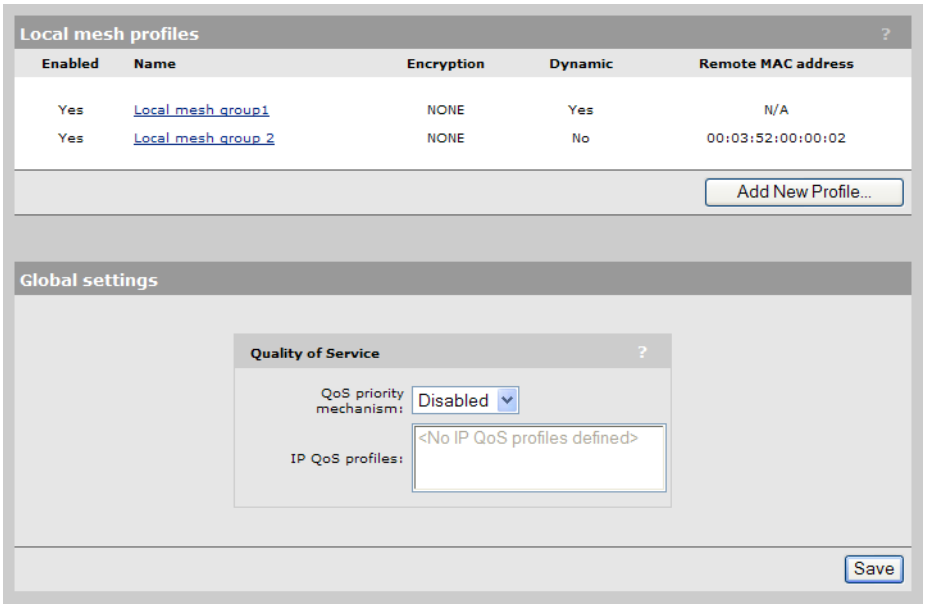
A local mesh profile defines the characteristics for the type of links that can be established with other nodes. Each node supports up to six profiles, each of which can be either static or dynamic.

- If a profile defines a static local mesh link, the profile can only be used to connect with another node with a profile that has matching settings.
- If a profile defines a dynamic local mesh link, it establishes links to other nodes as follows:

Role	Upstream link	Downstream link
Master	None.	Up to nine links with alternate master or slave nodes.
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.

When a dynamic profile is active, the AP constantly scans and tries to establish links as defined by the profile.

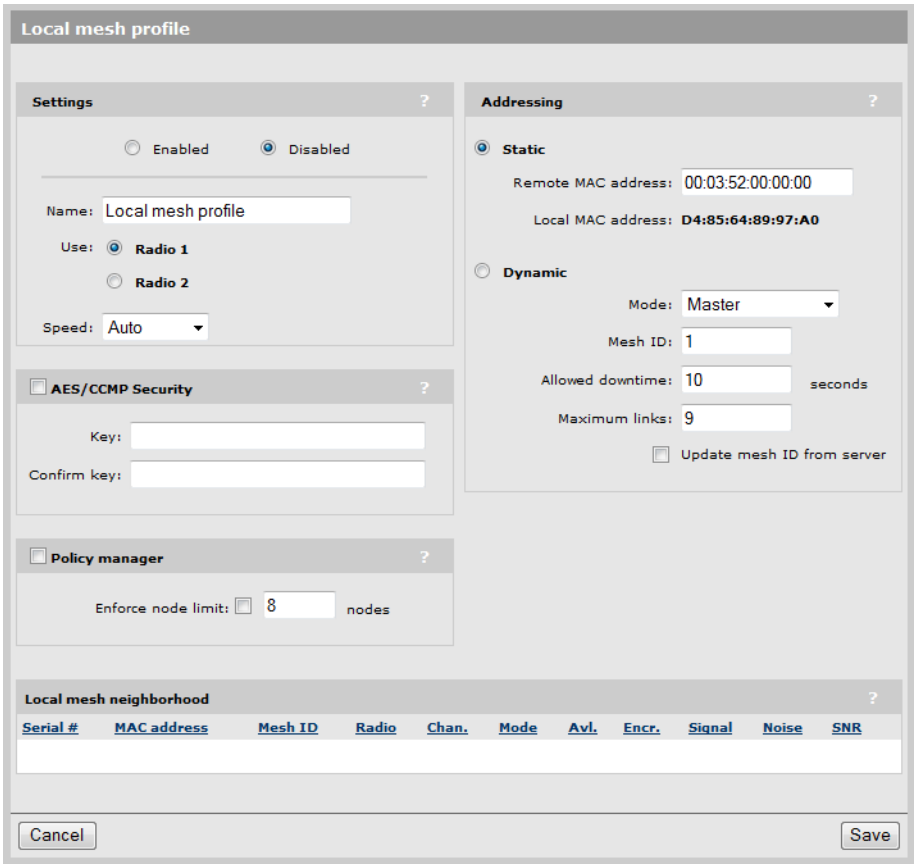
To view or add profiles select **Wireless > Local mesh**.



To configure a profile, select its name in the list. Or to add a profile, select **Add New Profile**.

Configuring a local mesh profile

To configure a profile, select its name in the list. The **Local mesh profile** page opens.



Settings

Enabled/Disabled

Specify if the profile is enabled or disabled. The profile is only active when enabled.

Name

Name of the profile.

Use

Select the interface to use for this link.

Speed

(Static links only)

Sets the speed the link will operate at. For load balancing, you may want to limit the speed of a link when connecting to multiple destinations.

AES/CCMP

Enables AES with CCMP encryption to secure traffic on the link.

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 64 ASCII characters in length. It is recommended that the key be at least 20 characters long and be a mix of letters and numbers.

Policy manager

The policy manager controls global configuration settings that apply to all nodes that are part of the local mesh.

For proper operation you should configure only one node as the policy manager. Setting more than one node as the policy manager will prevent policies from being properly implemented.

Although the policy manager can be any node, it is strongly recommended that you make the master node the policy manager.

When the local mesh is established, all nodes search for the policy manager and report to it.

Enforce node limit

This policy lets you limit the total number of nodes that can make up a local mesh. When the node limit is reached, additional nodes will not be able to join the local mesh.

This policy is primarily intended to be used in train applications to prevent unwanted connections from neighboring train cars. For example, if there are eight cars in a train and two APs in each car, except for the first one, there are a total of 15 APs in the train. By setting the node limit policy to 15 nodes, when the 15 nodes in the train's local mesh are connected together, then no more nodes will be allowed to join the mesh.

Addressing

Static

Use this option to create simple back-to-back links between two APs. When creating static links, both APs must be operating on the same wireless channel. Make sure that the channel selection on the **Wireless > Radio(s)** page is not set to **Automatic**.

- **Remote MAC address:** MAC address of the radio on the remote AP on which the link will be established.
- **Local MAC address:** MAC address of the radio on this AP on which the link will be established.

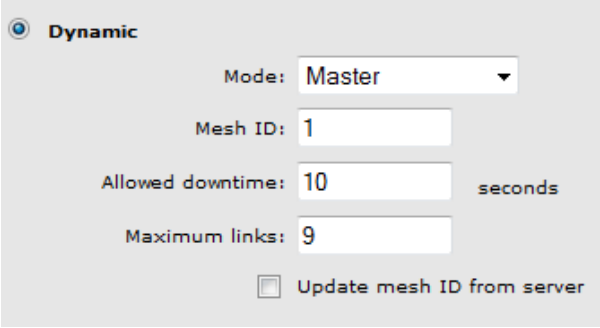
Dynamic

Use this option to create dynamic local mesh installations.

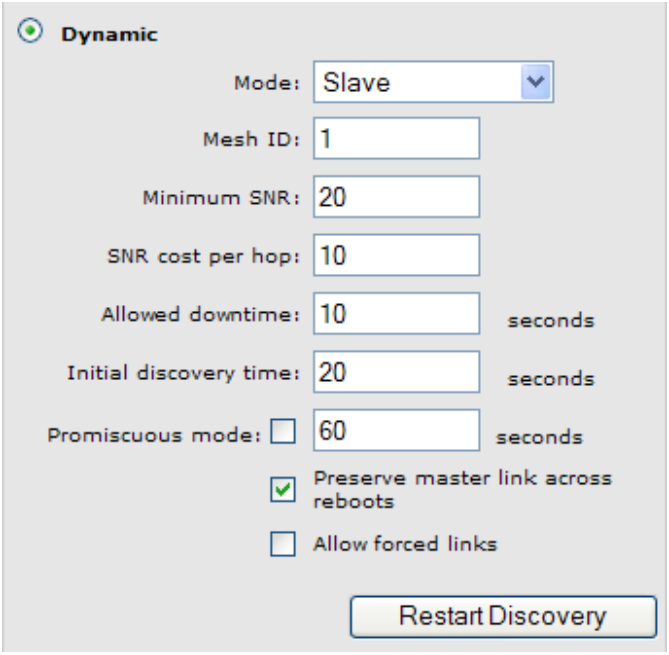
Mode

Three different roles can be assigned to a node: master, alternate master, or slave. The role assigned to a node, governs how the node will establish upstream or downstream links with its peers. The available configuration settings change depending on the role that is selected.

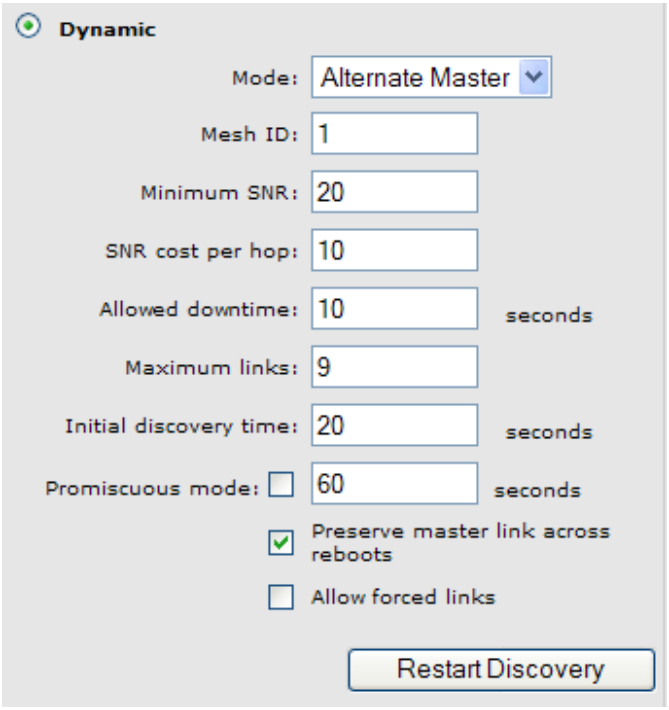
- **Master:** The master is the root node that provides the upstream connection to the *ground network* that the other nodes want to reach. The master will only create downstream links to alternate master or slave nodes.



- **Slave:** Slave nodes can only establish upstream links with master or alternate master nodes. Slave nodes cannot establish downstream links with any 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 link 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.

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.

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.

Maximum links

(Master or alternate master nodes only)

The maximum number of upstream and downstream links that this node can support.

Update mesh ID from server

(Master only)

When this option is enabled, every time the node restarts, it retrieves the configuration file defined under **Scheduled operations** on the **Maintenance > Config file management** page. If the retrieved configuration file is different from the current configuration, the node loads the retrieved configuration.

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.

Maximum links

The maximum number of upstream and downstream links that this node can support.

Promiscuous mode

(Alternate master or slave nodes)

Although it could be used in other applications, the promiscuous mode is primarily intended to solve issues specific to local mesh networks aboard trains. The main issue that it addresses is train configuration changes. When a car is taken out for maintenance and replaced with a new one, the AP in that new car will not be able to connect to the train local mesh network because it is configured with a different mesh ID. This is where the promiscuous mode comes into play. Its goal is to allow a node to connect to a different mesh when it could not find any available master (alt-master) in its mesh for a certain, configurable, amount of time.

When a node joins a new mesh, it is considered to be the consequence of a car change (or replacement of an AP). This event triggers the following actions:

- The node software is updated, given that a software update URL is configured.
- The node configuration is updated, given that a configuration file URL is configured. This will consequently change the node mesh ID to the one found in the configuration file. If no configuration file URL is provided, the node will immediately proceed with updating its mesh ID.
- An SNMP trap is sent.

After completing a configuration or software download, a local mesh node will wait an additional 30 seconds before rebooting if a downstream link was established with another node in promiscuous mode. The purpose of this delay is to give downstream nodes some more time to download their software and configuration, improving the total convergence time of an entire train network after a master car change.

Preserve master link across reboots

(Alternate master or slave nodes)

When this option is enabled, the AP will first try re-connecting to the master (alt-master) it was connected to before rebooting (or disabling/re-enabling the profile). This re-connection happens during the initial discovery time. After that period, the regular best master identification mechanism will take over.

Allow forced links

(Alternate Master, Slave only)

When enabled, the node will accept any connection forced from a master and it will change its mesh ID in order to use the master mesh ID.

Allow forced links

(Alternate master or slave nodes)

This option allows the AP to accept forced links from a master (alt-master). A link is forced from the master by using the force link button next to the slave`s entry in the local mesh scan. A link can be forced to a slave (alt-master) in a different mesh. This will cause the slave to save the new mesh ID and use it from that point onward.

Update mesh ID from server

(Master nodes only)

This is similar to promiscuous mode, but for a master. It is primary used in train application. When this option is enabled, the master will check if the mesh ID in the configuration file on the server is the same as the mesh ID locally configured. The server (and configuration file name) is specified in the URL located in **Maintenance > Config file management > Scheduled operations**.

This allows a master AP to be replaced without changing the mesh ID of a train and without having to configure that AP to use this mesh ID. The mesh ID is stored on the server.

Restart Discovery

(Alternate master or slave nodes)

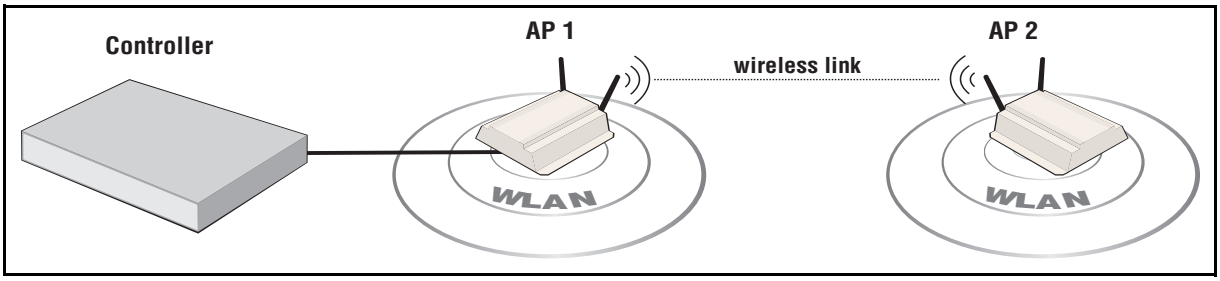
This button tells the AP to bring down any link it has already established and restart looking for the best master to which it can connect. It can be used when a new master is installed close to a slave and you want the slave to connect to that master, without rebooting.

Sample local mesh deployments

RF extension

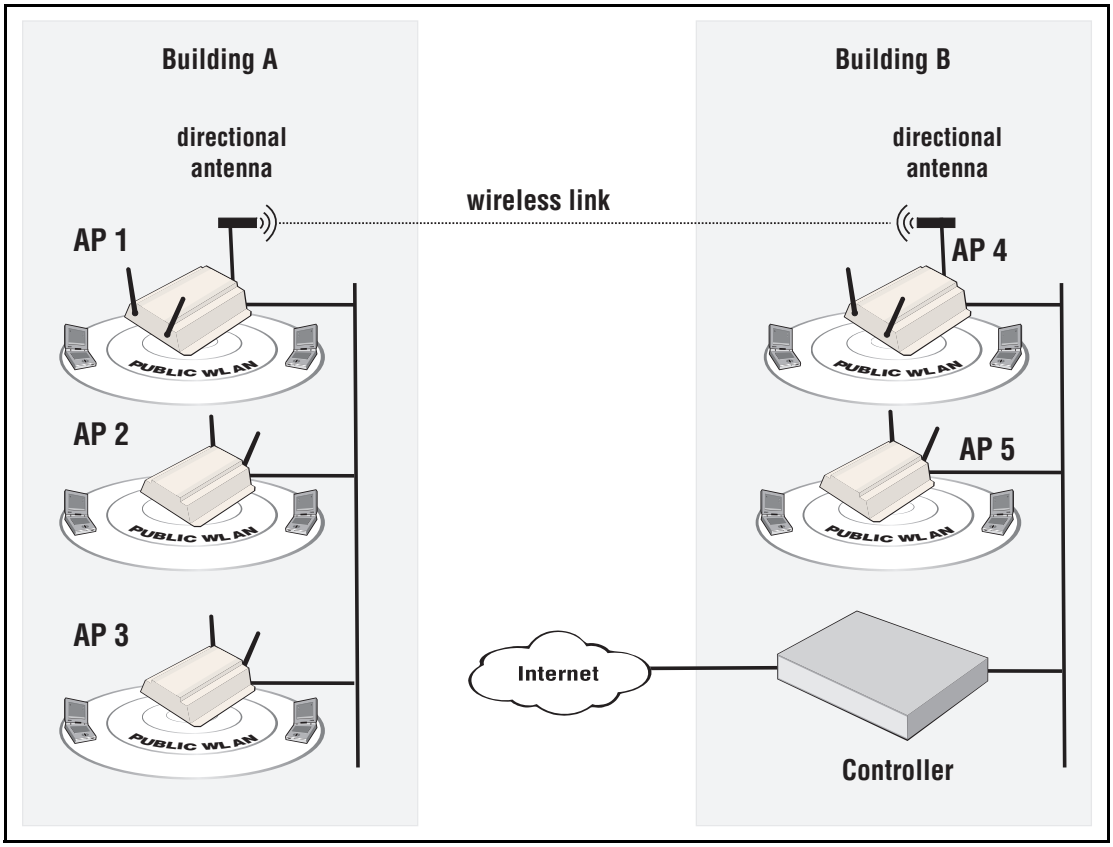
Local mesh provides an effective solution for extending wireless coverage in situations where it is impractical or expensive to run cabling to an AP.

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 connections

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.

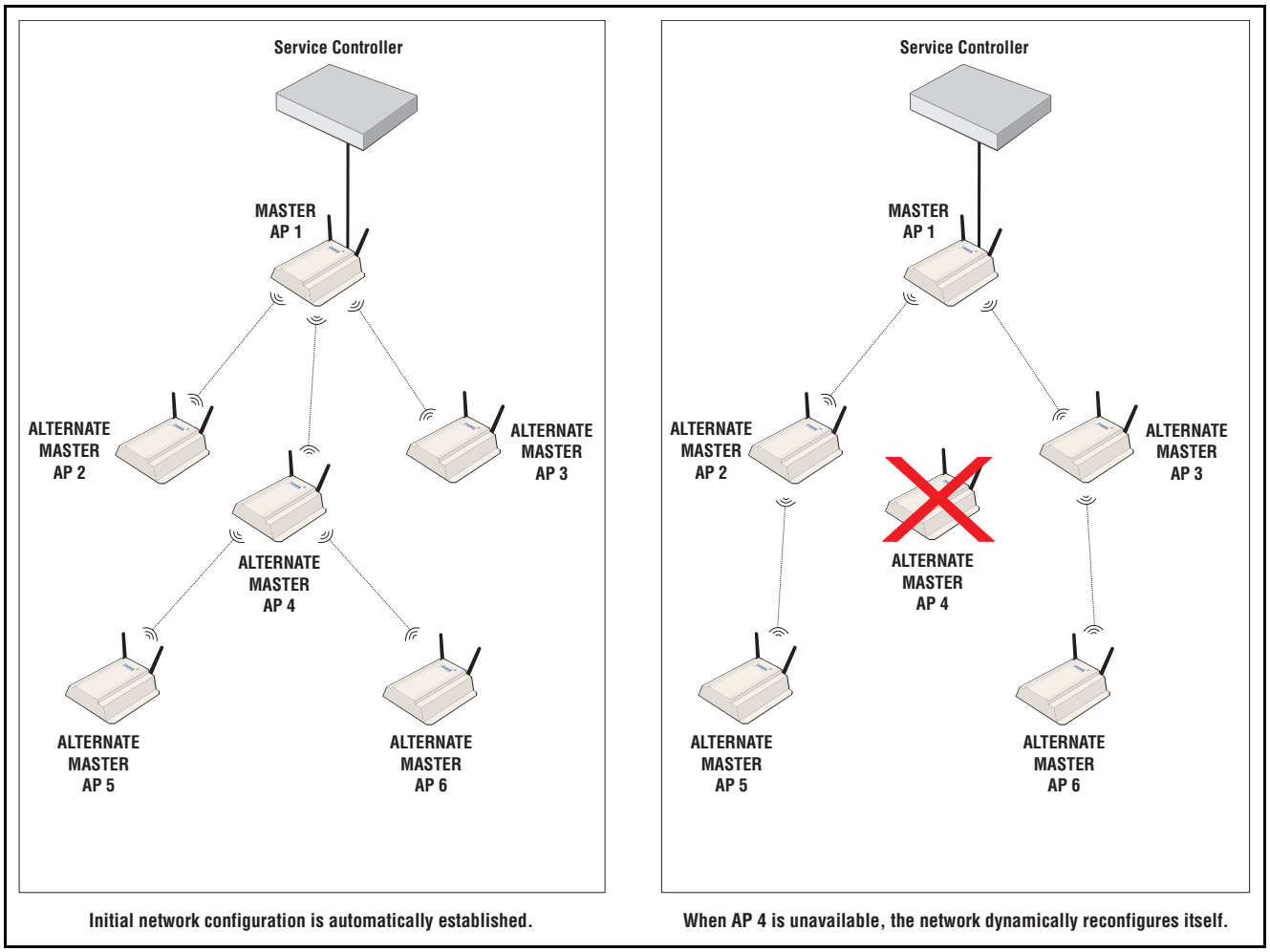


Dynamic networks

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.



8

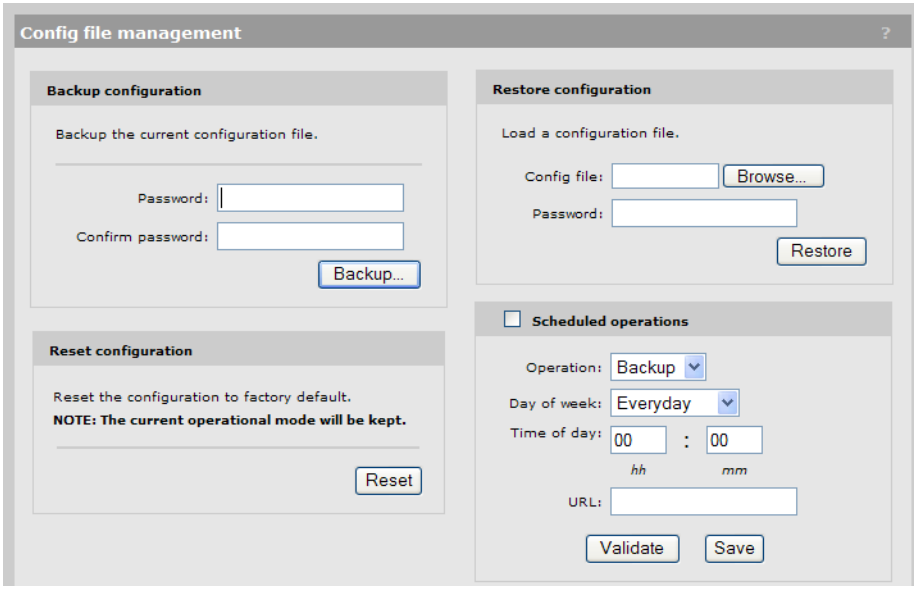
Maintenance

Contents

Config file management

The configuration file contains all the settings that customize the operation of the AP. You can save and restore the configuration file manually or automatically.

Select **Maintenance > Config file management**.



Manual configuration file management

The following options are available for manual configuration file management.

Backup configuration

The **Backup configuration** feature enables you to back up your configuration settings so that they can be easily restored in case of failure. You can also use this option if you want to directly edit the configuration file.

Before you install new software, you should always back up your current configuration. Select **Backup** to start the process. You are prompted for the location in which to save 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 *Resetting to factory defaults on page D-1*.

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 AP or if you are managing several APs from a central site.

Use the following steps to restore a saved configuration file.

1. Select **Maintenance > Config file management.** The **Config file management** page opens.
2. Under **Restore configuration,** select **Browse** to navigate to and select the configuration file that you want to restore.
3. If the configuration file is protected with a password you must supply the correct password to restore the complete configuration. If you supply an invalid password, all settings are restored except for certificates and private keys.
4. Select **Restore** to load the selected file**.**

Note The AP automatically restarts when once the configuration file has been loaded.

Scheduled operations

The **Scheduled operations** feature enables you to schedule unattended backups or restorations of the configuration file.

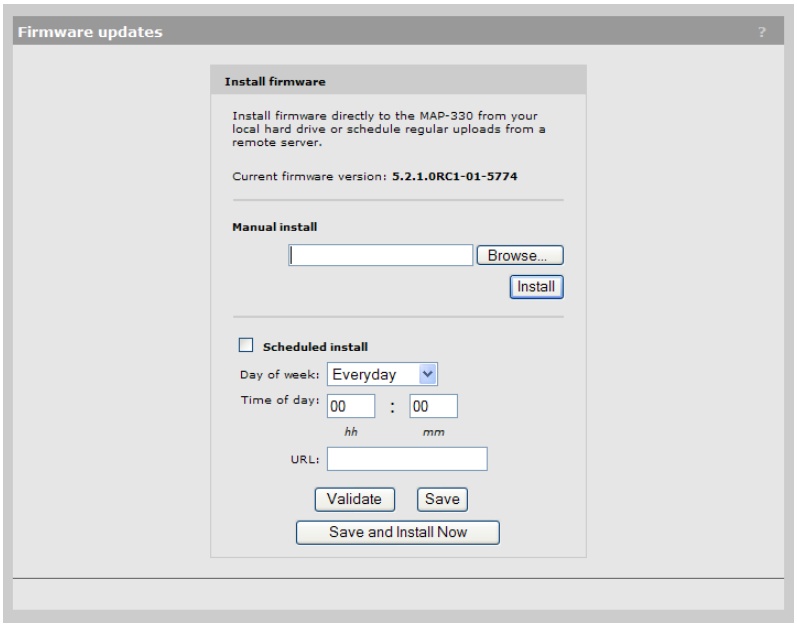
Use the following steps to schedule a backup or restoration of the configuration file.

1. Select **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

To update AP software, select **Maintenance > Firmware updates**.



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. See *Manual configuration file management on page 8-2*.
- At the end of the update process, the AP automatically restarts, causing all users to be disconnected. Once the AP resumes operation, all users must reconnect. To minimize network disruption, use the scheduled install option to have updates performed outside of peak usage hours.
- When using a controller in conjunction with one or more autonomous APs, you must (1) always update the controller before updating the APs, and (2) never load an earlier software version on the APs than is installed on the controller.

Performing an immediate software update

To update the AP software now, **Browse** to the software file (extension .cim) and then select **Install.**

Performing a scheduled update

The AP can automatically retrieve and install software from a local or 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.

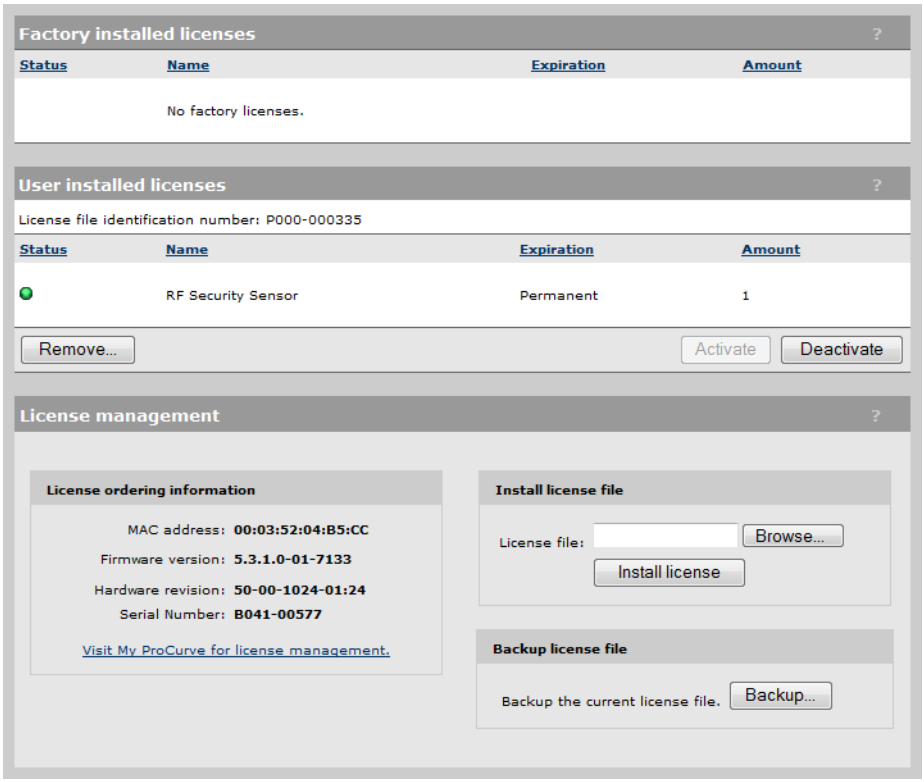
Licenses

Applicable only to the MSM335, MSM320, and MSM320-R.

On some APs, certain features are activated by installation of optional licenses. For example, the RF Security sensor feature requires a license. Such features are only enabled when a valid license is installed.

If you purchased an optional-feature license at original AP purchase time, the license is factory-installed. Feature licenses purchased later must be installed manually.

Select **Maintenance > Licenses**. An example from the MSM320 is shown.



Factory installed licenses

This table lists all licenses that were installed on the AP 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

When an AP is reset to factory default settings, all user-installed licenses are deactivated to ensure a true factory-default configuration. You must manually enable these licenses once the AP has restarted. (Factory-installed licenses are always active.)

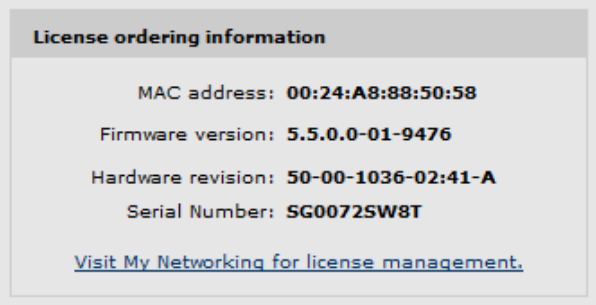
Generating and installing a feature license

When you purchase an optional feature license, a physical license registration card is shipped to you. License registration cards are not matched to your AP until you go to the **My Networking** portal and generate a license file for a specific AP.

Once you receive your license registration card, follow this procedure to generate and install a feature license on your AP.

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 AP already on file, open its management tool in a separate Web browser window, and select **Maintenance > Licenses.** Under **License ordering information**, copy the **MAC address** onto your clipboard. For example:



5. Back on the My Networking portal Web page, paste or type the MAC address of your AP in the **MAC Address** field.
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.

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 AP, go back to the AP management tool and do the following:

1. Select **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

Console ports

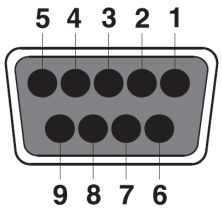
Contents

Console port connector specifications

The console ports are wired as described in this section.

MSM335 and MSM422 console port

The MSM335 and MSM422 provide a DB-9 (female) console (serial) port connector. The DB-9 connector (DCE) has pin assignments as follows:

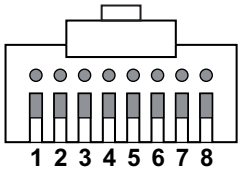
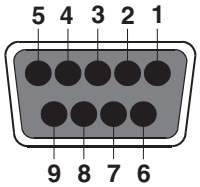
Pin	Signal	Direction	Connector
1	DCD	→ to PC	
2	RXD	→ to PC	
3	TXD	← from PC	
4	DTR	← from PC	
5	GND		
6	DSR	→ to PC	
7	RTS	← from PC	
8	CTS	→ to PC	
9	Unused		

DB-9 (female)

To connect to a computer, use a standard (straight-through) serial cable (male-to-female).

MSM410, E-MSMS430, E-MSM460, E-MSM466 console port

These APs provide an RJ-45 console (serial) port connector. Use an RJ-45 to DB-9 adapter cable (not supplied) with an RJ-45 (male) connector on one end and a DB-9 (female) connector on the other end. Wire the cable as follows:

RJ-45 (male)	Pins	Signal	Direction	Pins	DB-9 (female)
	1	CTS	to PC	8	
	2	DSR	to PC	6	
	3	TXD	from PC	3	
	4	GND			
	5	GND		5	
	6	RXD	to PC	2	
	7	DTR	from PC	4	
	8	RTS	from PC	7	

Note The DSR and DTR signals are only supported on the MSM410.

B

Regulatory information

Contents

Notice for U.S.A.

Manufacturer's FCC Declaration of Conformity Statement

Manufacturer: Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1185 USA

For questions regarding this declaration, contact the Product Regulations Manager at the above address or phone number.

FCC Class B statement

(Applies to: MSM310, MSM310-R, MSM320, MSM325, MSM320-R, MSM335, MSM422, E-MSM430, E-MSM460, and E-MSM466.)

This FCC Class B device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: 1) this device may not cause harmful interference, and 2) this device must accept any interference received, including interference that may cause undesired operation.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These 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 on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

The FCC requires the user to be notified that any changes or modifications made to the device that are not expressly approved by the Hewlett-Packard Company may void the user's authority to operate the equipment.

FCC Class A statement

(Applies to: MSM410)

This is an FCC Class A device. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

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 harmful 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 harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Warning

Exposure to Radio Frequency Radiation

The radiated output power of this device is below the FCC radio exposure limits. Nevertheless, the device should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antennas should not be less than 20 cm (8 inches) during normal operation.

Notice for Canada

For MSM310, MSM310-R, MSM320, MSM325, MSM320-R, MSM335, MSM422, E-MSM430, E-MSM460, and E-MSM466:

- This device complies with the limits for a Class B digital device and conforms to Industry Canada standard ICES-003. Products that contain a radio transmitter comply with Industry Canada standard RSS210 and are labeled with an IC approval number.
- Cet appareil numérique de la classe B est conforme à la norme ICES-003 de Industry Canada. La radio sans fil de ce dispsitif est conforme à la certification RSS 210 de Industry Canada et est étiquetée avec un numéro d'approbation IC.
- This device complies with the Class B limits of Industry Canada. Operation is subject to the following two conditions: 1) this device may not cause harmful interference, and 2) this device must accept interference received, including interference that may cause undesired operation.

For MSM410:

- This is an FCC Class A device. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.
- This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la Classe A est conforme à la norme NMB-003 du Canada.

To reduce potential radio interference with other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

Notice for the European Community

This device complies with the EMC Directive 2004/108/EC, Low Voltage Directive 2006/95/EC and R&TTE Directive 1999/5/EC. Compliance with these directives implies conformity to harmonized European standards (European Norms) that are listed on the EU Declaration of Conformity that has been issued by HP for this device.

See also *DOCs for the European Community on page B-6*.

Countries of Operation & Conditions of Use

This device may be used in the following EU and EFTA countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom. Requirements for indoor vs. outdoor operation, licensing and allowed channels of operation apply in some countries as described below.

Note

The user must use the configuration utility provided with this device to ensure the channels of operation are in conformance with the spectrum usage rules for EU and EFTA countries as described below.

2.4 GHz Operation

- This device may be operated indoors or outdoors in all EU and EFTA countries using the 2.4 GHz band (Channels 1 - 13), except where noted below.
- In **France**, this device may use the entire 2400 - 2483.5 MHz band (Channels 1 through 13) for indoor applications. For outdoor use, only the 2400 - 2454 MHz frequency band (Channels 1 through 9) may be used. For the latest requirements, see http://www.art-telecom.fr.

  L'utilisation de cet equipement (2.4 GHz wireless LAN) est soumise à certaines restrictions: cet equipement peut être utilisé à l'interieur d'un batiment en utilisant toutes les frequences de 2400 a 2483.5 MHz (Chaine 1-13). Pour une utilisation en environnement exterieur, vous devez utiliser les frequencies comprises entre 2400 a 2454-MHz (Chaine 1-9). Pour les dernières restrictions, voir http://www.art-telecom.fr.

5 GHz Operation

- This device requires the user or installer to properly enter the **current country of operation** in the 5 GHz Radio Configuration Window.
- This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other systems. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this guide.

- This device employs **a radar detection feature** required for European Community and EFTA country operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community or EFTA country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.
- This device is restricted to **indoor** use when operated in EU and EFTA countries using the 5.15-5.35 GHz band (Channels 36, 40, 44, 48, 52, 56, 60 and 64). See the table below for the allowed 5 GHz channels in each band.

Operation Using 5 GHz Channels in the European Community

The user/installer must use the provided configuration utility to check the current channel of operation and make necessary configuration changes to ensure operation occurs in conformance with European National spectrum usage laws as described below and elsewhere in this guide.

Frequency Band (MHz)	Allowed Channels	Usage	Maximum EIRP (mW)
5150 - 5250	36, 40, 44, 48	Indoor use only	200
5250 - 5350	52, 56, 60, 64	Indoor use only	200
5470 - 5725	100, 104, 108, 112, 116, 132, 136, 140.	Indoor or outdoor use	1000

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.

Supported External Antennas

For antenna information, consult *Appendix C: Connecting external antennas on page C-1*.

Notice for Brazil, Aviso aos usuários no Brasil

Este equipamento opera em caráter secundário, isto é, não tem direito à proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Notice for Taiwan

DGT LPD (Low Power Device) Statement

低功率電波輻射性電機管理辦法

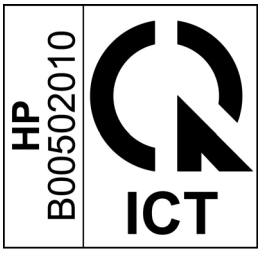
第十四條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十七條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Notice for Vietnam

HP Type Approval License:



DOCs for the European Community

The following DOCs (Declarations of Conformity) apply to the European Community.

DECLARATION OF CONFORMITY

according to ISO/IEC 17050-1 and EN 17050-1

DoC #: MRLBB-0901-09

Supplier's Name: Hewlett-Packard Company

Manufacturer's Address: 8000 Foothills Blvd., Roseville, CA 95747 U.S.A.

declares, that the product

Product Name: HP E-MSM310,E-MSM313 Access Point

Product Number(s): J9379B, J9350B

Regulatory Model No: MRLBB-0901

Product Options: J8441A, J8444A, J8997A, J8999A, J9401A, J9405A/B, J9407A

conforms to the following Product Specifications:

Safety: IEC 60950-1:2005 / EN 60950-1:2006

EMC: EN 55022:2006 Class B
EN 55011:1998 +A1:1999 +A2:2002
EN 60601-1-2:2007
EN 50121-3-2:2001

Telecom: EN 300 328 V1.7.1 (2006-10)
EN 301 893 V1.5.1 (2008-12)
EN 301 489-17 V2.1.1 (2009-05)

Health: EN 50385:2002

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EEC and the R&TTE Directive 1999/5/EC and carries the CE marking accordingly.

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is MRLBB-0901. The RMN should not be confused with the marketing name or Product Numbers.

This product includes an integral wireless radio module, model CM9.

Roseville, October 14, 2010

Michael E. Avery, Regulatory Engineering Mgr

Local contact for regulatory information:

EMEA: Hewlett-Packard GmbH, HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen, Germany
www.hp.com/go/certificates

U.S.: Hewlett-Packard, 3000 Hanover St., Palo Alto, CA 94304, U.S.A. 650-857-1501

DECLARATION OF CONFORMITY

according to ISO/IEC 17050-1 and EN 17050-1

DoC #: MRLBB-0902-08

Supplier's Name: Hewlett-Packard Company

Manufacturer's Address: 8000 Foothills Blvd., Roseville, CA 95747 U.S.A.

declares, that the product

Product Name: HP E-MSM320, E-MSM325 Access Point

Product Number(s): J9364B, J9373B

Regulatory Model No: MRLBB-0902

Product Options: J8441A, J8444A, J8997A, J8999A, J9401A, J9405A/B, J9407A

conforms to the following Product Specifications:

Safety: IEC 60950-1:2005 / EN 60950-1:2006

EMC: EN 55022:2006 Class B
EN 55011:1998 +A1:1999 +A2:2002
EN 60601-1-2:2007
EN 50121-3-2:2001

Telecom: EN 300 328 V1.7.1 (2006-10)
EN 301 893 V1.5.1 (2008-12)
EN 301 489-17 V2.1.1 (2009-05)

Health: EN 50385:2002

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EEC and the R&TTE Directive 1999/5/EC and carries the CE marking accordingly.

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is MRLBB-0902. The RMN should not be confused with the marketing name or Product Numbers.

This product includes an integral wireless radio module, model CM9.

Roseville, October 14, 2010

Michael E. Avery, Regulatory Engineering Mgr

Local contact for regulatory information:

EMEA: Hewlett-Packard GmbH, HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen, Germany
www.hp.com/go/certificates

U.S.: Hewlett-Packard, 3000 Hanover St., Palo Alto, CA 94304, U.S.A. 650-857-1501

DECLARATION OF CONFORMITY
according to ISO/IEC 17050-1 and EN 17050-1

DoC #: MRLBB-0904-06

Supplier's Name: Hewlett-Packard Company
Manufacturer's Address: 8000 Foothills Blvd., Roseville, CA 95747 U.S.A.

declares, that the product

Product Name: HP E-MSM310-R Access Point
Product Number(s): J9383B
Regulatory Model No: MRLBB-0904

conforms to the following Product Specifications:

Safety: IEC 60950-1:2005 / EN 60950-1:2006

EMC: EN 55022:1998 +A1:2000 +A2:2003, Class B
EN 55011:1998 +A1:1999 +A2:2002
EN 60601-1-2:2001
EN 50121-3-2:2001

Telecom: EN 300 328 V1.7.1 (2006-10)
EN 301 893 V1.5.1 (2008-12)
EN 301 489-17 V2.1.1 (2009-05)

Health: EN 50385:2002

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EEC and the R&TTE Directive 1999/5/EC and carries the CE marking accordingly.

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is MRLBB-0904. The RMN should not be confused with the marketing name or Product Numbers.

This product includes an integral wireless radio module, model CM9.

Roseville, October 15, 2010

Michael E. Avery, Regulatory Engineering Mgr

Local contact for regulatory information:

EMEA: Hewlett-Packard GmbH, HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen, Germany
www.hp.com/go/certificates

U.S.: Hewlett-Packard, 3000 Hanover St., Palo Alto, CA 94304, U.S.A. 650-857-1501

DECLARATION OF CONFORMITY

according to ISO/IEC 17050-1 and EN 17050-1

DoC #: MRLBB-0903-05

Supplier's Name: Hewlett-Packard Company

Manufacturer's Address: 8000 Foothills Blvd., Roseville, CA 95747 U.S.A.

declares, that the product

Product Name: HP E-MSM320-R Access Point

Product Number(s): J9368B

Regulatory Model No: MRLBB-0903

conforms to the following Product Specifications:

Safety: IEC 60950-1:2005 / EN 60950-1:2006

EMC: EN 55022:2006, Class B
EN 55011:1998 +A1:1999 +A2:2002
EN 60601-1-2:2007
EN 50121-3-2:2001

Telecom: EN 300 328 V1.7.1 (2006-10)
EN 301 893 V1.5.1 (2008-12)
EN 301 489-17 V2.1.1 (2009-05)

Health: EN 50385:2002

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EEC and the R&TTE Directive 1999/5/EC and carries the CE marking accordingly.

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is MRLBB-0903. The RMN should not be confused with the marketing name or Product Numbers.

This product includes an integral wireless radio module, model CM9.

Roseville, October 14, 2010

Michael E. Avery, Regulatory Engineering Mgr

Local contact for regulatory information:

EMEA: Hewlett-Packard GmbH, HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen, Germany
www.hp.com/go/certificates

U.S.: Hewlett-Packard, 3000 Hanover St., Palo Alto, CA 94304, U.S.A. 650-857-1501

DECLARATION OF CONFORMITY

according to ISO/IEC 17050-1 and EN 17050-1

DoC #: MRLBB-0910-05

Supplier's Name: Hewlett-Packard Company

Manufacturer's Address: 8000 Foothills Blvd., Roseville, CA 95747 U.S.A.

declares, that the product

Product Name: HP E-MSM335 Access Point

Product Number(s): J9357B

Regulatory Model No: MRLBB-0910

Product Options: J8441A, J8444A, J8997A, J8999A, J9401A, J9406A, J9407A

conforms to the following Product Specifications:

Safety: IEC 60950-1:2005 / EN 60950-1:2006

EMC: EN 55022:1998 +A1:2000 +A2:2003, Class A
EN 60601-1-2:2007
EN 50121-3-2:2001

Telecom: EN 300 328 V1.7.1 (2006-10)
EN 301 893 V1.5.1 (2008-12)
EN 301 489-17 V2.1.1 (2009-05)

Health: EN 50385:2002

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EEC and the R&TTE Directive 1999/5/EC and carries the CE marking accordingly.

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is MRLBB-0910. The RMN should not be confused with the marketing name or Product Numbers.

This product includes an integral wireless radio module, model CM9.

Roseville, October 15, 2010

Michael E. Avery, Regulatory Engineering Mgr

Local contact for regulatory information:

EMEA: Hewlett-Packard GmbH, HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen, Germany
www.hp.com/go/certificates

U.S.: Hewlett-Packard, 3000 Hanover St., Palo Alto, CA 94304, U.S.A. 650-857-1501

DECLARATION OF CONFORMITY

according to ISO/IEC 17050-1 and EN 17050-1

DoC #: MRLBB-0802-08

Supplier's Name: Hewlett-Packard Company

Manufacturer's Address: 200 Forest Street, Marlborough, MA 01752-3085 U.S.A.

declares, that the product

Product Name: HP E-MSM410 Access Point

Product Number(s): J9427A, J9427B, J9626A

Regulatory Model No: MRLBB-0802

conforms to the following Product Specifications:

Safety: IEC 60950-1:2005 / EN 60950-1:2006

EMC: EN 55022:2006
EN 60601-1-2:2007

Telecom: EN 300 328 V1.7.1 (2006-10)
EN 301 893 V1.5.1 (2008-12)
EN 301 489-17 V2.1.1 (2009-05)

Health: EN 50385:2002

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EEC and the R&TTE Directive 1999/5/EC and carries the CE marking accordingly.

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is MRLBB-0802. The RMN should not be confused with the marketing name or Product Numbers.

This product includes an integral wireless radio module, model DNMA-83.

Roseville, October 15, 2010

Michael E. Avery, Regulatory Engineering Mgr

Local contact for regulatory information:

EMEA: Hewlett-Packard GmbH, HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen, Germany
www.hp.com/go/certificates

U.S.: Hewlett-Packard, 3000 Hanover St., Palo Alto, CA 94304, U.S.A. 650-857-1501

DECLARATION OF CONFORMITY

according to ISO/IEC 17050-1 and EN 17050-1

DoC #: MRLBB-0909-07

Supplier's Name: Hewlett-Packard Company

Manufacturer's Address: 8000 Foothills Blvd., Roseville, CA 95747 U.S.A.

declares, that the product

Product Name: HP E-MSM422 Access Point

Product Number(s): J9359B, J9617A

Regulatory Model No: MRLBB-0909

Product Options: J8441A, J8444A, J8997A, J8999A, J9401A, J9406A, J9407A

conforms to the following Product Specifications:

Safety: IEC 60950-1:2005 / EN 60950-1:2006

EMC: EN 55022:1998 +A1:2000 +A2:2003, Class B
EN 60601-1-2:2007
EN 50121-3-2:2001

Telecom: EN 300 328 V1.7.1 (2006-10)
EN 301 893 V1.5.1 (2008-12)
EN 301 489-17 V2.1.1 (2009-05)

Health: EN 50385:2002

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EEC and the R&TTE Directive 1999/5/EC and carries the CE marking accordingly.

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is MRLBB-0909. The RMN should not be confused with the marketing name or Product Numbers.

This product includes integral wireless radio modules, models CM9 and DNMA-83.

Roseville, October 15, 2010

Michael E. Avery, Regulatory Engineering Mgr

Local contact for regulatory information:

EMEA: Hewlett-Packard GmbH, HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen, Germany
www.hp.com/go/certificates

U.S.: Hewlett-Packard, 3000 Hanover St., Palo Alto, CA 94304, U.S.A. 650-857-1501

DECLARATION OF CONFORMITY

according to ISO/IEC 17050-1 and EN 17050-1

DoC #: MRLBB-1001-03

Supplier's Name: Hewlett-Packard Company

Manufacturer's Address: 8000 Foothills Blvd., Roseville, CA 95747 U.S.A.

declares, that the product

Product Name: HP E-MSM430 Dual Radio 802.11n AP
HP E-MSM460 Dual Radio 802.11n AP

Product Number(s): J9651A, J9653A
J9591A, J9618A

Regulatory Model No: MRLBB-1001

Product Options: N/A

conforms to the following Product Specifications:

Safety: IEC 60950-1:2005 / EN 60950-1:2006 +A11:2009

EMC: EN 55022:2006 +A1:2007, Class B
EN 60601-1-2:2007

Telecom: EN 300 328 V1.7.1 (2006-10)
EN 301 893 V1.5.1 (2008-12)
EN 301 489-17 V2.1.1 (2009-05)
EN 62311:2008

Energy Use: Regulation (EC) No. 1275/2008

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EEC and the R&TTE Directive 1999/5/EC and carries the CE marking accordingly.

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is MRLBB-1001. The RMN should not be confused with the marketing name or Product Numbers.

This product includes integral wireless radio modules, model MRLBB-1003.

Roseville, November 29, 2010

Michael E. Avery, Regulatory Engineering Mgr

Local contact for regulatory information:

EMEA: Hewlett-Packard GmbH, HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen, Germany
www.hp.com/go/certificates

U.S.: Hewlett-Packard, 3000 Hanover St., Palo Alto, CA 94304, U.S.A. 650-857-1501

DECLARATION OF CONFORMITY

according to ISO/IEC 17050-1 and EN 17050-1

DoC #: MRLBB-1002-03

Supplier's Name: Hewlett-Packard Company

Manufacturer's Address: 8000 Foothills Blvd., Roseville, CA 95747 U.S.A.

declares, that the product

Product Name: HP E-MSM466 Dual Radio 802.11n AP

Product Number(s): J9622A, J9619A

Regulatory Model No: MRLBB-1002

Product Options: J9169A, J9170A, J9171A, J9659A

conforms to the following Product Specifications:

Safety: IEC 60950-1:2005 / EN 60950-1:2006 +A11:2009

EMC: EN 55022:2006 +A1:2007, Class B
EN 60601-1-2:2007

Telecom: EN 300 328 V1.7.1 (2006-10)
EN 301 893 V1.5.1 (2008-12)
EN 301 489-17 V2.1.1 (2009-05)
EN 62311:2008

Energy Use: Regulation (EC) No. 1275/2008

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EEC and the R&TTE Directive 1999/5/EC and carries the CE marking accordingly.

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is MRLBB-1002. The RMN should not be confused with the marketing name or Product Numbers.

This product includes integral wireless radio modules, model MRLBB-1003.

Roseville, November 29, 2010

Michael E. Avery, Regulatory Engineering Mgr

Local contact for regulatory information:

EMEA: Hewlett-Packard GmbH, HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen, Germany
www.hp.com/go/certificates

U.S.: Hewlett-Packard, 3000 Hanover St., Palo Alto, CA 94304, U.S.A. 650-857-1501

C

Connecting external antennas

Contents

Introduction

Caution

This appendix provides mandatory radio power-level settings that must be configured to ensure that your device complies with regulatory requirements in your region. Depending on the country of use, the antenna selected, and your radio settings, it may be mandatory to reduce the radio transmission power level to maintain regulatory compliance. For specific power limits for your country, consult the Antenna Power-Level Setting Guide (for MSM Products) available from www.hp.com/networking/support.

This appendix applies to you if you use any of the HP antennas discussed in this appendix with HP MSM access points.

Guides for the antennas discussed in this appendix are available online from: www.hp.com/networking/support. For **Product Brand**, select **ProCurve**.

802.11n MIMO antennas for the E-MSM466

These four 802.11n MIMO antennas are certified only for use with the E-MSM466 Access Point:

Part	Type	Band	Gain	Use	Elements
J9171A	Omni-directional	2.4/5GHz	3/4dBi	Indoor	3
J9659A	Omni-directional	2.4/5GHz	1.5/5dBi	Indoor	6
J9169A	Narrow Beam Sector	2.4/5GHz	8/10.7dBi	Outdoor (Indoor)	3
J9170A	Directional	2.4/5GHz	10.9/13.5dBi	Outdoor (Indoor)	3

Caution

Antennas J9169A and J9170A
In the European Community, these antennas can only be used in the 5470-5725 MHz band. In the USA, these antennas can be only be used in the 5725-5850 MHz band.

802.11a/b/g antennas for MSM APs

Antennas included with MSM310, MSM310-R, MSM320, and MSM320-R

Included with	Antenna Type	Antenna Band (GHz)			
		2.4	5.15 - 5.35	5.47 - 5.725	5.725 - 5.850
MSM310 & MSM320 (J9401A)	Omni	2.5 dBi	3.0 dBi	3.4 dBi	3.4 dBi
MSM310-R & MSM320-R	Omni	5.6 dBi	N/A	NA	N/A

Caution

When using antennas outdoors, a lightning arrestor is required for lightning protection. Consider placing the lightning arrestor immediately before the antenna cable enters the building. HP offers a lightning arrestor as an accessory, HP product number J8996A.

All HP devices are designed to be compliant with the rules and regulations in locations they are sold and will be labeled as required. Any changes or modifications to HP equipment, not expressly approved by HP, could void the user's authority to operate this device. Use only antennas approved for use with this device. Unauthorized antennas, modifications, or attachments could cause damage and may violate local radio regulations in your region.

Optional 802.11a/b/g antennas for MSM APs

These four optional 802.11a/b/g antennas are certified for use with these MSM APs:

AP	Freq. Band	Antenna			
		4.4 dBi 2.4GHz (J8441A)	7.4 dBi 2.4GHz (J8444A)	3/4 dBi Dual Band (J8997A)	6.9/7.7 dBi Dual Band (J8999A)
MSM310	2.4	Y	Y	Y	Y
	5			Y	Y
MSM310-R	2.4	Y	Y	Y	Y
	5			Y	Y
MSM320 and MSM325	2.4	Y	Y	Y	Y
	5			Y	Y
MSM320-R	2.4	Y	Y	Y	Y
	5			Y	Y
MSM335	2.4	Y	Y	Y	Y
	5			Y	Y
MSM422 Radio 2	2.4	Y	Y		Y
	5				Y
MSM422 Radio 1	2.4				
	5				

Y=Yes, supported.

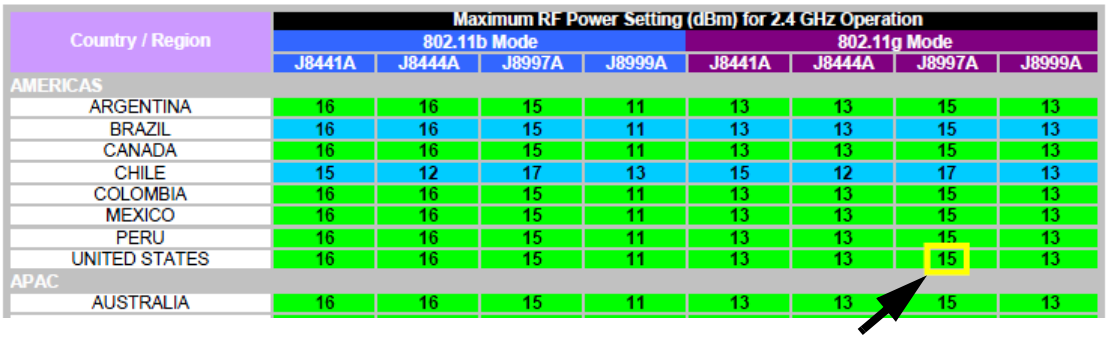
Antenna Notes:

- **4.4 dBi 2.4GHz Indoor/ Outdoor Omnidirectional antenna (J8441A)** is a high-performance omnidirectional collinear antenna used for 2.4 GHz RF-distribution systems. Its flattened radiation pattern focuses energy along the horizontal plane to provide extended coverage in large rooms or vaulted areas. It may also be pole-mounted.
- **7.4 dBi 2.4GHz Outdoor Omnidirectional antenna (J8444A)** is a mast-mounted antenna.
- **3/4 dBi Dual Band Diversity indoor antenna (J8997A, indoor only)** is a ceiling-mounted spatial omnidirectional array. Two independent vertically polarized radiators provide null-free omnidirectional coverage for meeting rooms, offices, or other enclosed spaces.
- **6.9/7.7 dBi Dual Band Directional antenna (J8999A, indoor / outdoor)** is a directional patch array enclosed in a UV-stable weatherproof radome. The focused radiation pattern may be used to extend point-to-point link coverage or to provide targeted sector coverage.

Radio power-level setting example

You need to get the *HP Antennas Power-Level Setting Guide* available online from: www.hp.com/networking/support. Search for the part number of your antenna.

In this example, an optional HP antenna J8997A is to be used on an autonomous MSM AP configured for 802.11g in the USA. Per the Maximum RF Power Setting chart screenshot below, the intersection of row **UNITED STATES** and column **802.11g Mode/J8997A**, indicates that the maximum radio power level is **15 dBm**. (Please check the actual charts in the *HP Antennas Power-Level Setting Guide* for current values).

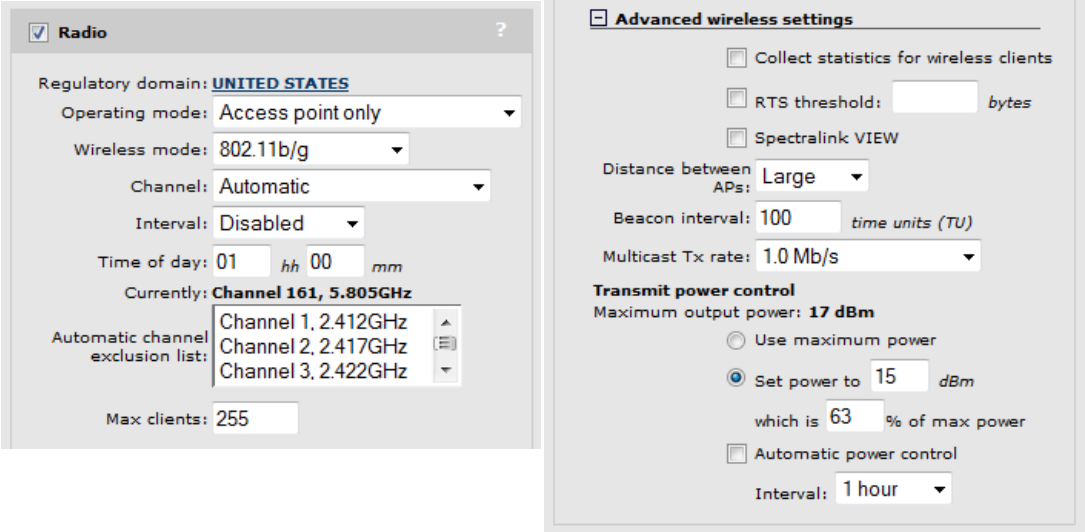


Country / Region	Maximum RF Power Setting (dBm) for 2.4 GHz Operation							
	802.11b Mode				802.11g Mode			
	J8441A	J8444A	J8997A	J8999A	J8441A	J8444A	J8997A	J8999A
AMERICAS								
ARGENTINA	16	16	15	11	13	13	15	13
BRAZIL	16	16	15	11	13	13	15	13
CANADA	16	16	15	11	13	13	15	13
CHILE	15	12	17	13	15	12	17	13
COLOMBIA	16	16	15	11	13	13	15	13
MEXICO	16	16	15	11	13	13	15	13
PERU	16	16	15	11	13	13	15	13
UNITED STATES	16	16	15	11	13	13	15	13
APAC								
AUSTRALIA	16	16	15	11	13	13	15	13

Set the maximum power level of 15 dBm as follows (MSM310 used as example):

1. Launch the MSM AP management tool and log in.
2. Select **Wireless > Radio**.
3. For **Wireless mode**, select **802.11g**.
4. Set **Antenna gain** to the gain of the attached antenna.
5. Select **Advanced wireless settings** to expand the dialog box.
6. Under **Transmit power control** disable **Maximum available output power**.

7. To the left of **dBm**, specify the value, **15** in this example. The dialog box should now look similar to this (in this screenshot the tall dialog box is split in two):



8. Select **Save**.

Additional information is available as follows:

- For autonomous access points, see *Transmit power control on page 3-31*.
- For controlled access points, see *Transmit power control* in the *MSM7xx Controllers Management and Configuration Guide*.

Documentation is available online from: www.hp.com/networking/support. For **Product Brand**, select **ProCurve**.

D

Resetting to factory defaults

Contents

Read this before resetting to factory defaults

Resetting an AP to factory defaults has the following effects:

- The AP is returned to controlled mode operation. If required, switch the AP back to autonomous mode as described in the product Quickstart.
- All user-defined configuration settings are deleted and returned to factory default settings, which includes:
  - The manager username and password are set to **admin.**
  - The DHCP client is enabled on any Ethernet ports. If no DHCP server assigns an address to the AP, its address defaults to 192.168.1.1.
- User-installed licenses are deactivated **but are not deleted**. You must manually enable these licenses once the AP has restarted. (Factory-installed licenses are always active.)

Resetting to factory defaults

Use the procedures in this section to set an AP to its factory default settings.

Using the reset button

Note Not applicable to ruggedized APs.

This technique forces the AP into its factory defaults state including switching the AP back into controlled mode.

Using a tool such as a paper clip, press and hold the reset button for a few seconds until the front status lights blink three times.

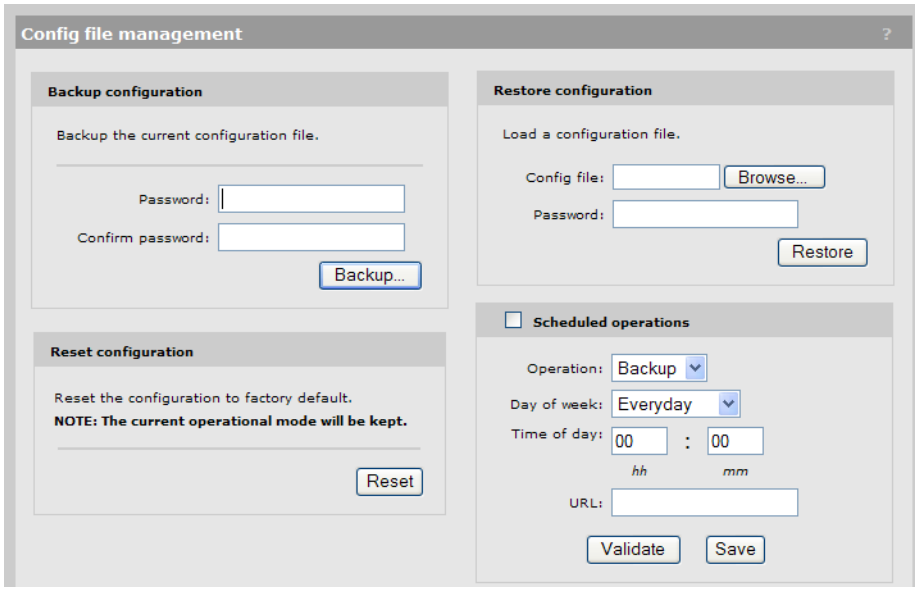
Using the management tool

Launch the management tool (default https://192.168.1.1).

To reset the AP to factory defaults, **keeping it in autonomous mode**, follow this procedure:

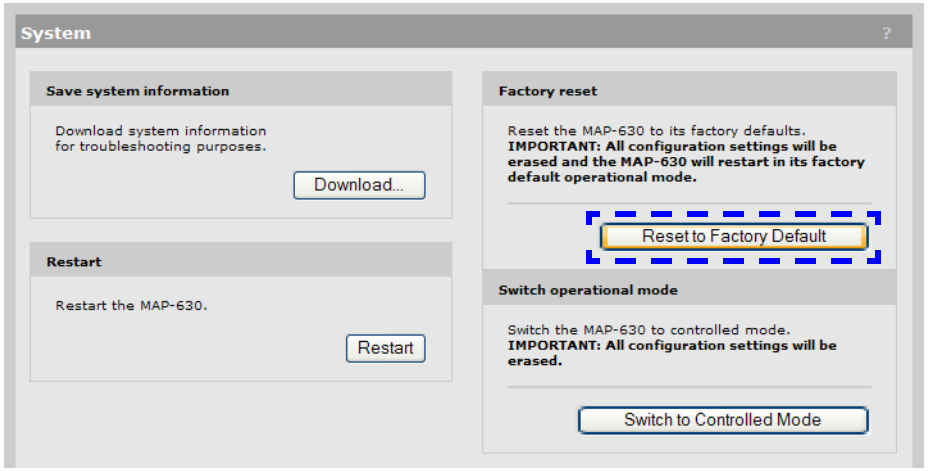
1. Select **Maintenance > Config file management**.

2. Under **Reset configuration**, select **Reset**.



To reset the AP to factory defaults and **FORCE it back into its default controlled mode**, follow this procedure:

1. Select **Maintenance > System**.
2. Under **Factory reset**, select **Reset to Factory Default**.



Factory defaulting ruggedized products

This section describes how to reset the MSM310-R and MSM320-R ruggedized APs to factory defaults without using the management tool.

Note

If you have access to the management tool, you do not to need to follow this procedure. Instead, see *Using the management tool on page D-2*.

You need the following additional items

- The factory default script file. Visit www.hp.com/networking/support and find your product (for **Product Brand**, select **ProCurve**). Look for a zip file with the Factory Default Scripts for the HP MSM310-R and MSM320-R. Download the zip file and extract its content to a folder on your computer.
- A Cat 5 Ethernet crossover cable
- A Cat 5 Ethernet cable
- An 802.3af PoE power injector.

From the zip file, extract the script file that corresponds to your version of Microsoft Windows into a folder such as **C:\scripts**. These scripts are provided:

- English: MSMRemote-en.bat
- French: MSMRemote-fr.bat
- German: MSMRemote-gr.bat
- Italian: MSMRemote-it.bat
- Spanish: MSMRemote-sp.bat.

Note

Microsoft Vista users must install and activate the TFTP service, because it is not active by default. Go to **Start > Control Panel > Programs & Features > Turn Windows Features on & off**, and select **TFTP Client**.

The script runs in a Windows command-line session. It uses the syntax:

```
MSMRemote-<language identifier> [factory | restart | cimfile]
```

- Specify `MSMRemote-<language identifier> factory` to factory reset the unit.
- Specify `MSMRemote-<language identifier> restart` to perform a simple restart (same as powering off and back on).
- The `cimfile` option is used by HP support personnel for loading special software files.

To reset a ruggedized product to factory defaults, follow this procedure:

1. Disconnect any cable from the AP.
2. Disconnect power from the PoE injector.
3. Configure your computer LAN port with a static IP address of **192.168.1.2** and a subnet mask of **255.255.255.0**.
4. Use a Cat 5 Ethernet crossover cable to connect your computer LAN port directly to the PoE injector **Data In** port.
5. Connect a Cat 5 Ethernet cable from the PoE injector **Data and Power Out** port directly to the AP.
6. Open a command line session on the computer.
7. In the folder containing the script, specify the script name including its language identifier and the factory parameter like this:
   `MSMRemote-en factory`
   Press **Enter** to execute the script.
8. Power on the PoE injector. The script performs the reset and confirms success with a message like this:
   `Your "R" product has been successfully factory reset!`
9. Once the factory reset completes, perform the procedure found in the *Initial software configuration* section of the AP Quickstart.

Technology for better business outcomes

To learn more, visit www.hp.com/networking

May 2011

Manual Part Number
5998-1147