HP MSM3xx / MSM4xx APs Configuration Guide

Abstract

This document describes how to configure and manage the MSM3xx / MSM4xx Access Points (APs) in autonomous mode. This document applies to these 802.11n APs: MSM410, MSM422, MSM430, MSM460, MSM466, and MSM466-R. It also applies to these 802.11a/b/g APs: MSM310, MSM310-R, MSM320, MSM320-R, MSM325, and MSM335. These products are hereafter referred to generically as *AP*.

HP Part Number: 5998-5805
Published: May 2014
Edition: 1

The information contained herein is subject to change without notice. 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.

Acknowledgments

Microsoft®, Windows®, and Windows XP® are U.S. registered trademarks of the Microsoft group of companies. Java® is a registered trademark of Oracle and/or its affiliates. Apple® and Bonjour® are trademarks of Apple Inc.

sFlow

Warranty

WARRANTY STATEMENT: See the warranty information sheet provided in the product box.

Contents

1 Introduction

This guide explains how to configure and manage the HP MSM3xx/MSM4xx Access Points that are operating in autonomous mode. For instructions on working with these APs when operating in controlled mode, see the *MSM7xx Controllers Configuration Guide*.

NOTE: The HP 425 AP does not support autonomous mode.

New in release 6.4.0.0

Information on what is new and changed in release 6.4.0.0 is located as follows:

New or changed in this release	For information, see...
New local mesh feature: A new parameter, **Search for better link on minimum SNR**, has been added to local mesh configuration for Alternate Masters and Slaves. When enabled, if the current SNR on the link drops below the value set for **Minimum SNR**, the node will search for a connection to another master with a better SNR.	"Addressing" (page 113)
Parameter renamed: The parameter **Allow 802.11n clients only** on the radio page has been renamed to **Client restriction**.	"Client restriction" (page 46)

2 Using the management tool

Starting the management tool

Using Microsoft Internet Explorer 8+ or Mozilla Firefox 3+ (with SSL v3 support enabled), open page: **https://192.168.1.1** and then log in. This assumes you are connected to the LAN port on the controller (ports 1, 2, 3, or 4 on the MSM720).

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 "Passwords" (page 11).

About the security warning:

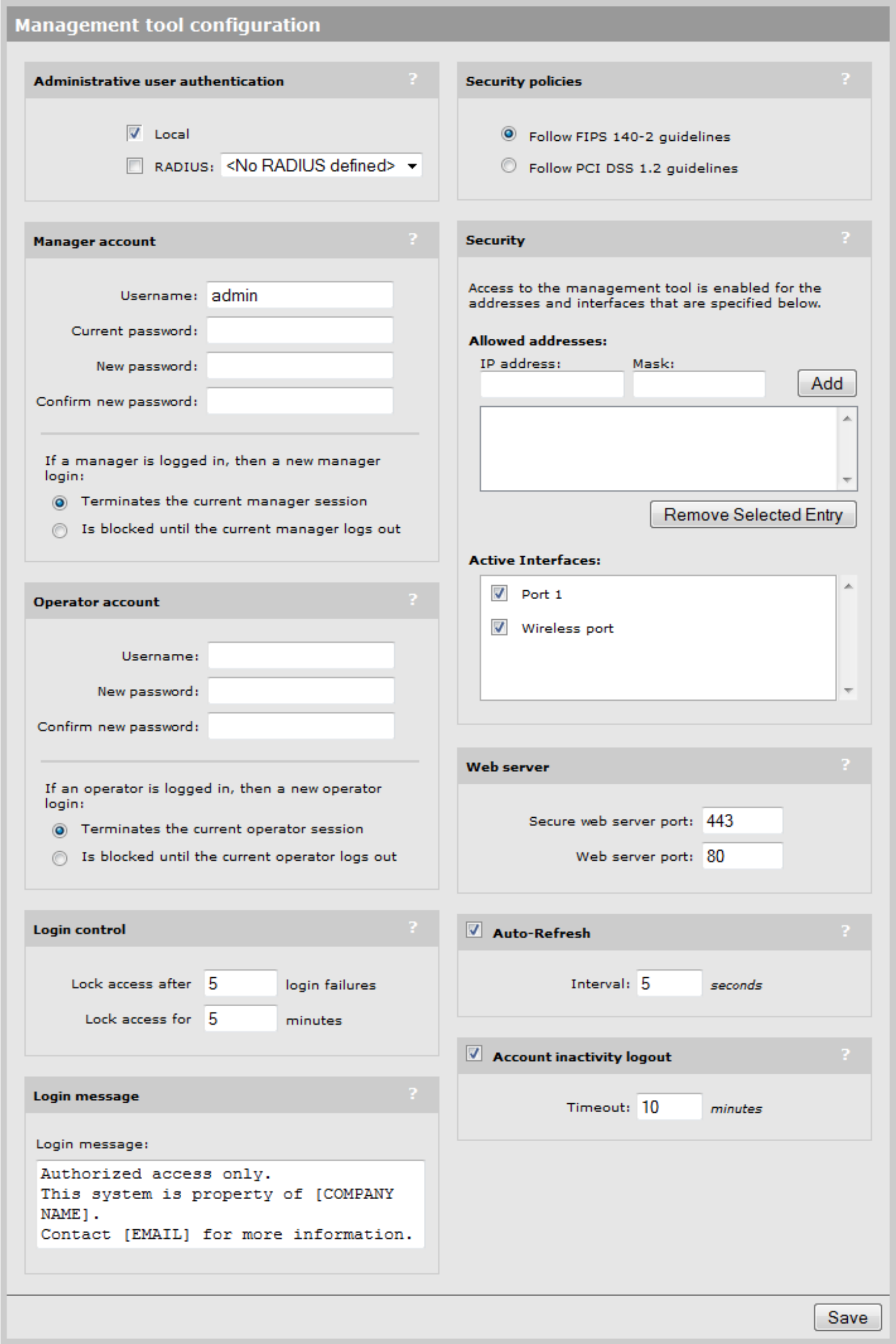
A security certificate warning is displayed the first time that you connect to the management tool. This is normal. Select whatever option is needed in your Web browser to continue to the management tool. The default certificate provided with the AP will trigger a warning message on most browsers because it is self-signed. To remove this warning message, you must replace the default certificate. See "Managing certificates" (page 99).

Setting up manager and operator accounts

Two types of administrative user accounts are defined on the AP: 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.

To configure the accounts, select **Management > Management tool**.



Management tool configuration

Administrative user authentication

☑ Local

□ RADIUS: <No RADIUS defined>

Manager account

Username: admin

Current password:

New password:

Confirm new password:

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

● Terminates the current manager session

○ Is blocked until the current manager logs out

Operator account

Username:

New password:

Confirm new password:

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

● Terminates the current operator session

○ Is blocked until the current operator logs out

Login control

Lock access after 5 login failures

Lock access for 5 minutes

Login message

Login message:

```
Authorized access only.
This system is property of [COMPANY
NAME].
Contact [EMAIL] for more information.
```

Security policies

● Follow FIPS 140-2 guidelines

○ Follow PCI DSS 1.2 guidelines

Security

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

Allowed addresses:

IP address: Mask:

Active Interfaces:

☑ Port 1

☑ Wireless port

Web server

Secure web server port: 443

Web server port: 80

☑ Auto-Refresh

Interval: 5 *seconds*

☑ Account inactivity logout

Timeout: 10 *minutes*

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 operators 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.

Administrative user authentication

Login credentials can be verified using local account settings and/or an external RADIUS sever. This also affects how many accounts you can have.

- **Local:** Select this option to use a single manager and operator account. Configure the settings for these accounts under **Manager account** and **Operator account**.
- **RADIUS:** Using a RADIUS server enables you to have multiple manager and operator accounts, each with a unique login name and password. To setup this option, see "Authenticating manager logins using a third-party RADIUS server" (page 91).

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

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 follows.

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

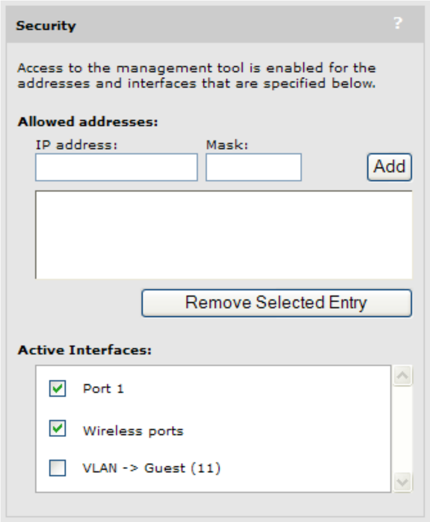
  For more information on these guidelines, refer to the *Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules*.

- **Follow PCI DSS 1.2 guidelines:** When selected, implements the following requirements from the PCI DSS 1.2 guidelines:
  - All administrator passwords must be at least seven characters long.
  - All administrator passwords must contain both numeric and alphabetic characters.
  - The settings under **Login control** must be configured as follows:
    - **Lock access after** *nn* **login failures** must be set to 6 or less.
    - **Lock access for** *nn* **minutes** must be set to 30 minutes or more.
  - The settings under **Account inactivity logout** must be configured as follows:
    - **Timeout** must be set to 15 minutes or less.

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

Configuring management tool security

Select **Management > Management tool** and configure the settings under **Security**.



Security

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

Allowed addresses:

IP address: Mask:

Active Interfaces:

☑ Port 1

☑ Wireless ports

□ VLAN -> Guest (11)

Allowed addresses

Enables you to define a list of IP address from which to permit access to the management tool. To add an entry, specify the IP address and appropriate mask and select **Add**. When the list is empty, access is permitted from any IP address. For example: To allow access for a single computer with IP address 192.168.1.209, specify:

IP address = 192.168.1.209

Mask = 255.255.255.255

To allow access for several computers in the IP address range 192.168.10.16 to 192.168.10.31, specify:

IP address = 192.168.10.16

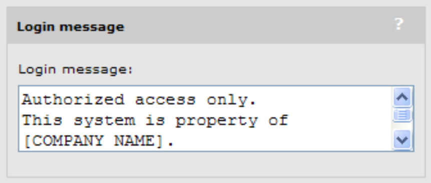
Mask = 255.255.255.240

Active interfaces

Select the interfaces through which access to the management tool will be permitted. (These settings also apply when SSH is used to access the command line interface.)

Configuring the Login page message

You can customize the message that is displayed at the top of the login page by selecting **Management > Management tool** and entering a new message under **Login message**.



Login message

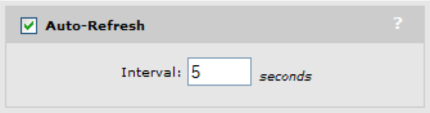
Login message:

```
Authorized access only.
This system is property of
[COMPANY NAME].
```

Configuring Auto-refresh

Select **Management > Management tool** and configure the settings under **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.

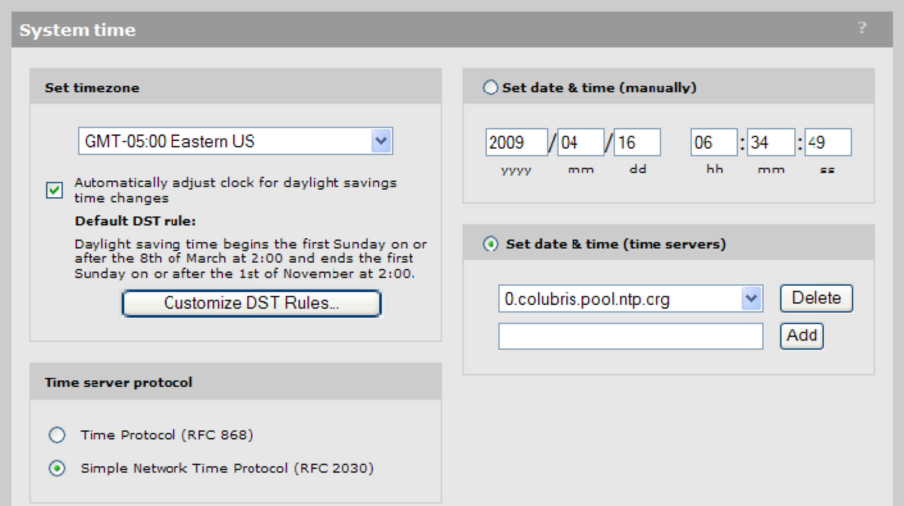


☑ Auto-Refresh

Interval: 5 *seconds*

Setting the 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.



System time

Set timezone

GMT-05:00 Eastern US

☑ Automatically adjust clock for daylight savings time changes

Default DST rule:

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

Customize DST Rules...

Time server protocol

○ Time Protocol (RFC 868)

● Simple Network Time Protocol (RFC 2030)

○ Set date & time (manually)

2009 / 04 / 16 06 : 34 : 49

yyyy mm dd hh mm ss

● Set date & time (time servers)

0.colubris.pool.ntp.crg Delete

Add

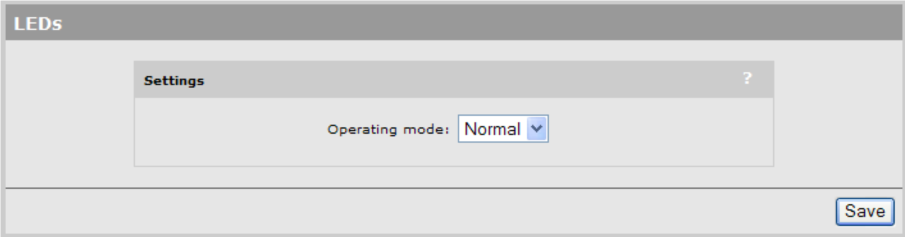
1. Set **timezone & DST** as appropriate.
2. Set **Time server protocol**, to **Simple Network Time Protocol**.

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. 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.
4. 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.

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.


LEDs

Settings

Operating mode: Normal

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

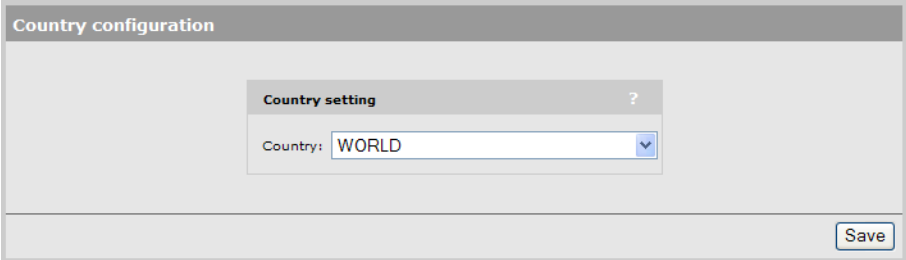
The following settings are available:

- **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 AP operates.

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


Country configuration

Country setting

Country: WORLD

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.

3 Network configuration

Working with network profiles

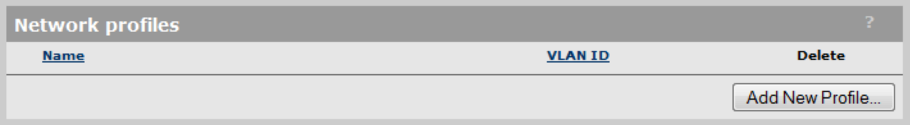
The AP uses logical entities called network profiles to manage the configuration of network settings. Network profiles let you define the characteristics of a network and assign a friendly name to it. Once defined, network profiles can then be bound to a port, or VLAN as required. Network profiles make it easy to use the same settings in multiple places on the AP.

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

- Map VLAN 10 to an AP port using the **Network > VLANs** page.
- Set VLAN 10 as the egress network for a VSC using the **VSC > Profiles** page.

To define a new network profile

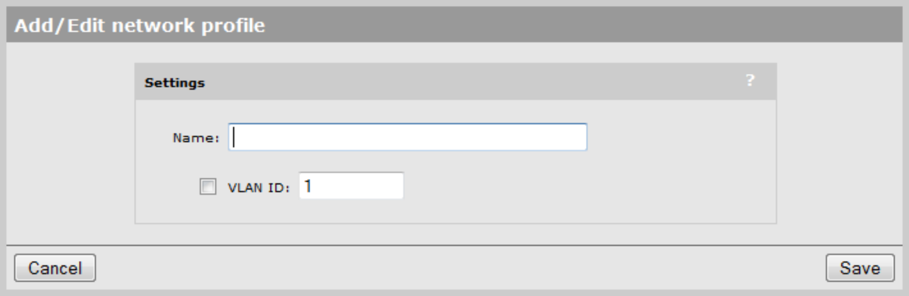
1. Select **Network > Network profiles**.



Network profiles

Name	VLAN ID	Delete

2. Select **Add New Profile**.



Add/Edit network profile

Settings

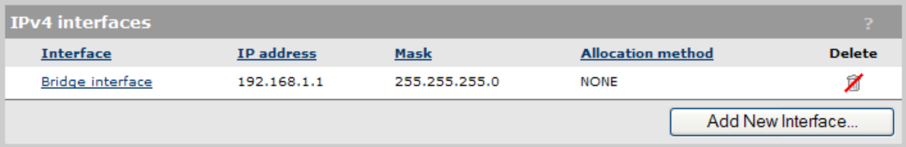
Name:

□ VLAN ID: 1

3. Configure profile settings as follows:
   - Under **Settings**, specify a **Name** for the profile.
   - Optionally, assign a **VLAN ID**. Select **VLAN ID** and then specify a number. 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. An IP address cannot be assigned to a VLAN range. You can define more than one VLAN range by using multiple profiles. Each range must be distinct and contiguous.
4. Select **Save**.

Configuring IP interfaces

The IP interfaces page lists all network profiles to which an IPv4 address is assigned. To open the IP interfaces page, select **Network > IP interfaces**.



IPv4 interfaces

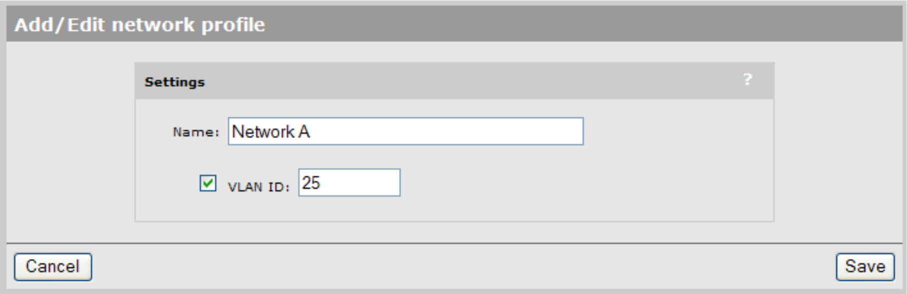
Interface	IP address	Mask	Allocation method	Delete
Bridge interface	192.168.1.1	255.255.255.0	NONE	☒

The Bridge interface is created by default. It can be edited, but not deleted. It is mapped to the wireless port and all Ethernet port(s) on the AP. (These ports are bridged and share the same IP address.)

To assign an IP address to a new interface

Any network profile that has a VLAN ID and is mapped to a physical port can have an IP address assigned to it. The following steps illustrate how to create a new profile and assign an IP address to it.

1. Select **Network > Network profiles**.
2. Select **Add New Profile**.
3. Specify a name for the profile and assign a VLAN ID to it. This example uses the profile name **Network A** and a VLAN ID of **25**. Select **Save**.



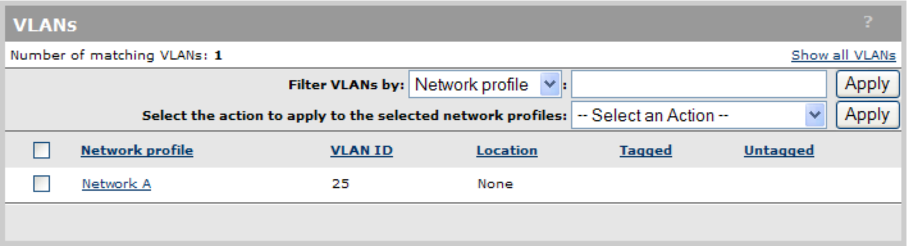
Add/Edit network profile

Settings

Name: Network A

☑ VLAN ID: 25

4. Select **Network > VLANs** to open the VLANs page.



VLANs

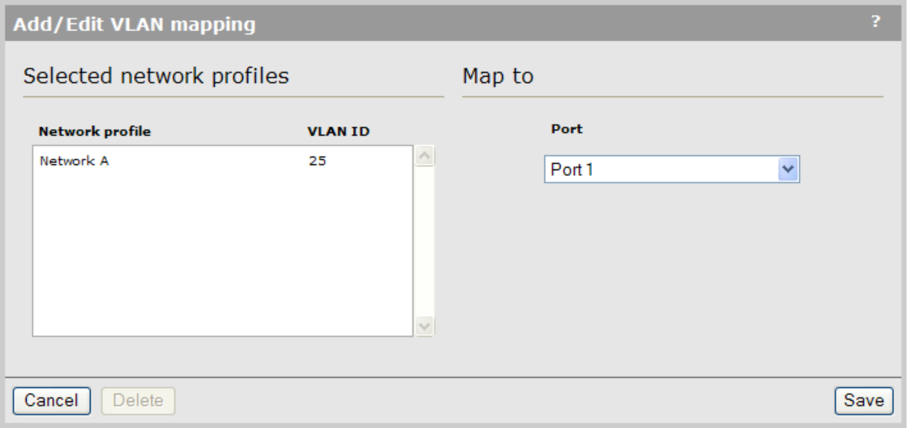
Number of matching VLANs: **1**

Filter VLANs by: Network profile :

Select the action to apply to the selected network profiles: -- Select an Action --

□	Network profile	VLAN ID	Location	Tagged	Untagged
□	Network A	25	None		

5. Select the new profile in the table to open the Add/Edit VLAN mapping page.



Add/Edit VLAN mapping

Selected network profiles

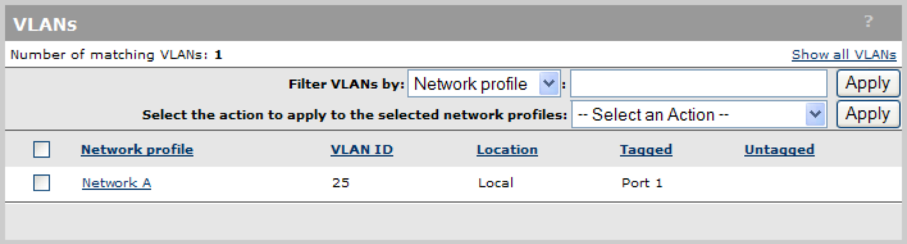
Network profile	VLAN ID
Network A	25

Map to

Port: Port 1

6. Select the port to which you want to map the profile (in this case **Port 1)**.

7. Select **Save**. The profile is mapped to Port 1 tagged.



VLANs

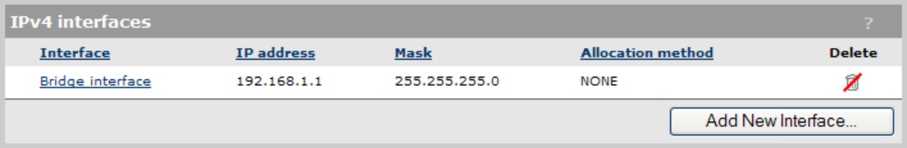
Number of matching VLANs: 1

Filter VLANs by: Network profile :

Select the action to apply to the selected network profiles: -- Select an Action --

□	Network profile	VLAN ID	Location	Tagged	Untagged
□	Network A	25	Local	Port 1	

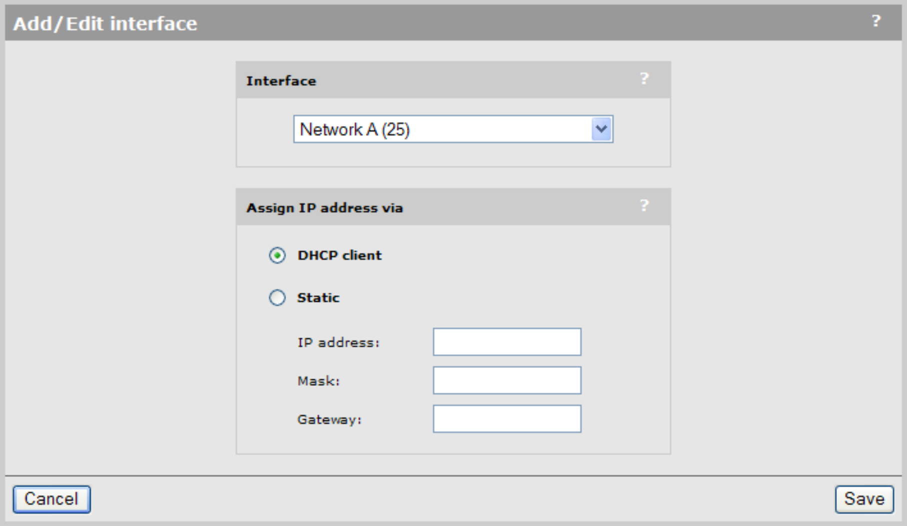
8. Select **Network > IP interfaces** to open the IPv4 interfaces page.



IPv4 interfaces

Interface	IP address	Mask	Allocation method	Delete
Bridge interface	192.168.1.1	255.255.255.0	NONE	

9. Select **Add New Interface** to open the Add/Edit interface page.



Add/Edit interface

Interface

Network A (25)

Assign IP address via

● DHCP client

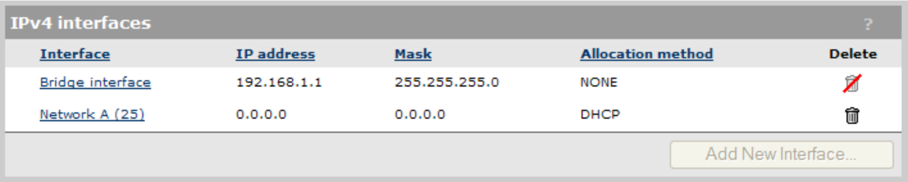
○ Static

IP address:

Mask:

Gateway:

10. Under **Interface**, select the network profile that you defined earlier.
11. Under **Assign IP address via**, select the addressing method to use.
    - **DHCP client:** Dynamic host configuration protocol. The DHCP server will automatically assign an address to the network profile, which functions as a DHCP client.
    - **Static:** Specify an **IP address**, **Mask**, and **Gateway**.
12. Select **Save**.
13. The new interface is added to the IPv4 interfaces table.

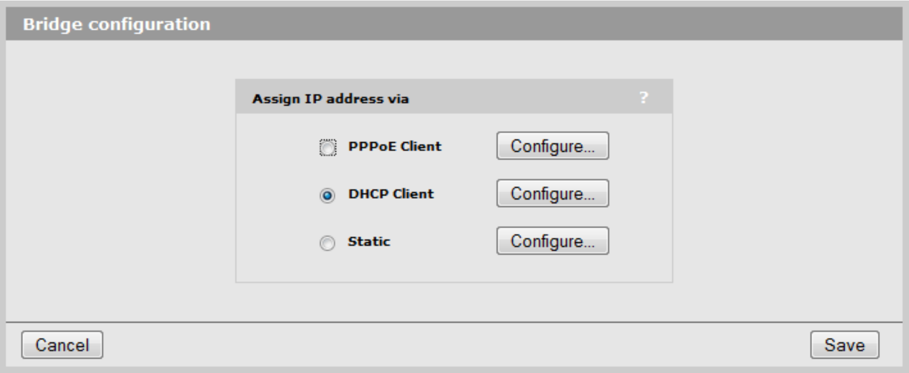


IPv4 interfaces

Interface	IP address	Mask	Allocation method	Delete
Bridge interface	192.168.1.1	255.255.255.0	NONE	
Network A (25)	0.0.0.0	0.0.0.0	DHCP	🗑

Configuring the Bridge interface

All wireless and Ethernet ports on an AP are bridged. As a result, they all share the same configuration settings defined by the Bridge interface. The following configuration options are available if you select the **Bridge interface** in the table.



Bridge configuration

Assign IP address via

○ PPPoE Client

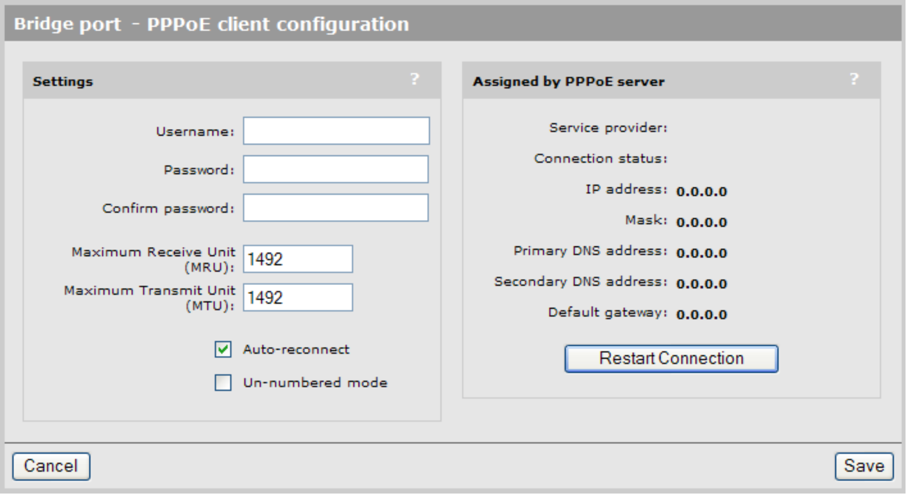
● DHCP Client

○ Static

By default, the Bridge interface operates as a DHCP client. Select the option you want to use and select **Configure**. Refer to the following sections for additional configuration information.

- "Configuring the PPPoE client" (page 17)
- "Configuring the DHCP client" (page 18) (default setting)
- "Static addressing" (page 19)

Configuring the PPPoE client



Bridge port - PPPoE client configuration

Settings

Username:

Password:

Confirm password:

Maximum Receive Unit (MRU): 1492

Maximum Transmit Unit (MTU): 1492

☑ Auto-reconnect

□ Un-numbered mode

Assigned by PPPoE server

Service provider:

Connection status:

IP address: 0.0.0.0

Mask: 0.0.0.0

Primary DNS address: 0.0.0.0

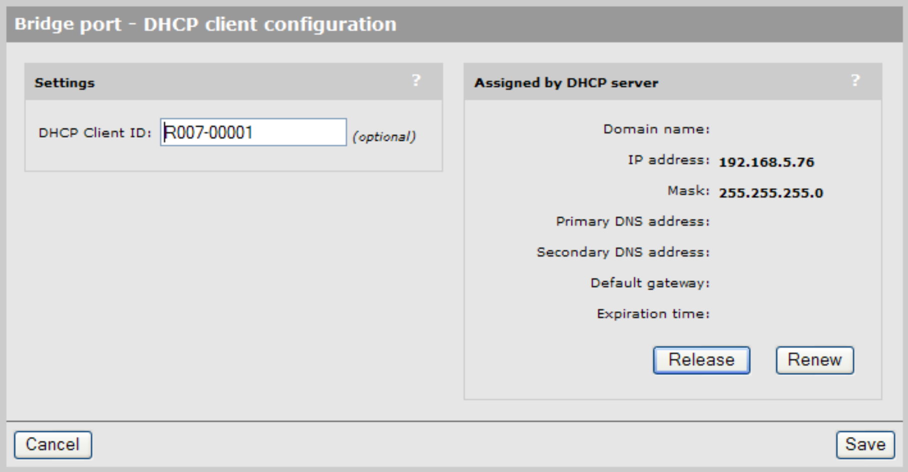
Secondary DNS address: 0.0.0.0

Default gateway: 0.0.0.0

1. Under **Settings**, define the following:
   - **Username**: Specify the username assigned to you by your ISP. The AP will use this username to log on to your ISP when establishing a PPPoE connection.
   - **Password/Confirm password**: Specify the password assigned to you by your ISP. The AP will use this password to log on to your ISP when establishing a PPPoE connection.
   - **Maximum Receive Unit (MRU)**: Maximum size (in bytes) of a PPPoE packet when receiving. Changes to this parameter only should be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.
   - **Maximum Transmit Unit (MTU)**: Maximum size (in bytes) of a PPPoE packet when transmitting. Changes to this parameter should only be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.
   - **Auto-reconnect**: The AP will automatically attempt to reconnect if the connection is lost.
   - **Un-numbered mode**: This feature is useful when the AP is connected to the Internet and NAT is not being used. Instead of assigning two IP addresses to the AP, one to the Internet port and one to the LAN port, both ports can share a single IP address.

   This is especially useful when a limited number of IP addresses are available to you.
2. Under **Assigned by PPPoE server**, select **Restart Connection**. Once you are connected to the server, the following fields will display information about your connection. The Internet connection is not active until this occurs. Refer to the online help for a description of each field.

Configuring the DHCP client



Bridge port - DHCP client configuration

Settings

DHCP Client ID: R007-00001 (optional)

Assigned by DHCP server

Domain name:

IP address: 192.168.5.76

Mask: 255.255.255.0

Primary DNS address:

Secondary DNS address:

Default gateway:

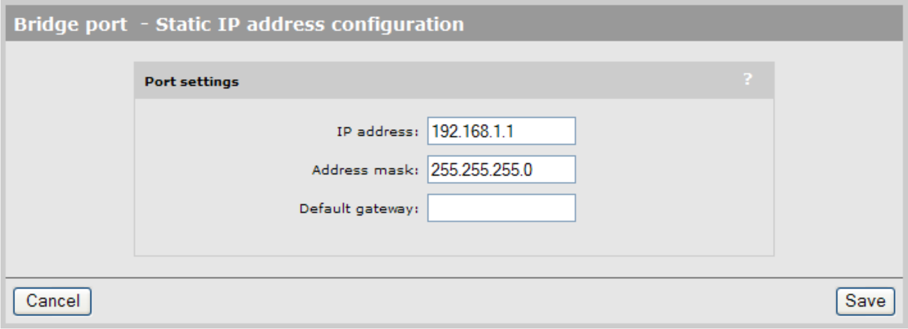
Expiration time:

The DHCP client does not require any configuration, unless you need to set a value for the optional **DHCP Client ID** parameter for proper operation with your DHCP server.

Once you are connected to the server, the fields under **Assigned by DHCP server** show the settings assigned to the AP by the DHCP server. The connection is not active until this occurs. Refer to the online help for a description of each field.

If you want to force the DHCP client to obtain a new lease, select **Release** and then **Renew**.

Static addressing



Bridge port - Static IP address configuration

Port settings

IP address: 192.168.1.1

Address mask: 255.255.255.0

Default gateway:

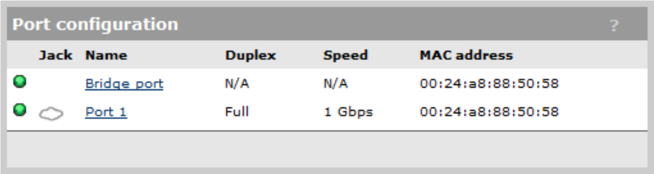
Cancel Save

Under **Port settings**, define the following:

- **IP address:** Specify the static IP address you want to assign to the port.
- **Address mask:** Specify the appropriate mask for the IP address you specified.
- **Default gateway:** Specify the address of the default gateway on the network.

Configuring port settings

To configure settings for the physical ports on the AP, select **Network > Ports**.



Port configuration

	Jack	Name	Duplex	Speed	MAC address
●		Bridge port	N/A	N/A	00:24:a8:88:50:58
●	⬭	Port 1	Full	1 Gbps	00:24:a8:88:50:58

Status light

- **Green:** Port is properly configured and ready to send and receive data.
- **Red:** Port is not properly configured or is disabled.

Jack

Indicates the jack (physical interface) to which a port is assigned.

Name

Identifies the port.

Duplex

Indicates if the port is Full or Half duplex.

Speed

Indicates the speed at which the port is operating.

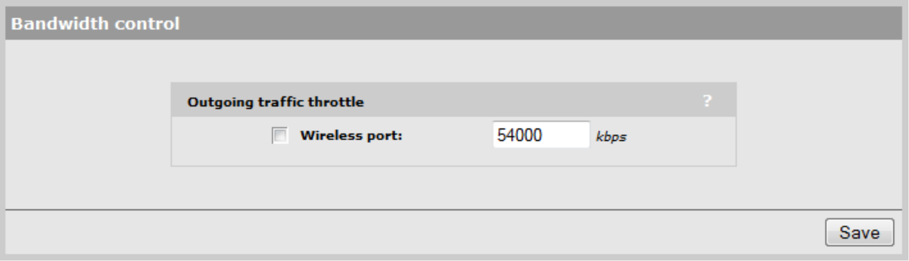
MAC address

Indicates the MAC address of the port.

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**.



Bandwidth control

Outgoing traffic throttle

☐ Wireless port: 54000 kbps

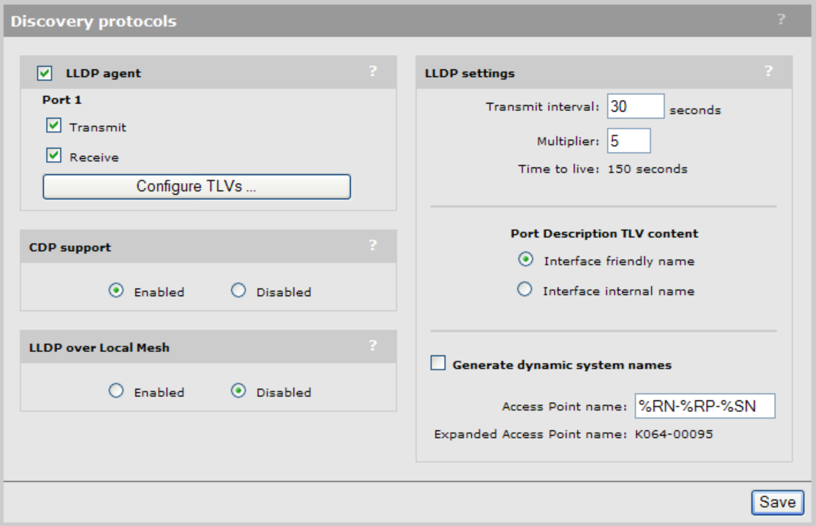
- If outgoing traffic arrives at the rate defined by the specified bandwidth limit (or less), it is processed without delay.
- If outgoing traffic arrives at a rate that is greater than the defined bandwidth limit, it causes the AP to throttle the traffic. If the traffic rate is over-limit for just a 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

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

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



Discovery protocols

☑ LLDP agent

Port 1

☑ Transmit

☑ Receive

CDP support

● Enabled ○ Disabled

LLDP over Local Mesh

○ Enabled ● Disabled

LLDP settings

Transmit interval: 30 seconds

Multiplier: 5

Time to live: 150 seconds

Port Description TLV content

● Interface friendly name

○ Interface internal name

☐ Generate dynamic system names

Access Point name: %RN-%RP-%SN

Expanded Access Point name: K064-00095

CDP configuration

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.

LLDP configuration

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.

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**.

Port Description TLV content

Select the content to be included in and advertised as part of the port description TLV.

Interface friendly name: Use the friendly name for the interface (the name you see in the management tool). For example: LAN port, Internet port.

Interface internal name: Use the internal name for the interface. For example: eth0, eth1.

Generate dynamic system names

When enabled, this feature replaces the system name with a dynamically generated value which you can define.

Access Point name

Specify how the dynamically generated name will be created. You can use regular text in combination with placeholders to create the name. Placeholders are automatically expanded each time the name is regenerated.

If the placeholders cause the generated name to exceed 32 characters, it is truncated.

Placeholders

%RN: System name of the neighboring device to which the port is connected, obtained via the System Name TLV. Since this is an optional TLV, if it is not available, the Chassis ID TLV is used instead.

%RP: Port description of the port on the neighboring device to which the local port is connected, obtained via the Port Description TLV. Since this is an optional TLV, if it is not available, the Port ID TLV is used instead.

%SN: AP name suffix (if specified). Up to 16 characters can be appended to the name.

%IP: AP's IP address. An IP address can require up to 15 characters (nnn.nnn.nnn.nnn).

Expanded Access Point name

Specify how the dynamically generated name will be created. You can use regular text in combination with placeholders to create the name. Placeholders are automatically expanded each time the name is regenerated.

If the placeholders cause the generated name to exceed 32 characters, it is truncated.

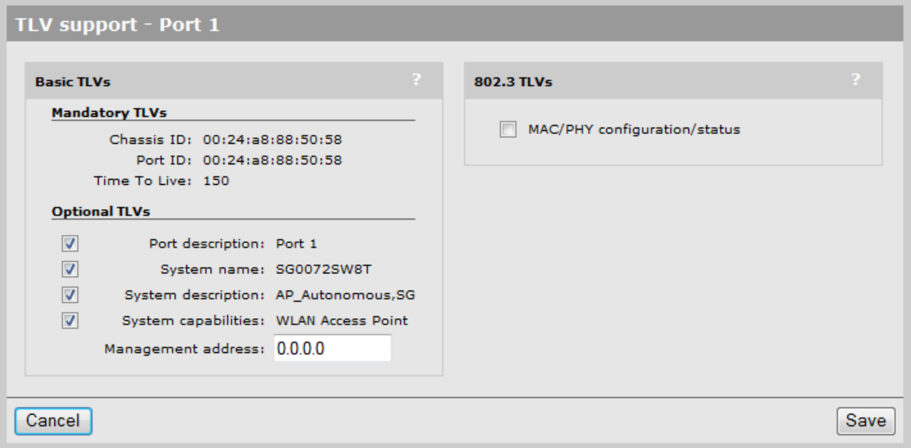
To create the system name, the items are concatenated using a hyphen as separator. For example:

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.



TLV support - Port 1

Basic TLVs

Mandatory TLVs

Chassis ID: 00:24:a8:88:50:58
Port ID: 00:24:a8:88:50:58
Time To Live: 150

Optional TLVs

☑ Port description: Port 1
☑ System name: SG0072SW8T
☑ System description: AP_Autonomous,SG
☑ System capabilities: WLAN Access Point
Management address: 0.0.0.0

802.3 TLVs

□ MAC/PHY configuration/status

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 **Generate dynamic system names** option is enabled, the system name is replaced by the dynamically generated name.

System description

(Type 6): Description of the system, comprised of the following information: operational mode, hardware type, hardware revision, and firmware version.

System capabilities

(Type 7): Indicates the primary function of the device. Set to:

WLAN access point

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.

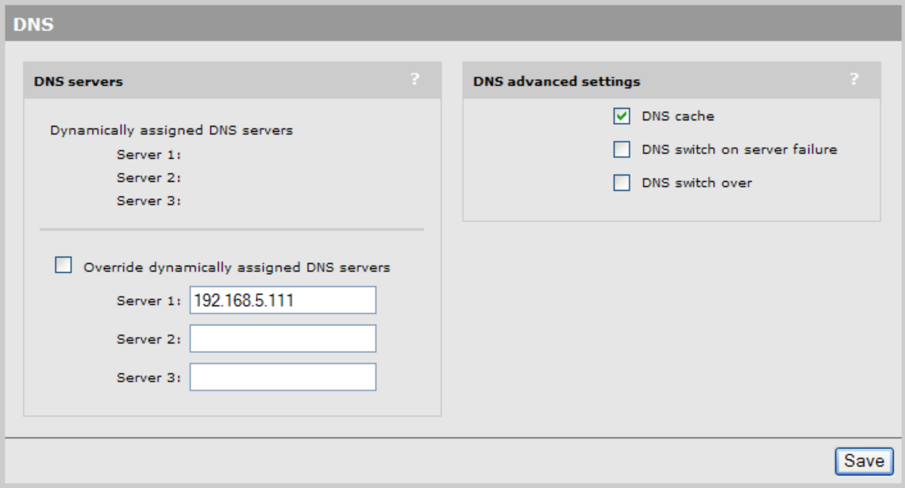
MAC/PHY configuration/status

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 configuration

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



DNS

DNS servers

Dynamically assigned DNS servers

Server 1:

Server 2:

Server 3:

□ Override dynamically assigned DNS servers

Server 1: 192.168.5.111

Server 2:

Server 3:

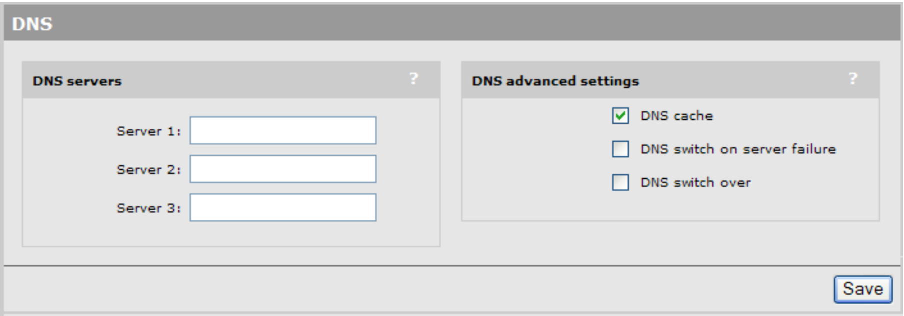
DNS advanced settings

☑ DNS cache

□ DNS switch on server failure

□ DNS switch over

When the Bridge port is configured to use a static IP address:



DNS

DNS servers

Server 1:

Server 2:

Server 3:

DNS advanced settings

☑ DNS cache

□ DNS switch on server failure

□ DNS switch over

DNS servers

Dynamically assigned servers

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

Override dynamically assigned DNS servers

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

Server 1

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

Server 2

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

Server 3

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

DNS advanced settings

DNS cache

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

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

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

DNS switch on server failure

Controls how the AP switches between 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 server does not reply to a DNS request.

DNS switch over

Controls how the AP switches back to the primary server.

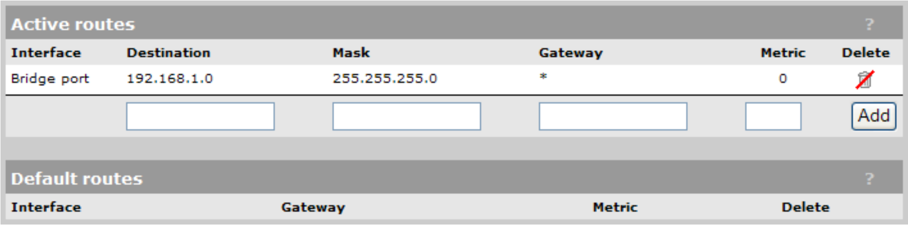
- When enabled, the AP switches back to the primary server once the primary server becomes available again.
- When disabled, the AP switches back to the primary server only when the secondary server becomes unavailable.

Defining 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.

Configuring IP routes

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



Active routes ?

Interface	Destination	Mask	Gateway	Metric	Delete
Bridge port	192.168.1.0	255.255.255.0	*	0	🗑
					Add

Default routes ?

Interface	Gateway	Metric	Delete

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 or subnet is routed.
- **Mask**: Number of bits in the destination address that are checked for a match.

- **Gateway**: IP address of the gateway to which the 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).

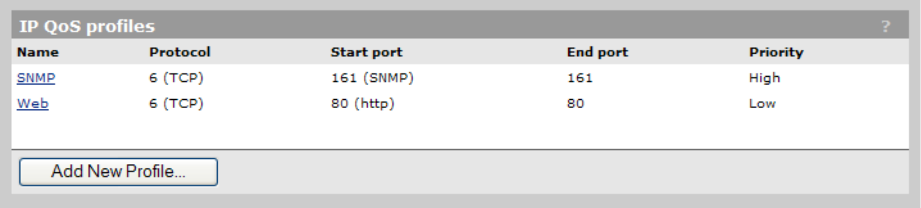
  An asterisk is used by system routes to indicate a directly connected network.
- **Metric**: Priority of a route. If two routes exist for a destination address, the AP chooses the one with the lower metric.
- **Delete**: Select the garbage can icon to delete a route. If the icon has a red line through 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” (page 69)) or with local mesh profiles (“Quality of service” (page 110)). You can configure up to 32 IP QoS profiles on the AP. You can associate up to 10 IP QoS profiles to a VSC.

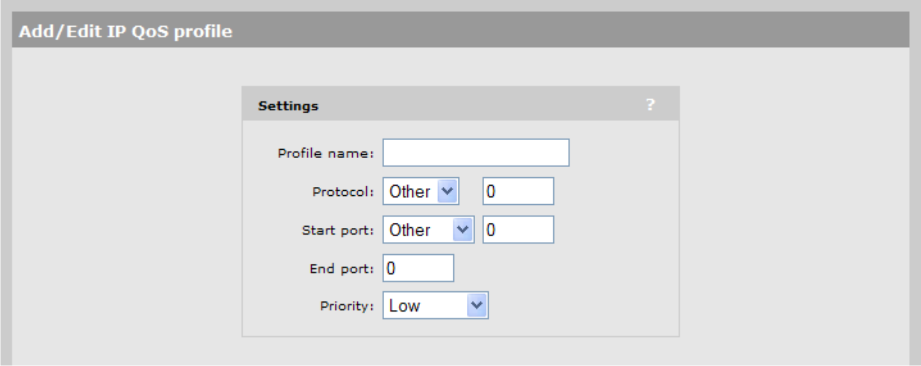
Configuring IP QoS profiles

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



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

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



Add/Edit IP QoS profile

Settings

Profile name:

Protocol: Other 0

Start port: Other 0

End port: 0

Priority: Low

Settings

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

  NOTE: To accept traffic on all ports for a specified protocol, set **Start port** to **Other** and **0**. Also set **End port** to **65535**.
- **Priority:** Select the priority level that will be assigned to traffic that meets the criteria specified in this IP QoS profile.

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

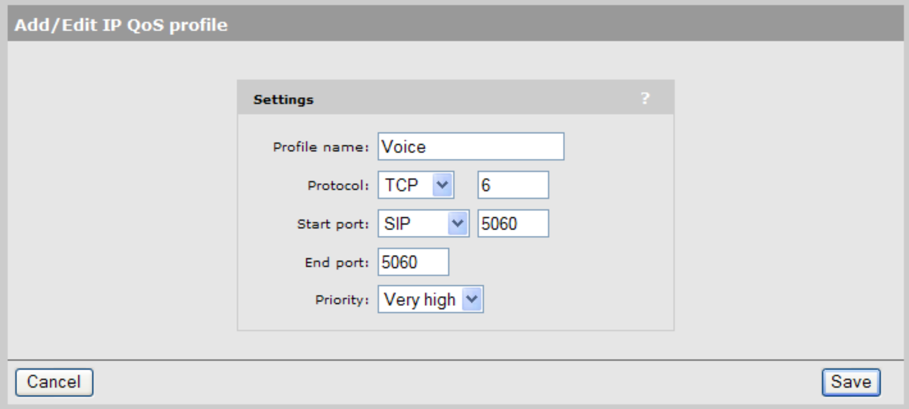
Example

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

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

Create the profiles

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



Add/Edit IP QoS profile

Settings

Profile name: Voice

Protocol: TCP 6

Start port: SIP 5060

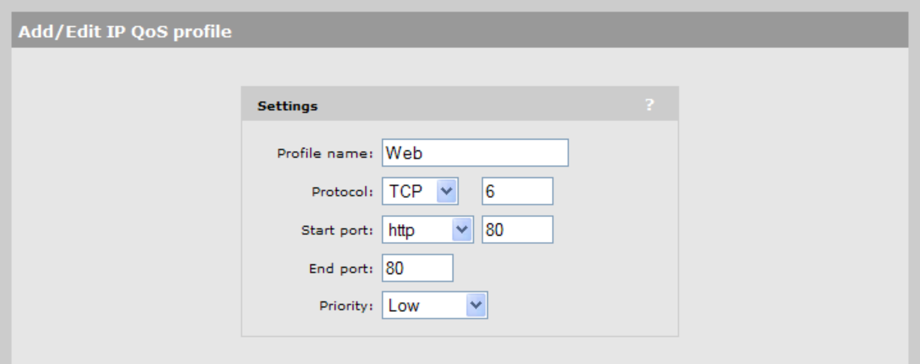
End port: 5060

Priority: Very high

6. Select **Save**.

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

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



Add/Edit IP QoS profile

Settings

Profile name: Web

Protocol: TCP 6

Start port: http 80

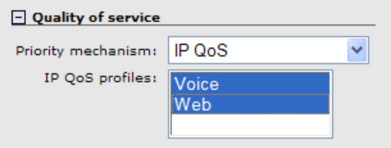
End port: 80

Priority: Low

12. Select **Save**.

Assign the profiles to a VSC

1. Select **VSC > Profiles**, and then select one of the VSC profiles in the **Name** column. Scroll down to the **Quality of service** section in the **Virtual AP** box.



⊟ Quality of service

Priority mechanism: IP QoS

IP QoS profiles: Voice, Web

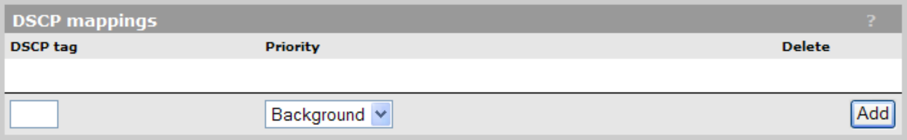
2. Under **Quality of service**, set **Priority mechanism** to **IP QoS**.
3. In **IP QoS profiles**, Ctrl-click each profile.
4. Select **Save**.

Customizing DiffServ DSCP mappings

(These settings do not apply to IP QoS.)

You can create custom DSCP mappings that let you override the standard DSCP mappings that are defined by default when you enable DiffServ as the QoS priority mechanism for a VSC or for local mesh links. This enables you to customize how traffic is assigned to the QoS priority queues.

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



DSCP mappings

DSCP tag	Priority	Delete
	Background	

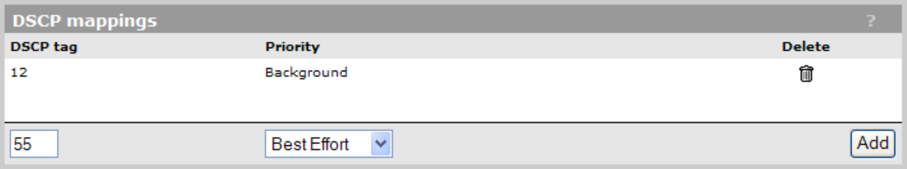
DSCP tag DSCP codepoint value.

Priority Indicates the priority level assigned to traffic that matches the DSCP tag.

- **Background:** Assigns the traffic to queue 4 (Lowest priority).
- **Best effort:** Assigns the traffic to queue 3.
- **Video:** Assigns the traffic to queue 2.
- **Voice:** Assigns the traffic to queue 1 (Highest priority).

To create a new mapping

Specify a value for **DSCP tag**, select a **Priority**, and then select **Add**.

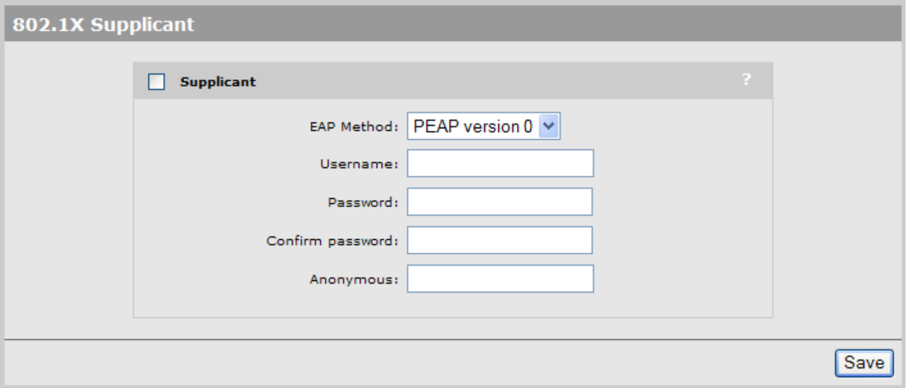


DSCP mappings

DSCP tag	Priority	Delete
12	Background	🗑
55	Best Effort	

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**.



802.1X Supplicant

□ Supplicant

EAP Method: PEAP version 0

Username:

Password:

Confirm password:

Anonymous:

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.

4 Wireless configuration

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" (page 51)) to determine the optimal settings and location for the AP.

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" (page 36). To set the regulatory domain, see "Country" (page 13).

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" (page 49).

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" (page 36).

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

- Select **Wireless > Overview** to view information about each connected wireless client.
- Select **Wireless > Neighborhood** to view a list of wireless radios operating nearby.
- Enable the **Severe interface detection/mitigation** feature on the Radio configuration page to automatically switch channels when interference is detected. See "Severe interference detection/mitigation" (page 47).

△ **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

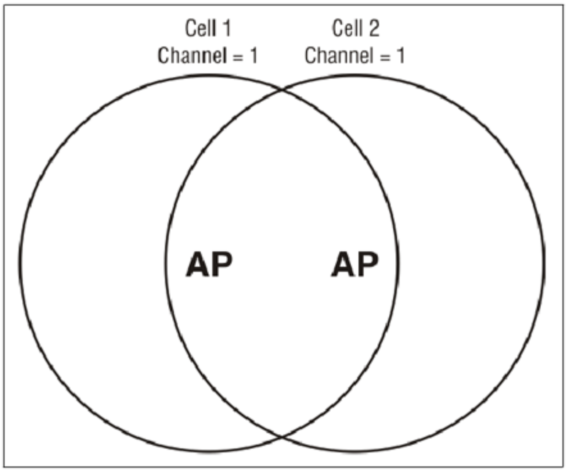
Overlapping wireless cells occur when two or more APs are operating within transmission range of each other. This may be under your control, (for example, when you use several cells to cover a large location), or out of your control (for example, when your neighbors set up their own wireless networks). 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	Channel	Center frequency	Overlaps channels
1	2412	2, 3	8	2447	6, 7, 9, 10
2	2417	1, 3, 4	9	2452	7, 8, 10, 11
3	2422	1, 2, 4, 5	10	2457	8, 9, 11, 12
4	2427	2, 3, 5, 6	11	2462	9, 10, 12, 13
5	2432	3, 4, 6, 7	12	2467	10, 11, 13
6	2437	4, 5, 7, 8	13	2472	11, 12
7	2442	5, 6, 8, 9	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. (See "Country" (page 13)). This means that the number of non-overlapping channels available to you varies by geographical location.

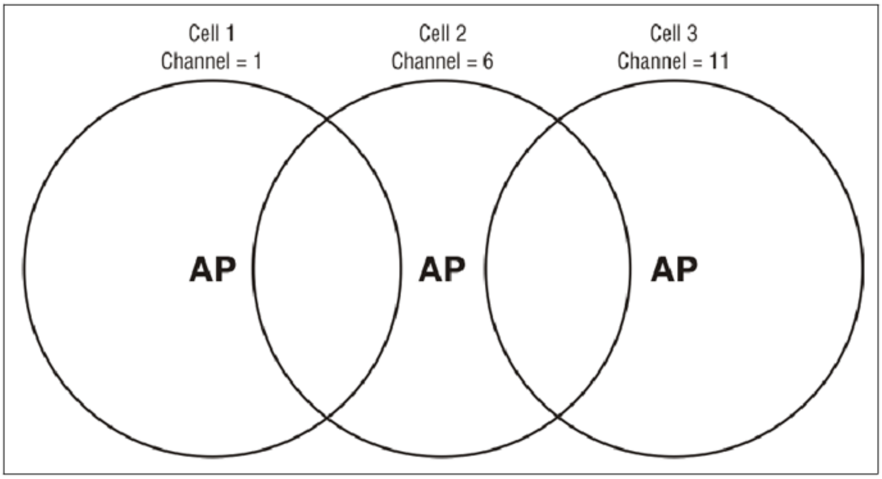
The following table shows the number of channels that are available in North America, Japan, and Europe.

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).

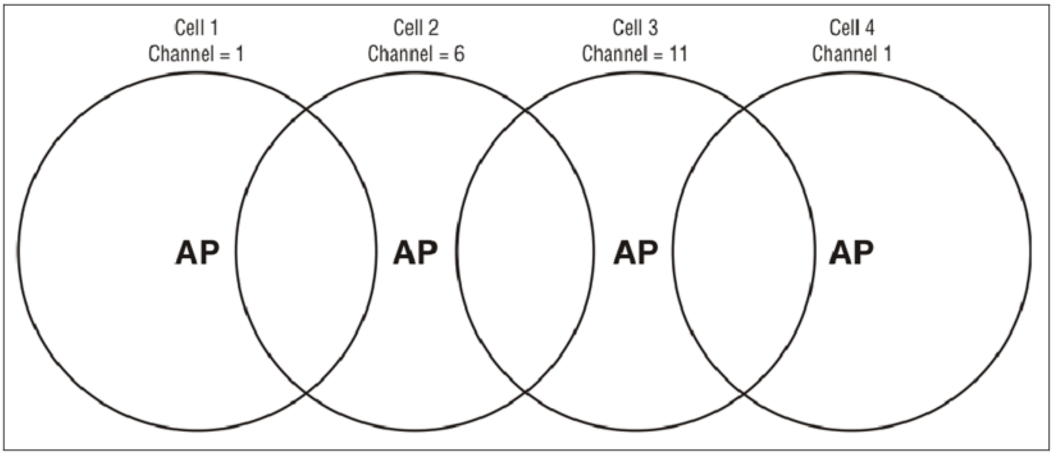
North America	Japan	Europe
cell 1 on channel 1	cell 1 on channel 1	cell 1 on channel 1
cell 2 on channel 6	cell 2 on channel 7	cell 2 on channel 7
cell 3 on channel 11	cell 3 on channel 14	cell 3 on channel 13

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



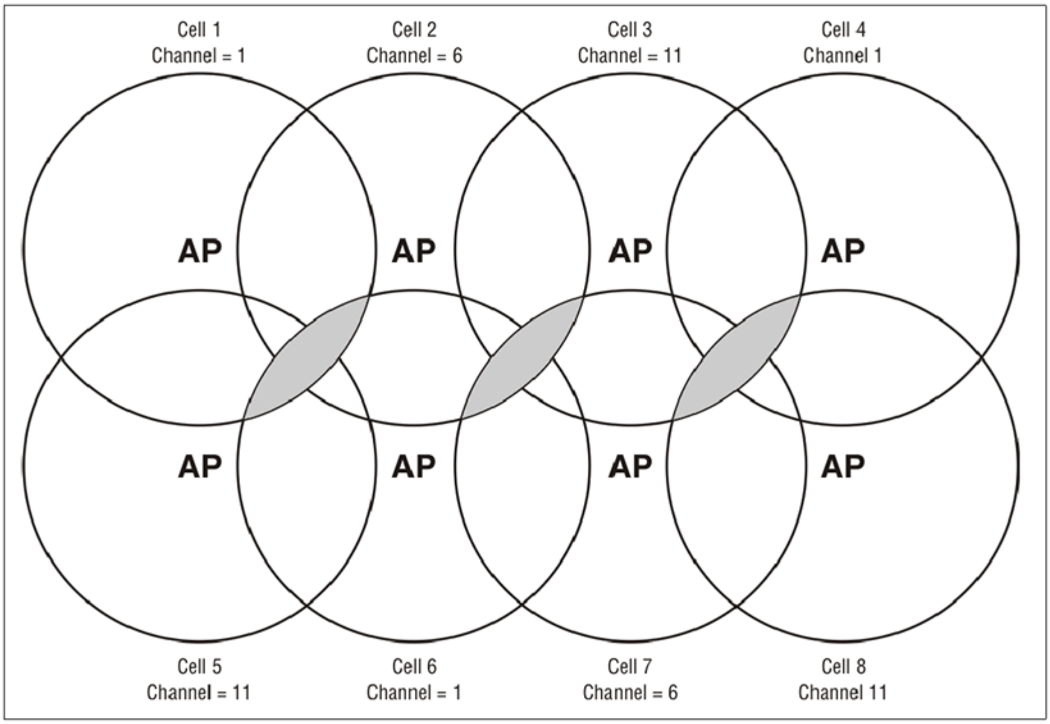
Reducing transmission delays by using different operating frequencies in North America.

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

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** 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" (page 49).

Supporting 802.11a 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.

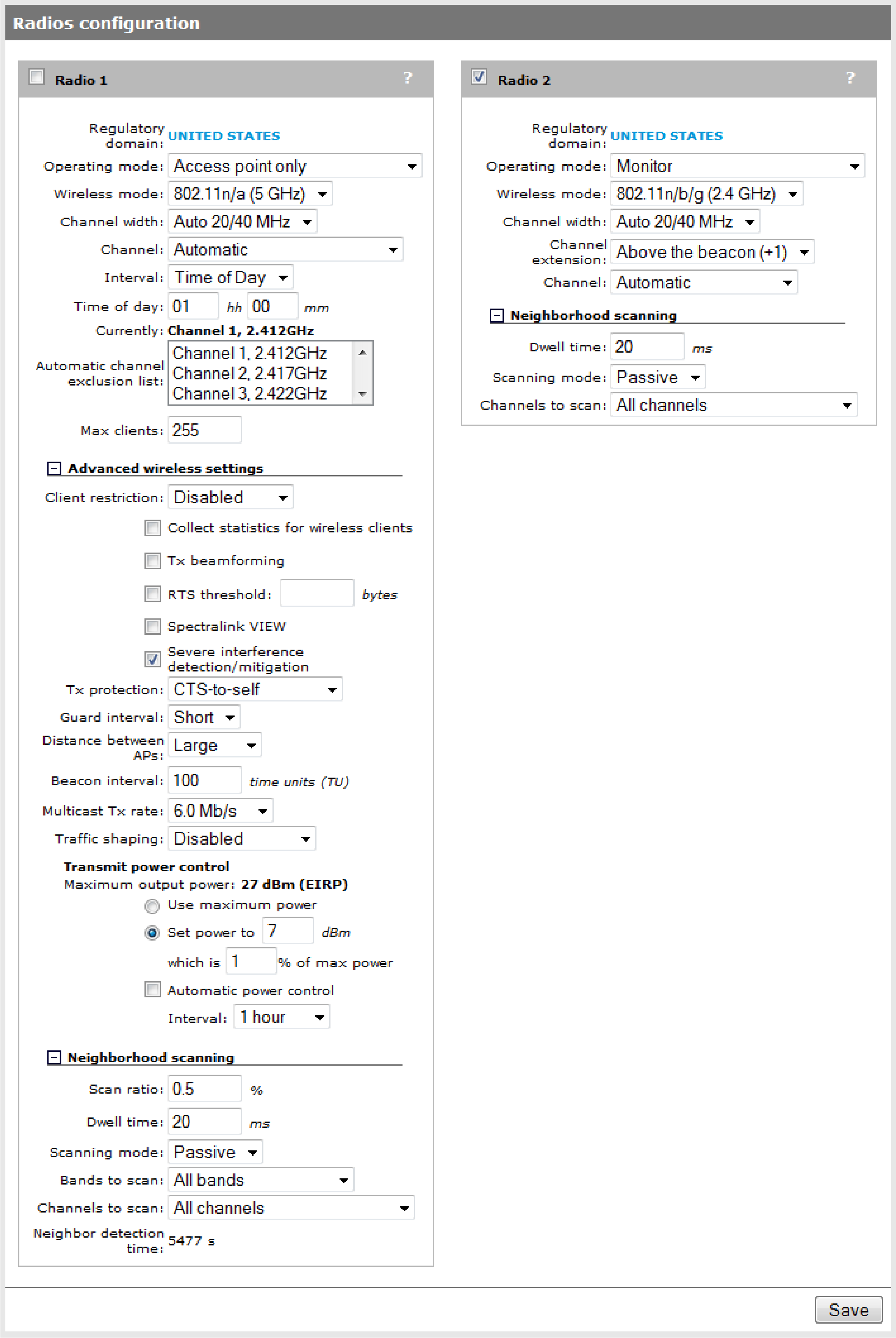
If protection is not used, 802.11b clients may transmit a frame while an 802.11g frame is already being sent. This leads to a collision and both devices need to re-transmit. If there are enough devices in the network, the collision rate will grow exponentially and prevent any useful throughput from the 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 MSM430, MSM460, MSM466, and MSM466-R can be configured (see "Tx protection" (page 47)) 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. You can use the **Allow 802.11n clients only** setting to segregate 802.11n traffic to ensure that 802.11n clients do not experience performance degradation by sharing a wireless network with legacy (slower) client stations.

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 varies depending on the product. The following screen shows the Radio(s) configuration page for the MSM460. Configuration settings are the same on other products.



Radios configuration

□ Radio 1

Regulatory domain: UNITED STATES
Operating mode: Access point only
Wireless mode: 802.11n/a (5 GHz)
Channel width: Auto 20/40 MHz
Channel: Automatic
Interval: Time of Day
Time of day: 01 *hh* 00 *mm*
Currently: **Channel 1, 2.412GHz**
Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz
Max clients: 255

Advanced wireless settings

Client restriction: Disabled
□ Collect statistics for wireless clients
□ Tx beamforming
□ RTS threshold: *bytes*
□ Spectralink VIEW
☑ Severe interference detection/mitigation
Tx protection: CTS-to-self
Guard interval: Short
Distance between APs: Large
Beacon interval: 100 *time units (TU)*
Multicast Tx rate: 6.0 Mb/s
Traffic shaping: Disabled

Transmit power control
Maximum output power: **27 dBm (EIRP)**
○ Use maximum power
● Set power to 7 *dBm*
which is 1 % of max power
□ Automatic power control
Interval: 1 hour

Neighborhood scanning

Scan ratio: 0.5 *%*
Dwell time: 20 *ms*
Scanning mode: Passive
Bands to scan: All bands
Channels to scan: All channels
Neighbor detection time: 5477 s

☑ Radio 2

Regulatory domain: UNITED STATES
Operating mode: Monitor
Wireless mode: 802.11n/b/g (2.4 GHz)
Channel width: Auto 20/40 MHz
Channel extension: Above the beacon (+1)
Channel: Automatic

Neighborhood scanning

Dwell time: 20 *ms*
Scanning mode: Passive
Channels to scan: All channels

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" (page 13).

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.) 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.
- **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 "Managing licenses" (page 121).

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

Product	Access point and Local mesh	Access point only	Local mesh only	Monitor	Sensor
MSM310 MSM310-R	✔	✔	✔	✔	×
MSM320 MSM320-R	✔	✔	✔	✔	✔
MSM325	✔	✔	✔	✔	✔
MSM335 (Radio 1 + 2)	✔	✔	✔	✔	✔
MSM335 (Radio 3)	×	×	✔	✔	✔
MSM410	✔	✔	✔	✔	×
MSM422	✔	✔	✔	✔	×
MSM430	✔	✔	✔	✔	×
MSM460	✔	✔	✔	✔	×
MSM466 MSM466-R	✔	✔	✔	✔	×

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" (page 37)	✔	✔	✔	✔	✔
"Wireless mode" (page 39)	✔	✔	✔	✔	×
"Channel width" (page 41)	✔	✔	✔	✔	×

Parameter	Access point and Local mesh	Access point only	Local mesh only	Monitor	Sensor
“Channel extension” (page 42)	✔	✔	✔	✔	✕
“Channel” (page 42)	✔	✔	✔	✔	✕
“Interval” (page 43)	✔	✔	✔	✕	✕
“Time of day” (page 44)	✔	✔	✔	✕	✕
“Automatic channel exclusion list” (page 44)	✔	✔	✔	✕	✕
“Antenna selection” (page 44)	✔	✔	✔	✕	✔
“Antenna gain” (page 45)	✔	✔	✔	✕	✕
“Max clients” (page 46)	✔	✔	✔	✕	✕
“Client restriction” (page 46)	✔	✔	✔	✔	✔
“Collect statistics for wireless clients” (page 46)	✔	✔	✔	✕	✕
“Tx beamforming” (page 46)	✔	✔	✔	✕	✕
“RTS threshold” (page 46)	✔	✔	✔	✕	✕
“Spectralink VIEW” (page 47)	✔	✔	✔	✕	✕
“Severe interference detection/mitigation” (page 47)	✔	✔	✔	✕	✕
“Tx protection” (page 47)	✔	✔	✔	✕	✕
“Guard interval” (page 47)	✔	✔	✔	✕	✕
“Maximum range (ack timeout)” (page 48)	✔	✕	✔	✕	✕
“Distance between APs” (page 48)	✔	✔	✔	✕	✕
“Beacon interval” (page 48)	✔	✔	✔	✕	✕
“Multicast Tx rate” (page 48)	✔	✔	✔	✕	✕
“Transmit power control” (page 49)	✔	✔	✔	✕	✕

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” (page 13).

802.11n/a (5 GHz)

Supported on	MSM410, MSM466, MSM466-R Radio 1 on: MSM422, MSM430, MSM460
Frequency band	5 GHz
Data rates	**For 802.11n clients:** Up to 450 Mbps on the MSM466, MSM466-R, MSM460, and up to 300 Mbps on the MSM410, MSM422, and MSM430. **For 802.11a clients:** Up to 54 Mbps.

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 .

802.11a (5 GHz)

Supported on	MSM310, MSM320, MSM335, MSM410, MSM422, MSM466 Radio 1 on: MSM430, MSM460 (not supported in Monitor mode)
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.

802.11n/b/g (2.4 GHz)

Supported on	MSM410, MSM422 Radio 2 on: MSM430, MSM460, MSM466
Frequency band	2.4 GHz
Data rates	**For 802.11n clients:** Up to 130 Mbps on the MSM410, MSM422, MSM430, MSM460, MSM466, MSM466-R. (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.

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 .

802.11b/g (2.4 GHz)

Supported on	MSM310, MSM320, MSM335, MSM410, MSM422

	Radio 2 on: MSM430, MSM460, MSM466
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 (2.4 GHz)

Supported on	MSM310, MSM320, MSM335
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.

802.11b (2.4 GHz)

Supported on	MSM310, MSM320, MSM335
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.

802.11a Turbo

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

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

Channel width

Supported on: MSM410, MSM422 (radio 1), MSM430, MSM460, MSM466, MSM466-R

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** from one of the following options:

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

On the HP 517, when **Wireless mode** is set to **802.11n/b/g**, **Channel width** is automatically set to **20 MHz** and cannot be changed.

Channel extension

Supported on: MSM410, MSM422 (radio 1), MSM430 (radio 2), MSM460 (radio 2), MSM466 (radio 2), MSM466-R (radio 2)

Not available in Sensor mode.

This setting only appears when **Wireless mode** is set to **802.11n/b/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. If the **Interval** parameter is set to any value other than **Time of day**. and a wireless client is associated with the radio, automatic channel selection is delayed. The AP will retry at one minute intervals until the radio is unused by wireless clients.

- **On the MSM430, MSM460, MSM466, MSM466-R:** Scanning during the channel selection process can cause interruptions to voice calls. This only occurs each time the Interval expires. Therefore, HP does not recommend configuring a short **Interval**.
- **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" (page 49).

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” (page 51) to view a list of APs currently operating in your area. For detailed information on selecting channels when operating at 2.4 GHz, see “Configuring overlapping wireless cells” (page 32).

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), MSM430, MSM460, MSM466, MSM466-R:** When **Wireless mode** is **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/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 HP recommends 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, or when the auto-channel feature is enabled.

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

- Select **Time of day** to have the channel setting re-evaluated at a specific time of day. Note that to prevent all APs from re-evaluating their channel at the same time, a random delay between 0 and 2 hours is added to the time of day for each AP. If the **Interval** parameter is set to any value other than **Time of day**. and a wireless client is associated with the radio, automatic channel selection is delayed. The AP will retry at one minute intervals until the radio is unused by wireless clients.
- Select **a time interval** in hours to define how often the channel setting is re-evaluated. If a wireless client is associated with the radio when the interval occurs, automatic channel selection is delayed (at one minute intervals) until the radio is unused by wireless clients. Background scanning is not supported when you select this option.
- 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, or when the auto-channel feature is enabled.

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, or when the auto-channel feature is enabled.

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

Antenna selection

Supported on: MSM310, MSM320, MSM335, MSM422

Not available in Monitor or Sensor modes.

Select the antenna(s) to use for each radio. Antenna support varies on each AP. For a list of supported external antennas, see “Connecting external antennas” (page 130).

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” (page 49).
- When creating a point-to-point local mesh link, HP recommends 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, HP recommends 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:

Radio 1

- Radio 1 features three internal antennas in the lower flap supporting 802.11n/a/b/g. Each antenna has a corresponding connector (A, B, C) for the installation of an optional external antenna.
- Radio 1 supports diversity on its internal and external antennas. In 802.11n modes, a special form of diversity, called MIMO, is used.

  MIMO uses spatial multiplexing to transport two or more data streams simultaneously on the same channel to increase throughput. For example, under most conditions, multiplexing two streams can result in double the throughput of a single stream.

  MIMO mode 3x3 is automatically used, which means that three antennas are used to transmit and three antennas are used to receive.
- 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 when receiving.

Radio 2

- Radio 2 features two internal antennas in the upper flap supporting 802.11a/b/g. These antennas have a single connector (D) for the installation of an optional external antenna.
- Radio 2 provides support for diversity only on its two internal antennas. Diversity is not supported when using an external antenna.

Antenna gain

Supported on: MSM310. MSM310-R, MSM320, MSM320-R, MSM466, MSM466-R.

Not available in Monitor or Sensor modes.

For optimum performance, this parameter must be set to the gain of the antenna.

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

Client restriction

*Only available when **Wireless mode** supports 802.11n.*

Use this option to restrict access to the wireless network to specific types of wireless clients.

- **802.11n only:** Only wireless clients supporting 802.11n can connect. This prevents 802.11a/b/g client stations from accessing the wireless network.

Collect statistics for wireless clients

Not available in Monitor or Sensor modes.

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

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

Tx beamforming

Supported on: MSM430, MSM460, MSM466, MSM466-R

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: MSM310, MSM320, MSM335, MSM410, MSM422, MSM430, MSM460, MSM466, MSM466–R

Not available in Monitor or Sensor modes.

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

Severe interference detection/mitigation

Supported on: MSM410, MSM430, MSM460, MSM466, MSM466-R

Not available in Monitor or Sensor modes.

When an AP detects severe degradation in the channel quality of the current operating channel on a radio (that persists for tens of seconds), the AP does an intensive spectrum analysis scan to identify the type of interference (only on the MSM430, MSM460, and MSM466/466-R). The AP then chooses the best channel using the same methods as when auto-channel is enabled. (The AP may decide not to switch to a different channel. For example, if the RF interference source affects all channels in the band.)

After switching to an alternative channel, the AP continues to monitor the channel quality of the non-operating channels. Eventually, it is expected that the interference will go away. (Most interference sources are temporary.) The AP then decides whether it should switch back to the original channel or to continue operating on the alternate channel.

Tx protection

Supported on: MSM410, MSM430, MSM460, MSM466, MSM466-R

Not available in Monitor or Sensor modes.

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

The following options are available:

- **CTS-to-self:** 802.11n transmissions are protected by sending a Clear To Send (CTS) frame that blocks other wireless clients from accessing the wireless network.
- **RTS/CTS:** 802.11n transmissions are protected by sending a Request To Send (RTS) frame followed by a CTS frame. This is a more robust, but slower, solution than CTS-to-self. However, this method resolves the hidden station problem (where certain legacy stations may not see only a CTS frame).
- **No MAC protection:** This setting gives the best performance for 802.11n clients in the presence of 802.11g or 802.11a legacy clients or APs. No protection frames (CTS-to-self or RTS/CTS) are sent at the MAC layer by the AP. PHY-based protection remains active, which alerts legacy clients to stay off the air while the AP is transmitting data to 802.11n clients. This method of protection is supported by most 802.11g or 802.11a clients, but is not supported for 802.11b-only clients and should not be used if such clients are expected on the network.

Guard interval

Supported on: MSM410, MSM422 (radio 1), MSM430, MSM460, MSM466, MSM466-R

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 available in Monitor or Sensor modes.

Use this parameter to adjust the receiver sensitivity of the AP only if you have a very dense deployment where many APs are close together. In all other cases, use the default setting of **Large**.

If you have installed multiple APs, reducing the receiver sensitivity helps to keep clients with low signal quality from connecting, thereby increasing the probability that client stations connect with the nearest AP.

Available settings

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

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

Beacon interval

Not available in Monitor or Sensor modes.

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

Multicast Tx rate

Not available in Monitor or Sensor modes.

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

Transmit power control

Not available in Monitor or Sensor modes.

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

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

Important

For a list of supported external antennas, see "Connecting external antennas" (page 130).

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

△ **CAUTION:** For specific power limits according to your regulatory domain, consult the *Antenna Power-Level Settings Guide* available at www.hp.com/support/manuals. Search for the part number of your antenna.

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

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

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

Maximum output power

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

- **On the MSM410, MSM430, MSM460:** Shows the maximum EIRP (Effective/Equivalent Isotropic Radiated Power) that can be delivered by the AP based on the regulatory domain. The displayed EIRP power is equivalent to the Conducted RF transmit power of the radio (dBm) plus the array gain of the antenna (dBi).
- **On the MSM466 and MSM466-R:** Shows the maximum conducted RF power (dBm) that can be delivered to the external antenna. The EIRP can be calculated by adding the antenna array gain (dBi).

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 click **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.

Supported power levels are as follows:

- 0 - 20 dBm: MSM310, MSM320, MSM335, MSM410, MSM422, MSM466, MSM466-R
- 5 - 25 dBm: MSM430, MSM460 operating at 2.4 GHz.
- 7 - 20 dBm: MSM430, MSM460 operating at 5 GHz.

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.

Neighborhood scanning

Supported on: MSM410, HP 425, MSM430, MSM460, MSM466, MSM466-R

*Not configurable when **Operating mode** is set to **Access point and Local mesh** or **Local mesh only.***

Scan ratio

(Not configurable when **Operating mode** is set to **Monitor**.)

The percentage of time the radio will spend scanning channels other than the operating channel.

Dwell time

The amount of time (in milliseconds) that a radio remains on a channel while performing channel scanning. The default value is 30 milliseconds.

Set a value between 10 and 32 milliseconds when **Operating mode** is set to **Access point only**. (Use a value of 30 milliseconds on the MSM410.)

Set a value between 10 and 1000 milliseconds when **Operating mode** is set to **Monitor.**

Scanning mode

- **Passive:** The AP listens to the channel to detect wireless traffic, but does not transmit any probes. The AP will receive beacon frames and probe response frames, and use them to identify neighbors. (When IDS is enabled, other frames are also received and sent to the IDS system for analysis.) The key point is that no frames are transmitted. This is the default setting.
- **Active:** The AP uses probe request frames to speed up neighbor detection. Active scanning only occurs on channels permitted by the regulatory domain. Transmission of probes is not allowed on DFS channels, so no probes are sent on DFS channels even when this option is selected.

Bands to scan

(Not configurable in **Monitor mode**. The **All bands** option is automatically used.)

- **All bands:** Scan both 802.11 bands (2.4 GHz and 5 GHz).
- **Operating band only:** Scan only the band in which the radio is currently operating.

Recommended settings for single radio APs:

- With IDS disabled, select **Operating band only**.
- With IDS enabled, select **All bands**.

Recommended settings for dual radio APs:

- With IDS disabled, configure both radios for **Operating band only**.
- With IDS enabled, configure the 2.4 GHz radio for **Operating band only** (with a small scan ratio), and configure the 5 GHz radio for **All bands** (with a larger scan ratio). The 2.4 GHz band is probably much busier than the 5 GHz band, so IDS scanning using the 5 GHz radio has a reduced performance impact.

Channels to scan

- **All channels:** Scan all channels supported by the current operating mode.
- **Regulatory channels only:** Scan only channels supported by the current regulatory domain (country).
- **Non-excluded channels only:** When enabled, the AP will not scan any channels in the **Automatic channel exclusion list**.

Neighbor detection time

Estimated time in seconds to detect a neighbor.

Wireless neighborhood

You can use the wireless neighborhood feature to discover the operating frequencies of radios 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. 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 MSM430, MSM460, MSM466, MSM466-R:** 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

Supported on: MSM310, MSM320, MSM335, MSM410, and MSM422.

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.

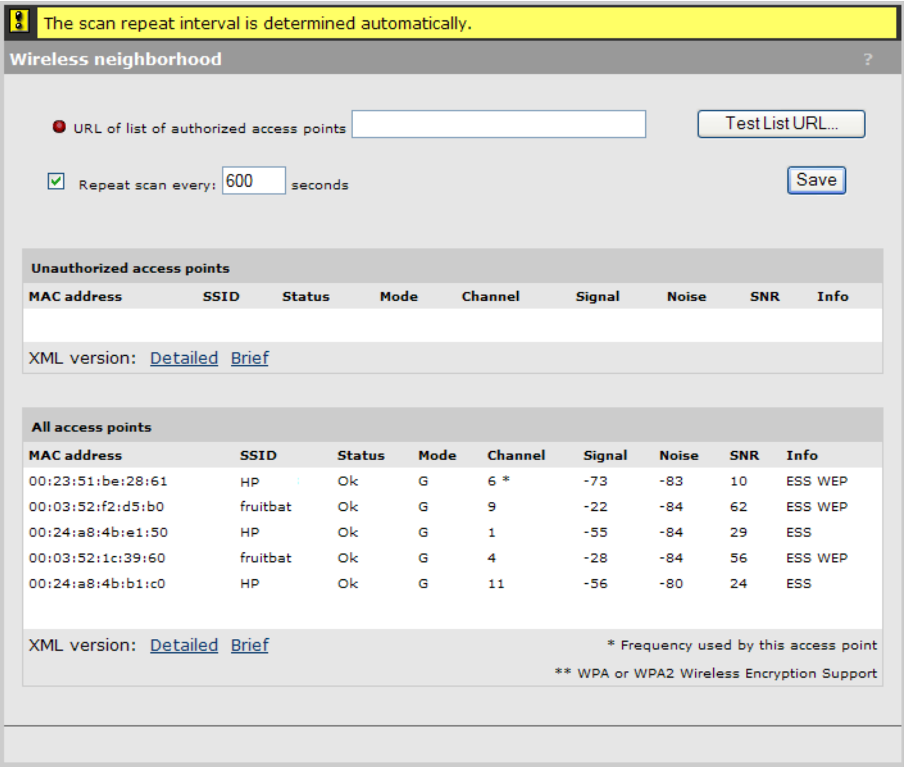
NOTE:

- 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.

  When a radio is configured to support automatic channel selection, background scanning is only supported when the **Time of Day** option is selected for the automatic channel selection **Interval**.

Viewing scan results

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



The scan repeat interval is determined automatically.

Wireless neighborhood

● URL of list of authorized access points

☑ Repeat scan every: 600 seconds

Unauthorized access points

MAC address	SSID	Status	Mode	Channel	Signal	Noise	SNR	Info

XML version: Detailed Brief

All access points

MAC address	SSID	Status	Mode	Channel	Signal	Noise	SNR	Info
00:23:51:be:28:61	HP	Ok	G	6 *	-73	-83	10	ESS WEP
00:03:52:f2:d5:b0	fruitbat	Ok	G	9	-22	-84	62	ESS WEP
00:24:a8:4b:e1:50	HP	Ok	G	1	-55	-84	29	ESS
00:03:52:1c:39:60	fruitbat	Ok	G	4	-28	-84	56	ESS WEP
00:24:a8:4b:b1:c0	HP	Ok	G	11	-56	-80	24	ESS

XML version: Detailed Brief

* Frequency used by this access point

** WPA or WPA2 Wireless Encryption Support

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.

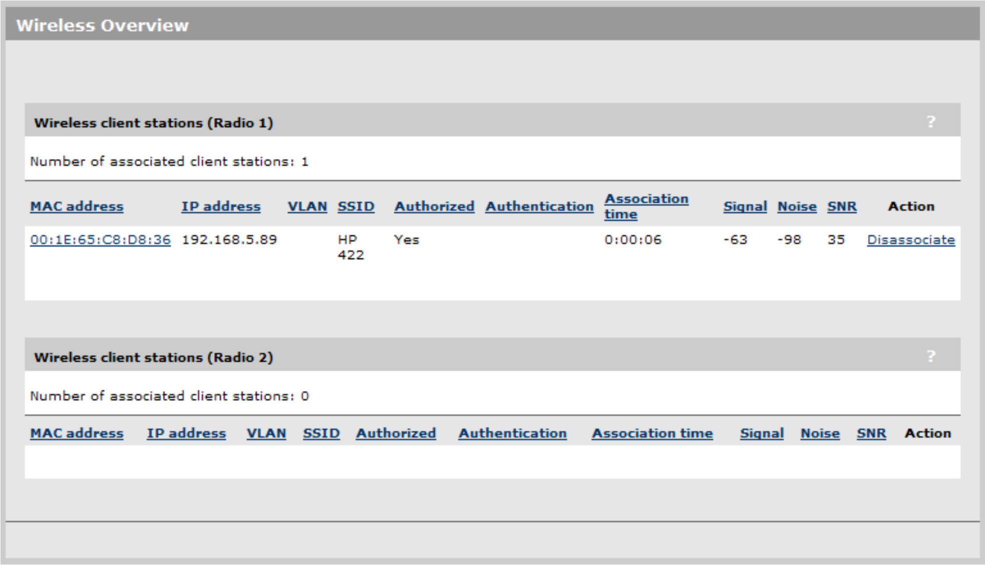
Creating the list of authorized APs

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**.

Viewing wireless information

Viewing all wireless clients

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



Wireless Overview

Wireless client stations (Radio 1)

Number of associated client stations: 1

MAC address	IP address	VLAN	SSID	Authorized	Authentication	Association time	Signal	Noise	SNR	Action
00:1E:65:C8:D8:36	192.168.5.89		HP 422	Yes		0:00:06	-63	-98	35	Disassociate

Wireless client stations (Radio 2)

Number of associated client stations: 0

MAC address	IP address	VLAN	SSID	Authorized	Authentication	Association time	Signal	Noise	SNR	Action

This page lists all wireless clients associated with all VSCs.

Settings

MAC Address

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

IP address

IP address assigned to the client station.

Username

Name with which the user logged in.

VLAN

VLAN assigned to the client station.

SSID

SSID assigned to the client station.

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.

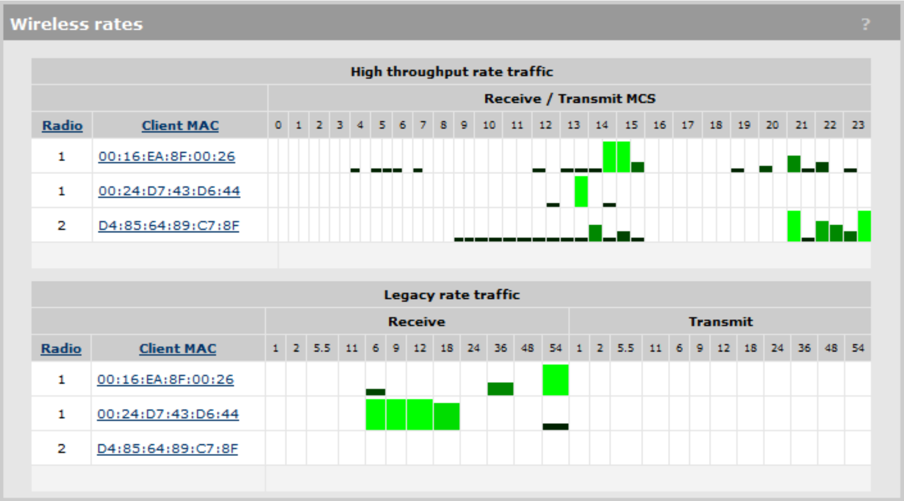
In most environments, SNR is a good indicator for the quality of the radio link between the client stations and the AP. A higher SNR value means a better quality radio link.

Action

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

Viewing wireless client data rates

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



Wireless rates ?

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

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

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

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.

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
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	19.50	21.70	40.50	45.00
17	39.00	43.30	81.00	90.00
18	58.50	65.00	121.50	135.00
19	78.00	86.70	162.00	180.00
20	117.00	144.40	243.00	270.00
21	156.00	173.30	324.00	360.00
22	175.50	195.00	364.50	405.00
23	195.00	216.70	405.00	450.00

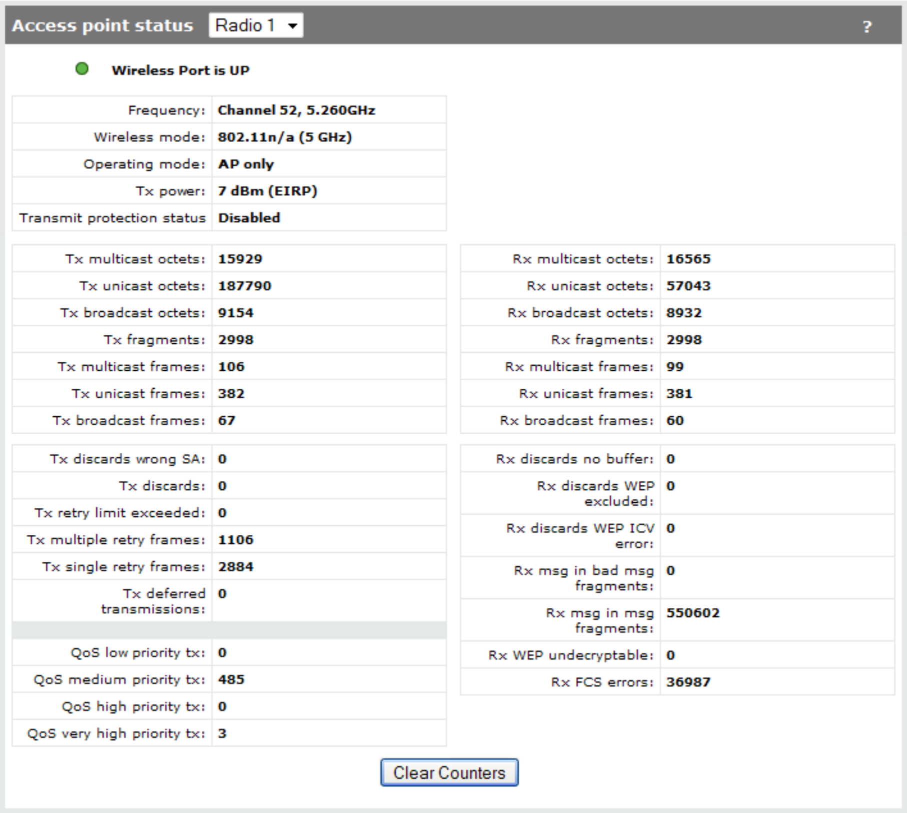
- MHz = megahertz
- ns = nanoseconds
- MCS 0 to MCS 15 are supported by the MSM410, MSM422, MSM430, MSM460, MSM466, and MSM466-R.

- MCS 16 to MCS 23 are supported by the MSM460, MSM466, and MSM466-R.
- For HT traffic, the MCS rate implies the number of spatial streams:
  - MCS 0 to 7: 1 spacial stream
  - MCS 8 to 15: 2 spacial stream
  - MCS 16 to 23: 3 spacial stream

Wireless access points

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

The information you see will vary depending on the AP. For example, this is the status page for an MSM460:



● Wireless Port is UP

Frequency:	Channel 52, 5.260GHz
Wireless mode:	802.11n/a (5 GHz)
Operating mode:	AP only
Tx power:	7 dBm (EIRP)
Transmit protection status	Disabled

Tx multicast octets:	15929
Tx unicast octets:	187790
Tx broadcast octets:	9154
Tx fragments:	2998
Tx multicast frames:	106
Tx unicast frames:	382
Tx broadcast frames:	67

Rx multicast octets:	16565
Rx unicast octets:	57043
Rx broadcast octets:	8932
Rx fragments:	2998
Rx multicast frames:	99
Rx unicast frames:	381
Rx broadcast frames:	60

Tx discards wrong SA:	0
Tx discards:	0
Tx retry limit exceeded:	0
Tx multiple retry frames:	1106
Tx single retry frames:	2884
Tx deferred transmissions:	0
QoS low priority tx:	0
QoS medium priority tx:	485
QoS high priority tx:	0
QoS very high priority tx:	3

Rx discards no buffer:	0
Rx discards WEP excluded:	0
Rx discards WEP ICV error:	0
Rx msg in bad msg fragments:	0
Rx msg in msg fragments:	550602
Rx WEP undecryptable:	0
Rx FCS errors:	36987

Access pointstatus

Wireless port

- **Up:** Port is operating normally.
- **Down:** Port is not operating.

Frequency

The current operating frequency.

Wireless mode

Current wireless mode.

Operating mode

Current operating mode.

Tx power

Current transmission power.

Transmit protection status

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

Tx multicast octets

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

Tx unicast octets

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

Tx fragments

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

Tx multicast frames

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

Tx unicast frames

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

Tx discards wrong SA

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

Tx discards

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

Tx retry limit exceeded

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

Tx multiple retry frames

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

Tx single retry frames

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

Tx deferred transmissions

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

QoS low priority tx

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

QoS medium priority tx

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

QoS high priority tx

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

QoS very high priority tx

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

Tx packets

Not shown on the MSM410, MSM430, MSM460, MSM466, and MSM466–R.

The total number of packets transmitted.

Tx dropped

Not shown on the MSM410, MSM430, MSM460, MSM466, and MSM466–R.

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 MSM410, MSM430, MSM460, MSM466, and MSM466–R.

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 MSM410, MSM430, MSM460, MSM466, and MSM466–R.

The total number of packets received.

Rx dropped

Not shown on the MSM410, MSM430, MSM460, MSM466, and MSM466–R.

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

Rx multicast octets

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

Rx unicast octets

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

Rx fragments

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

Rx multicast frames

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

Rx unicast frames

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

Rx discards no buffer

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

Rx discards WEP excluded

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

Rx discards WEP ICV error

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

Rx MSG in bad msg fragments

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

Rx MSG in msg fragments

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

Rx WEP undecryptable

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

Rx FCS errors

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

Clear counters

Select this button to reset all counters to zero.

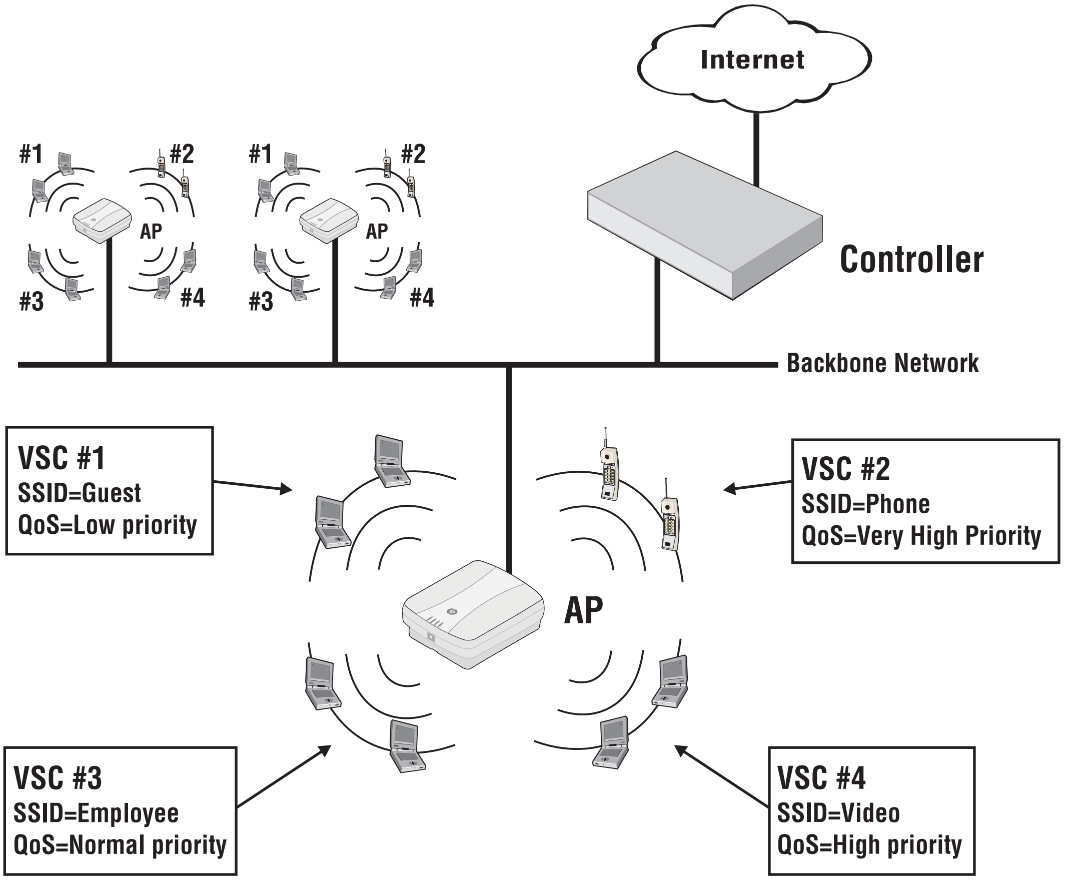
5 Working with VSCs

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.

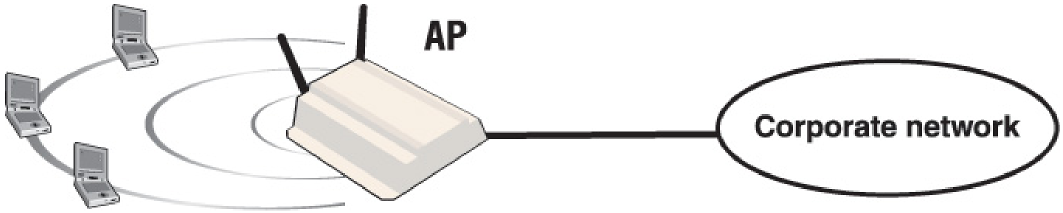
Multiple VSCs can be active at the same time, allowing for great flexibility in the configuration of services. Up to 64 VSC profiles can be configured, provided proper licensing is used.

In the following scenario, four VSCs are used to support different types of wireless users. Each VSC is configured with a different wireless network name (SSID), and the quality of service (QoS) feature is used to classify user traffic priority.



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.

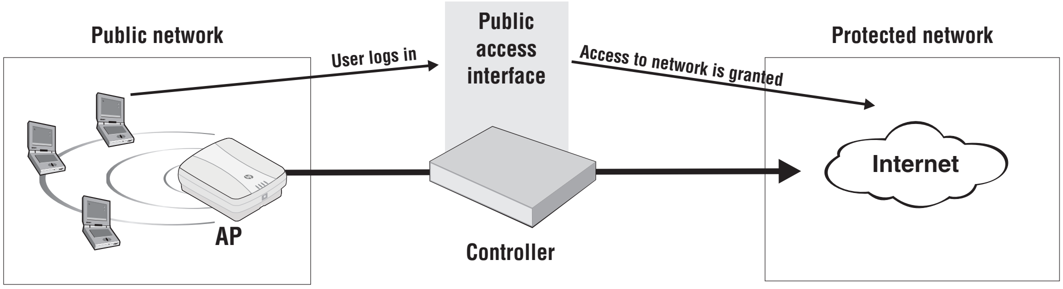
Using more than one authentication type in a VSC

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

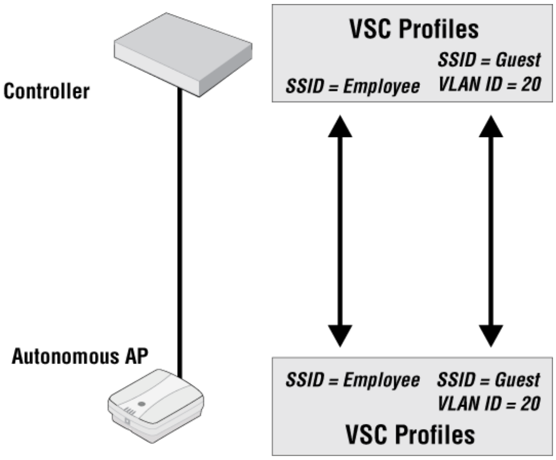
Autonomous APs can also be used with a controller to create a public access network infrastructure. In this type of deployment, all VSCs are access-controlled, which means that the AP forwards all wireless user traffic to the controller which handles user authentication and access control.

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



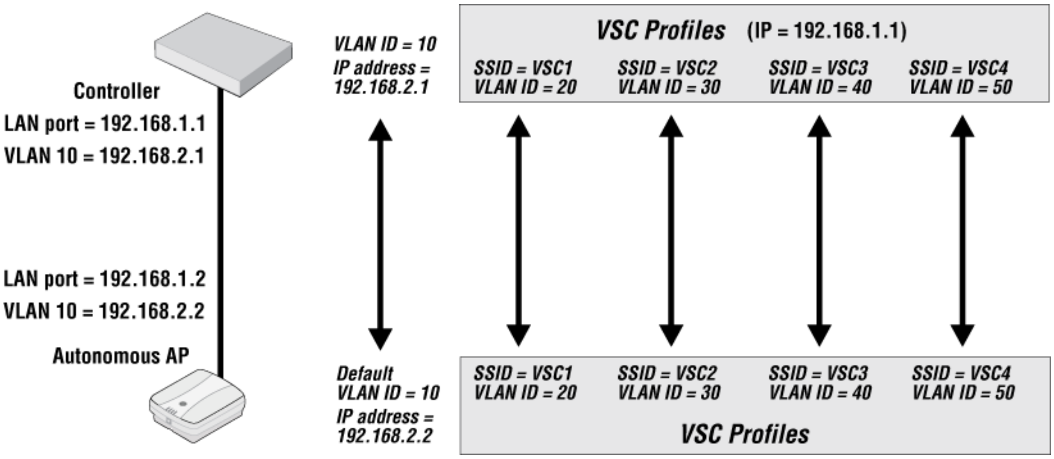
The following authentication types are supported on the controller: WPA / WPA2, 802.1X, MAC, HTML. For more information on controller authentication features, see the *MSM7xx Controllers Configuration Guide*.

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

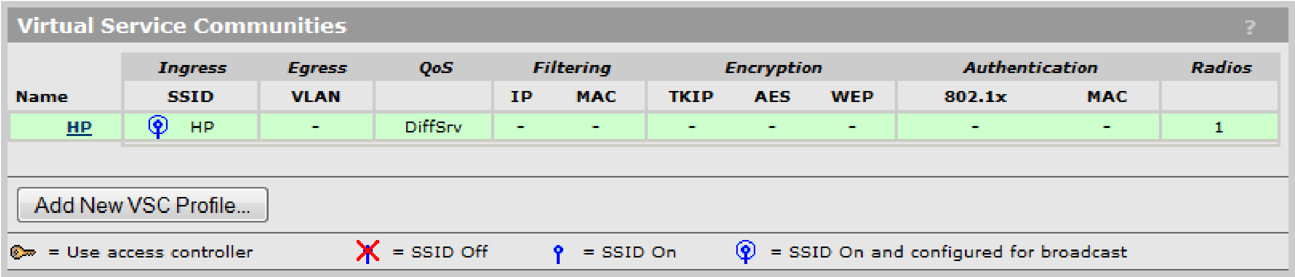
When operating in a VLAN environment, management traffic can be carried on its own VLAN. Configure the VSC on both the autonomous AP and the controller as illustrated.



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.



Virtual Service Communities

	Ingress	*Egress*	*QoS*	*Filtering*		*Encryption*			*Authentication*		*Radios*
Name	**SSID**	**VLAN**		**IP**	**MAC**	**TKIP**	**AES**	**WEP**	**802.1x**	**MAC**	
HP	📡 HP	-	DiffSrv	-	-	-	-	-	-	-	1

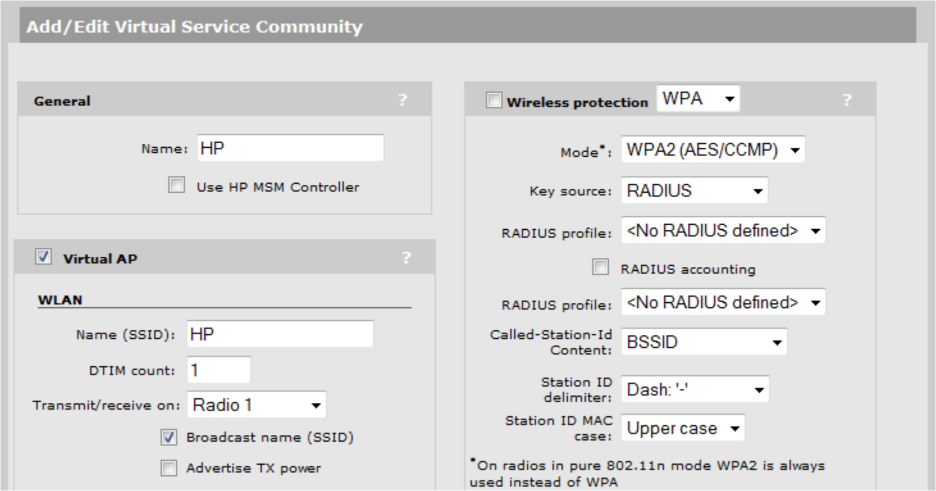
Add New VSC Profile...

🔑 = Use access controller ✗ = SSID Off 📡 = SSID On 📡 = SSID On and configured for broadcast

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.



Add/Edit Virtual Service Community

General

Name: HP

□ Use HP MSM Controller

☑ Virtual AP

WLAN

Name (SSID): HP

DTIM count: 1

Transmit/receive on: Radio 1

☑ Broadcast name (SSID)

□ Advertise TX power

□ Wireless protection WPA

Mode*: WPA2 (AES/CCMP)

Key source: RADIUS

RADIUS profile: <No RADIUS defined>

□ RADIUS accounting

RADIUS profile: <No RADIUS defined>

Called-Station-Id Content: BSSID

Station ID delimiter: Dash: '-'

Station ID MAC case: Upper case

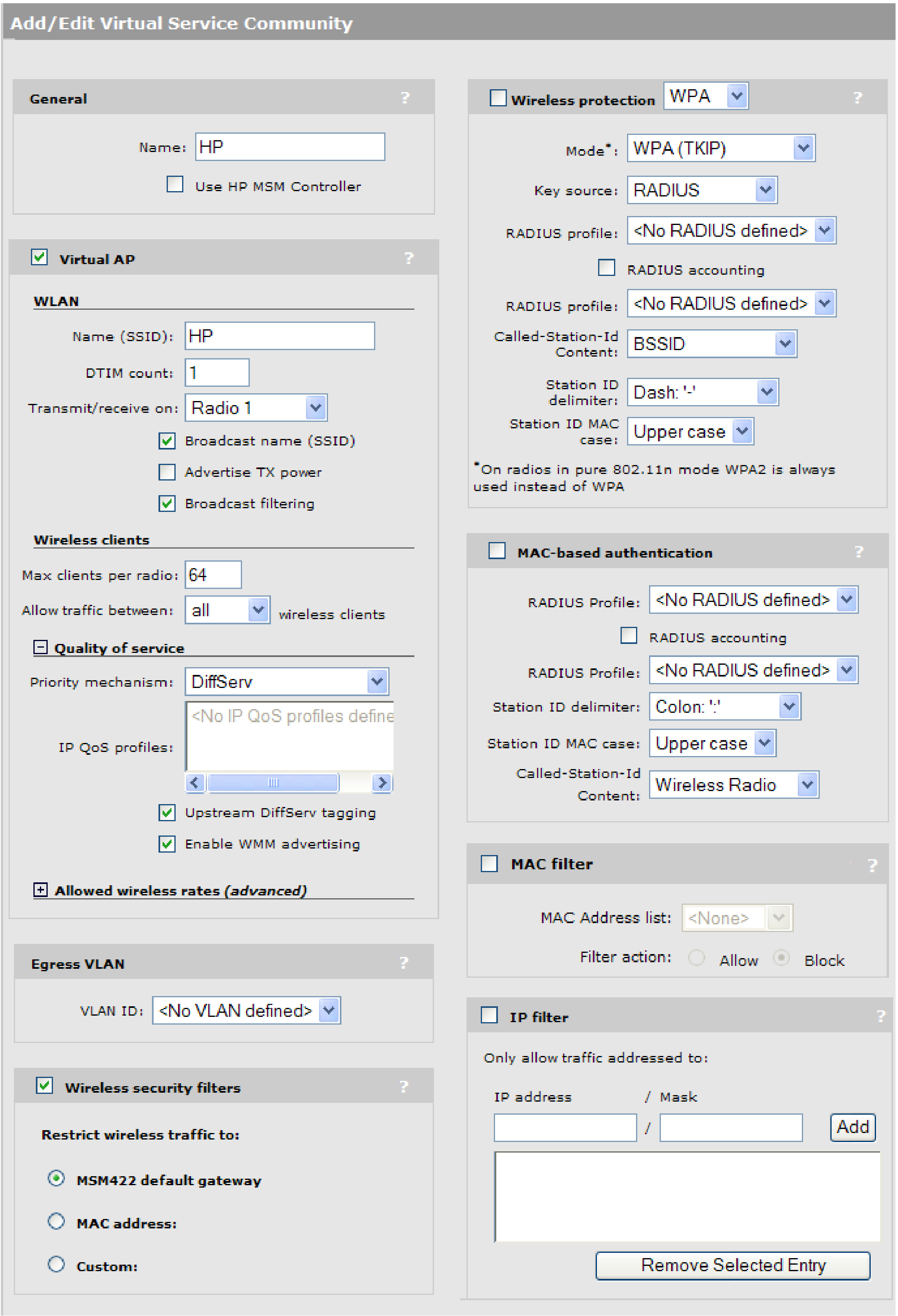
*On radios in pure 802.11n mode WPA2 is always used instead of WPA

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



Add/Edit Virtual Service Community

General

Name: HP

□ Use HP MSM Controller

☑ Virtual AP

WLAN

Name (SSID): HP

DTIM count: 1

Transmit/receive on: Radio 1

☑ Broadcast name (SSID)

□ Advertise TX power

☑ Broadcast filtering

Wireless clients

Max clients per radio: 64

Allow traffic between: all wireless clients

⊟ Quality of service

Priority mechanism: DiffServ

IP QoS profiles: <No IP QoS profiles define

☑ Upstream DiffServ tagging

☑ Enable WMM advertising

⊞ Allowed wireless rates *(advanced)*

Egress VLAN

VLAN ID: <No VLAN defined>

☑ Wireless security filters

Restrict wireless traffic to:

● MSM422 default gateway

○ MAC address:

○ Custom:

□ Wireless protection WPA

Mode*: WPA (TKIP)

Key source: RADIUS

RADIUS profile: <No RADIUS defined>

□ RADIUS accounting

RADIUS profile: <No RADIUS defined>

Called-Station-Id Content: BSSID

Station ID delimiter: Dash: '-'

Station ID MAC case: Upper case

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

□ MAC-based authentication

RADIUS Profile: <No RADIUS defined>

□ RADIUS accounting

RADIUS Profile: <No RADIUS defined>

Station ID delimiter: Colon: ':'

Station ID MAC case: Upper case

Called-Station-Id Content: Wireless Radio

□ MAC filter

MAC Address list: <None>

Filter action: ○ Allow ● Block

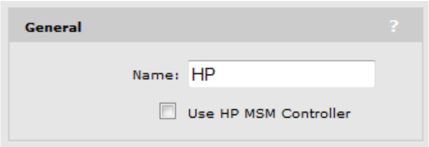
□ IP filter

Only allow traffic addressed to:

IP address / Mask

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.

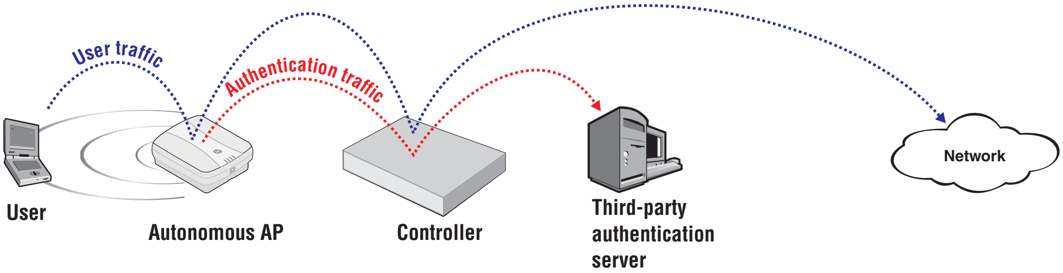


Name: HP

□ Use HP MSM Controller

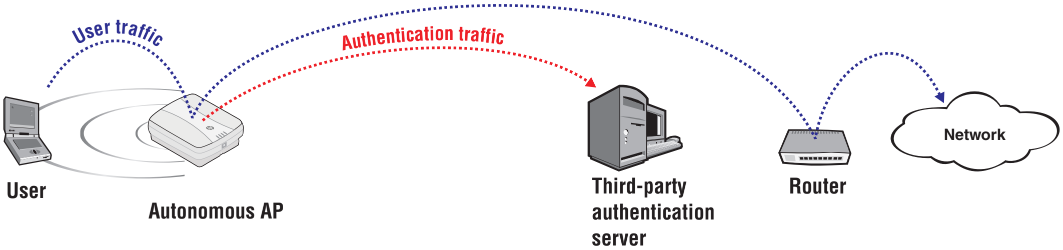
If the *Use HP MSM Controller* option is enabled

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 the *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.

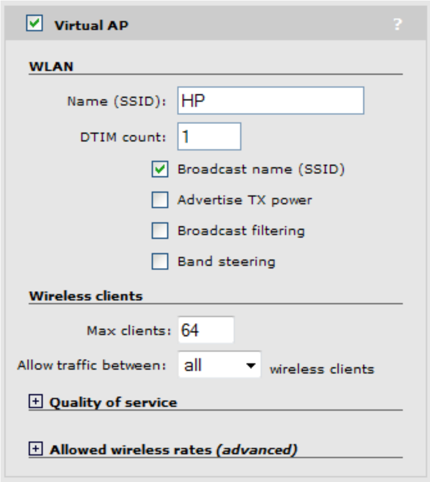
	The *Use HP MSM Controller* option is ...	
VSC option	**Enabled**	**Disabled**
Virtual AP	Available.	Available.
Egress VLAN	Available.	Available.
Wireless security filters	Available, but wireless traffic is restricted to the controller.	Available, but wireless traffic is restricted to the default gateway. Can be changed.

VSC option	The *Use HP MSM Controller* option is ...	
	Enabled	**Disabled**
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.
MAC filter	Available.	Available.
Wireless IP filter	Available.	Available.

Virtual AP

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

APs with a single radio



☑ Virtual AP

WLAN

Name (SSID): HP

DTIM count: 1

☑ Broadcast name (SSID)

□ Advertise TX power

□ Broadcast filtering

□ Band steering

Wireless clients

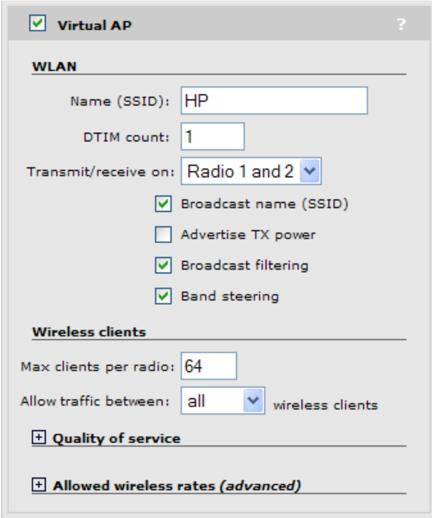
Max clients: 64

Allow traffic between: all wireless clients

⊞ Quality of service

⊞ Allowed wireless rates *(advanced)*

APs with dual radios



☑ Virtual AP

WLAN

Name (SSID): HP

DTIM count: 1

Transmit/receive on: Radio 1 and 2

☑ Broadcast name (SSID)

□ Advertise TX power

☑ Broadcast filtering

☑ Band steering

Wireless clients

Max clients per radio: 64

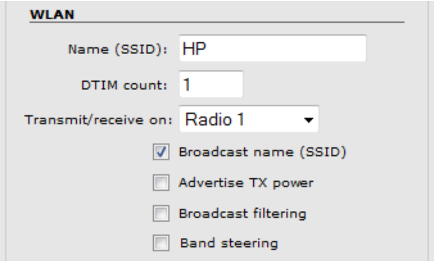
Allow traffic between: all wireless clients

⊞ Quality of service

⊞ Allowed wireless rates *(advanced)*

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

WLAN



WLAN

Name (SSID): HP

DTIM count: 1

Transmit/receive on: Radio 1

☑ Broadcast name (SSID)

□ Advertise TX power

□ Broadcast filtering

□ Band steering

Settings

Name (SSID)

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

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

DTIM count

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

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

Transmit/receive on

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

Broadcast name (SSID)

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

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

Advertise Tx power

When this option is enabled, APs broadcast their current transmit power setting in the wireless beacon. It also enables support for 802.11h 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, MSM430, MSM460, MSM466, MSM466-R

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

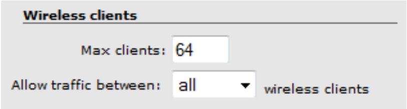
An AP uses the following methods to encourage a wireless client to associate at 5 GHz instead of 2.4 GHz.

- The AP waits 200 ms 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 clients signal strength at 5 GHz is greater than -80 dBm (decibel milliwatt). If the clients signal strength falls below -80 dBm, then the AP will respond to 2.4 GHz probes from the client without delay.

NOTE:

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

Wireless clients



Wireless clients

Max clients: 64

Allow traffic between: all wireless clients

Settings

Max clients per radio

Specify the maximum number of wireless client stations that can be associated with this SSID at the same time on each radio. On dual radio products the limit applies separately on each radio.

Allow traffic between nn wireless clients

Use this option to control how non-access-controlled wireless clients that are connected to the same VSC can communicate with each other. The following settings are available:

- **no**: Blocks all inter-client communications.
- **802.1X**: Only authenticated 802.1X clients can communicate.
- **all**: All authenticated and unauthenticated clients can communicate. Default setting.
- **IPv6**: Only authenticated clients using IP version 6 can communicate.

Communication between users connected to different non-access-controlled VSCs can only occur if the same VLAN is assigned in the **Egress VLAN** 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:

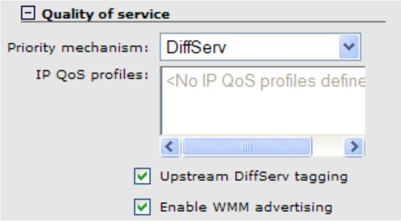
- Unicast traffic exchanged between VSCs on the **same** radio is controlled by the setting of either the sender's or the receiver's VSC.
- Unicast traffic exchanged between VSCs on **different** radios is controlled by the setting of the sender's VSC.
- Multicast traffic exchanged between VSCs is always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

Generally, most clients will be involved in the bidirectional exchange of unicast packets. In this case, the rules can be simplified by assuming that the most restrictive setting for this option takes precedence. For example:

- If VSC1 is set to **No** and VSC2 is set to **All**, no communication is permitted between clients on the two VSCs, or between clients on VSC1. However, all clients on VSC2 can communicate with each other.
- If VSC1 is set to **802.1X** and VSC2 set to **All**, only 802.1X clients can communicate between the two VSCs.

Quality of service

The quality of service (QoS) feature provides a number of different mechanisms to prioritize wireless traffic sent to wireless client stations. See “Quality of service” (page 77).



⊟ **Quality of service**

Priority mechanism: DiffServ

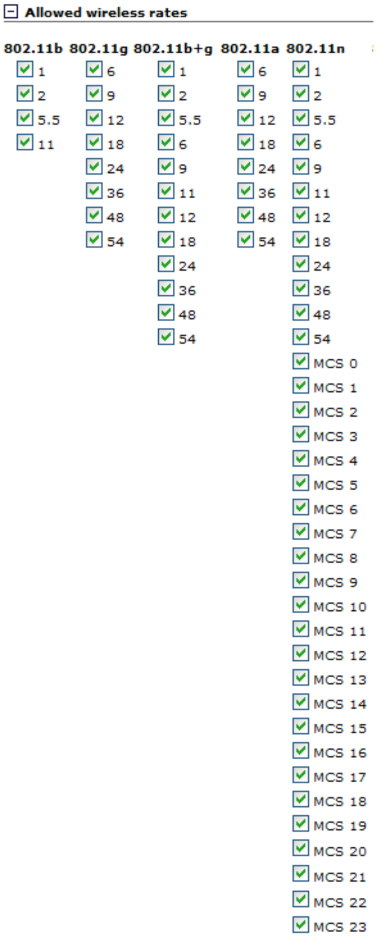
IP QoS profiles: <No IP QoS profiles define

☑ Upstream DiffServ tagging

☑ Enable WMM advertising

Allowed wireless rates

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



⊟ **Allowed wireless rates**

802.11b	802.11g	802.11b+g	802.11a	802.11n
☑ 1	☑ 6	☑ 1	☑ 6	☑ 1
☑ 2	☑ 9	☑ 2	☑ 9	☑ 2
☑ 5.5	☑ 12	☑ 5.5	☑ 12	☑ 5.5
☑ 11	☑ 18	☑ 6	☑ 18	☑ 6
	☑ 24	☑ 9	☑ 24	☑ 9
	☑ 36	☑ 11	☑ 36	☑ 11
	☑ 48	☑ 12	☑ 48	☑ 12
	☑ 54	☑ 18	☑ 54	☑ 18
		☑ 24		☑ 24
		☑ 36		☑ 36
		☑ 48		☑ 48
		☑ 54		☑ 54
				☑ MCS 0
				☑ MCS 1
				☑ MCS 2
				☑ MCS 3
				☑ MCS 4
				☑ MCS 5
				☑ MCS 6
				☑ MCS 7
				☑ MCS 8
				☑ MCS 9
				☑ MCS 10
				☑ MCS 11
				☑ MCS 12
				☑ MCS 13
				☑ MCS 14
				☑ MCS 15
				☑ MCS 16
				☑ MCS 17
				☑ MCS 18
				☑ MCS 19
				☑ MCS 20
				☑ MCS 21
				☑ MCS 22
				☑ MCS 23

All APs do not support all wireless modes and rates.

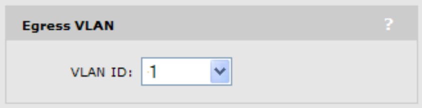
- **MCS 0 to MCS 15** are supported by the MSM410, MSM422, MSM430, MSM460, MSM466, MSM466-R.
- **MCS 16 to MCS 23** are supported by the MSM460, MSM466, MSM466-R.

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.

Egress VLAN

Sets the VLAN to which this profile forwards traffic. If you do not select a VLAN, traffic is sent untagged. VLANs can also be assigned using other methods, some of which may override the Egress VLAN. See “Working with VLANs” (page 86) for details.



Egress VLAN

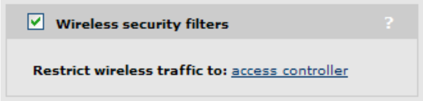
VLAN ID: 1

Wireless security filters

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

Settings

If **Use HP MSM Controller** is enabled under **General**, the AP will only forward user traffic that is addressed to the 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.

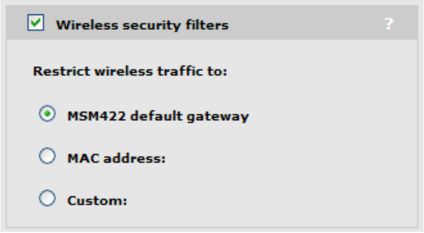


☑ Wireless security filters

Restrict wireless traffic to: access controller

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.



☑ Wireless security filters ?

Restrict wireless traffic to:

● MSM422 default gateway

○ MAC address:

○ Custom:

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

Custom wireless security filter definitions

Use this option to define your own security filters to control incoming and outgoing wireless traffic. To use the default filters as a starting point, select **Get Default Filters**.

Filters are specified using standard pcap syntax with the addition of a few HP-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.

Wireless mobility considerations

If you enable the wireless mobility feature (to support roaming across different subnets), configuration of the wireless security filters must respect the following guidelines so as not to interfere with roaming functionality.

- The **Restrict wireless traffic to: Access point default gateway** option is not supported.
- The **Restrict wireless traffic to: MAC** or **Custom** options can be used provided that they restrict traffic to destinations that are reachable from all subnets in the mobile domain.

Wireless protection

Three types of wireless protection are offered: WPA, 802.1X, and WEP.

WPA

This option enables support for users with WPA / WPA2 client software.

Mode

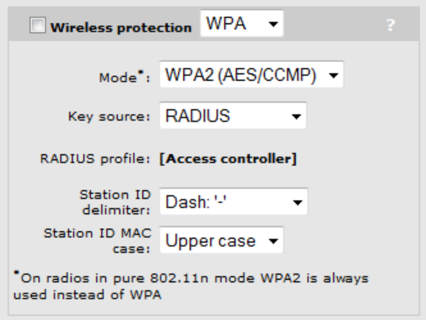
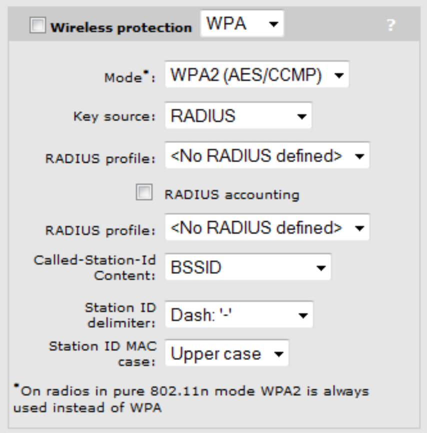
Support is provided for:

- **WPA (TKIP):** WPA with TKIP encryption. When you enable this option, the VSC can only support legacy a/b/g traffic. All 802.11n features on a radio are disabled for this VSC..
- **WPA2 (AES/CCMP):** WPA2 (802.11i) with AES/CCMP encryption.
- **WPA or WPA2:** Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time. Some legacy WPA clients may not work if this mode is selected. This mode is slightly less secure than using the pure WPA2 (AES/CCMP) option. **Note:** On radios that have

Client restriction set to 802.11n only or 802.11ac only, WPA2 is always used instead of WPA.

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
 ☐ Wireless protection: WPA Mode*: WPA2 (AES/CCMP) Key source: RADIUS RADIUS profile: [Access controller] Station ID delimiter: Dash: '-' Station ID MAC case: Upper case *On radios in pure 802.11n mode WPA2 is always used instead of WPA	 ☐ Wireless protection: WPA Mode*: WPA2 (AES/CCMP) Key source: RADIUS RADIUS profile: <No RADIUS defined> ☐ RADIUS accounting RADIUS profile: <No RADIUS defined> Called-Station-Id Content: BSSID Station ID delimiter: Dash: '-' Station ID MAC case: Upper case *On radios in pure 802.11n mode WPA2 is always used instead of WPA

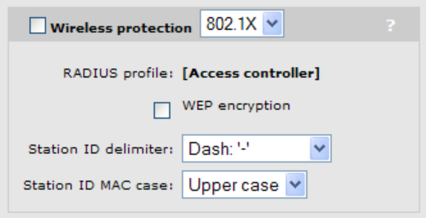
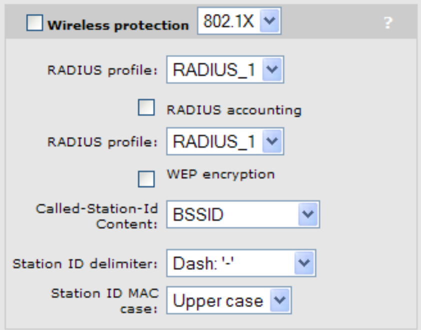
For a complete description of all options see the online help.

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.

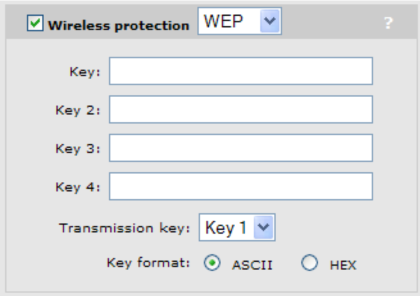
802.1X options supported when the
***Use HP MSM controller* option is ...**

Enabled	Disabled
 ☐ Wireless protection: 802.1X RADIUS profile: [Access controller] ☐ WEP encryption Station ID delimiter: Dash: '-' Station ID MAC case: Upper case	 ☐ Wireless protection: 802.1X RADIUS profile: RADIUS_1 ☐ RADIUS accounting RADIUS profile: RADIUS_1 ☐ WEP encryption Called-Station-Id Content: BSSID Station ID delimiter: Dash: '-' Station ID MAC case: Upper case

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

WEP

This option provides support for users using WEP encryption.



☑ Wireless protection WEP ?

Key:

Key 2:

Key 3:

Key 4:

Transmission key: Key 1

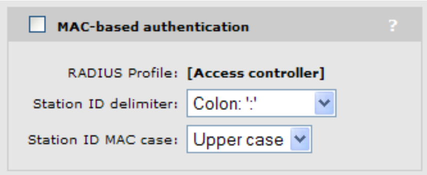
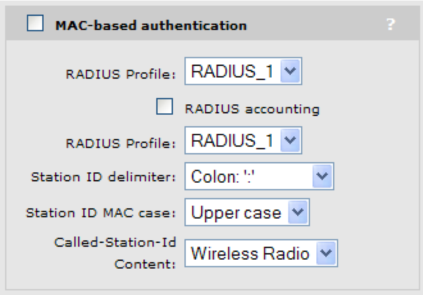
Key format: ● ASCII ○ HEX

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

NOTE: When the radio used by a VSC is configured to support 802.11n, and the VSC is configured to use WEP, the VSC can only support legacy a/b/g traffic. (Except on the MSM422, where WEP is not supported when the radio is configured for 802.11n.)

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.

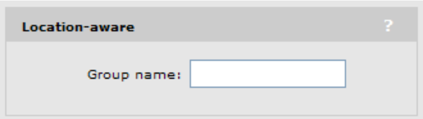
MAC-based authentication options supported when the *Use HP MSM Controller* option is ...	
Enabled	**Disabled**
 □ MAC-based authentication ? RADIUS Profile: [Access controller] Station ID delimiter: Colon: ':' Station ID MAC case: Upper case	 □ MAC-based authentication ? RADIUS Profile: RADIUS_1 □ RADIUS accounting RADIUS Profile: RADIUS_1 Station ID delimiter: Colon: ':' Station ID MAC case: Upper case Called-Station-Id Content: Wireless Radio

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**.

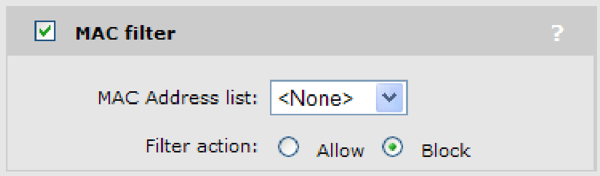


Location-aware ?

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. Select the MAC address list to use. Each list can contain up to 256 MAC addresses.



☑ MAC filter

MAC Address list: <None>

Filter action: ○ Allow ● Block

To define a MAC address list, see "Configuring MAC address lists" (page 104).

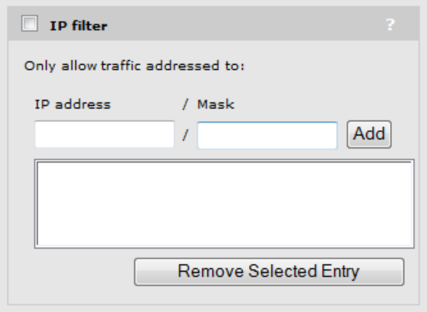
The following table describes how the MAC filter functions when it is used alone and in combination with other authentication options:

Client address	Filter action	When used alone	When used with MAC-based authentication	When used with 802.1X authentication
Client address is in the MAC address list.	Allow	Access is granted.	Access is granted. MAC-based authentication is not performed.	Access is granted or denied based on result of 802.1X authentication.
Client address is in the MAC address list.	Block	Access is denied.	Access is denied. MAC-based authentication is not performed.	Access is denied.
Client address is **not** in the MAC address list.	Allow	Access is denied.	Access is granted or denied based on result of MAC-based authentication. (Not supported on access-controlled VSCs.)	Access is granted or denied based on result of 802.1X authentication.
Client address is **not** in the MAC address list.	Block	Access is granted.	Access is granted or denied based on result of MAC-based authentication.	Access is granted or denied based on result of 802.1X authentication.

IP filter

When this option is enabled, the VSC only allows wireless traffic that is addressed to an IP address that is defined in the list. All other traffic is blocked, except for:

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



□ IP filter

Only allow traffic addressed to:

IP address / Mask

A maximum of two addresses can be defined. Each address can target a specific device or a range of addresses.

Examples

To only allow traffic addressed to a gateway at the address 192.168.130.1, define the filter as follows:

- Address = 192.168.130.1
- Mask = 255.255.255.255

To only allow traffic addressed to the network 192.168.130.0, define the filter as follows:

- Address = 192.168.130.0
- Mask = 255.255.255.0

VSC data flow

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” (page 76).
- **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” (page 70).
- **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” (page 75).
- **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” (page 75).

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 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” (page 70).

- **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" (page 75).
- **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" (page 75).

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 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.

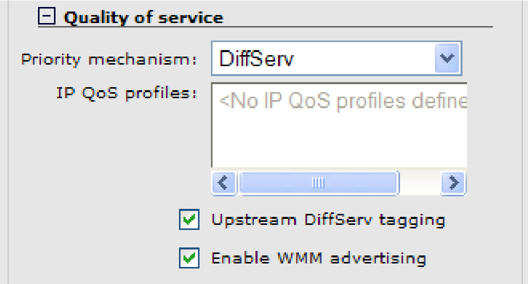
Egress

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 can be enabled on a VSC, see "Quality of service" (page 77), or on a local mesh link, see "Quality of service" (page 110).

The quality of service (QoS) setting (under Virtual AP in a VSC) 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.



⊟ Quality of service

Priority mechanism: DiffServ

IP QoS profiles: <No IP QoS profiles define

☑ Upstream DiffServ tagging

☑ Enable WMM advertising

The QoS feature defines four traffic queues based on the Wi-Fi Multimedia (WMM) access categories. In order of priority, these queues are:

Queue	WMM access category	Typically used for
1	AC_VO	Voice traffic
2	AC_VI	Video traffic
3	AC_BE	Best effort data traffic
4	AC_BK	Background data traffic

Outgoing wireless traffic on the VSC is assigned to a queue based on the selected priority mechanism. Traffic delivery is based on strict priority (per the WMM standard). Therefore, if excessive traffic is present on queues 1 or 2, it will reduce the flow of traffic on queue 3 and queue 4.

Regardless of the priority mechanism that is selected:

- Traffic that cannot be classified by a priority mechanism is assigned to queue 3.
- SVP (SpectraLink Voice Protocol) traffic is always assigned to queue 1, except if you select the VSC-based priority mechanism, in which case SVP traffic is assigned to the configured queue.

Priority mechanisms

Priority mechanisms are used to classify traffic on the VSC and assign it to the appropriate queue. The following mechanisms are available:

802.1p

This mechanism classifies traffic based on the value of the VLAN priority field present within the VLAN header.

Queue	802.1p (VLAN priority field value)
1	6, 7
2	4, 5
3	0, 3
4	1, 2

VSC-based priority

This mechanism is unique to HP. It enables you to assign a single priority level to all traffic on a VSC. If you enable the VSC-based priority mechanism, it takes precedence regardless of the priority mechanism supported by associated client stations. For example, if you set VSC-based low priority, then all devices that connect to the VSC have their traffic set at this priority, including SVP clients.

Queue	VSC-based priority value
1	VSC-based Very High
2	VSC-based High
3	VSC-based Normal
4	VSC-based Low

DiffServ (Differentiated Services)

This mechanism classifies traffic based on the value of the Differentiated Services (DS) codepoint field in IPv4 and IPv6 packet headers (as defined in RFC2474). The codepoint is composed of the six most significant bits of the DS field.

Queue	DiffServ (DS codepoint value)
1	111000 (Network control) 110000 (Internetwork control)
2	101000 (Critical) 100000 (Flash override)
3	011000 (Flash) 000100 (Routine)
4	010000 (Immediate) 001000 (Priority)

TOS

This mechanism classifies traffic based on value of the TOS (Type of Service) field in an IP packet header.

Queue	TOS (Type of Service field value)
1	0x30, 0xE0, 0x88, 0xB8
2	0x28, 0xA0
3	0x08, 0x20
4	All other TOS traffic

IP QoS

This option lets you assign traffic to the queues based on the criteria in one or more IP QoS profiles. Each profile lets you target traffic on specific ports or using specific protocols.

Disabled

When QoS traffic prioritization is disabled, all traffic is sent to queue 3.

IP QoS profiles

This option is only available if you set the **Priority mechanism** to **IP QoS**.

Select the IP QoS profiles to use for this profile. To add QoS profiles to the list, use the **Network > IP QoS** page.

Up to 10 profiles can be selected. To select more than one profile, hold down the CTRL key as you select profile names in the list.

To define an IP QoS profile, see "Configuring IP QoS profiles" (page 26).

Upstream DiffServ tagging

Enable this option to have the AP apply differentiated services marking to upstream traffic.

Layer 3 upstream marking ensures end-to-end quality of service in your network. Data originating on the wireless network can now be carried throughout the network (wireless *and* wired) with a consistent quality of service and priority. This feature is enabled by default.

When this feature is enabled, packets received on the wireless interface that include Wi-Fi Multimedia (WMM) QoS values are remarked using IP DiffServ values when transmitted to the wired network. (Remarking is only done for packets that have a DiffServ value of 0. The original DiffServ value from the wireless client is preserved for all other packets.)

Upstream/downstream traffic marking

Depending on the priority mechanism that is active, upstream and downstream traffic is marked as described in this section.

Upstream traffic marking

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

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.) If L3 marking is enabled and the L3 marking value is higher than the L2 marking value, then the L3 marking value is used for L2 marking.	DiffServ (Remarking is only done for packets that have a DiffServ value of 0, otherwise the original value is preserved.)	Pass-through (Original layer 3 marking, if any, is preserved.)
DiffServ	DiffServ		Pass-through (Original layer 3 marking, if any, is preserved.)	
TOS	TOS		Pass-through (Original layer 3 marking, if any, is preserved.)	
VSC-based	WMM, Non-WMM		Uses the selected VSC-based value (very high, high, normal, low).	
IP QoS	WMM		Pass-through (Original layer 3 marking, if any, is preserved.)	

Downstream traffic marking

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

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

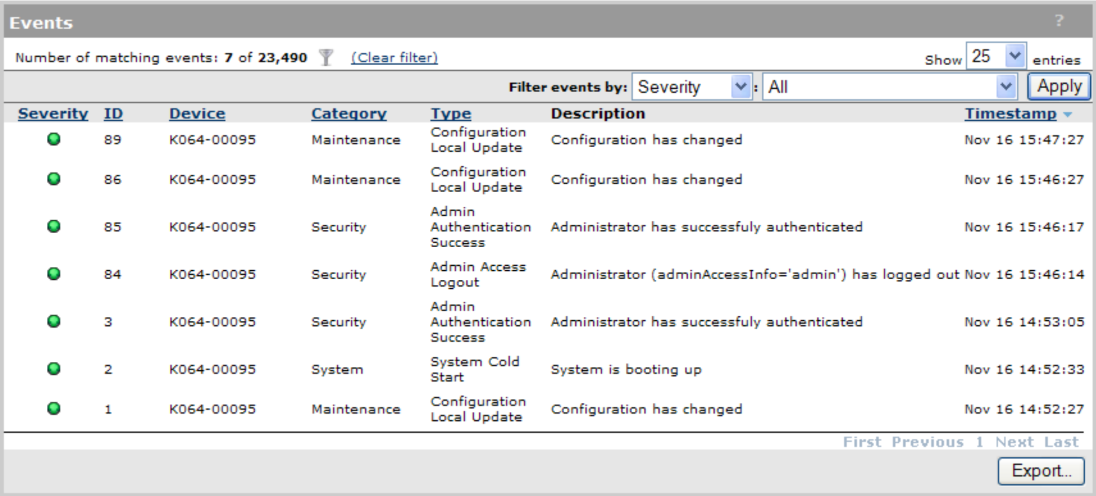
6 Events

The events feature provides a logging system that can be used by administrators and support personnel to easily monitor and troubleshoot system issues.

Note: For backward compatibility, the system log feature that was available in previous releases is still available on the **Tools** menu.

An event is the occurrence of a condition that has been detected in the network infrastructure. For example, wireless client association/disassociation, radios turned on/off, radio power/channel changes and more. A record of events is typically stored over relatively long periods of time to assist with OAM&P and auditing activities.

A new Events page has been created on the Tools menu that replaces and enhances the old client event log. The following screen capture shows the Events page with a number of events.



Number of matching events: 7 of 23,490 (Clear filter) Show 25 entries

Filter events by: Severity : All Apply

Severity	ID	Device	Category	Type	Description	Timestamp
●	89	K064-00095	Maintenance	Configuration Local Update	Configuration has changed	Nov 16 15:47:27
●	86	K064-00095	Maintenance	Configuration Local Update	Configuration has changed	Nov 16 15:46:27
●	85	K064-00095	Security	Admin Authentication Success	Administrator has successfuly authenticated	Nov 16 15:46:17
●	84	K064-00095	Security	Admin Access Logout	Administrator (adminAccessInfo='admin') has logged out	Nov 16 15:46:14
●	3	K064-00095	Security	Admin Authentication Success	Administrator has successfuly authenticated	Nov 16 14:53:05
●	2	K064-00095	System	System Cold Start	System is booting up	Nov 16 14:52:33
●	1	K064-00095	Maintenance	Configuration Local Update	Configuration has changed	Nov 16 14:52:27

The Severity, Device, Alarm, and Timestamp columns display detailed information if you hover the mouse pointer over an entry in the table as shown.

You can also sort events in any column (except Description) by clicking the column title.

Filter events by

To see only a subset of all events, select a filter condition and click **Apply**. Filters are saved across sessions and can be cleared by selecting **Clear filters.** To see only a subset of all events, select a filter condition and click **Apply**.

Filters are saved across sessions and can be cleared by selecting **Clear filters.**

Table

Severity

- **Critical (Red):** Events of this type indicate a failure and signal the need for immediate attention.
- **Major (Orange):** Events of this type indicate an impending failure.
- **Minor (Yellow):** Events of this type indicate a warning condition that can escalate into a more serious problem.
- **Informational (Green):** Events of this type require no action. They are provided for information purposes.

ID

Unique number assigned to the event.

Device

Indicates the device that detected the event. Hover the mouse pointer over the device name to see the device type and its MAC address.

Category

Events are classified into categories so that they can be sorted. Categories include:

- 802.1X
- Controlled AP
- DHCP
- MAC Authentication
- Maintenance
- MTM
- Public Access
- REI
- RRM
- Satellite Management
- Security
- Syslog
- System
- Teamed Controller
- Teaming
- VPN
- VSC
- Wireless
- WPA

Type

Classifies the event within a category. Categories are predefined and cannot be changed.

Alarm

If an event triggers an alarm, the appropriate alarm indicator appears in this column. Hover the mouse pointer over the alarm to see its severity and ID. The association between an event and an alarm is predefined and is not configurable.

Description

Detailed information about the event.

Timestamp

Date and time that the event occurred.

Button

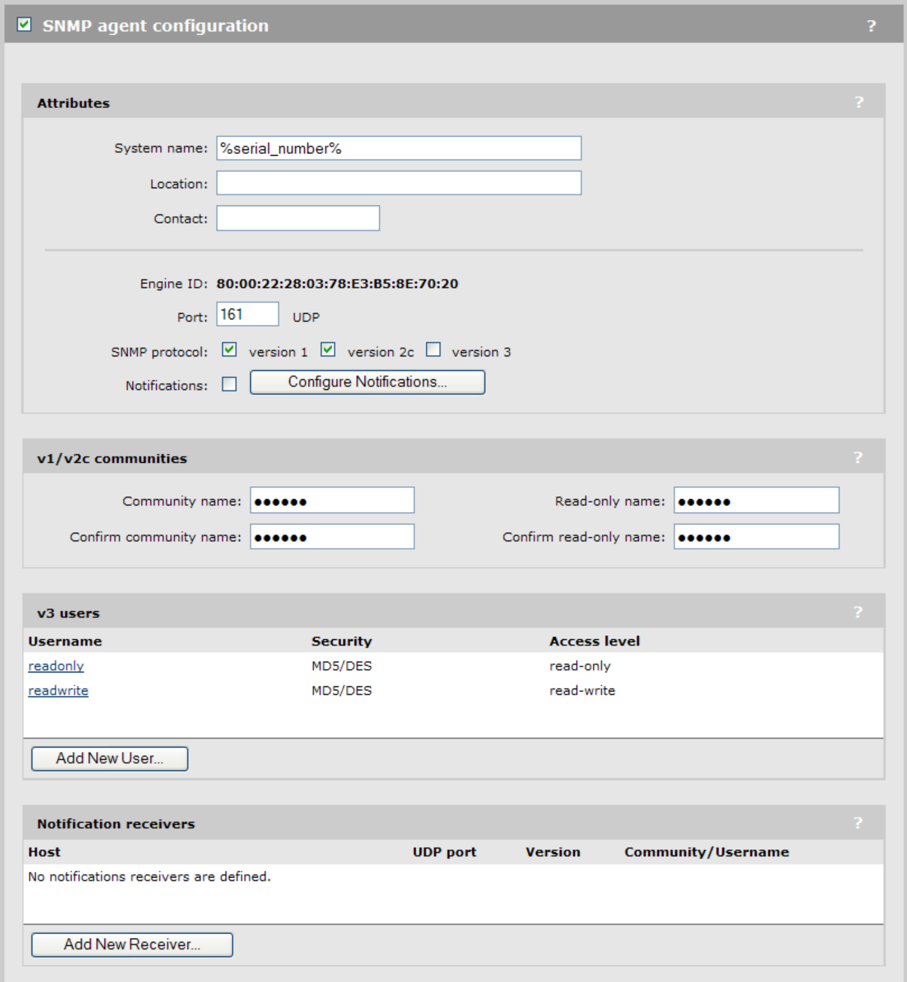
Export

Click this button to export all the events that are visible in the table to a CSV (comma-separated values) file for use in other applications.

Configuring SNMP notifications for events

Notifications can be set via SNMP for specific events as follows:

1. Select **Management > SNMP**. The SNMP agent configuration page opens.



☑ SNMP agent configuration ?

Attributes ?

System name:	%serial_number%
Location:	
Contact:	
Engine ID:	80:00:22:28:03:78:E3:B5:8E:70:20
Port:	161 UDP
SNMP protocol:	☑ version 1 ☑ version 2c ☐ version 3
Notifications:	☐ Configure Notifications...

v1/v2c communities ?

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

v3 users ?

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

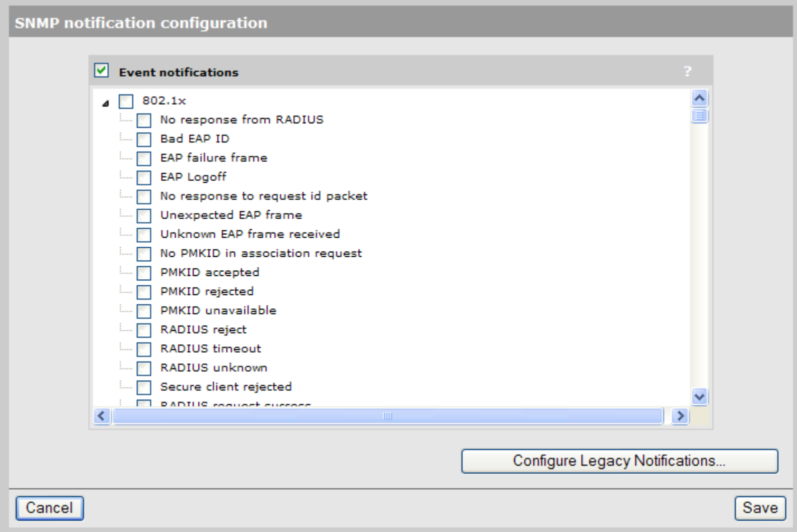
Add New User...

Notification receivers ?

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

Add New Receiver...

2. Select the **SNMP agent configuration** checkbox.
3. Under **Attributes**, select the **Notifications** checkbox.
4. Select **Configure Notifications**. The SNMP notification configuration page opens.



SNMP notification configuration

☑ Event notifications

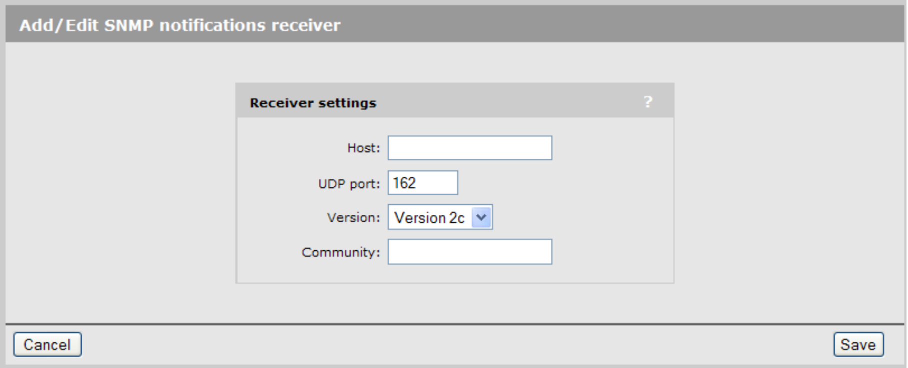
- □ 802.1x
  - □ No response from RADIUS
  - □ Bad EAP ID
  - □ EAP failure frame
  - □ EAP Logoff
  - □ No response to request id packet
  - □ Unexpected EAP frame
  - □ Unknown EAP frame received
  - □ No PMKID in association request
  - □ PMKID accepted
  - □ PMKID rejected
  - □ PMKID unavailable
  - □ RADIUS reject
  - □ RADIUS timeout
  - □ RADIUS unknown
  - □ Secure client rejected
  - □ RADIUS request success

Configure Legacy Notifications...

Cancel

Save

5. Enable **Event notifications** and select the notifications that you want to send.
6. Select **Save**. You are returned to he SNMP agent configuration page.
7. In the **Notifications receivers** box, select **Add New Receiver**. The Add/Edit SNMP notifications receiver page opens.



Add/Edit SNMP notifications receiver

Receiver settings

Host:	
UDP port:	162
Version:	Version 2c
Community:	

Cancel

Save

8. Define the settings for the receiver as follows:
   - **Host:** Specify the domain name or IP address of the SNMP notifications receiver to which the controller will send notifications.
   - **UDP port:** Specify the port on which notifications will be sent.
   - **SNMP version:** Select the SNMP version (v1, v2c, v3) for this receiver.
   - **Community:** For SNMP v1 and v2c, specify the SNMP community name of the receiver. For SNMP v3, select the SNMP v3 username of the receiver.
9. Select **Save**.

7 Working with VLANs

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 users account.

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

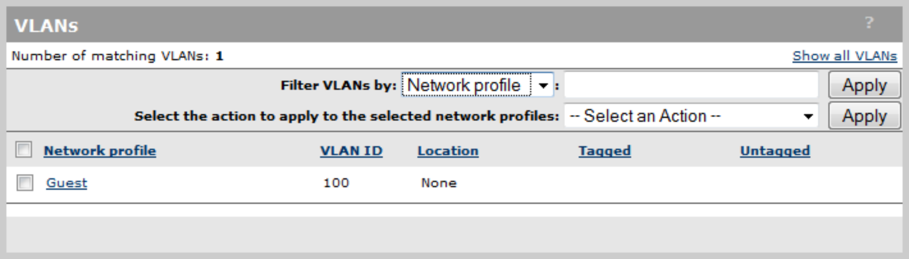
The following AP features can be supported on a VLAN:

- Management tool access
- SNMP access
- SOAP access

Defining a VLAN on a port

Define a VLAN on AP port as follows:

1. Define a network profile with the required VLAN as described under "To define a new network profile" (page 14). This example uses a new network profile called Guest, assigned to VLAN 100.
2. Select **Network > VLANs**.



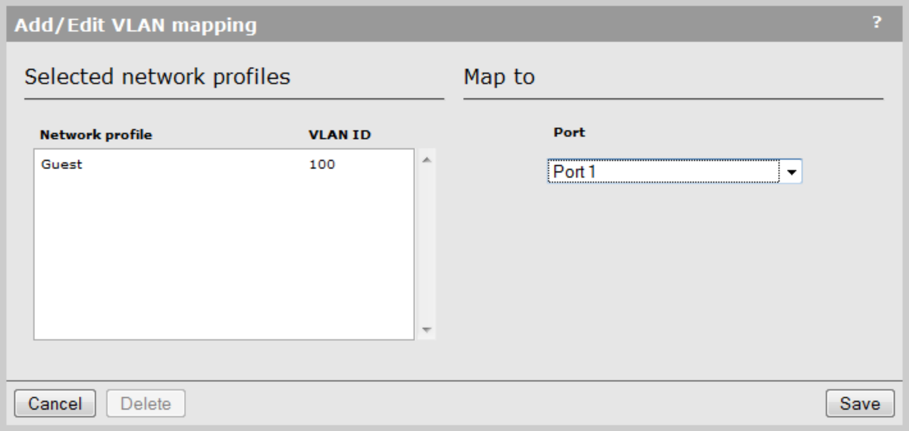
Number of matching VLANs: 1

Filter VLANs by: Network profile :

Select the action to apply to the selected network profiles: -- Select an Action --

□ Network profile	VLAN ID	Location	Tagged	Untagged
□ Guest	100	None		

3. Select the network profile you defined in step 1 (Guest). This opens the Add/Edit VLAN mapping page.



Network profile	VLAN ID
Guest	100

Port: Port 1

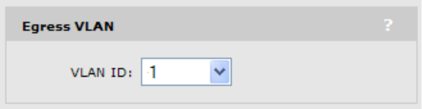
4. Under **Map to,** select the port to which the VLAN will be bound.
5. Select **Save**.

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 a **VLAN ID**. To be included in the drop-down list, the VLAN must mapped to a port on the **Network > VLANs** page and not be assigned to a VLAN range.



Egress VLAN

VLAN ID: 1

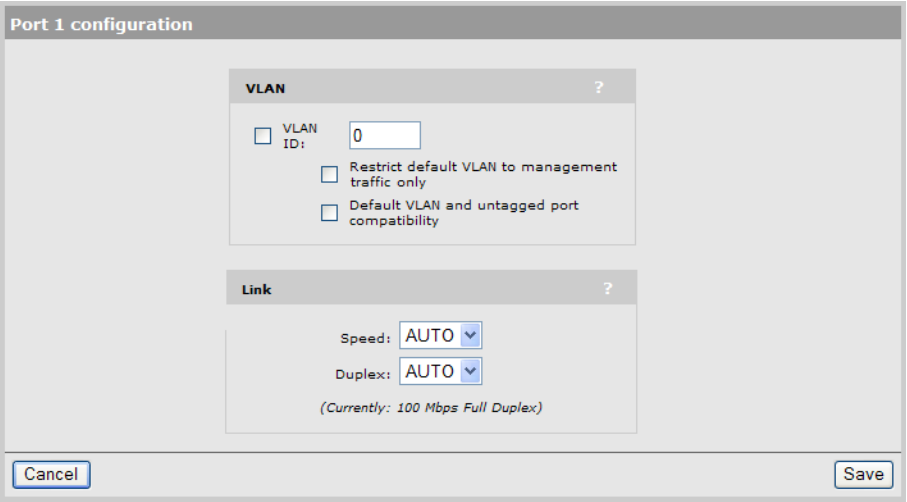
3. Select **Save**.

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.

To configure a default VLAN, do the following:

1. Select **Network > Ports**. Select Port 1 or Port 2 if available. This displays the Port configuration page.



Port 1 configuration

VLAN

□ VLAN ID: 0

□ Restrict default VLAN to management traffic only

□ Default VLAN and untagged port compatibility

Link

Speed: AUTO

Duplex: AUTO

(Currently: 100 Mbps Full Duplex)

2. Under **VLAN**, configure the following settings:
   - Enable the **VLAN ID** check box and specify a VLAN number.
   - If required, enabled the **Restrict default VLAN to management traffic only** check box. This restricts the 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.
  - If required, enable the **Default VLAN and untagged port compatibility** check box. This causes any traffic sent on the default VLAN to also be sent untagged on the port:

3. Select **Save**.

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 users 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.

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

8 Authentication services

Using a third-party 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 manager logins using a third-party RADIUS server" (page 91).
Validating user login credentials for WPA, 802.1X, or MAC-based authentication types on non-access-controlled VSCs.	"Wireless protection" (page 72). "MAC-based authentication" (page 74).
Retrieving RADIUS attributes on a per-user basis on non-access-controlled VSCs.	"Configuring user accounts on a RADIUS server" (page 92).
Storing accounting information for each user on non-access-controlled VSCs.	Accounting support is enabled under "Wireless protection" (page 72) or "MAC-based authentication" (page 74).

NOTE:

- On VSCs that have the **Use HP MSM controller** option enabled (creating an access-controlled VSC), see the *MSM7xx Controllers 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 server profile

The AP enables you to define up to 64 RADIUS profiles (depending on the license that is installed). 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.

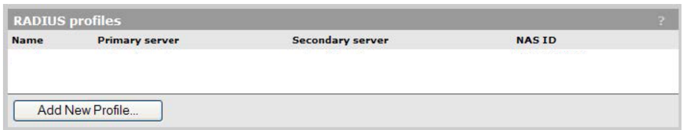
For backup redundancy, each profile supports a primary and secondary server.

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, PAP, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA, EAP-FAST, and EAP-GTC. (EAP-MD5 is not supported on VSCs that have WEP with dynamic keys enabled.)

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

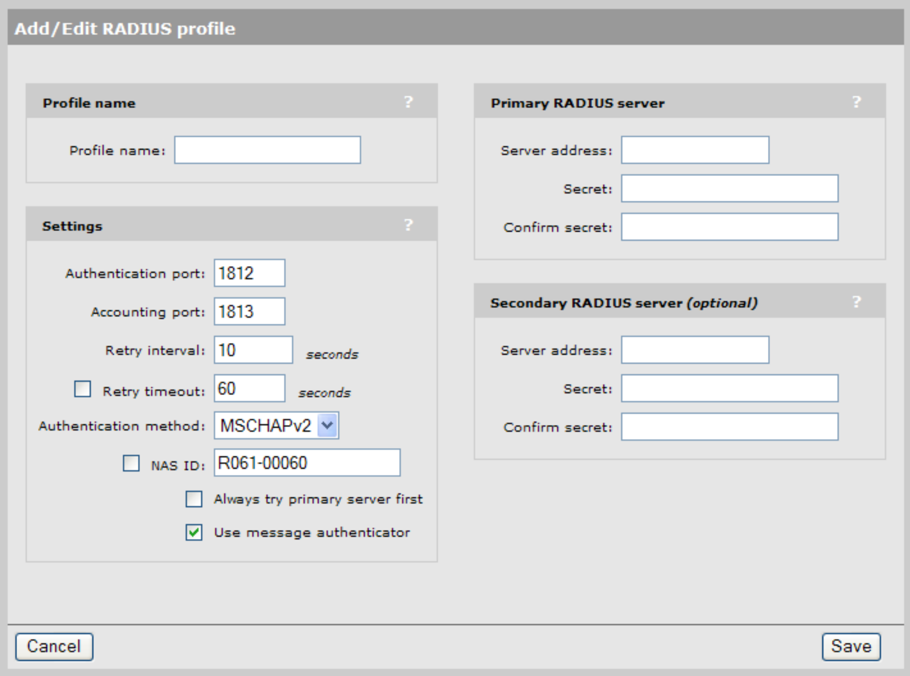
Configuration procedure

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



Name	Primary server	Secondary server	NAS ID

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



Add/Edit RADIUS profile

Profile name

Profile name:

Settings

Authentication port: 1812

Accounting port: 1813

Retry interval: 10 *seconds*

□ Retry timeout: 60 *seconds*

Authentication method: MSCHAPv2

□ NAS ID: R061-00060

□ Always try primary server first

☑ Use message authenticator

Primary RADIUS server

Server address:

Secret:

Confirm secret:

Secondary RADIUS server *(optional)*

Server address:

Secret:

Confirm secret:

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

Configuration parameters

Profile name

Specify a name to identify the profile.

Settings

Authentication port:

Specify a port on the RADIUS server to use for authentication. By default RADIUS servers use port 1812.

Accounting port

Specify a port on the RADIUS server to use for accounting. By default RADIUS servers use port 1813.

Retry interval

Specify the number of seconds that the AP waits before access and accounting requests time out. If the AP 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 or operator access to the management tool
- User authentication by way of HTML
- MAC-based authentication of devices
- Authentication of the AP
- Authentication of the controlled AP

You can determine the maximum number of retries as follows:

- HTML-based logins: Calculate the number of retries by taking the setting for the HTML-based logins **Authentication Timeout** parameter and dividing it by the value of this parameter. Default settings result in 4 retries (40 / 10).
- MAC-based and AP 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, HP recommends that you use either EAP-MD5 or MSCHAP V2 (if supported by your RADIUS server). PAP and MSCHAP V1 are less secure protocols. (EAP-MD5 is not supported on VSCs that have WEP with dynamic keys enabled.)

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 configured, 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

Specify the IP address or fully-qualified domain name of the 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.

Authentication realms

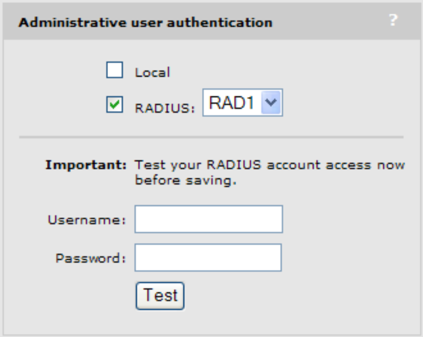
Authenticating manager logins using a third-party RADIUS server

Using a RADIUS server enables you to have multiple manager accounts, each with a unique login name and password. Identify manager accounts using the vendor specific attribute **web-administrative-role**. Valid values for this attribute are **Manager** and **Operator**. For attribute information, see “Configuring administrative accounts on a RADIUS server” (page 97). To use a RADIUS server, you must define a RADIUS profile on the **Authentication > RADIUS profiles** page.

NOTE: Login credentials for managers can be verified using local account settings and/or an third-party RADIUS sever. If both options are enabled, the RADIUS server is always checked first.

Configure RADIUS authentication as follows:

1. Define an account for the administrator on the RADIUS server. See “Configuring administrative accounts on a RADIUS server” (page 97).
2. On the controller, create a RADIUS profile that will connect the controller to the RADIUS server. See “Configuring a RADIUS server profile” (page 89).
3. Select **Management > Management tool**.
4. Under **Administrator authentication**, set **Authenticate via** to the RADIUS profile you created. In this example, the profile is called **RAD1**.



Administrative user authentication

□ Local

☑ RADIUS: RAD1

Important: Test your RADIUS account access now before saving.

Username:

Password:

Test

5. 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.)

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

Attribute	Admin login	802.1X	MAC	Format
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	✔	✕

Attribute	802.1X	MAC
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:

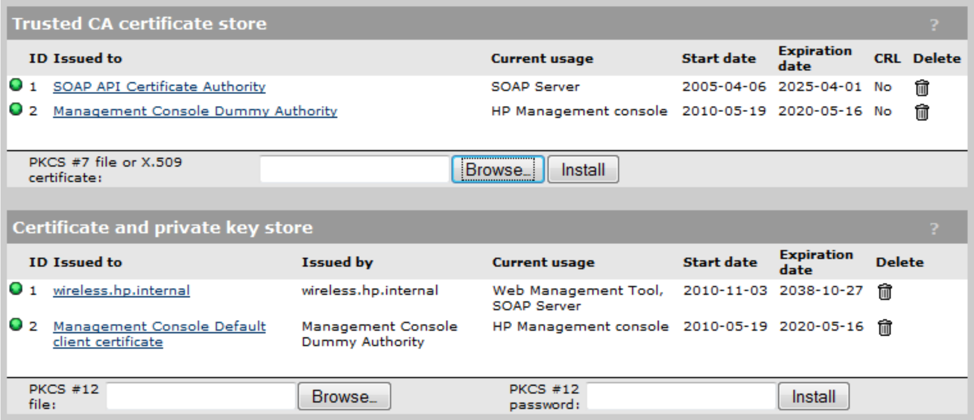
Parameter	Description
role	Use one of the following values to identify the role of the account: ◦ **Manager:** A manager is able to access all configuration pages and can change and save all configuration settings. ◦ **Operator:** An operator is able to view all configuration pages, but is limited in the types of changes that can be made.

9 Security

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



Trusted CA certificate store

	ID	Issued to	Current usage	Start date	Expiration date	CRL	Delete
●	1	SOAP API Certificate Authority	SOAP Server	2005-04-06	2025-04-01	No	🗑
●	2	Management Console Dummy Authority	HP Management console	2010-05-19	2020-05-16	No	🗑

PKCS #7 file or X.509 certificate:

Certificate and private key store

	ID	Issued to	Issued by	Current usage	Start date	Expiration date	Delete
●	1	wireless.hp.internal	wireless.hp.internal	Web Management Tool, SOAP Server	2010-11-03	2038-10-27	🗑
●	2	Management Console Default client certificate	Management Console Dummy Authority	HP Management console	2010-05-19	2020-05-16	🗑

PKCS #12 file:

PKCS #12 password:

Trusted CA certificate store

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

The AP uses these certificates to validate certificates supplied by:

- Managers or operators accessing the AP's management tool.
- SOAP clients communicating with the AP's SOAP server.

The following information is presented for each certificate in the list:

- **Status light:** Indicates the certificate state.
  - **Green:** Certificate is valid.
  - **Yellow:** Certificate will expire soon.
  - **Red:** Certificate has expired.
- **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.
- **Start/Expiration date:** Indicates the period during which the certificate is valid.
- **CRL:** Indicates if a certificate revocation list is bound to the certificate. An X.509 certificate revocation list is a document produced by a certificate authority (CA) that provides a list of serial numbers of certificate that have been signed by the CA but that should be rejected.
- **Delete:** Select to remove the certificate from the certificate store.

Installing a new CA certificate

1. Specify the name of the certificate file or select **Browse** to choose from a list. CA certificates must be in X.509 or PKCS #7 format.
2. Select **Install** to install a new CA certificate.

CA certificate import formats

The import mechanism supports importing the ASN.1 DER encoded X.509 certificate directly or as part of two other formats:

- PKCS #7 (widely used by Microsoft products)
- PEM, defined by OpenSSL (popular in the Unix world)
- The CRL can be imported as an ASN.1 DER encoded X.509 certificate revocation list directly or as part of a PEM file.

Content and file format	Items carried in the file	Description
ASN.1 DER encoded X.509 certificate	One X.509 certificate	This is the most basic format supported, the certificate without any envelope.
X.509 certificate in PKCS #7 file	One X.509 certificate	Popular format with Microsoft products.
X.509 certificate in PEM file	One or more X.509 certificates	Popular format in the Unix world. X.509 DER certificate is base64 encoded and placed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines. Multiple certificates can be repeated in the same file.
ASN.1 DER encoded X.509 CRL	One X.509 CRL	Most basic format supported for CRL.
X.509 CRL in PEM file	One X.509 CRL	Same format as X.509 certificate in PEM format, except that the lines contain BEGIN CRL and END CRL.

Default CA certificates

The following certificates are installed by default:

- **SOAP API Certificate Authority:** Before allowing a SOAP client to connect, the AP checks the certificate supplied by a SOAP client to ensure that it is issued by a trusted certificate authority (CA).
- **Dummy Authority:** Used by the internal RADIUS server. You should replace this with your own CA certificate.

NOTE: For security reasons, you should replace the default certificates with your own.

Certificate and private key store

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

Items provided in this list are as follows:

Status indicator

Indicates the certificate state.

- **Green:** Certificate is valid.
- **Yellow:** Certificate will expire soon.
- **Red:** Certificate has expired.

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.

Start/Expiration date

Indicates the period during which the certificate is valid.

Delete

Select to remove the certificate from the certificate store.

Installing a new private key/public key certificate chain pair

NOTE: RADIUS EAP certificates must have the X.509 extensions. Information about this is available in the Microsoft knowledgebase at: http://support.microsoft.com/kb/814394/en-us

The certificate you install must:

- Be in PKCS #12 format.
- Contain a private key (a password controls access to the private key).
- Not have a name that is an IP address. The name should be a domain name containing at least one dot. If you try to add a certificate with an invalid name, the default certificate is restored.

The common name in the certificate is automatically assigned as the domain name of the 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:

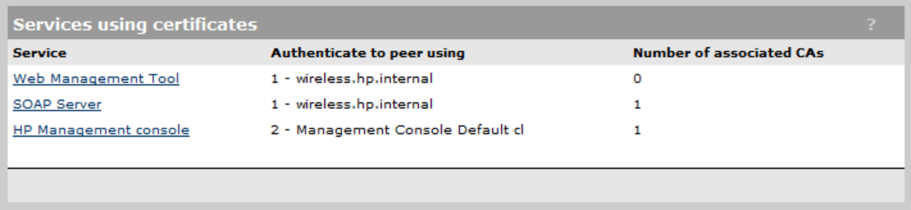
- **wireless.hp.internal:** Default certificate used by the management tool, SOAP server, and HTML-based authentication.
- **Dummy Server Certificate:** Used by the internal RADIUS server. This certificate is present only to allow EAP-PEAP to work if the client chooses not to verify the server's certificate. You should replace this with your own certificate for maximum security.
- **Management Console 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/TLS, the AP sends only its own X.509 certificate to the browser. This means that if the certificate has been signed by an intermediate certificate authority, and if the Web browser only knows about the root certificate authority that signed the public key certificate of the intermediate certificate authority, the Web browser does not get the whole certificate chain it needs to validate the identity of the AP. 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: An SNMP notification can be sent to let you know when the AP SSL certificate is about to expire. To enable this notification, select **Management > SNMP** and enable the **Notifications** option. Then select **Configure Notifications**, enable **Event notifications**, and then select the event **Maintenance certificate about to expire** under **System**. See "Configuring SNMP notifications for events" (page 84).

Certificate usage

To see the services that are associated with each certificate, select **Security > Certificate usage**. With the factory default certificates installed, the page will look like this:



Services using certificates

Service	Authenticate to peer using	Number of associated CAs
Web Management Tool	1 - wireless.hp.internal	0
SOAP Server	1 - wireless.hp.internal	1
HP Management console	2 - Management Console Default cl	1

Service

Name of the service that is using the certificate. To view detailed information on the certificate select the service name.

Authenticate to peer using

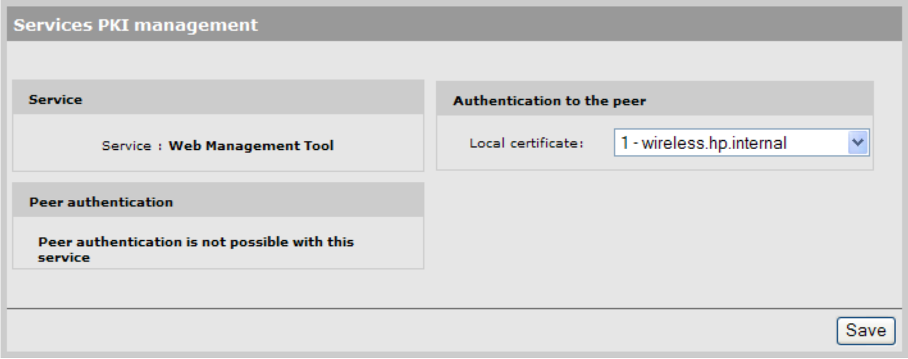
Name of the certificate and private key. The AP is able to prove that it has the private key corresponding to the public key in the certificate. This is what establishes the AP as a legitimate user of the certificate.

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:



Services PKI management

Service

Service : Web Management Tool

Authentication to the peer

Local certificate: 1 - wireless.hp.internal

Peer authentication

Peer authentication is not possible with this service

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.

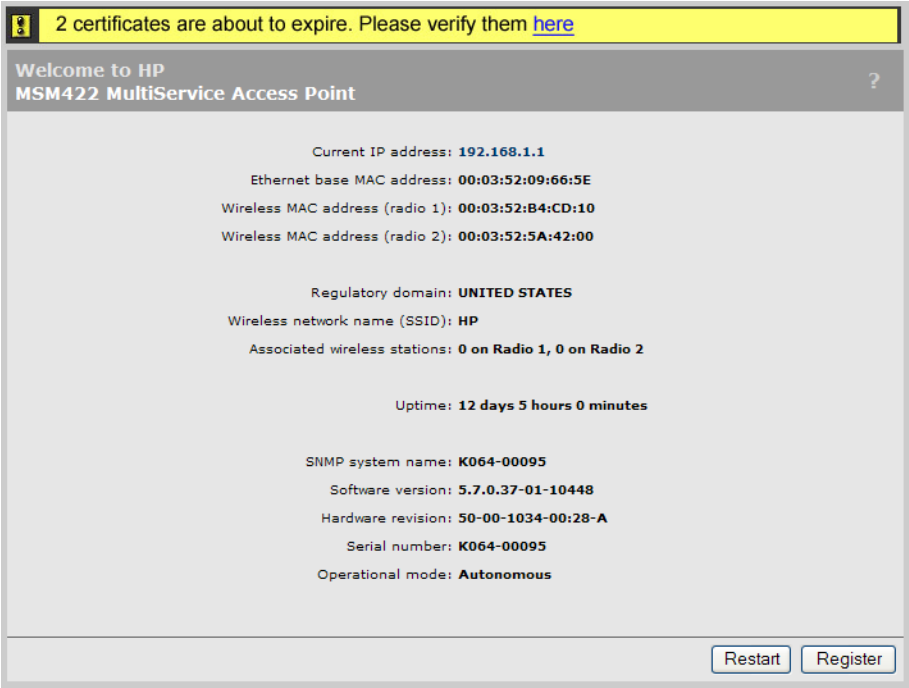
To eliminate these warnings you can do one of the following:

- 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.

Certificate expiration alerts

The following warnings are generated when a certificate is about to expire:

- The status light for the certificate turns yellow. See "Trusted CA certificate store" (page 99).
- A message appears on the management tool home page. For example:



2 certificates are about to expire. Please verify them here

Welcome to HP
MSM422 MultiService Access Point

Current IP address: 192.168.1.1
Ethernet base MAC address: 00:03:52:09:66:5E
Wireless MAC address (radio 1): 00:03:52:B4:CD:10
Wireless MAC address (radio 2): 00:03:52:5A:42:00

Regulatory domain: UNITED STATES
Wireless network name (SSID): HP
Associated wireless stations: 0 on Radio 1, 0 on Radio 2

Uptime: 12 days 5 hours 0 minutes

SNMP system name: K064-00095
Software version: 5.7.0.37-01-10448
Hardware revision: 50-00-1034-00:28-A
Serial number: K064-00095
Operational mode: Autonomous

- The following syslog message is sent every 24 hours:

  Warning: n certificate(s) is(are) about to expire. Please go to the Certificates page for more information.

  Where n is the number of certificates that are about to expire.
- When logging into the CLI, a message similar to the syslog message above is displayed.

MAC lockout

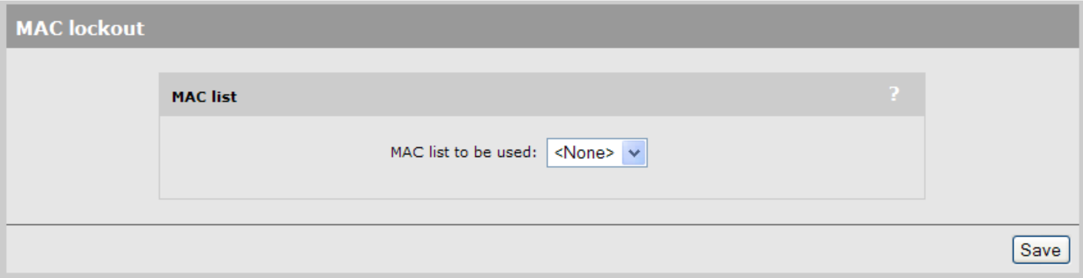
This feature lets you to block traffic from client stations based on their MAC address. MAC lockout applies to client stations connected to:

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

Configuring MAC lockout

Before you can configure MAC lockout, you must define one or more MAC address lists.

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



MAC lockout

MAC list

MAC list to be used: <None>

2. Select the MAC address list to use.
3. Select **Save**.

Configuring MAC address lists

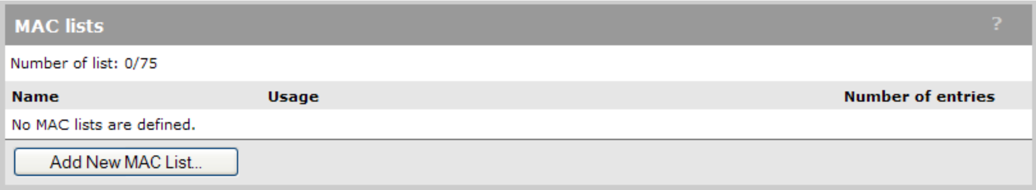
MAC lists are used by several options to allow/deny access to client stations. You can define up to 75 MAC address lists with up to 256 entries in each list. The lists can be used to define MAC addresses for the following features:

- The **MAC filter** option in a VSC. When used with this feature, a maximum of 256 addresses are supported per list.
- The **MAC lockout** feature. When used with this feature, a maximum of 64 addresses are supported per list.

The total number of MAC addresses defined for all lists cannot exceed 4800.

To define a MAC list, do the following:

1. Select **Security > MAC lists**.



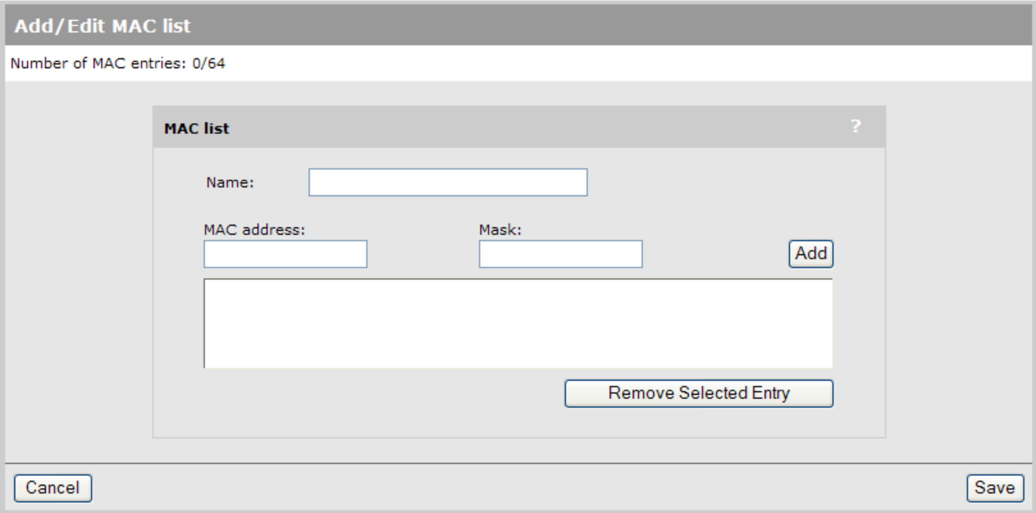
MAC lists

Number of list: 0/75

Name	Usage	Number of entries
No MAC lists are defined.		

2. Select **Add New MAC List**. The Add/Edit MAC list page opens.

   Each entry in the MAC list contains a MAC address and its associated mask. By varying the mask, an entry can be defined to match a single address or a range of addresses.



3. Specify a **Name** to identify the MAC address list.
4. Specify the **MAC address** and **Mask** that you want to match, then select **Add.** Setting the **Mask** to **00:00:00:00:00:00** is allowed, but not recommended since it will match all MAC addresses.
5. Repeat step 4 until you have defined all needed entries.
6. Select **Save**.

Matching MAC addresses

Matching a single MAC address

To match a single MAC address, specify the address using 12 hexadecimal numbers in the format: **nn:nn:nn:nn:nn:nn**, and set the **Mask** to: **FF:FF:FF:FF:FF:FF**

For example, this definition matches a single MAC address:

MAC address = 00:03:52:07:2B:43

Mask = FF:FF:FF:FF:FF:FF

Matching a range of MAC addresses

To match a range of MAC addresses, you need to use the wildcard feature. A value of **00** in a mask means that the corresponding position in the address is a wildcard (i.e., it can be any value).

For example, to match all address that begin with the prefix 00:03:52 you would define:

MAC address = 00:03:52:00:00:00

Mask = FF:FF:FF:00:00:00

Wildcards can be placed anywhere (but must always be 00, half-byte masks such as F0 are not supported). Multiple wildcards can be used.

For example, this entry matches all the addresses that have their first three bytes set to 00:03:52 and the final bytes set to AA:FF

MAC address = 00:03:52:00:AA:FF

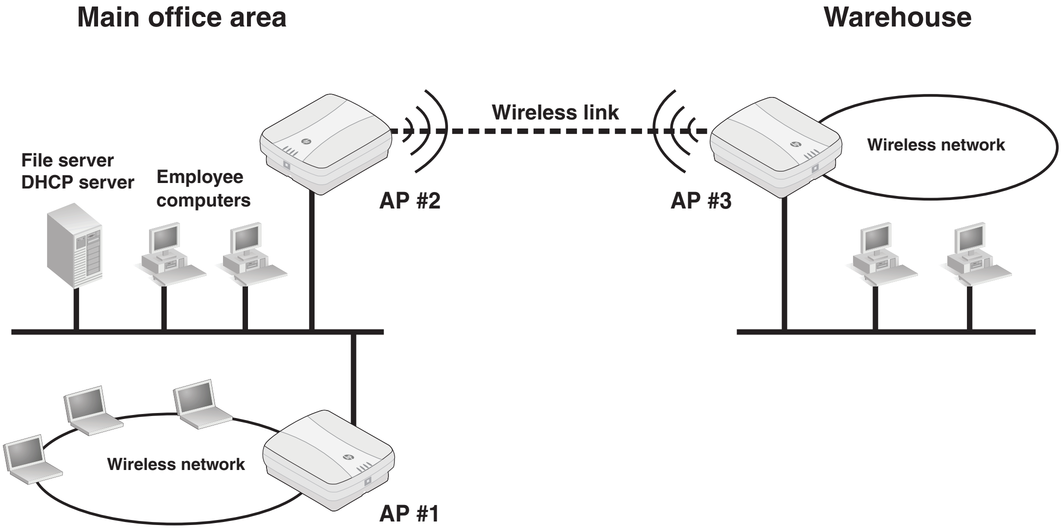
Mask = FF:FF:FF:00:FF:FF

10 Local mesh

Key concepts

The local mesh feature enables you to create wireless links between two or more APs. These links provide a wireless bridge that interconnects the networks connected to the Ethernet port on each AP.

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.



The local mesh feature replaces the need for Ethernet cabling between APs, making it easy to extend your network in hard-to-wire locations or in outdoor areas.

Key local mesh features include:

- **Automatic link establishment:** Nodes automatically establish wireless links to create a full-connected network. A dynamic network identifier (local mesh group ID) restricts connectivity to groups of nodes, enabling distinct groups to be created with nodes in the same physical area.
- **Provides fall-back operation to recover from node failure.** In a properly designed implementation, redundant paths can be provided. If a node fails, the mesh will automatically reconfigure itself to maintain connectivity.
- **Maintains network integrity when using DFS channels.** In accordance with the 802.11h standard, dynamic frequency selection (DFS) detects the presence of certain radar devices on a channel and automatically switches the network node to another channel if such signals are detected. 802.11h is intended to resolve interference issues with military radar systems and medical devices.

NOTE: Depending on the radio regulations of some countries, DFS channels are only available on the 802.11a/n bands, which are the preferred band for local mesh backhaul. If more than one node detects radar simultaneously and must switch channels, each node does not necessarily switch to the same channel, and the network might never reconverge. To avoid this problem, local mesh detects a change in channel and provides a means to reconnect on other channels by scanning on multiple channels. See “Operating channel” (page 110).

Simultaneous AP and local mesh support

APs can be configured to support both access point and local mesh functionality whether they have a single radio, or multiple radios.

Single radio APs

A single radio can be configured to simultaneously support wireless users and one or more local mesh links. Although this offers flexibility it does have the following limitations:

- The total available bandwidth on the radio is shared between all local mesh links and wireless users. This can result in reduced throughput if lots of traffic is being sent by both wireless users and the local mesh links. You can use the QoS feature to prioritize traffic.
- It limits you to using the same radio options for both wireless clients and local meshes.

Multiple radio APs

On APs with more than one radio, one radio can be dedicated to support wireless users and another to provide local mesh links. Each radio can be configured optimally according to its application.

Controlled APs

Controlled APs can be managed over local mesh links.

Using 802.11a/n for local mesh

HP recommends 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:

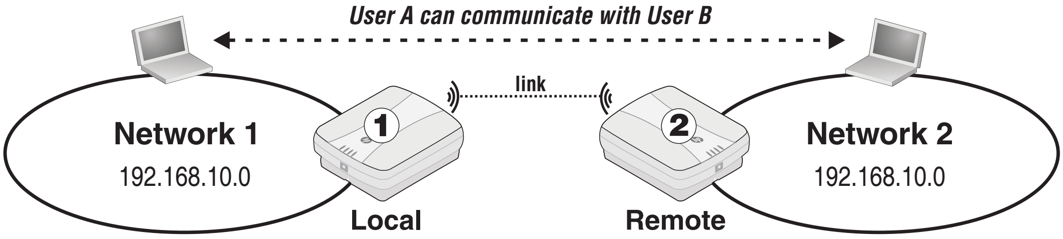
- Since the same radio options must be used for both wireless clients and local mesh links, support for 802.11b/g clients is not possible on APs with a single radio.
- The 5 GHZ band has a shorter reach when compared to the 2.4 GHz band. This could be a factor depending on the distance your links must span.

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.

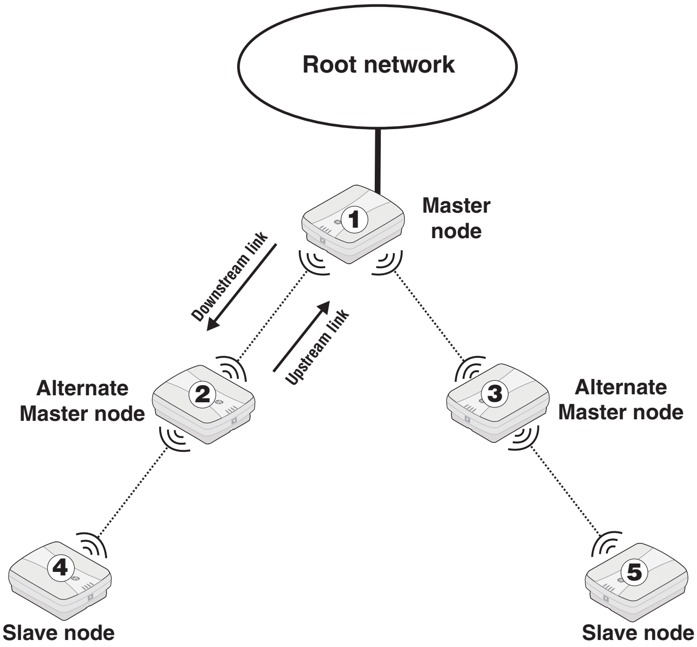
Configuration guidelines

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.
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.

When an AP is attempting to establish a local mesh link, the radio status light on its chassis will blink. Once the local mesh link is established, the radio status light will return to its normal operation.

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:

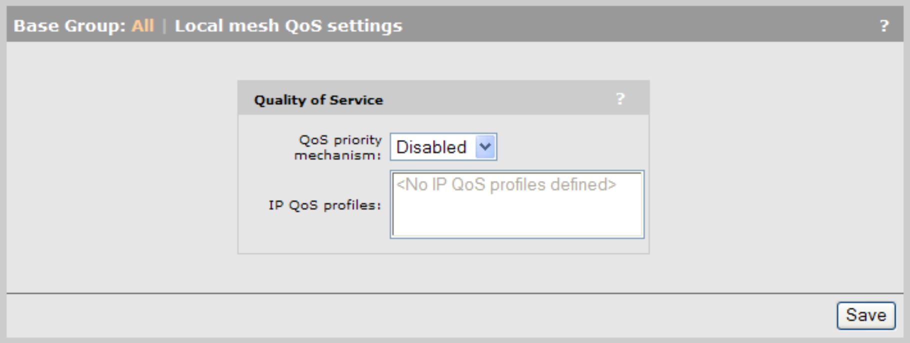
- Configure the radios on all nodes to use the same fixed channel.
- Configure the radios for automatic channel selection. In this case the master selects the least noisy channel. Slaves and alternate masters scan channels until they find the master, then tune to the master channel and link with the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



Base Group: All | Local mesh QoS settings

Quality of Service

QoS priority mechanism: Disabled

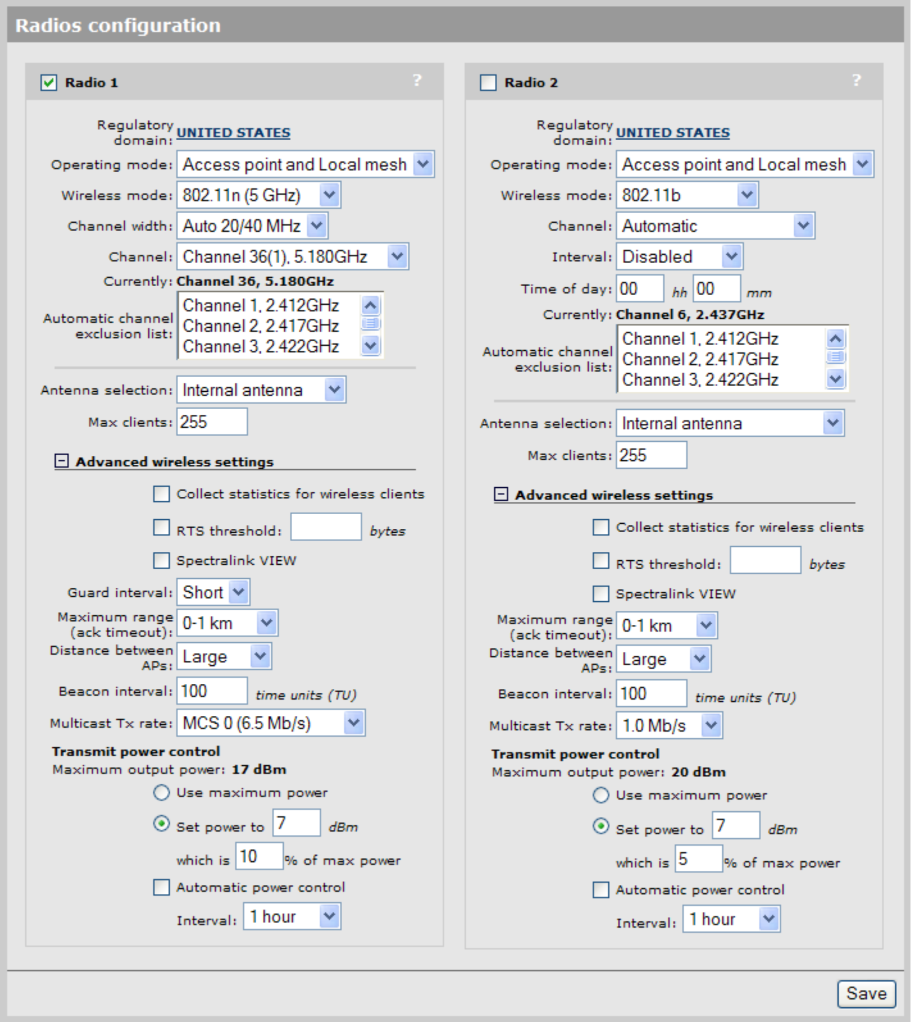
IP QoS profiles: <No IP QoS profiles defined>

NOTE: When traffic is forwarded onto a local mesh link from a VSC, the QoS settings on the VSC take priority. For example, if you define a VSC with a QoS setting of **VSC-based High**, then traffic from this VSC will traverse the local mesh on queue 2 even if the QoS setting on the local mesh is **VSC-based Low** (queue 4).

Maximum range (ack timeout)

This is a global setting that is configurable on the **Radio** page when the **Operating mode** is set to support **Local mesh**. It fine tunes internal timeout settings to account for the distance that a link spans. For normal operation, it is set to less than 1 km.

This is a global setting that applies to all wireless connections made with a radio, not just for local mesh links. Therefore, if you are also using a radio to access an AP, adjusting this setting may lower the performance for users with marginal signal strength or when interference is present. (Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)



Radios configuration

☑ Radio 1

Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11n (5 GHz)
Channel width: Auto 20/40 MHz
Channel: Channel 36(1), 5.180GHz
Currently: Channel 36, 5.180GHz
Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz
Antenna selection: Internal antenna
Max clients: 255

⊟ Advanced wireless settings

□ Collect statistics for wireless clients
□ RTS threshold: bytes
□ Spectralink VIEW
Guard interval: Short
Maximum range (ack timeout): 0-1 km
Distance between APs: Large
Beacon interval: 100 time units (TU)
Multicast Tx rate: MCS 0 (6.5 Mb/s)

Transmit power control
Maximum output power: 17 dBm
○ Use maximum power
● Set power to 7 dBm
which is 10 % of max power
□ Automatic power control
Interval: 1 hour

□ Radio 2

Regulatory domain: UNITED STATES
Operating mode: Access point and Local mesh
Wireless mode: 802.11b
Channel: Automatic
Interval: Disabled
Time of day: 00 hh 00 mm
Currently: Channel 6, 2.437GHz
Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz
Antenna selection: Internal antenna
Max clients: 255

⊟ Advanced wireless settings

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

Transmit power control
Maximum output power: 20 dBm
○ Use maximum power
● Set power to 7 dBm
which is 5 % of max power
□ Automatic power control
Interval: 1 hour

Local mesh profiles

A local mesh profile defines the characteristics for the type of links that can be established with other nodes as follows:

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.

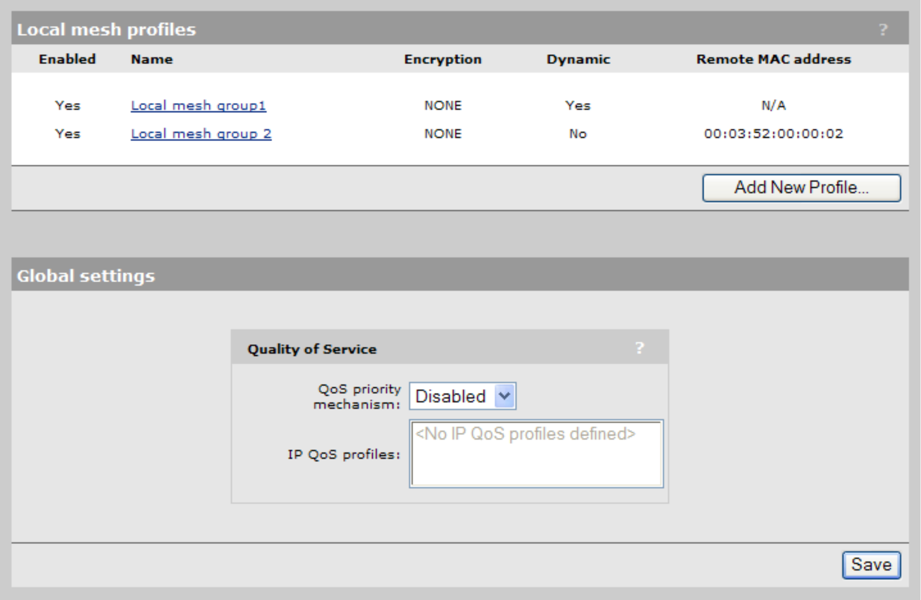
If a profile defines a dynamic local mesh link, it establishes links to other nodes as follows:

Role	Upstream link	Downstream link
Master	None.	Up to nine links with alternate master or slave nodes per profile.
Alternate master	A single link to a master node or alternate master node.	Up to eight links with alternate master or slave nodes.
Slave	A single link to a master node or alternate master node.	None.

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

Configuring a local mesh profile

Select **Wireless > Local mesh**.



Local mesh profiles

Enabled	Name	Encryption	Dynamic	Remote MAC address
Yes	Local mesh group1	NONE	Yes	N/A
Yes	Local mesh group 2	NONE	No	00:03:52:00:00:02

Add New Profile...

Global settings

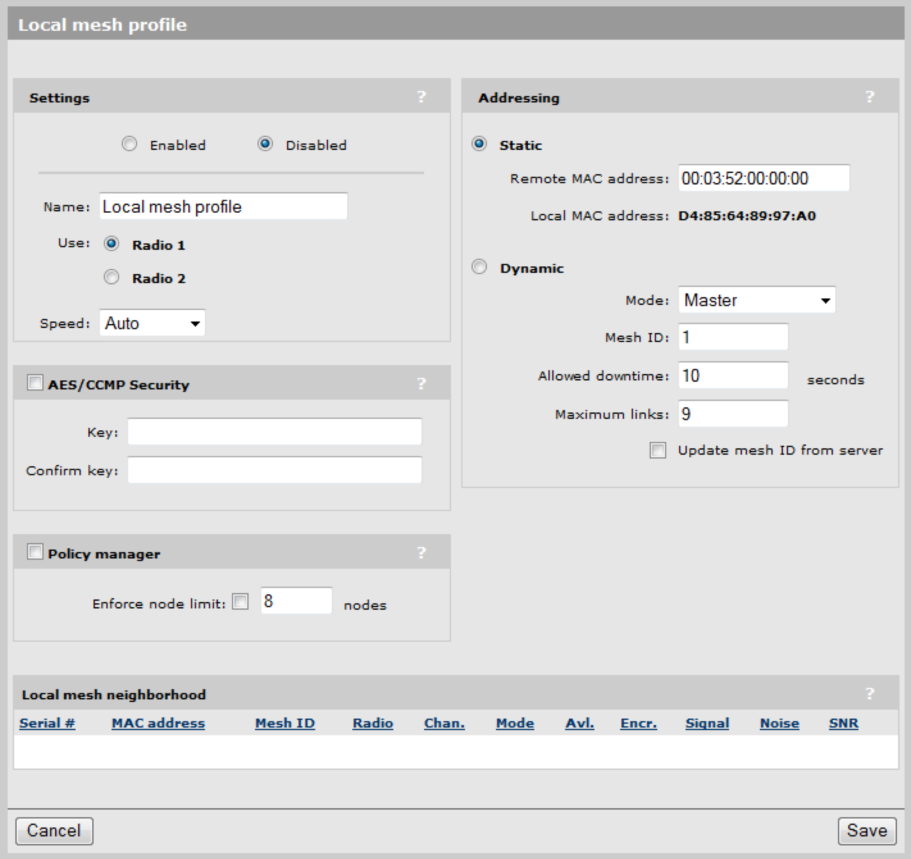
Quality of Service

QoS priority mechanism: Disabled

IP QoS profiles: <No IP QoS profiles defined>

Save

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



Local mesh profile

Settings

○ Enabled ● Disabled

Name: Local mesh profile

Use: ● Radio 1
○ Radio 2

Speed: Auto

□ **AES/CCMP Security**

Key:

Confirm key:

□ **Policy manager**

Enforce node limit: □ 8 nodes

Addressing

● **Static**

Remote MAC address: 00:03:52:00:00:00

Local MAC address: **D4:85:64:89:97:A0**

○ **Dynamic**

Mode: Master

Mesh ID: 1

Allowed downtime: 10 seconds

Maximum links: 9

□ Update mesh ID from server

Local mesh neighborhood

Serial #	MAC address	Mesh ID	Radio	Chan.	Mode	Avl.	Encr.	Signal	Noise	SNR

Cancel

Save

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 wireless link. The node uses the key you specify in the **Key** field to generate the keys that encrypt the wireless data stream.

Specify a key that is between 8 and 63 ASCII characters in length. HP recommends 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.

Mesh ID

A 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)

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

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.

Update mesh ID from server

(Master nodes)

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.

Promiscuous mode

(Alternate master or slave nodes)

Allows a node to connect to a different mesh when it cannot find a master or alternate master with its currently configured mesh ID within the specified amount of time.

Once a new master or alternate master is found, the following actions are triggered:

- The node firmware is updated using the settings configured under **Scheduled operations** on the **Maintenance > Firmware** page.
- The node configuration is updated using the settings configured under **Scheduled operations** on the **Maintenance > Config file management** page. This changes the node mesh ID to the one found in the configuration file. If no configuration file is defined, the node updates its mesh ID to match the new master or alternate master.
- An SNMP notification is sent if the configuration file or firmware fails to load.

After loading new firmware or a new configuration file, the node waits 30 seconds before restarting if a downstream link was established with another node in promiscuous mode. This provides downstream nodes with additional time during which to download new firmware and configuration files, thus improving the total convergence time of the entire network.

Preserve master link across reboots

(Alternate master or slave nodes)

When enabled, the address of the current master to which the node is connected is saved so that if the node restarts it will reconnect to the same master bypassing the initial discovery period.

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. 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 (alternate master) in a different mesh. This will cause the slave to save the new mesh ID and use it from that point onward.

Search for better link on minimum SNR

(Alternate Master, Slave only)

When enabled, if the current SNR on the link drops below the value set for Minimum SNR, the node will search for a connection to another master with a better SNR.

Restart Discovery

(Alternate master or slave nodes)

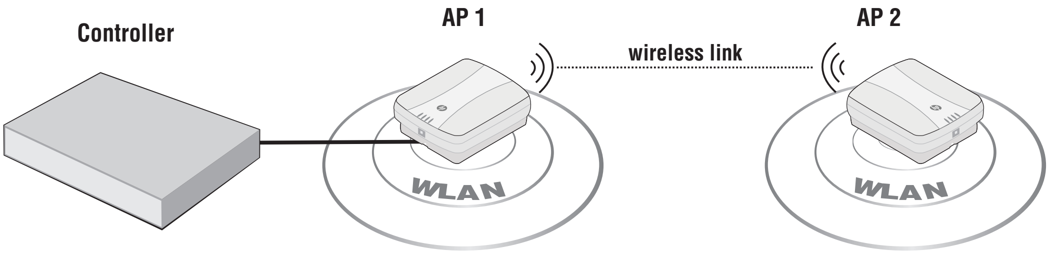
This button tells the AP to bring down any link it has already established and restart looking for the best master to which it can connect. It can be used when a new master is installed close to a slave and you want the slave to connect to that master, without rebooting.

Sample local mesh deployments

RF extension

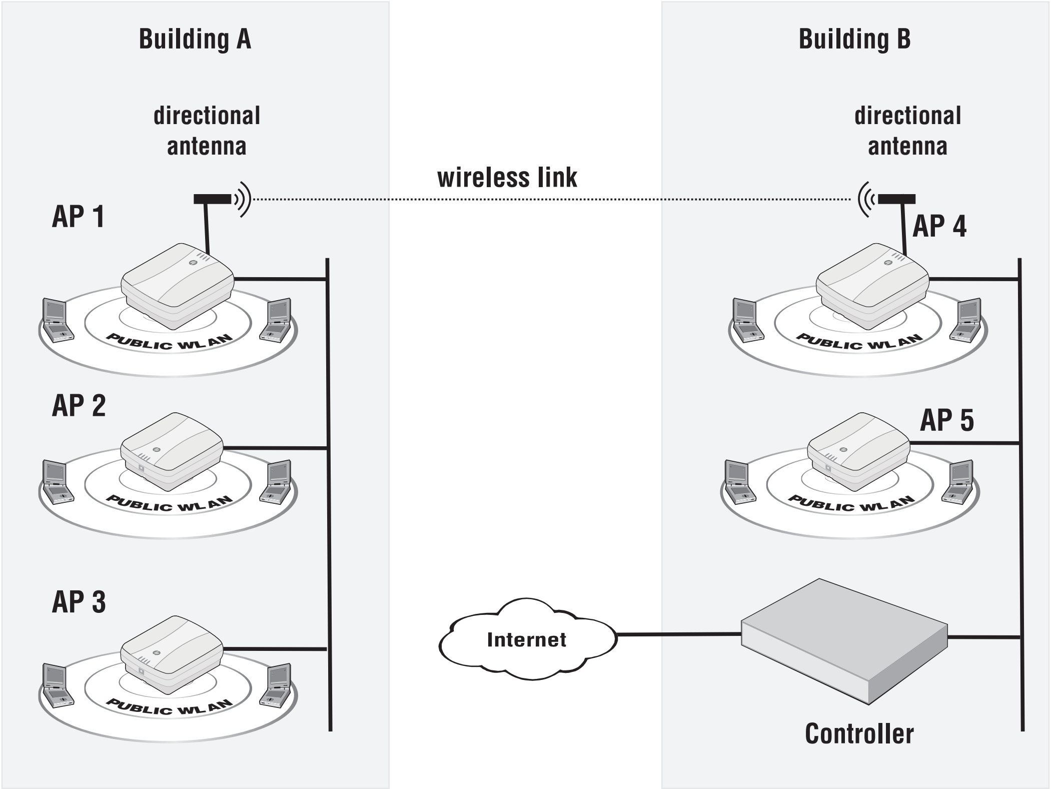
Local mesh provides an effective solution for extending wireless coverage in situations where it is impractical or expensive to run cabling to an AP.

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 connection

You can also use local mesh to create point-to-point links over longer distances. in this scenario, two dual-radio APs create a wireless link between networks in two adjacent buildings. Each AP is equipped with a directional external antenna attached to radio 1 to provide the wireless link. Omnidirectional antennas are installed on radio 2 to provide AP capabilities. The two APs are placed within line of sight.



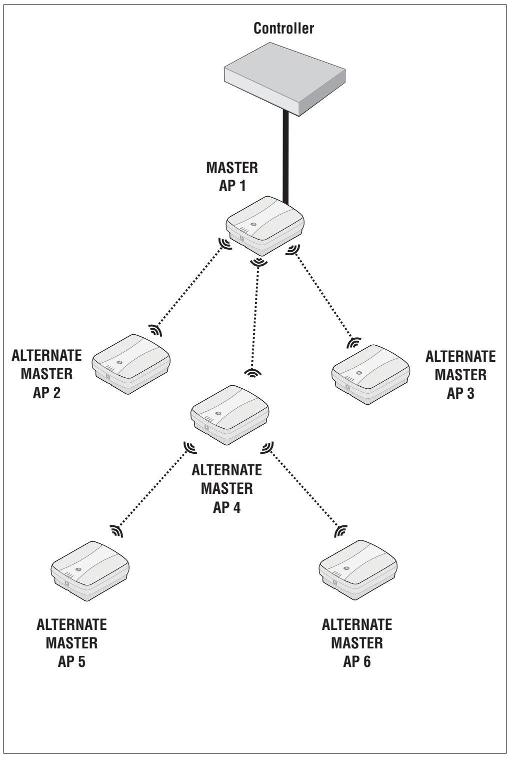
NOTE: In the above example, all APs must connect to the backbone network via port 1.

Dynamic network

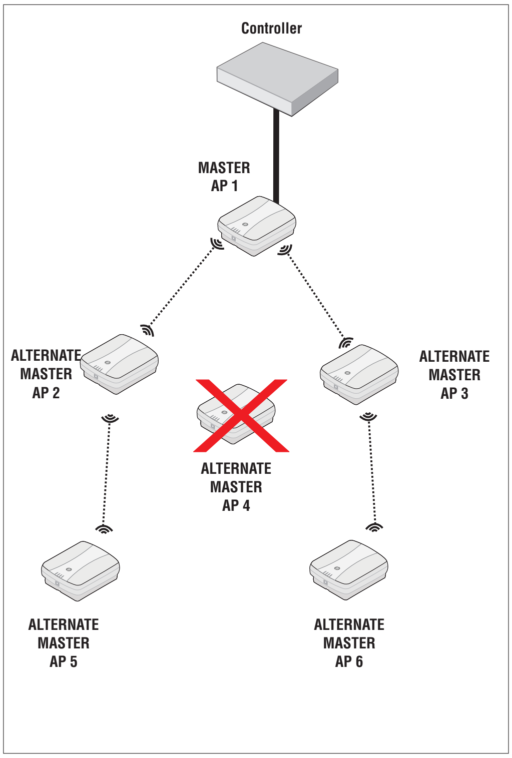
In this scenario, a controller is deployed with several APs to provide wireless coverage of a large area. Instead of using a backbone LAN, wireless links are used to interconnect all APs.

AP 1 is the *master*. It provides the connection to the wired network and a wireless link to the other APs. The other APs automatically established their links to the master based on a balance between SNR (signal to noise ratio) and hops, to provide the most efficient network topology.

If a node becomes unavailable, the links dynamically adjust to find the optimum path to the master.



Initial network configuration is automatically established.



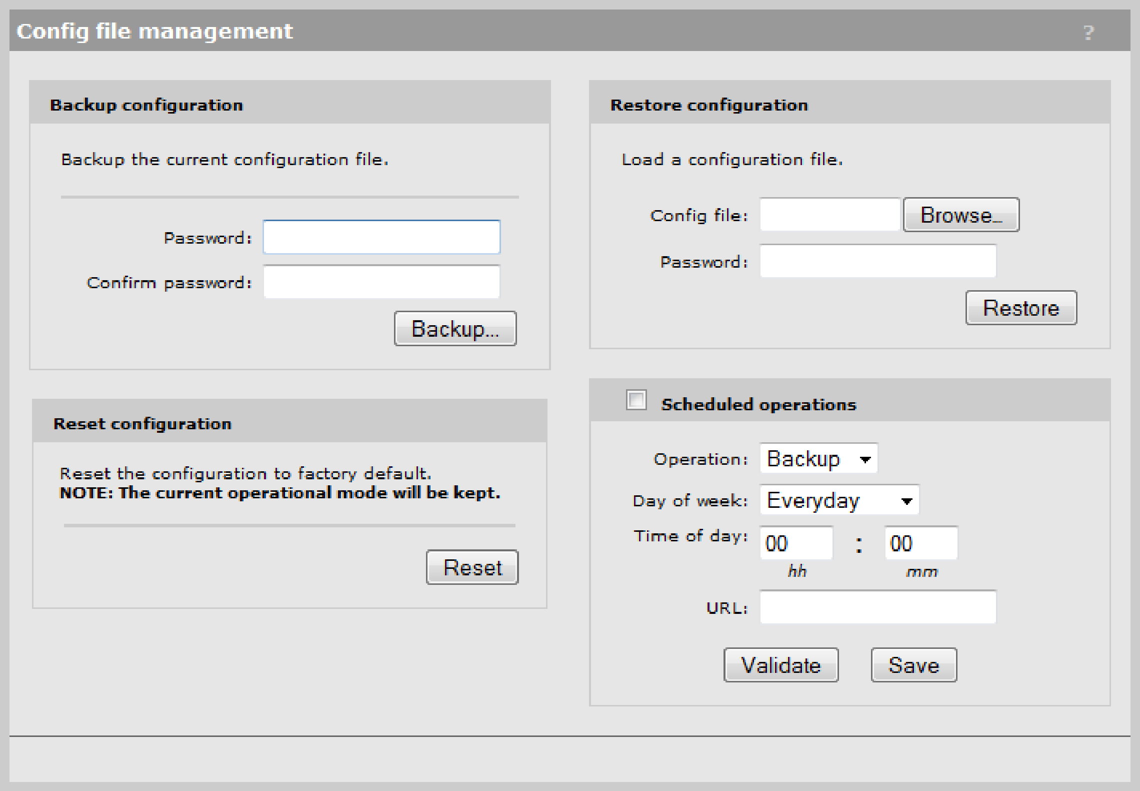
When AP 4 is unavailable, the network dynamically reconfigures itself.

11 Maintenance

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**.



Config file management

Backup configuration

Backup the current configuration file.

Password:

Confirm password:

Reset configuration

Reset the configuration to factory default.
NOTE: The current operational mode will be kept.

Restore configuration

Load a configuration file.

Config file:

Password:

□ Scheduled operations

Operation: Backup

Day of week: Everyday

Time of day: 00 : 00

URL:

Manual configuration file management

The following options are available for manual configuration file management.

Backup configuration

This option enables you to backup your configuration settings so they can be easily restored in case of failure. This option is also used when you want to directly edit the configuration file.

Before you install new software, you should always make a backup of your current configuration. Select **Backup** to start the process. You will be prompted for the location to place the configuration file.

Configuration information is saved in the backup file as follows:

- **Certificates and private keys:** If you specify a password when saving the configuration file, certificates and private keys are encrypted with a key based on the password. If you do not specify a password, certificates and private keys are still encrypted, but with a default key that is identical on all APs.
- **Manager and operator username/password:** This information is not saved in the backup configuration file. This means that if you restore a configuration file, the current username and password on the AP is 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” (page 126).

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 **Browse** and then locate the configuration file you want to restore.
2. Select **Restore** to upload it to the AP. If the configuration file is protected with a password, you must supply the password to restore the complete configuration. If you supply an invalid password, all settings are restored except for any certificates and private keys.

NOTE: The AP automatically restarts when once the file has been loaded.

Scheduled operations

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

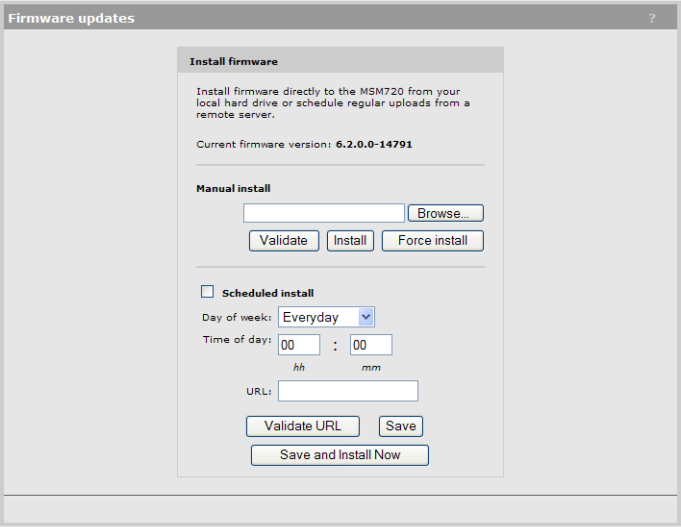
Use the following steps to schedule a backup or restoration of the configuration file.

1. Select **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**

   Secure transfers are supported using HTTPS or FTPS.
7. Select **Validate** to test that the specified **URL** is correct.
8. Select **Save**.

Software updates

Software updates are managed by selecting **Maintenance > Firmware updates**.



Install firmware directly to the MSM720 from your local hard drive or schedule regular uploads from a remote server.

Current firmware version: **6.2.0.0-14791**

□ **Scheduled install**

Day of week: Everyday

Time of day: 00 : 00 (*hh* *mm*)

URL:

CAUTION:

- 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, do the following:

1. Select **Browse,** and then locate a firmware file and select it.
2. Select **Validate** if you want to test the integrity of the selected firmware file without installing it. A message will appear at the top of the page indicating whether the firmware signature is valid or invalid.
3. Select **Install**. This will automatically test the integrity of the firmware by validating its signature. If the signature is valid, the firmware will be installed and the AP will restart. If the signature is invalid, the firmware will not be installed.

NOTE: Select **Force install** to install a firmware file without validating its integrity. Installing firmware without validating its integrity may result in the AP becoming inoperative.

Performing a scheduled software update

The AP can automatically retrieve and install software from a remote 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 address like this:
   - **ftp://username:password@192.168.132.11/newsoftware.cim**
   - **http://192.168.132.11/newsoftware.cim**

   Secure transfers are supported using HTTPS or FTPS.
4. Select **Validate URL** to test that the specified URL points to a firmware file.

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.

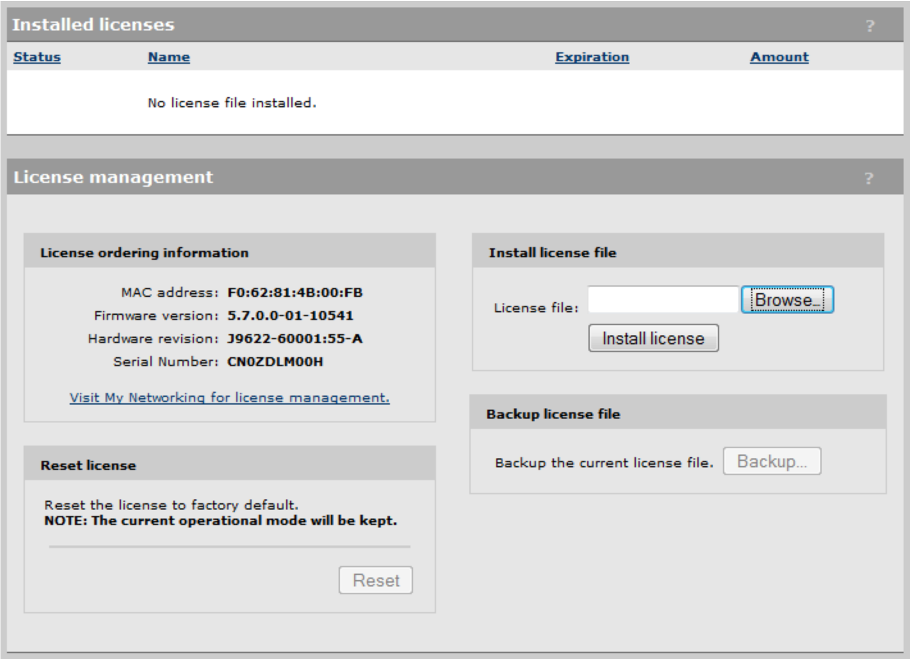
Managing licenses

Supported on: 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.

To view and manage licenses, select **Maintenance > Licenses**.



Installed licenses

Status	Name	Expiration	Amount
	No license file installed.		

License management

License ordering information

MAC address: **F0:62:81:4B:00:FB**
Firmware version: **5.7.0.0-01-10541**
Hardware revision: **J9622-60001:55-A**
Serial Number: **CN0ZDLM00H**

Visit My Networking for license management.

Install license file

License file:

Backup license file

Backup the current license file.

Reset license

Reset the license to factory default.
NOTE: The current operational mode will be kept.

Installed licenses

This table lists all licenses that are installed on the AP.

Status

Indicates if the license is active or not.

Name

Identifies the license.

Expiration

Indicates the expiry date for the license.

Amount

Indicates the license quantity. This is set to a value of 1 for all licenses.

License management

Use these options to order, install, and backup license files.

License ordering information

When ordering a license file from HP you will need to supply the information displayed in this box. Once you receive your License Registration card for your purchased license, you will need to generate and install the license as described in "Generating and installing a feature license" (page 122).

Reset licenses

Reset the installed license to factory default configuration

Install license file

- Select **Browse** and locate the license file you received from HP.
- Select **Install License** to install the file.

Backup license file

Select **Backup** to save a backup copy of the current license file.

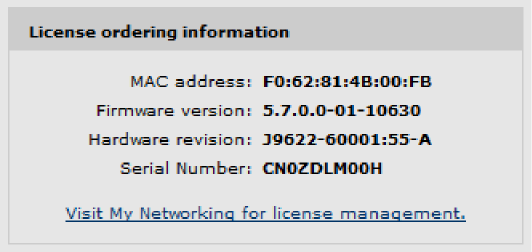
Generating and installing a feature license

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

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:



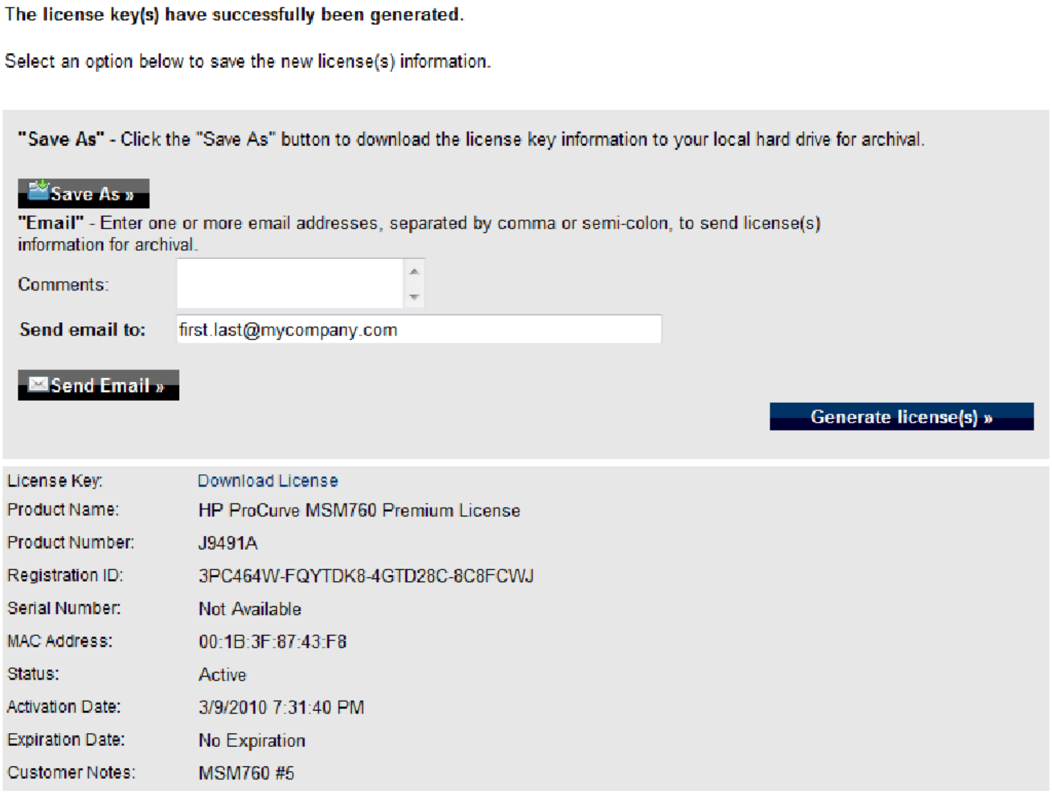
License ordering information

MAC address: F0:62:81:4B:00:FB
Firmware version: 5.7.0.0-01-10630
Hardware revision: J9622-60001:55-A
Serial Number: CN0ZDLM00H

Visit My Networking for license management.

5. Back on the My Networking portal Web page, paste or type the MAC address of your AP in the **MAC Address** field. For example:
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 E-mail. For example:



The license key(s) have successfully been generated.

Select an option below to save the new license(s) information.

"Save As" - Click the "Save As" button to download the license key information to your local hard drive for archival.

"Email" - Enter one or more email addresses, separated by comma or semi-colon, to send license(s) information for archival.

Comments:

Send email to: first.last@mycompany.com

License Key:	Download License
Product Name:	HP ProCurve MSM760 Premium License
Product Number:	J9491A
Registration ID:	3PC464W-FQYTDK8-4GTD28C-8C8FCWJ
Serial Number:	Not Available
MAC Address:	00:1B:3F:87:43:F8
Status:	Active
Activation Date:	3/9/2010 7:31:40 PM
Expiration Date:	No Expiration
Customer Notes:	MSM760 #5

8. Use the **Save As** button to save the license key file on your system or use **Send Email** to send the license key file and information to an E-mail address. The E-mail 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, 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.

12 Support and other resources

Online documentation

You can download documentation from the HP Support Center website at: www.hp.com/support/manuals. Search by product number or name.

Contacting HP

For worldwide technical support information, see the HP Support Center website: www.hp.com/networking/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Problem description and any detailed questions

HP websites

For additional information, see the following HP websites:

- www.hp.com/networking
- www.hp.com

Typographic conventions

Table 1 Document conventions

Convention	Element
Blue text: Table 1 (page 124)	Cross-reference links
Blue, underlined text: www.hp.com	Website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes

WARNING! Indicates that failure to follow directions could result in bodily harm or death.

CAUTION: Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

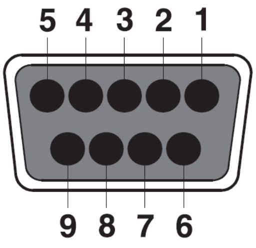
A Console ports

Console port connector specifications

The console ports are wired as described in this section.

MSM335 and MSM422 console port

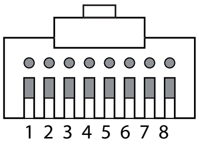
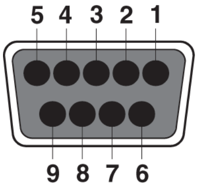
The MSM335 and MSM422 provide a DB-9 (female) console (serial) port connector. The DB-9 connector (DCE) has pin assignments as follows:

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

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

MSM410, MSM430, MSM460, and 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 Resetting to factory defaults

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 retained after a reset to factory defaults.

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 the MSM310-R and MSM320-R.

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.

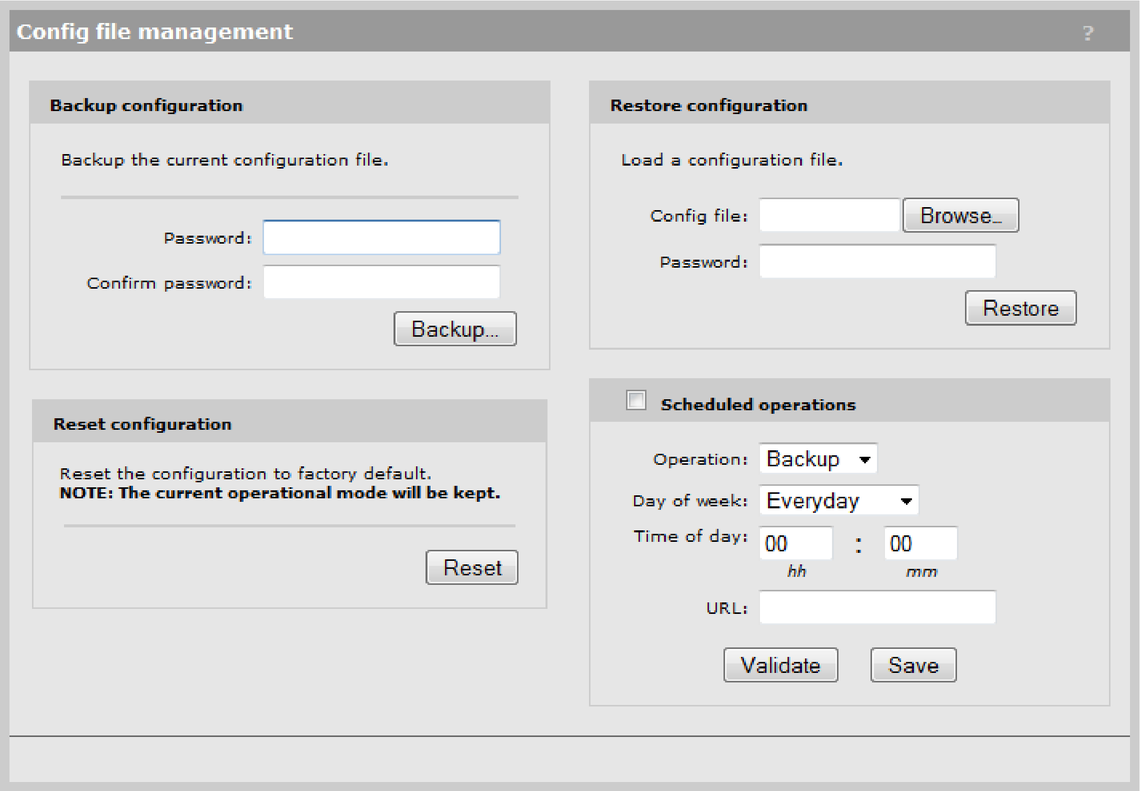
Using the management tool

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**.



Config file management ?

Backup configuration

Backup the current configuration file.

Password:

Confirm password:

Backup...

Restore configuration

Load a configuration file.

Config file: Browse...

Password:

Restore

Reset configuration

Reset the configuration to factory default.
NOTE: The current operational mode will be kept.

Reset

□ Scheduled operations

Operation: Backup

Day of week: Everyday

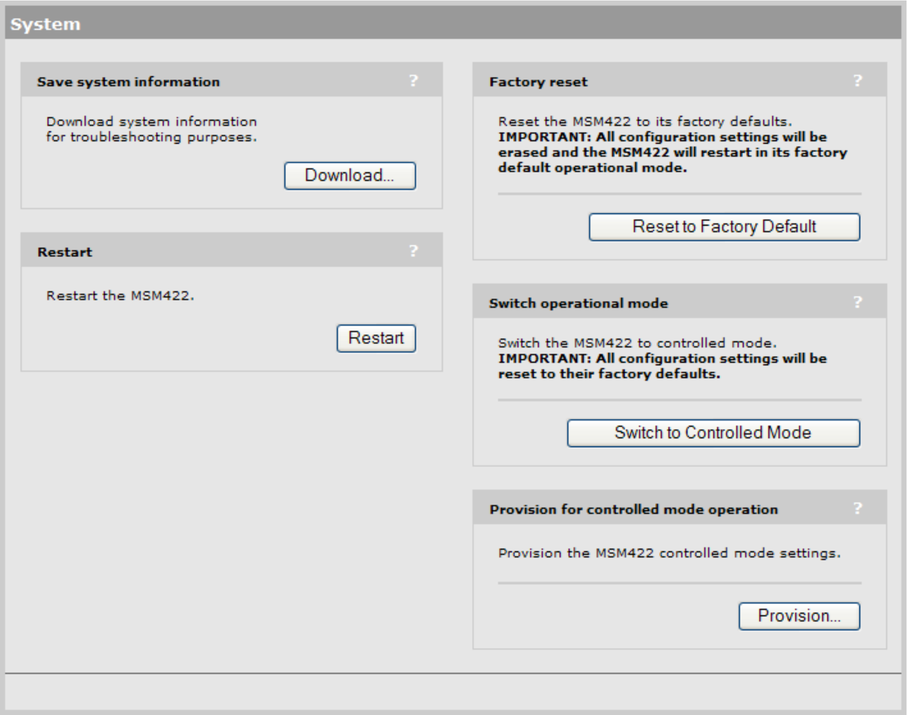
Time of day: 00 : 00
hh mm

URL:

Validate Save

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**.



System

Save system information ?

Download system information for troubleshooting purposes.

Download...

Restart ?

Restart the MSM422.

Restart

Factory reset ?

Reset the MSM422 to its factory defaults.
IMPORTANT: All configuration settings will be erased and the MSM422 will restart in its factory default operational mode.

Reset to Factory Default

Switch operational mode ?

Switch the MSM422 to controlled mode.
IMPORTANT: All configuration settings will be reset to their factory defaults.

Switch to Controlled Mode

Provision for controlled mode operation ?

Provision the MSM422 controlled mode settings.

Provision...

Factory defaulting the MSM310-R and MSM320-R

This section describes how to reset the MSM310-R and MSM320-R 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" (page 126)

You need the following additional items:

- The factory default script file. Visit www.hp.com/support/manuals and search by product number or name. 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 MSM310-R and MSM320-R 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:

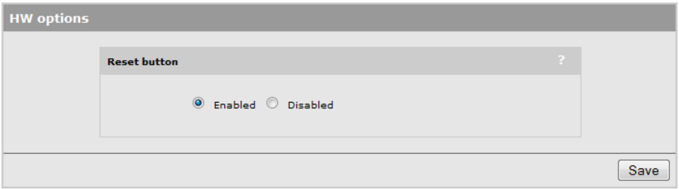
   Your "R" product has been successfully factory reset!

9. Once the factory reset completes, perform the procedure found in the *Initial software configuration* section of the AP Quickstart.

Disabling the reset button on an AP

In certain cases it may be useful to disable the functionality of the reset button on an AP as follows:

1. Select **Management > Hardware**.



Reset button: ● Enabled ○ Disabled

2. Under **Reset button**, select **Disabled**.
3. Select **Save**.

Once this is done, pressing the reset button on the AP will have no effect, **except** during a brief time period after the AP is powered-on. During this brief period the reset button functions as normal.

C Connecting external antennas

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/support/manuals.

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/support/manuals. Search by product number or name.

802.11n MIMO antennas for the MSM466 and MSM466-R

These 802.11n MIMO antennas are certified only for use with the MSM466 and MSM466-R Access Points.

Part	Type	Band	Gain	Use	Elements
J9171A	Omni-directional	2.4/5 GHz	3/4 dBi	Indoor	3
J9659A	Omni-directional	2.4/5 GHz	1.5/5 dBi	Indoor	6
J9169A	Narrow Beam Sector	2.4/5 GHz	8/10.7 dBi	Outdoor	3
J9170A	Directional	2.4/5 GHz	10.9/13.5 dBi	Outdoor	3
J9719A	Omni-directional	2.4 GHz	6 dBi	Outdoor	3
J9720A	Omni-directional	5 GHz	8 dBi	Outdoor	3

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.

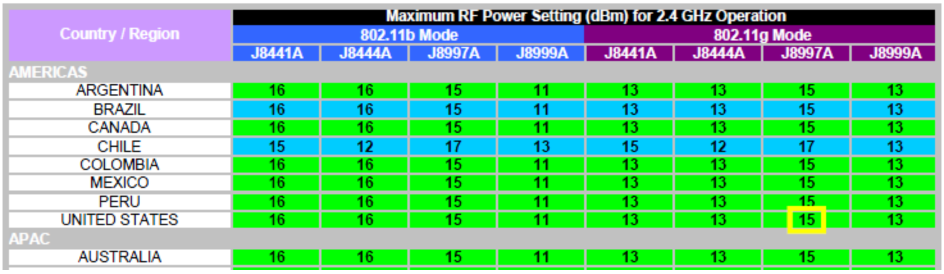
Antenna Notes:

- **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/support/manuals. Search for the part number of your antenna.

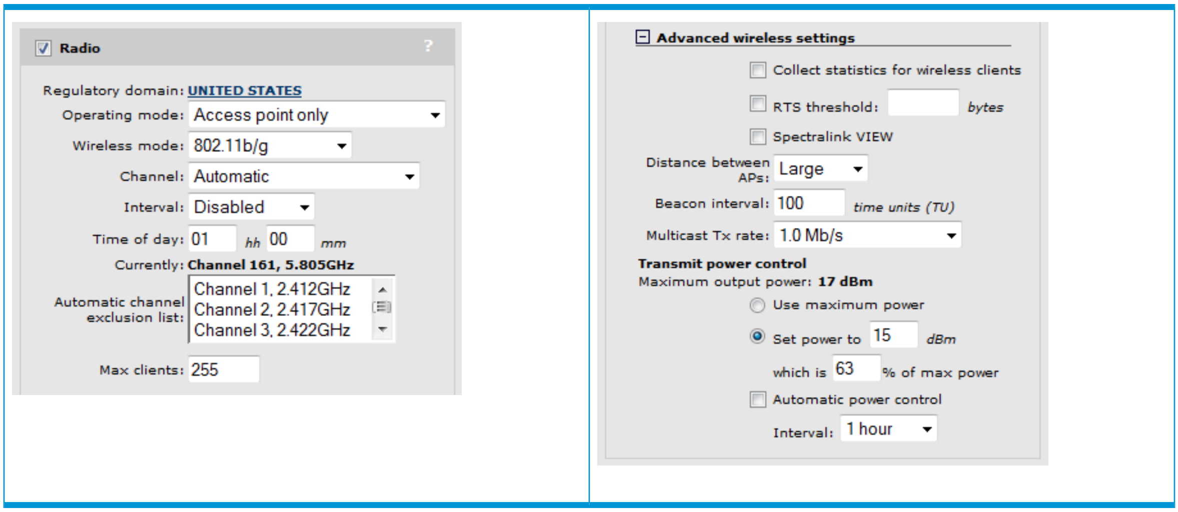
In this example, an optional HP antenna J8997A is to be used on an autonomous MSM AP configured for 802.11g in the USA. Per the Maximum RF Power Setting chart screenshot below, the intersection of row **UNITED STATES** and column **802.11g Mode/J8997A**, indicates that the maximum radio power level is **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):



☑ Radio

Regulatory domain: UNITED STATES

Operating mode: Access point only

Wireless mode: 802.11b/g

Channel: Automatic

Interval: Disabled

Time of day: 01 hh 00 mm

Currently: Channel 161, 5.805GHz

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

Max clients: 255

⊟ Advanced wireless settings

□ Collect statistics for wireless clients

□ RTS threshold: bytes

□ Spectralink VIEW

Distance between APs: Large

Beacon interval: 100 time units (TU)

Multicast Tx rate: 1.0 Mb/s

Transmit power control

Maximum output power: 17 dBm

○ Use maximum power

● Set power to 15 dBm

which is 63 % of max power

□ Automatic power control

Interval: 1 hour

8. Select **Save**.

Additional information is available as follows:

- For autonomous access points, see "Transmit power control" (page 49).
- For controlled access points, see *Transmit power control* in the *MSM7xx Controllers Configuration Guide*.

Documentation is available online from: www.hp.com/support/manuals. Search by product number or name.