Publication Number
5992-5937
May 2009

Applicable Products

<table>
<thead>
<tr>
<th>Product</th>
<th>USA part</th>
<th>WW part</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSM310 Access Point</td>
<td>J9374A</td>
<td>J9379A</td>
</tr>
<tr>
<td>MSM310-R Access Point</td>
<td>J9380A</td>
<td>J9383A</td>
</tr>
<tr>
<td>MSM320 Access Point</td>
<td>J9360A</td>
<td>J9364A</td>
</tr>
<tr>
<td>MSM320-R Access Point</td>
<td>J9365A</td>
<td>J9368A</td>
</tr>
<tr>
<td>MSM325 Access Point with Sensor</td>
<td>J9369A</td>
<td>J9373A</td>
</tr>
<tr>
<td>MSM335 Access Point with Sensor</td>
<td>J9356A</td>
<td>J9357A</td>
</tr>
<tr>
<td>MSM410 Access Point</td>
<td>J9426A</td>
<td>J9427A</td>
</tr>
<tr>
<td>MSM422 Access Point</td>
<td>J9358A</td>
<td>J9359A</td>
</tr>
</tbody>
</table>

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

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

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein. Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty
See the Customer Support/Warranty booklet included with the product.

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

Open Source Software Acknowledgement Statement
This software incorporates open source components that are governed by the GNU General Public License (GPL), version 2. In accordance with this license, HP ProCurve Networking will make available a complete, machine-readable copy of the source code components covered by the GNU GPL upon receipt of a written request. Send a request to:
Hewlett-Packard Company, L.P.
GNU GPL Source Code
Attn: ProCurve Networking Support
Roseville, CA 95747 USA

Safety
Before installing and operating this product, please read Safety information on page 1-11.
Contents

1 Introduction

About this guide ........................................................................................................... 1-2
Products covered .......................................................................................................... 1-2
HP ProCurve Networking product naming ............................................................. 1-2
Important terms ......................................................................................................... 1-3
Conventions ............................................................................................................... 1-4
  Management tool .................................................................................................... 1-4
  Warnings and cautions ....................................................................................... 1-4
  Commands and program listings ...................................................................... 1-4

New in this release ...................................................................................................... 1-5

Introducing the MSM3xx/4xx Access Points ......................................................... 1-6
Key features ............................................................................................................. 1-7

Controlled mode versus autonomous mode ......................................................... 1-8
  Controlled mode .................................................................................................. 1-8
  Autonomous mode ............................................................................................... 1-9
  Summary ............................................................................................................. 1-10

Safety information ...................................................................................................... 1-11
  Professional Installation Required .............................................................. 1-11
  Servicing ............................................................................................................ 1-11

HP ProCurve Networking support ........................................................................... 1-12
  Before contacting support ............................................................................. 1-12

Getting started ............................................................................................................ 1-12

Online documentation ............................................................................................... 1-12

2 Working with VSCs

Key concepts ............................................................................................................. 2-2
  Stand-alone deployment ..................................................................................... 2-2
  User authentication ............................................................................................ 2-2
  Using more than one authentication type in a VSC ........................................... 2-3
  Deployment with a service controller ................................................................. 2-3
3 Wireless configuration

Wireless coverage.................................................................................................3-2
  Wireless mode ..................................................................................................3-2
Factors limiting wireless coverage.....................................................................3-3
  Radio power ....................................................................................................3-3
  Antenna configuration ....................................................................................3-3
  Interference .....................................................................................................3-3
  Physical characteristics of the location .......................................................3-3
Configuring overlapping wireless cells.............................................................3-4
  Performance degradation and channel separation ......................................3-4
  Selecting channels ..........................................................................................3-5
  Automatic power control ...............................................................................3-7
802.11n best practices...........................................................................................3-8
  Supporting legacy clients ................................................................................3-8
    Available 802.11n modes ..............................................................................3-9
    802.11n (5 GHz) and 802.11n (2.4 GHz) ......................................................3-9
    802.11n/a, 802.11n/b/g ...............................................................................3-9
    802.11n/g ....................................................................................................3-10
  Channel width ..................................................................................................3-10
  Guard interval ..................................................................................................3-10
Conducting a site survey......................................................................................3-11
  Scanning frequency ........................................................................................3-11
  Identifying unauthorized APs ...........................................................................3-12
Radio configuration ............................................................................................3-13
  Configuration parameters ...............................................................................3-14
    Operating mode ..........................................................................................3-14
    Wireless mode ............................................................................................3-15
    Channel width ............................................................................................3-16
    Channel extension ......................................................................................3-16

TOS .......................................................................................................................2-20
IP QoS ..................................................................................................................2-20
Upstream DiffServ tagging .................................................................................2-20
Upstream/downstream traffic marking ............................................................2-21
  Upstream traffic marking ..........................................................................2-21
  Downstream traffic marking .......................................................................2-22
Channel ..........................................................................................................3-16
Interval ...........................................................................................................3-17
Time of day ....................................................................................................3-17
Automatic channel exclusion list................................................................3-18
Antenna selection .........................................................................................3-18
Antenna gain..................................................................................................3-19
Guard interval................................................................................................3-19
Spectralink VIEW..........................................................................................3-20
Maximum range (ack timeout)....................................................................3-20
Distance between access points .................................................................3-20
RTS threshold................................................................................................3-20
Beacon interval .............................................................................................3-21
Multicast Tx rate ............................................................................................3-21

4 Network configuration

Ports configuration ..........................................................................................4-2
Port configuration information .....................................................................4-2
Bridge port configuration .............................................................................4-3
Assign IP address via ....................................................................................4-3
Bridge spanning tree protocol .....................................................................4-3
Port configuration ..........................................................................................4-4
VLAN ..............................................................................................................4-4
Link ..................................................................................................................4-5
Wireless port configuration ............................................................................4-5

VLAN support ..................................................................................................4-5
Using a default VLAN ....................................................................................4-5
Assigning traffic to a VLAN ...........................................................................4-6
Assigning a VLAN to a VSC ...........................................................................4-6
Assigning VLANs to individual users ..........................................................4-6
VLAN bridging .................................................................................................4-7
VLAN configuration .......................................................................................4-7
General ............................................................................................................4-8
Assign IP address via .....................................................................................4-8
5 Management

Management tool ........................................................................................................ 5-2
  Management station ................................................................................................. 5-2
  Starting the management tool .................................................................................. 5-2
  Customizing management tool settings ..................................................................... 5-3
    Administrative user authentication ........................................................................ 5-3
    Manager and Operator accounts .......................................................................... 5-4
    Security policies .................................................................................................... 5-5
    Security .................................................................................................................... 5-6
    Web server ............................................................................................................... 5-6
    Auto-refresh ............................................................................................................ 5-7
    Web inactivity logout ............................................................................................. 5-7

SNMP ............................................................................................................................. 5-7
  Configuring SNMP settings ..................................................................................... 5-8
    Attributes ................................................................................................................. 5-9
    v1/v2c communities ............................................................................................... 5-9
    v3 users ..................................................................................................................... 5-9
    Notification receivers ............................................................................................. 5-10
    Security ..................................................................................................................... 5-10
### 6 Security

Using a RADIUS server ........................................................................................................ 6-2
  Configuring a RADIUS client profile on the AP ................................................................. 6-2
    Configuration procedure .................................................................................................. 6-2
    Configuration parameters ............................................................................................... 6-3
  Configuring user accounts on a RADIUS server .............................................................. 6-5
    Access Request attributes .............................................................................................. 6-5
    Access Accept attributes ............................................................................................... 6-7
    Access Reject ................................................................................................................ 6-8
    Access Challenge attributes ......................................................................................... 6-8
    Accounting Request attributes ..................................................................................... 6-8
  Configuring administrative accounts on a RADIUS server ........................................... 6-11
    Access Request attributes ............................................................................................ 6-11
  Colubris AV-Pair attribute values ...................................................................................... 6-12
    Administrative role ........................................................................................................ 6-12

Managing certificates ........................................................................................................... 6-12
  Trusted CA certificate store ............................................................................................. 6-13
    Installing a new CA certificate ...................................................................................... 6-13
  CA certificate import formats ........................................................................................... 6-13
  Default CA certificates ...................................................................................................... 6-14
  Certificate and private key store ...................................................................................... 6-14
    Installing a new private key/public key certificate chain pair ...................................... 6-15
    Default installed private key/public key certificate chains ......................................... 6-15
Certificate usage .................................................................................................. 6-16
Changing the certificate assigned to a service ........................................ 6-17
About certificate warnings .............................................................................. 6-17

7 Local mesh

Key concepts ........................................................................................................ 7-2
Benefits .............................................................................................................. 7-2

Local mesh terminology .................................................................................... 7-2
Static local mesh links ....................................................................................... 7-2
Dynamic local mesh links ................................................................................. 7-3
  Operational modes ......................................................................................... 7-4
  Node discovery ............................................................................................... 7-4
  Operating channel .......................................................................................... 7-4

Local mesh profiles ............................................................................................ 7-5
Configuring a local mesh profile ...................................................................... 7-6
  Settings ........................................................................................................... 7-7
  Security .......................................................................................................... 7-7
  Policy manager ............................................................................................... 7-7
  Addressing ...................................................................................................... 7-8

Configuration considerations ............................................................................ 7-12
  Single radio vs. multiple radios .................................................................. 7-12
  Simultaneous AP and local mesh ................................................................. 7-12
  Using two radios for local mesh .................................................................. 7-13
  Using 802.11a for local mesh ...................................................................... 7-13
  Maximum range ............................................................................................. 7-13

Quality of service ............................................................................................... 7-13

Configuration summary .................................................................................... 7-14

Sample local mesh deployments ...................................................................... 7-14
  RF extension .................................................................................................. 7-14
  Building-to-building connections ................................................................. 7-15
  Dynamic networks ........................................................................................ 7-15
8 Maintenance

Config file management ........................................................................................................ 8-2
  Manual configuration file management .......................................................................... 8-2
  Backup configuration ........................................................................................................ 8-2
  Reset configuration .......................................................................................................... 8-3
  Restore configuration ........................................................................................................ 8-3
  Scheduled operations ........................................................................................................ 8-3

Software updates ................................................................................................................. 8-4
  Performing an immediate software update ........................................................................ 8-5
  Performing a scheduled update ......................................................................................... 8-5

Licenses ................................................................................................................................ 8-6
  Factory reset considerations ............................................................................................. 8-7

A Regulatory information

Notice for U.S.A ....................................................................................................................... A-2
Notice for Canada .................................................................................................................... A-3
Notice for the European Community ..................................................................................... A-3
Supported External Antennas ............................................................................................... A-5
Notice for Brazil ...................................................................................................................... A-6
Notice for Japan ...................................................................................................................... A-6
Notice for Taiwan ................................................................................................................... A-6
Notice for Korea ..................................................................................................................... A-7

B Resetting to factory defaults

Introduction ............................................................................................................................ B-2
  Using the reset button ....................................................................................................... B-2
  Using the management tool .............................................................................................. B-2

Factory defaulting ruggedized products ............................................................................... B-4
Introduction

Contents

About this guide ........................................................................................................... 1-2
Products covered ...................................................................................................... 1-2
HP ProCurve Networking product naming ............................................................ 1-2
Important terms ........................................................................................................ 1-3
Conventions .............................................................................................................. 1-4
New in this release .................................................................................................... 1-5
Introducing the MSM3xx/4xx Access Points ......................................................... 1-6
Key features .............................................................................................................. 1-7
Controlled mode versus autonomous mode .......................................................... 1-8
Controlled mode ..................................................................................................... 1-8
Autonomous mode .................................................................................................. 1-9
Summary ................................................................................................................... 1-10
Safety information ................................................................................................... 1-11
HP ProCurve Networking support .......................................................................... 1-12
Getting started ........................................................................................................ 1-12
Online documentation ............................................................................................. 1-12
About this guide

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

Products covered

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

<table>
<thead>
<tr>
<th>Model</th>
<th>USA part</th>
<th>WW part</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSM310 Access Point</td>
<td>J9374A</td>
<td>J9379A</td>
</tr>
<tr>
<td>MSM310-R Access Point</td>
<td>J9380A</td>
<td>J9383A</td>
</tr>
<tr>
<td>MSM320 Access Point</td>
<td>J9360A</td>
<td>J9364A</td>
</tr>
<tr>
<td>MSM320-R Access Point</td>
<td>J9365A</td>
<td>J9368A</td>
</tr>
<tr>
<td>MSM325 Access Point with Sensor</td>
<td>J9369A</td>
<td>J9373A</td>
</tr>
<tr>
<td>MSM335 Access Point with Sensor</td>
<td>J9356A</td>
<td>J9357A</td>
</tr>
<tr>
<td>MSM410 Access Point</td>
<td>J9426A</td>
<td>J9427A</td>
</tr>
<tr>
<td>MSM422 Access Point</td>
<td>J9358A</td>
<td>J9359A</td>
</tr>
</tbody>
</table>

**HP ProCurve Networking product naming**

As of October 1st, 2008, Colubris Networks was acquired by HP ProCurve Networking. HP ProCurve Networking has integrated the Colubris product line into its Networking product portfolio ([www.procurve.com/news/colubris-10-01-08.htm](http://www.procurve.com/news/colubris-10-01-08.htm)).

In the online help and this guide, Colubris product names have been changed to their equivalent HP ProCurve Networking product names.

**Note**

SOAP and SNMP MIBs retain the Colubris naming so you do not need to change your existing SOAP and MIB usage.
The Colubris Networks product names and their corresponding new HP ProCurve Networking product names are as follows:

<table>
<thead>
<tr>
<th>Colubris name</th>
<th>HP ProCurve Networking name</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSC-5100 MultiService Controller</td>
<td>MSM710 Controller</td>
</tr>
<tr>
<td>MSC-5200 MultiService Controller</td>
<td>MSM730 Controller</td>
</tr>
<tr>
<td>MSC-5500 MultiService Controller</td>
<td>MSM750 Controller</td>
</tr>
<tr>
<td>MAP-320 MultiService Access Point</td>
<td>MSM310 Access Point</td>
</tr>
<tr>
<td>MAP-320R MultiService Access Point</td>
<td>MSM310-R Access Point</td>
</tr>
<tr>
<td>MAP-330 MultiService Access Point</td>
<td>MSM320 Access Point</td>
</tr>
<tr>
<td>MAP-330R MultiService Access Point</td>
<td>MSM320-R Access Point</td>
</tr>
<tr>
<td>MAP-330 AP+Sensor MultiService Access Point</td>
<td>MSM325 Access Point with Sensor</td>
</tr>
<tr>
<td>MAP-625 MultiService Access Point</td>
<td>MSM422 Access Point</td>
</tr>
<tr>
<td>MAP-630 AP+Sensor MultiService Access Point</td>
<td>MSM335 Access Point with Sensor</td>
</tr>
<tr>
<td>WCB-200 Wireless Client Bridge</td>
<td>M111 Client Bridge</td>
</tr>
<tr>
<td>Visitor Management Tool</td>
<td>Guest Management Software</td>
</tr>
<tr>
<td>RF Manager 1500 Enterprise</td>
<td>RF Manager 100 IDS/IPS system</td>
</tr>
<tr>
<td>RF Manager 1300 Basic</td>
<td>RF Manager 50 IDS/IPS system</td>
</tr>
<tr>
<td>RF Planner</td>
<td>RF Planner</td>
</tr>
</tbody>
</table>

**Important terms**

The following terms are used in this guide.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP or MSM AP</td>
<td>Refers to any HP ProCurve Networking MSM3xx or MSM4xx Access Point.</td>
</tr>
<tr>
<td>service controller</td>
<td>Refers to any HP ProCurve Networking MSM7xx Controller, including both Access Controller and Mobility Controller variants.</td>
</tr>
</tbody>
</table>
Conventions

Management tool

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

![Management tool screenshot]

<table>
<thead>
<tr>
<th>Example directions in this guide</th>
<th>What to do in the user interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select <strong>Wireless &gt; Local Mesh.</strong></td>
<td>On the main menu select <strong>Wireless</strong> and then select <strong>Local mesh</strong> on the sub-menu.</td>
</tr>
<tr>
<td>For <strong>Password</strong> specify <strong>secret22</strong>.</td>
<td>In the field <strong>Password</strong> enter the text <strong>secret22</strong> exactly as shown.</td>
</tr>
</tbody>
</table>

Warnings and cautions

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

**Warning**

Identifies a hazard that can cause physical injury or death.

**Caution**

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

Commands and program listings

Monospaced text identifies commands and program listings as follows:

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>use-access-list</td>
<td>Command name. Specify it as shown.</td>
</tr>
<tr>
<td>ip_address</td>
<td>Items in italics are parameters for which you must supply a value.</td>
</tr>
<tr>
<td>ssl-certificate=URL [%s]</td>
<td>Items enclosed in square brackets are optional. You can either include them or not. Do not include the brackets. In this example you can either include the “%s” or omit it.</td>
</tr>
<tr>
<td>[ONE</td>
<td>TWO]</td>
</tr>
</tbody>
</table>
New in this release

The following new features and enhancements have been added in releases 5.3.x:

<table>
<thead>
<tr>
<th>New feature or enhancement</th>
<th>For information see...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for MSM410 Access Point</td>
<td>This guide and the <em>MSM410 Access Point Quickstart</em>.</td>
</tr>
<tr>
<td>Configurable status light.</td>
<td><em>LEDs on page 5-15</em>.</td>
</tr>
<tr>
<td>Support for manager and operator accounts</td>
<td><em>Customizing management tool settings on page 5-3</em>.</td>
</tr>
<tr>
<td>Support for SNMP v3</td>
<td><em>SNMP on page 5-7</em>.</td>
</tr>
</tbody>
</table>
Introducing the MSM3xx/4xx Access Points

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

When operating in controlled mode, APs are managed by an MSM7xx Controller (service controller), making it easy to provide roaming, enforce consistent security and QoS policies, and automate AP configuration to minimize deployment and operation costs.

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

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

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

Security
- Enforcement of client authorization based on user credentials (802.1X/EAP), hardware identifiers (MAC address, WEP key), and HTML login
- Hardware-assisted encryption using WPA2/AES (IEEE 802.11i), WPA/RC4 and/or WEP
- Dedicated RF sensor and dedicated client access eliminate time-slicing on the MSM325 and MSM335.
- Layer-2 client isolation per VSC
- Wireless Network Design Process
- Designing a New Wireless Network
- Trusted Network Connect (TNC) network access control for user quarantine
- Protocol filtering per VSC to deny unwanted traffic
- IP filtering per-user and per-VSC to forward traffic to a pre-defined location
- Management communication through SSH/SSL, IPsec, and digital certificates
- Kensington lock compatible for physical security on the MSM335, MSM410, and MSM422
- Controlled-mode security to prevent data from being recovered from stolen APs
Controlled mode versus autonomous mode

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

Controlled mode

When operating in controlled mode, the AP must establish a management tunnel with a service controller before it becomes fully operational. The service controller manages the AP and provides all configuration settings. Discovery of the service controller is automatic if default settings are used on the AP and the service controller, and both devices are on the same subnet.

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

An autonomous AP operates as an isolated AP based on its current configuration, which is managed locally using its integrated management tool. Autonomous APs do not provide the benefits of centralized management and monitoring.

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Feature/function</th>
<th>Controlled mode AP</th>
<th>Autonomous mode AP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset AP to factory default settings</td>
<td>AP remains in controlled mode.</td>
<td>AP changes from autonomous to controlled mode.</td>
</tr>
<tr>
<td>Network connection (Ethernet)</td>
<td>Supported on Port 1 only.</td>
<td>Supported on Port 1 or Port 2.</td>
</tr>
<tr>
<td>Centralized configuration/software management</td>
<td>Fully automated using the management tool on a service controller. Allows APs to be configured individually or in groups.</td>
<td>New configuration/software can be downloaded from a central location at a preset day and time.</td>
</tr>
<tr>
<td>Configuration changes</td>
<td>Performed using the management tool on a service controller. Multiple APs can be updated at the same time.</td>
<td>Performed locally using each the management tool on each AP.</td>
</tr>
<tr>
<td>Remote configuration and management</td>
<td>Automatic establishment of a secure tunnel to protect management and control traffic.</td>
<td>Via secure HTTPS browser session.</td>
</tr>
<tr>
<td>Local mesh groups (wireless links)</td>
<td>Dynamic links.</td>
<td>Dynamic and static links.</td>
</tr>
<tr>
<td>L2 fast authentication and L3 Mobility</td>
<td>Supported (with the appropriate license).</td>
<td>Not supported.</td>
</tr>
<tr>
<td>Centralized access control</td>
<td>Supported.</td>
<td>Not supported.</td>
</tr>
<tr>
<td>STP</td>
<td>Disabled by default.</td>
<td>Enabled by default.</td>
</tr>
</tbody>
</table>
Safety information

**Warning**

**Professional Installation Required**

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

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

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

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

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

- If your network covers an area served by more than one power distribution system, be sure all safety grounds are securely interconnected.

- Network cables may occasionally be subject to hazardous transient voltages (caused by lightning or disturbances in the electrical power grid).

- Handle exposed metal components of the network with caution.

- The AP and all interconnected equipment must be installed indoors within the same building (except for outdoor models / antennas), including all PoE-powered network connections as described by Environment A of the IEEE 802.3af standard.

**Servicing**

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

HP ProCurve Networking offers support 24 hours a day, seven days a week through a number of automated electronic services. See the Customer Support/Warranty booklet included with your product.

The HP ProCurve Networking Web site, [www.procurve.com/customercare](http://www.procurve.com/customercare) provides up-to-date support information.

Additionally, your HP-authorized network reseller can provide you with assistance, both with services that they offer and with services offered by HP.

**Before contacting support**

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

<table>
<thead>
<tr>
<th>Collect this information</th>
<th>Where to find it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product identification.</td>
<td>On the rear of the product.</td>
</tr>
<tr>
<td>Software version.</td>
<td>The AP management tool <a href="#">Login</a> page.</td>
</tr>
<tr>
<td>Network topology map, including the addresses assigned to all relevant devices.</td>
<td>Your network administrator.</td>
</tr>
</tbody>
</table>

**Getting started**

Get started with your AP by following the directions in the relevant Quickstart, then:

- If operating in autonomous mode, continue with the next chapter in this guide.

- If operating in controlled mode, see *Working with controlled APs* in the *MSM7xx Controllers Management and Configuration Guide*.

**Online documentation**

For the latest documentation, visit the HP ProCurve Networking manuals Web page at: [www.procurve.com/manuals](http://www.procurve.com/manuals).
Contents
Key concepts.................................................................................................................2-2
  Stand-alone deployment ..........................................................................................2-2
Deployment with a service controller.................................................................2-3
Management with VLANs .....................................................................................2-4
VSC configuration overview .......................................................................................2-5
  About the ‘Use HP ProCurve MSM controller’ option ......................................2-5
VSC configuration options ..........................................................................................2-7
  Virtual AP................................................................................................................2-7
  Wireless clients ......................................................................................................2-8
  Egress VLAN ........................................................................................................2-10
  Wireless security filters.......................................................................................2-11
  Wireless protection ..............................................................................................2-11
  MAC-based authentication .................................................................................2-14
  Location-aware ....................................................................................................2-14
  MAC filter .............................................................................................................2-14
  IP filter ..................................................................................................................2-15
VSC data flow .............................................................................................................2-16
  Stand-alone deployment .....................................................................................2-16
  AP deployed with a service controller..............................................................2-17
Quality of service (QoS)............................................................................................2-18
  Priority mechanisms ...........................................................................................2-19
  Upstream DiffServ tagging .................................................................................2-20
  Upstream/downstream traffic marking ............................................................2-21
Key concepts

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

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

Stand-alone deployment

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

User authentication

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

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

- 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 service controller

Autonomous APs can also be used with a service 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 service 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 service controller.

The following authentication types are supported on the service controller: WPA / WPA2, 802.1X, MAC, HTML. For more information on service controller authentication features, see the *MSM7xx Controllers Management and Configuration Guide*. 
In this type of installation, VSC definitions on both the AP and service controller must match so that traffic from wireless users connected to the AP can be sent to the service 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 service 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.
VSC configuration overview

The VSC page lists the defined VSC profiles and enables you to add new ones.

To edit a profile, select its link in the Name column. To add a new profile, select Add New VSC Profile. The Add/Edit Virtual Service Community page opens providing all VSC profile options.

About the ‘Use HP ProCurve MSM controller’ option

Availability of certain VSC features and their functionality are dependent on the setting of the Use HP ProCurve MSM controller in the VSC General box. This option determines how authentication and access control are handled by the VSC.
If ‘Use HP ProCurve MSM controller’ is enabled
This creates an access-controlled VSC. This means that the AP must be used in conjunction with a service controller, because the VSC is automatically configured to forward all user traffic to the service controller for authentication (Wireless protection and MAC-based authentication options are forced to use a service Controller as the RADIUS server). Also, once authenticated, user traffic is restricted by the Wireless security filters option. Only traffic addressed to the service controller is permitted. (These filters can be disabled if required.)

![Diagram showing user traffic and authentication traffic routed to service controller and then to network]

If ‘Use HP ProCurve MSM controller’ is disabled
This creates a non-access-controlled VSC, which allows the AP to manage user authentication 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 service controller, otherwise it will be interpreted and processed.

![Diagram showing user traffic and authentication traffic routed to third-party authentication server and then to network]
VSC configuration options

The following table lists the VSC configuration options that are available depending on how the Use HP ProCurve MSM controller option is configured.

<table>
<thead>
<tr>
<th>VSC configuration option</th>
<th>Use HP ProCurve MSM controller is:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>Virtual AP</td>
<td>n</td>
</tr>
<tr>
<td>Egress VLAN</td>
<td>n</td>
</tr>
<tr>
<td>Wireless security filters</td>
<td>User traffic restricted to service controller.</td>
</tr>
<tr>
<td>Wireless protection</td>
<td>User authentication is performed by the service controller.</td>
</tr>
<tr>
<td>MAC-based authentication</td>
<td>User authentication is performed by the service controller.</td>
</tr>
<tr>
<td>Location-aware</td>
<td>n</td>
</tr>
<tr>
<td>Wireless MAC filter</td>
<td>n</td>
</tr>
<tr>
<td>Wireless IP filter</td>
<td>n</td>
</tr>
</tbody>
</table>

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

Virtual AP

These settings define the characteristics of the wireless network created by the VSC, including its name, the number of clients supported, and quality of service settings.
Name (SSID)
Specify a name to uniquely identify the wireless network associated with this VSC. Each client computer that wants to connect to this VSC must use this name. The name is case-sensitive.

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

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

Transmit/receive on
Select the radio, Radio 1, 2 or both, on which this VSC will transmit and receive.

Broadcast name (SSID)
When enabled, the device will broadcast its wireless network name (SSID) to all client stations. Most wireless adapter cards have a setting that enables them to automatically discover APs that broadcast their names and automatically 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 WLAN name when they connect.

Advertise Tx power
When this option is enabled, the device will broadcast its current transmit power setting in the wireless beacon. It will also enable support for 802.1h and 802.11d.

Wireless clients
Max clients per radio
Specify the maximum number of wireless client stations that can be associated with this SSID at the same time on each radio.

Allow traffic between wireless clients
Use this option to control how wireless clients can communicate with each other. The following options apply directly to client stations connected to the same VSC.

- 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.
Configuring communication between different VSCs

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

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

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

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

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

Lets you prioritize traffic on the VSC. See Quality of service (QoS) on page 2-18 details.
**Allowed wireless rates**

Lets you select the wireless transmission speeds that are supported for each wireless mode.

(MSM410 and MSM422 radio 1 only)
For 802.11n, in addition to speeds 1 to 54, 16 MCS values (MCS0 to MCS15) are also included, with MCS0 being the slowest and MCS15 being the fastest.

**Egress VLAN**

Sets the VLAN to which this profile forwards data traffic. If you do not select a VLAN, traffic is sent untagged. Note however, that a VLAN may still be assigned on a per-customer basis via a setting in the customer's RADIUS account (if using RADIUS-based authentication). Also, a global VLAN setting is available on the **Network > Ports** page which will tag all traffic sent on port 1 and 2.
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.

- If **Use HP ProCurve MSM controller** is enabled (under **General**), the AP will only forward user traffic that is addressed to the access controller (service controller). All other traffic is blocked. Make sure that the access controller is set as the default gateway. If not, all user traffic will be blocked by the AP.

As a convenience, you can click the **access controller** link to display the **Security > Access controller** page.

- If **Use HP ProCurve MSM controller** is disabled (under **General**), then the security filters can be used to block traffic unless it is addressed to a specific device.

Use the **Custom** option to define a custom filter with standard pcap syntax and a few HP ProCurve-specific placeholders. See the online help for details.

Wireless protection

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

**(MSM410 and MSM422 only)**

When using 802.11n, wireless protection settings are enforced as follows:

- WEP protection is never permitted. If selected, WPA or WPA2 protection is used instead.
- When using pure 802.11n in either the 2.4 or 5 Ghz bands, WPA2 protection is used instead of WPA settings.
**WPA**

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

- **WPA (TKIP)**: WPA with TKIP encryption.
- **WPA2 (AES/CCMP)**: WPA2 (802.11i) with CCMP encryption.
- **WPA or WPA2**: Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time.

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

### Use HP ProCurve MSM controller feature

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Wireless protection" /></td>
<td><img src="image2.png" alt="Wireless protection" /></td>
</tr>
</tbody>
</table>

**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 ProCurve MSM controller** is enabled (under **General**), this must be an HP ProCurve service controller, otherwise a third-party RADIUS server can be used.

### Use HP ProCurve MSM controller feature

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Enabled" /></td>
<td><img src="image2.png" alt="Disabled" /></td>
</tr>
</tbody>
</table>

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

### WEP

This option provides support for users needing WEP encryption.
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 ProCurve MSM controller is enabled (under General), this must be an HP ProCurve service controller, otherwise a third-party RADIUS server can be used.

Use HP ProCurve MSM controller feature

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Use HP ProCurve MSM controller feature" /></td>
<td><img src="image2.png" alt="Use HP ProCurve MSM controller feature" /></td>
</tr>
</tbody>
</table>

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 ProCurve MSM controller is enabled (under General).

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

MAC filter

This option enables you to either block or allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses.
IP filter

This option enables you to only allow wireless-to-wired LAN traffic for specific destination addresses.

![IP filter window](image)

**Note** This option is applied on a per-radio basis.
VSC data flow

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

Stand-alone deployment

**VSC on autonomous AP**

**Ingress**
- SSID (from association)

**Features**
- Authentication (MAC, 802.1X)
- Wireless security filters
- Wireless MAC filter
- Wireless IP filter

**Egress**
- Bridged onto port 1+2
- VLAN

User and authentication traffic

AP deployed with a service controller

**VSC on autonomous AP**

**Ingress**
- SSID (from association)

**Features**
- Authentication (MAC, 802.1X)
- Wireless security filters
- Wireless MAC filter
- Wireless IP filter

**Egress**
- Bridged onto port 1+2
- VLAN

**VSC on service controller**

**Ingress**
- SSID (LAN port via location-ware)
- VLAN (LAN or Internet port)
- Untagged (LAN port)

**Features**
- Authentication (MAC, 802.1X, HTML)
- Access control features

**Egress**
- Routing table
- VLAN
- GRE tunnel

User and authentication traffic

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 service controller or a third-party device. For more information, see Authentication types in the chapter on User authentication in the MSM7xx Controllers Management and Configuration Guide.

- **Wireless security filters**: Enables the AP to block traffic unless it is addressed to a specific device (like the service controller). For more information, see Wireless security filters on page 2-11.

- **Wireless MAC filter**: Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses.

- **Wireless IP filter**: Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user IP addresses.

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.

- **VLAN**: All traffic on port 1 or 2 can be assigned to a VLAN.

AP deployed with a service 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 service controller. For more information, see Authentication types in the chapter on User authentication in the MSM7xx Controllers Management and Configuration Guide.

- **Wireless security filters**: Enables the AP to block traffic unless it is addressed to a specific device (like the service controller). For more information, see Wireless security filters on page 2-11.

- **Wireless MAC filter**: Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses.

- **Wireless IP filter**: Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user IP addresses.

Egress

- **Bridge onto port 1+2**: User and authentication traffic is bridged onto ports 1 and 2.

- **VLAN**: All traffic on port 1 or 2 can be assigned to a VLAN.
VSC on service controller

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

Ingress

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

Features

- **Authentication:** The service controller supports 802.1X, MAC, or HTML authentication. To validate user login credentials the service controller can use the local user accounts or make use of a third-party authentication server (Active Directory or RADIUS).
- **Access control features:** The service 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 service controller enables user traffic to be forwarded to different output interfaces, which include the routing table, VLAN ID, or IP GRE tunnel.

Quality of service (QoS)

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

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

<table>
<thead>
<tr>
<th>Queue</th>
<th>WMM access category</th>
<th>Typically used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AC_VO</td>
<td>Voice traffic</td>
</tr>
<tr>
<td>2</td>
<td>AC_VI</td>
<td>Video traffic</td>
</tr>
<tr>
<td>3</td>
<td>AC_BE</td>
<td>Best effort data traffic</td>
</tr>
<tr>
<td>4</td>
<td>AC_BK</td>
<td>Background data traffic</td>
</tr>
</tbody>
</table>
Outgoing wireless traffic on the VSC is assigned to a queue based on the selected priority mechanism. Traffic delivery is based on strict priority (per the WMM standard). Therefore, if excessive traffic is present on queues 1 or 2, it will reduce the flow of traffic on queues 3 and 4.

Regardless of the priority mechanism that is selected:

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

**Priority mechanisms**

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

**802.1p**

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

<table>
<thead>
<tr>
<th>Queue</th>
<th>802.1p (VLAN priority field value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6,7</td>
</tr>
<tr>
<td>2</td>
<td>4,5</td>
</tr>
<tr>
<td>3</td>
<td>0,2</td>
</tr>
<tr>
<td>4</td>
<td>1,3</td>
</tr>
</tbody>
</table>

**VSC-based priority**

This mechanism is unique to HP ProCurve. 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.

<table>
<thead>
<tr>
<th>Queue</th>
<th>VSC-based priority value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Very-based Very High</td>
</tr>
<tr>
<td>2</td>
<td>Very-based High</td>
</tr>
<tr>
<td>3</td>
<td>Very-based Normal</td>
</tr>
<tr>
<td>4</td>
<td>Very-based Low</td>
</tr>
</tbody>
</table>
Differentiated Services (DiffServ)
This mechanism classifies traffic based on the value of the Differentiated Services (DS) codepoint field in IPv4 and IPv6 packet headers (as defined in RFC2474). The codepoint is composed of the six most significant bits of the DS field.

<table>
<thead>
<tr>
<th>Queue</th>
<th>DiffServ (DS codepoint value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>111000 (Network control) 110000 (Internetwork control)</td>
</tr>
<tr>
<td>2</td>
<td>101000 (Critical) 100000 (Flash override)</td>
</tr>
<tr>
<td>3</td>
<td>011000 (Flash) 000100 (Routine)</td>
</tr>
<tr>
<td>4</td>
<td>010000 (Immediate) 001000 (Priority)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Queue</th>
<th>TOS (Type of Service field value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0x30, 0xE0, 0x88, 0xB8</td>
</tr>
<tr>
<td>2</td>
<td>0x28, 0xA0</td>
</tr>
<tr>
<td>3</td>
<td>0x08, 0x20</td>
</tr>
<tr>
<td>4</td>
<td>All other TOS traffic</td>
</tr>
</tbody>
</table>

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

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

Upstream DiffServ tagging
Enable this option to have the M111 apply differentiated services marking to upstream traffic.

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

When this feature is enabled, packets received on the wireless interface that include Wi-Fi Multimedia (WMM) QoS values are remarked using IP TOS/DiffServ values when transmitted to the wired network.
**Upstream/downstream traffic marking**

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

**Upstream traffic marking**

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

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>INCOMING TRAFFIC</th>
<th>OUTGOING TRAFFIC</th>
<th>L2 marking</th>
<th>L3 marking</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Wireless traffic sent from client stations to the AP</td>
<td>Traffic sent by the AP to the network</td>
<td>802.1p (requires an egress VLAN to be defined for the VSC)</td>
<td>Upstream DiffServ tagging is enabled</td>
</tr>
<tr>
<td>802.1p</td>
<td>WMM</td>
<td></td>
<td></td>
<td>Upstream DiffServ tagging is disabled</td>
</tr>
<tr>
<td>DiffServ</td>
<td>DiffServ</td>
<td></td>
<td></td>
<td>Pass-through (Original layer 3 marking, if any, is preserved.)</td>
</tr>
<tr>
<td>TOS</td>
<td>TOS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VSC-based</td>
<td>WMM Non-WMM</td>
<td>802.1p (requires an egress VLAN to be defined for the VSC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP QoS</td>
<td>WMM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Downstream traffic marking

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

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>INCOMING TRAFFIC</th>
<th>OUTGOING TRAFFIC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Traffic received from wired network</td>
<td>Wireless traffic sent from AP to client stations</td>
</tr>
<tr>
<td>802.1p</td>
<td>802.1p</td>
<td>WMM + HPQ (WMM marking done according to the rules for the mechanism.)</td>
</tr>
<tr>
<td>DiffServ</td>
<td>DiffServ</td>
<td>HPQ (hardware priority queueing)</td>
</tr>
<tr>
<td>TOS</td>
<td>TOS</td>
<td></td>
</tr>
<tr>
<td>VSC-based</td>
<td>All traffic on the VSC</td>
<td></td>
</tr>
<tr>
<td>IP QoS</td>
<td>All traffic that matches the ports/protocols specified in the selected IP QoS profiles</td>
<td></td>
</tr>
</tbody>
</table>

**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.)
# Wireless configuration

## Contents

- Wireless coverage ................................................................. 3-2
- Wireless mode ........................................................................ 3-2
- Factors limiting wireless coverage ........................................ 3-3
- Configuring overlapping wireless cells ............................... 3-4
- 802.11n best practices .......................................................... 3-8
  - Supporting legacy clients .................................................... 3-8
  - Channel width ................................................................. 3-10
  - Guard interval .................................................................. 3-10
- Conducting a site survey ....................................................... 3-11
  - Scanning frequency .......................................................... 3-11
  - Identifying unauthorized APs .............................................. 3-12
- Radio configuration ............................................................ 3-13
  - Configuration parameters ................................................. 3-14
Wireless coverage

As a starting point for planning your network, you can assume that when operating at high power, the 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 to determine the optimal settings and location for the AP.

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

Note

Supported wireless modes, operating channels, and power output are determined by the regulations of the country in which the AP is operating, and are controlled by the country setting on the AP. For more information, see Country on page 5-15.

Wireless mode

Supported wireless modes may include the following:

- **802.11b**: Up to 11 Mbps in the 2.4 GHz frequency band.
- **802.11g**: Up to 54 Mbps in the 2.4 GHz frequency band.
- **802.11 b + g**: Up to 11 Mbps and 54 Mbps in the 2.4 GHz frequency band.
- **802.11a**: Up to 54 Mbps in the 5 GHz frequency band.
- **802.11a Turbo**: Provides channel bonding in the 5 GHz frequency band for enhanced performance when creating local mesh links.

(MSM410 and MSM422 radio 1 only)

For 802.11n, in addition to speeds 1 to 54, 16 MCS values (MCS0 to MCS15) are also included, with MCS0 being the slowest and MCS15 being the fastest.

- **802.11n (5 GHz)**: (pure 802.11n) Up to 300 Mbps in the 802.11n 5 GHz frequency band. Only 802.11n clients can associate with an AP in this mode.
- **802.11n (2.4 GHz)**: (pure 802.11n) Up to 300 Mbps in the 802.11n 2.4 GHz frequency band. Only 802.11n clients can associate with an AP in this mode.
- **802.11n/a**: (Compatibility mode.) In the 5 GHz frequency band, up to 270 Mbps for 802.11n and 54 Mbps for 802.11a.
- **802.11n/g**: (Compatibility mode.) In the 2.4 GHz frequency band, up to 270 Mbps for 802.11n and 54 Mbps for 802.11g. Only use this setting when support for 802.11g is necessary.
- **802.11n/b/g**: (Compatibility mode.) In the 2.4 GHz frequency band, up to 270 Mbps for 802.11n, 54 Mbps for 802.11g, and 11 Mbps for 802.11b. Only use this setting when support for 802.11b is necessary.
Factors limiting wireless coverage

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

Radio power

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

Further, when more than one AP operates in an area, you must adjust wireless cell size to reduce interference between APs. An automatic power control feature is available to address this challenge. See Transmit power control on page 3-21.

Antenna configuration

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

Interference

Interference is caused by other APs or devices that operate in the same frequency band as the AP and can substantially affect throughput. Advanced wireless configuration features are available to automatically eliminate this problem. See Radio configuration on page 3-13.

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

- Select Wireless > Neighborhood to view detailed information about all wireless APs operating in the immediate area so that you can effectively set the operating frequencies. This wireless neighborhood feature also makes it easy for you to find rogue APs. See Conducting a site survey on page 3-11.
- Select Status > Wireless to view detailed information about packets sent and received, transmission errors, and other low-level events.
- Select Status > Client data rate matrix to view information about data rates for all connected client stations. This makes it easy to determine if low-speed clients are affecting network performance. To prevent low-speed clients from connecting, you can use the Allowed wireless rates option when defining a VSC. See Virtual AP on page 2-7.

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 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). In either case, the problems you face are similar.

**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 frequency. Since both APs are within range of each other, the number of deferred transmissions can be large.

![Diagram of overlapping wireless cells](image)

The solution to this problem is to set the two networks to different channels with as great a separation as possible in their operating frequencies. This reduces crosstalk and enables client stations connected to each AP to transmit at the same time.
Selecting channels

For optimal performance when operating in 802.11b or 802.11g modes, select an operating frequency that is different by at least 25 MHz from the frequency used by other wireless APs that operate in neighboring cells.

Two channels with the minimum 25 MHz frequency separation always perform worse than two channels that use maximum separation. It is always best to use the greatest separation possible between overlapping networks.

Note

All channels operating in 802.11a mode are non-overlapping.

With the proliferation of wireless networks, it is very 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 generate a list of all APs that operate near you and their operating frequencies.

The set of available channels is automatically determined based on the Country setting you define by selecting Management > Country. This means that the number of non-overlapping channels available to you varies by geographical location, which affects how you set up your multi-cell network.

Sample channel selections

For example, when operating in 802.11b mode, the AP supports the following 14 channels in the 2.4 GHz band.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2412</td>
</tr>
<tr>
<td>2</td>
<td>2417</td>
</tr>
<tr>
<td>3</td>
<td>2422</td>
</tr>
<tr>
<td>4</td>
<td>2427</td>
</tr>
<tr>
<td>5</td>
<td>2432</td>
</tr>
<tr>
<td>6</td>
<td>2437</td>
</tr>
<tr>
<td>7</td>
<td>2442</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>2447</td>
</tr>
<tr>
<td>9</td>
<td>2452</td>
</tr>
<tr>
<td>10</td>
<td>2457</td>
</tr>
<tr>
<td>11</td>
<td>2462</td>
</tr>
<tr>
<td>12</td>
<td>2467</td>
</tr>
<tr>
<td>13</td>
<td>2472</td>
</tr>
<tr>
<td>14</td>
<td>2477</td>
</tr>
</tbody>
</table>

However, the number of channels available for use in a particular country are determined by the regulations defined by the local governing body. The following table shows the number of channels that are available in North America, Japan, and Europe.

<table>
<thead>
<tr>
<th>Region</th>
<th>Available channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>1 to 11</td>
</tr>
<tr>
<td>Japan</td>
<td>1 to 14</td>
</tr>
<tr>
<td>Europe</td>
<td>1 to 13</td>
</tr>
</tbody>
</table>
Since the minimum recommended separation between overlapping channels is 25 MHz (five cells) 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 20 MHz channels in the 2.4 GHz band).

<table>
<thead>
<tr>
<th>North America</th>
<th>Japan</th>
<th>Europe</th>
</tr>
</thead>
<tbody>
<tr>
<td>• cell 1 on channel 1</td>
<td>• cell 1 on channel 1</td>
<td>• cell 1 on channel 1</td>
</tr>
<tr>
<td>• cell 2 on channel 6</td>
<td>• cell 2 on channel 7</td>
<td>• cell 2 on channel 7</td>
</tr>
<tr>
<td>• cell 3 on channel 11</td>
<td>• cell 3 on channel 14</td>
<td>• cell 3 on channel 13</td>
</tr>
</tbody>
</table>

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

![Diagram of cell towers in North America](image1)

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.

![Diagram of staggered cell towers](image2)

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(s)** and set the **Distance between access points** option.

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

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

**Automatic power control**

The automatic power control feature enables the AP to dynamically adjust its transmission power to avoid causing interference with neighboring HP ProCurve APs. For information see *Transmit power control on page 3-21*. 
**802.11n best practices**

This section provides recommendations on how to best use 802.11n wireless technology, especially when legacy (a/b/g) clients must also be supported. 802.11n is available on the MSM410 and MSM422 802.11n access points.

- The MSM422 features two radios: Radio 1 is an 802.11a/b/g/n radio and Radio 2 is an 802.11a/b/g radio (also referred to as a legacy radio).

- The MSM410 features a single 802.11a/b/g/n radio. This radio has the same features as Radio 1 on the MSM422. Therefore, all references to Radio 1 in this section apply to both the MSM422 and the MSM410.

**Supporting legacy 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 a/b/g 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 MSM422 can be configured to allow network administrators greater flexibility over their deployments. The protection behavior is determined based on the wireless mode of the MSM422 11n radio.

---

**Note**

802.11n clients can only achieve maximum data rates when legacy clients are not present on the same radio.
Available 802.11n modes

The Wireless Mode of Radio 1 can be set to one of the following values:

- 802.11n (5 GHz)
- 802.11n/a
- 802.11n (2.4 GHz)
- 802.11n/g
- 802.11n/b/g.

Note

Radio 1 can also be set to legacy (a/b/g) values with no 802.11n support.

802.11n (5 GHz) and 802.11n (2.4 GHz)

HP ProCurve refers to these two modes as Pure-N. When Radio 1 is in either of these modes, it will not allow non-802.11n clients to associate. Legacy clients can see the access point, and may attempt to associate, but they will be rejected. The AP makes this determination based on the supported rate set that the client presents during its association request. If the rate set does not include any of the HT rates (MCS0-MCS15), it is not allowed to associate.

In these modes, the AP will not use protection when sending HT frames to associated clients. If legacy APs or clients are using the same channel, this may lead to collisions. In the 5 GHz band, this will probably not be a common problem since the band isn’t heavily used. However in the 2.4 GHz band, this mode may cause serious performance deterioration for everyone on the channel (both the 802.11b/g and 802.11n clients).

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

Note

Note that some people may refer to this mode as Greenfield, which is not correct. Greenfield is an 802.11n-specific preamble that can be used by clients and APs. MSM APs do not support this preamble and therefore does not support Greenfield mode.

When to use these modes: the Pure-N modes can be used when there is no legacy wireless traffic present in or around the premises on the channels that will be used. All client devices must support 802.11n.

802.11n/a, 802.11n/b/g

These modes are referred to as compatibility modes. 802.11n/a, which supports 802.11n and 802.11a clients in the 5 GHz spectrum, is the default mode of Radio 1. 802.11n/b/g supports 802.11n and 802.11b/g clients in the 2.4 GHz spectrum. In either of these modes, the AP allows both 802.11n and legacy clients to associate. The MSM 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 HT data.
When to use these modes: these compatibility modes should be used when legacy clients are present in the network. HP ProCurve recommends 802.11n/a as the typical operating mode for Radio 1. Both modes allow for all wireless clients to connect and they use protection to avoid causing interference.

### 802.11n/g

This mode is the same as 802.11n/b/g except that 802.11b clients are prevented from associating. The AP does not advertise 1, 2, 5.5 and 11 Mbps as supported rates in its beacons or Probe-Responses. The AP does not tell 802.11g clients to use protection, and this can cause collisions with any 802.11b clients present on the same channel.

When to use this mode: this mode should only be used in special cases where 802.11b clients are causing problems in the network.

### Channel width

802.11n allows for the ability to use the standard channel width of 20 MHz or a double width of 40 MHz. 40 MHz widths are achieved by using two adjacent channels to send data simultaneously. The advantage of using a 40 MHz channel is that the available bandwidth is doubled leading to much higher throughput for clients. The available options for the Channel Width setting on Radio 1 are:

- 20 MHz
- Auto 20/40 MHz

When 20 MHz is selected as the channel width, the channel usage is the same as in legacy mode. In 2.4 GHz, channels 1, 6 and 11 can be used without overlapping. In 5 GHz, each channel is separate, with no overlapping.

When Auto 20/40 MHz is selected, Radio 1 uses a 40 MHz channel width. However, both 20 and 40 MHz clients can associate. The channel selected on the radio page is the primary channel and the secondary (or extension) channel is located adjacent to it. The secondary channel is either above or below depending on which channel was selected as the primary. In the 5 GHz band, the channels are paired: 36 and 40 are always used together, 44 and 48 are always used together, etc. It works slightly differently in the 2.4 GHz band: there you choose whether the extension channel should be above or below the beacon.

Due to the small number of non-overlapping channels available, HP ProCurve recommends only using a 20 MHz channel width when operating in the 2.4 GHz band. When using the 5 GHz band, Auto 20/40 MHz should be used as the channel width.

### Guard interval

The Guard Interval can be set to either Long Guard Interval (LGI) or Short Guard Interval (SGI). Using SGI allows for slightly better throughput (~10% improvement). Regardless of this setting, the AP allows both LGI and SGI clients to associate simultaneously and uses the proper GI when sending to each client. The current chipset does not allow SGI to be used when the channel width is 20 MHz. So if the Channel Width is set to 20 MHz, the option to change the GI is removed. When the channel width is Auto 20/40 MHz, the GI should be set to Short to get the best throughput.
**Conducting a site survey**

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

Select **Wireless > Neighborhood** and then select **Repeat scan every** and set the desired interval. The AP scans at the specified interval to find all active APs. For example:

![Wireless neighborhood interface](image)

**Note**

If an AP is not broadcasting its name, the corresponding SSID column is empty.

**Scanning frequency**

Scanning frequency depends on how the radio is configured.

Scanning is performed automatically if you defined any of the following on the **Wireless > Radio(s)** configuration page:

- Operating mode is set to Monitor and, on this Wireless neighborhood page,
- Repeat scan every x seconds is enabled.
- Channel is set to Automatic.
- Automatic power control is enabled.
The scanning interval is set based on the automatic power control and channel selection intervals that are defined.

In the case of Monitor mode, scanning is continuous, switching channels each 200 ms. If none of these options is defined, you must set the scanning interval manually.

Scanning is temporarily disabled when a Network trace is active.

Each time a scan is repeated, it moves up one channel in the range supported by the current wireless mode. To view a list of all APs operating on all channels, you must perform multiple scans. Define Repeat scan every accordingly. The results of each scan are shown in the All APs list.

When operating in Monitor mode, the AP scans all channels and all wireless modes. Scanning is automatically performed on all active radios.

To identify unauthorized APs, the AP compares the MAC address of each discovered AP against the list of authorized APs—which you must define. If the discovered AP does not appear in the list, it is shown in the Unauthorized APs list.

**Identifying unauthorized APs**

Improperly configured wireless APs can seriously compromise the security of a corporate network. It is therefore important that these APs be identified as quickly as possible.

You can configure the wireless neighborhood feature to automatically list all unauthorized APs that are operating nearby.

To identify unauthorized APs, the network neighborhood feature compares the MAC address of each discovered AP against the list of authorized APs that you have defined as discussed below. If the discovered AP does not appear in the list, its name is shown in the **Unauthorized access points** list.

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

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

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

reformat the list to appear as follows

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

To define configuration settings for a radio, select **Wireless > Radio(s)**. This opens the Radio(s) configuration page (examples are shown from the MSM422 and MSM320):

MSM422:
Configuration parameters

Operating mode

Select the operating mode. Available options are:

- **Access point and Local mesh**: Standard operating mode provides support for all wireless functions.
- **Access point only**: Only provides AP functionality, local mesh links cannot be created.
- **Local mesh only**: Only provides local mesh functionality. Wireless client stations cannot connect.
Monitor: Puts the radio in promiscuous mode (no transmissions). Both AP and local mesh functionality are disabled. Use this option for continuous scanning across all channels in all wireless modes. See the results of the scans on the Wireless > Neighborhood page. This mode also enables 802.11 traffic to be traced when using the Tools > Network trace command.

Sensor: Enables RF sensor functionality on this radio. This feature requires that the appropriate license is installed on the AP.

Wireless mode
Select the transmission speed and frequency band:

- **802.11b**: 11 Mbps in the 2.4 GHz frequency band.
- **802.11b/g**: 11 and 54 Mbps in the 2.4 GHz frequency band.
- **802.11g**: 54 Mbps in the 2.4 GHz frequency band.
- **802.11a**: 54 Mbps in the 5 GHz frequency band.
- **802.11a Turbo**: Provides channel bonding in the 5 GHz frequency band for enhanced performance when creating local mesh links. (MSM410 and MSM422 radio 1 only)
- **802.11n (5 GHz)**: (pure 802.11n) Up to 300 Mbps in the 802.11n 5 GHz frequency band. Only 802.11n clients can associate with an AP in this mode.
- **802.11n (2.4 GHz)**: (pure 802.11n) Up to 300 Mbps in the 802.11n 2.4 GHz frequency band. Only 802.11n clients can associate with an AP in this mode.
- **802.11n/a**: (Compatibility mode.) In the 5 GHz frequency band, up to 270 Mbps for 802.11n and 54 Mbps for 802.11a.
- **802.11n/g**: (Compatibility mode.) In the 2.4 GHz frequency band, up to 270 Mbps for 802.11n and 54 Mbps for 802.11g. Only use this setting when support for 802.11g is necessary.
- **802.11n/b/g**: (Compatibility mode.) In the 2.4 GHz frequency band, up to 270 Mbps for 802.11n, 54 Mbps for 802.11g, and 11 Mbps for 802.11b. Only use this setting when support for 802.11b is necessary.

Note: In **802.11n (2.4)** and **802.11n (5 GHz)** modes, the MSM422 does not permit non-802.11n clients to associate. Also in this mode, the MSM422 does not use protection mechanisms (RTS/CTS or CTS-to-self) to enable legacy APs to operate on the same frequency. This can potentially cause problems with legacy (802.11a/b/g) APs operating on the same channel, but provides the best throughput for the MSM422 and its 802.11n clients. In **802.11n/a**, **802.11n/g**, and **802.11n/b/g** modes, the MSM422 permits both 802.11n and legacy clients (802.11a/b/g) to associate. The MSM422 uses protection mechanisms (RTS/CTS or CTS-to-self) when sending 802.11n data to prevent disruption to legacy (802.11a/b/g) clients associated on the same channel.
Wireless configuration
Radio configuration

Channel width

(MSM410 and MSM422 radio 1 only)
(Not available in Monitor or Sensor modes.)

Select the Channel width that will be used when Wireless mode includes some type of 802.11n. The Channel width only applies to 802.11n users.

20 MHz: Sets channel width to 20 MHz.

Auto 20/40 MHz: Under most conditions this can double throughput by bonding adjacent channels to form a 40 MHz channel.

Note
Although some 802.11 clients only support 20 MHz channels, they can still associate with an MSM422 configured for 20/40 MHz.

Channel extension

(MSM410 and MSM422 radio 1 only)
Appears only when configuring Channel width of 20/40 MHz for 802.11n in the 2.4 GHz band.

When Channel extension is set to Above the beacon (+1), the extra 20 MHz of bandwidth is taken from the channels higher than the selected channel. When Channel extension is set to Below the beacon (-1), the extra 20 MHz of bandwidth is taken from the channels lower than the selected channel. See also, Channel.

Channel

Select channel and 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.

Use the Automatic option to have the AP select the best available channel.

If setting the channel manually, for optimal performance when operating in 802.11b or 802.11g modes, select a channel that differs from other wireless APs operating in neighboring cells by at least 25 MHz. See the Wireless > Neighborhood page to view a list of APs currently operating in your area.

When operating in 802.11a mode, this is not a consideration as all channels are non-overlapping.

Note
The AP supports 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.

Note
Channels used by dynamic frequency selection (DFS) for radar avoidance, are identified with an asterisk “*”.
(MSM410 and MSM422 radio 1 only)

When **Wireless mode** is **802.11n (5 GHz)** or **802.11n/a** and **Channel width** is **Auto 20/40 MHz**, the channel numbers in the **Channel** list include either a “(1)” or “(-1)” to their right. A “(1)” indicates that the 40 MHz channel is formed from the indicated channel plus the next channel. A “-1” indicates that the 40 MHz channel is formed from the indicated channel plus the previous channel.

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

<table>
<thead>
<tr>
<th>Channel selected</th>
<th>Channels used</th>
</tr>
</thead>
<tbody>
<tr>
<td>36(1)</td>
<td>36+40</td>
</tr>
<tr>
<td>40(-1)</td>
<td>40+36</td>
</tr>
<tr>
<td>44(1)</td>
<td>44+48</td>
</tr>
<tr>
<td>48(-1)</td>
<td>48+44</td>
</tr>
</tbody>
</table>

**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.

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

<table>
<thead>
<tr>
<th>2.4 GHz channels</th>
<th>Channel width</th>
<th>Recommended non-overlapping channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 13</td>
<td>20 MHz</td>
<td>1, 7, 13</td>
</tr>
<tr>
<td>1 to 13</td>
<td>40 MHz</td>
<td>1, 13 (If both are used, there will be some performance degradation.)</td>
</tr>
<tr>
<td>1 to 11</td>
<td>20 MHz</td>
<td>1, 6, 11</td>
</tr>
<tr>
<td>1 to 11</td>
<td>40 MHz</td>
<td>1, 11 (If both are used, there will be some performance degradation.)</td>
</tr>
</tbody>
</table>

**Interval**

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.

**Time of day**

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. Set hours in the range 0 to 23.
Automatic channel exclusion list

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

On a per-radio basis, select the antenna(s) to use.

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

For a point-to-point local mesh link, it is recommended that you use an external directional antenna.

Note

Make sure that whatever external antennas are configured in the management tool are actually installed.

MSM422

For Antenna selection, select either Internal or External according to the following guidelines:

- The MSM422 features three internal antennas in the lower flap for Radio 1 (802.11n/a/b/g) (corresponding to external connectors A, B, and C) and two internal antennas in the upper flap for Radio 2 (801.11a/b/g) (corresponding to external connector D). If desired, install optional antennas via the external connectors.

- Radio 1 supports diversity on its internal and external antennas (connectors A, B, and C). In 802.11n modes, a special form of diversity called MIMO is used.

- For point-to-point local mesh links on Radio 1, install two directional antennas on connectors A and B. Installing a third directional antenna on connector C will increase performance only on the receive side.

- Radio 2 supports diversity via its two internal antennas but not when using an external antenna.

MSM410

Antenna selection is not available on the MSM410 since it has an integrated antenna.

MSM335

For Antenna selection, 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.
**MSM310, MSM310-R, and MSM320**

For **Antenna selection**, select **Diversity**, **Main**, or **Auxiliary** according to the following guidelines:

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

**MSM320-R**

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

**Antenna gain**

This parameter is only applicable when the radio is set to a 5 GHz DFS (Dynamic Frequency Selection) channel. DFS channels are identified with an asterisk "*". DFS prevents interference with radar systems and other devices that already occupy the 5 GHz band.

This parameter does NOT affect the output power of the radio. It adjusts the sensitivity of the AP radar detection algorithm.

This parameter must be set to the amount of gain specified for the antenna at the selected frequency (DFS channel).

**Guard interval**

**(MSM410 and MSM422 radio 1 only)**

Configurable with any 802.11n **Wireless mode** when **Channel width** is set to **Auto 20/40 MHz**.

The **Guard interval** can be reduced from its default of 800 nanoseconds to 400 to further enhance performance.

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

**Short:** Sets the guard interval to 400 nanoseconds which can improve the data rate in some environments. The MSM422 remains compatible with clients that only support a long Guard interval.

**Long:** Sets the guard interval to the standard of 800 nanoseconds. This allows for transmission path differences of up to 800 feet between data streams.
Spectralink VIEW
(Not available in Monitor mode)

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

Maximum range (ack timeout)
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.

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 access points
(Not available in Monitor mode)

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

■ You have more than one wireless AP installed in your location.

■ You are experiencing throughput problems.

In all other cases use the default setting of Large.

If you have installed multiple APs, reducing this AP's receiver sensitivity:

■ Helps to reduce the amount of cross-talk between the wireless stations to better support roaming clients

■ Increases the probability that client stations connect with the nearest AP

Available settings
■ Large: Accepts all clients.

■ Medium: Accepts clients with an RSSI greater than 15 dB.

■ Small: Accepts clients with an RSSI greater than 20 dB.

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

RTS threshold
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, you should adjust this value until the errors clear up. Start with a value of 1024 and then decrease to 512 until errors are reduced or eliminated. Note that using a small value for RTS threshold can affect throughput. Range is 128 to 1540.
If a packet is larger than the threshold, the AP will hold it and issue a request to send (RTS) message to the client station. Only when the client station replies with a clear to send (CTS) message will the AP send the packet. Packets smaller than the threshold are transmitted without this handshake.

**Beacon interval**

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**

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

**Transmit power control**

Use this parameter to set the transmission power of the wireless radio. The maximum supported power setting depends on the radio that is installed. The actual Maximum output power is shown at the bottom of this group box.

Select the Maximum available output power checkbox to specify that the AP use maximum available power. Alternatively, you can enter transmission power in dBm (using a range between 0 and 20, even though not all radios can support up to 20 dBm), or as a percentage of the maximum available power (using a range between 0 and 100).

Actual transmit power used may be less than the specified value. The AP determines the power to be used based on the settings you make for regulatory domain, wireless mode, and operating frequency.

Select Automatic power control to enable the AP to determine the optimal power setting within the defined limits. Also select the Interval at which power is adjusted. (Interval is relevant only if Automatic power control is selected.)

**Note**

If the Automatic power control option is enabled, the AP may dynamically change the Minimum rate configured in all VSC profiles. This is done to maintain a reasonable connection speed for client stations when the AP is operating in environments with strong interference.

This feature works best when the entire network uses only MSM APs, because third-party products will not adjust output power.

If co-channel interference is discovered, all neighboring APs will shrink their cell size to minimize the interference. The first step is to adjust the transmit power. If this fails, the next step is to increase transmit power to maximum, if possible, and to change the minimum data rate to a higher value. 802.11b will change from 1 Mbps to 2 Mbps, 802.11a/g will change from 6 Mbps up to 18 Mbps.
Note

- Not all interference can be eliminated, as a majority of clients will still transmit at maximum power.

- Some older wireless client cards may not support a data rate of 2 Mbps and therefore may not be able to associate when Automatic power control is enabled.
Network configuration

Contents

Ports configuration ...................................................................................................... 4-2
  Bridge port configuration .................................................................................... 4-3
  Port configuration ............................................................................................... 4-4
  Wireless port configuration ................................................................................. 4-5

VLAN support ........................................................................................................ 4-5
  Using a default VLAN ....................................................................................... 4-5
  Assigning traffic to a VLAN ............................................................................. 4-6
  VLAN bridging .................................................................................................... 4-7
  VLAN configuration ........................................................................................... 4-7

Bandwidth control ................................................................................................. 4-9

CDP ....................................................................................................................... 4-9

DNS ....................................................................................................................... 4-10
  DNS servers ..................................................................................................... 4-10
  DNS advanced settings .................................................................................... 4-10

IP routes ............................................................................................................... 4-11
  Configuration .................................................................................................... 4-11

IP QoS .................................................................................................................. 4-12
  Configuration .................................................................................................... 4-12
  Example ............................................................................................................. 4-13
Ports configuration

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

### Port configuration information

- **Status indicator**: Operational state of each port, as follows:
  - **Green**: Port is properly configured and ready to send and receive data.
  - **Red**: Port is not properly configured, is disabled, or is disconnected.

- **Jack**: Physical interface to which a logical port is assigned.

- **Name**: Identifier for the port. To configure a port, click its name.

- **IP address**: IP addresses assigned to the port. An address of **0.0.0.0** means that no address is assigned.

- **Mask**: Subnet mask for the IP address.

- **MAC address**: MAC address of the port.
Bridge port configuration

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

Assign IP address via

The bridge port supports the following addressing options:

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

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

Bridge spanning tree protocol

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

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

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

Priority

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

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

VLAN

VLAN ID

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

Note

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

Restrict default VLAN to management traffic only

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

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

Default VLAN and untagged port compatibility

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

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

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

Wireless port configuration

See Radio configuration on page 3-13.

VLAN support

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

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

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

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

The following AP features can be supported on a VLAN:
- Management tool access
- SNMP access
- SOAP access

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

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

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

### Assigning traffic to a VLAN

You can assign wireless traffic to a VLAN for an entire VSC or for individual users.

**Note**

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

### Assigning a VLAN to a VSC

You can map 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 virtual service community.

For information on how to assign a VLAN to a VSC, see *Egress VLAN on page 2-10*.

### Assigning VLANs to individual users

You can assign a VLAN to an individual user by setting attributes in the user’s RADIUS account. Restrictions are as follows:

- A user cannot be assigned to a VLAN that is set as the default VLAN on port 1 or port 2.
- A user can only be assigned to a predefined VLAN.
- Only applicable to 802.1X client stations. (Not applicable to MAC authentication.)

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

---

4-6
**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 these 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.

<table>
<thead>
<tr>
<th>VLAN name</th>
<th>VLAN ID</th>
<th>Assigned to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge_1</td>
<td>50</td>
<td>Port 1</td>
</tr>
<tr>
<td>Bridge_2</td>
<td>50</td>
<td>Port 2</td>
</tr>
<tr>
<td>Bridge_3</td>
<td>50</td>
<td>Local mesh 1</td>
</tr>
</tbody>
</table>

**VLAN configuration**

To view and configure VLAN definitions, select **Network > Ports** and look in the **VLAN configuration** box:

To add a VLAN, click **Add New VLAN**. The **Add/Edit VLAN** page opens.

Define VLAN settings according to the information provided in the following sections.
General

- **Port**: Select the physical interface with which the VLAN is associated.

- **VLAN ID**: Specify a VLAN identifier. If the VLAN is assigned to port 1 or port 2, you can also define a range of VLANs in the form X-Y, where X and Y can be 1 to 4094. For example, 50-60. This enables a single VLAN definition to accept traffic for one or more VLAN IDs, making it easy to manage a large number of contiguously assigned VLANs. You can define more than one VLAN range, but each range must be distinct.

---

**Note**

VLANS with ranges cannot be used for VSC egress mapping and cannot be assigned an IP address.

- **VLAN name**: Specify a name to identify the VLAN definition on the AP. This name has no operational significance.

**Assign IP address via**

Specify how the VLAN obtains an IP address, as follows:

- **DHCP client**: Available only on VLANs that are assigned to port 1 or port 2. The VLAN obtains its IP address from a DHCP server on the same VLAN. There is no support for obtaining a default gateway from the DHCP server.

- **Static**: Enables you to manually assign an IP address to the VLAN. If you select this option, you must specify a static **IP address**, **Mask**, and **Gateway**.

- **None**: Specifies that this VLAN has no IP address. Use this option when the VLAN ID is defined as a range.
Bandwidth control

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

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

- If outgoing traffic arrives at the defined 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 traffic that can be sent to client stations on each wireless port is 5000 kbps.

CDP

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

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

To enable CDP transmission, select **Network > CDP**.
DNS

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

DNS servers

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

DNS advanced settings

**DNS cache**

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

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

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

**DNS switch on server failure**

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

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

**DNS switch over**

This setting controls how the AP switches back to the primary DNS server after it has switched to the secondary DNS server because the primary was unavailable.
When enabled, the AP switches back to the primary server after it becomes available again.

When disabled, the AP switches back to the primary server only if the secondary server becomes unavailable.

IP routes

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

Configuration

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

Active routes

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

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

The following information is shown for each active route:

- **Interface**: The port through which traffic is routed. When you add a route, the AP automatically determines the interface to be used based on the Gateway address.

- **Destination**: Traffic addressed to this IP address is routed.

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

- **Gateway**: IP address of the gateway to which the AP forwards routed traffic (known as the next hop).

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

**IP QoS**

- **Metric**: Priority of a route. If two routes exist for a destination address, the AP chooses the one with the lower metric.

**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.

---

**IP QoS**

You configure IP quality of service (QoS) by creating IP QoS profiles that you can then associate with a VSC (*Quality of service (QoS) on page 2-18*) or with Local mesh profiles (*Quality of service on page 7-13*). You can configure as many as 32 IP QoS profiles on the AP. You can associate as many as 10 IP QoS profiles with each VSC.

**Configuration**

To view and configure IP QoS profiles, select **Network > IP QoS**. Initially, no profiles are defined.
To create an IP QoS profile select Add New Profile.

Settings

- **Profile name**: Specify a unique name to identify the profile.
- **Protocol**: Specify an IP protocol to use to classify traffic by specifying its Internet Assigned Numbers Authority (IANA) protocol number. Protocol numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select Other and specify the appropriate number manually. You can find IANA-assigned protocol numbers at http://www.iana.org.
- **Start port/End port**: Optionally specify the first and last port numbers in the range of ports to which this IP QoS profile applies. To specify a single port, specify the same port number for both Start port and End port. Port numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select Other and specify the appropriate number manually.
  
  **Note**: To accept traffic on all ports for a specified protocol, set Start port to Other and 0.

- **Priority**: Select the priority level that will be assigned to traffic that meets the criteria specified in this IP QoS profile.
  
  **Note**: It is strongly recommended that you reserve Very high priority for voice applications.

Example

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

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

1. Select Network > IP QoS, and then Add New Profile. The 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.

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.

12. Select Save.
Assign the profiles to a VSC

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

2. Set Priority mechanism to IP QoS.

3. In IP QoS profiles, Ctrl-click each profile you want to add.

4. Select Save.
Management

Contents

Management tool..........................................................................................................5-2
Management station..............................................................................................5-2
Starting the management tool..............................................................................5-2
Customizing management tool settings..............................................................5-3

SNMP .............................................................................................................................5-7
Configuring SNMP settings ..................................................................................5-8

SOAP ............................................................................................................................5-11
Configuring the SOAP server .............................................................................5-11

CLI ................................................................................................................................5-13
Configuring CLI support.....................................................................................5-13

System time.................................................................................................................5-14

LEDs.............................................................................................................................5-15

Country........................................................................................................................5-15
Management tool

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

Management station

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

- Have at least Microsoft Internet Explorer 7.0 or Mozilla Firefox 2.0).
- Be able to establish an IP connection with the AP.

Starting the management tool

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

```
https://AP_IP_address
```

By default, the address 192.168.1.1 is assigned to Port 1. For information on starting the management tool for the first time, see the relevant document as described in Getting started on page 1-12.
Customizing management tool settings

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

Administrative user authentication

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

- **Local account settings**: A single manager and operator account can be configured locally under Manager account and Operator account on this page.
**RADIUS server:** Using a RADIUS server enables you to have multiple accounts, each with a unique login name and password. Identify accounts using the vendor specific attribute *web-administrative-role*. See *Configuring administrative accounts on a RADIUS server on page 6-11*. To use a RADIUS server, you must define a RADIUS profile on the **Authentication > RADIUS profiles** page.

If both options are enabled, the local account is always checked first. If login is refused by the local account, then the RADIUS server checked.

**Authenticating administrative credentials using an external RADIUS server**

Configure RADIUS authentication as follows:

1. Define an account for the manager or operator on the RADIUS server. Specify the appropriate value for the vendor specific attribute *web-administrative-role*. See *Configuring administrative accounts on a RADIUS server on page 6-11*.

2. On the AP, create a RADIUS profile that will connect the AP to the RADIUS server. See *Configuring a RADIUS client profile on the AP on page 6-2*.

3. Under **Administrative user authentication**, enable RADIUS and select the RADIUS profile you created. In this example, the profile is called **Rad1**.

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

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

**Manager and Operator accounts**

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

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

Only one administrator 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) is already logged in. In every case, the manager's rights supersede those of an operator.
The following options can be used to prevent the management tool from being locked by an idle manager or operator:

- **Terminates the current manager session:** When enabled, an active manager or operator session will be terminated by the login of another manager. This prevents the management tool from being locked by an idle session until the **Account inactivity logout** timeout expires.

- **Is blocked until the current manager logs out:** When enabled, access to the management tool is blocked until an existing manager logs out or is automatically logged out due to an idle session.

  An operator session is always terminated if a manager logs in. An active operator session cannot block a manager from logging in.

- **Terminates the current operator session:** When enabled, an active operator’s session will be terminated by the login of another operator. This prevents the management tool from being locked by an idle session until the **Account inactivity logout** timeout expires.

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

  An operator session is always terminated if a manager logs in. An active operator session cannot block a manager from logging in.

- **Login control:** If login to the management tool fails five times in a row (bad username and/or password), login privileges are blocked for five minutes. Once five minutes expires, login privileges are once again enabled. However, if the next login attempt fails, privileges are again suspended for five minutes. This cycle continues until a valid login occurs. You can configure the number of failures and the timeout.

- **Account inactivity logout:** By default, if a connection to the management tool remains idle for more than ten minutes, the service controller automatically terminates the session. You can configure the timeout.

**Caution**

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

**Security policies**

The default security policy is the US Government **FIPS-140-2 guidelines** (Federal Information Processing Standard); however, **PCI DSS 1.2 guidelines** (Payment Card Industry Data Security Standard) are also supported. The selected security policy affects the login rules in the following ways:

**FIPS-140-2 guidelines**

- The only part of the FIPS-140-2 guidelines that is supported is that passwords must be at least six characters long and contain at least four different characters.
PCI DSS 1.2 guidelines

- Passwords must be a minimum of seven characters.
- Passwords must contain both numeric and alphabetic characters.
- Users must be locked out after not more than six failed attempts.
- The lockout duration must be at least thirty minutes or until a manager enables the user ID.
- A user must re-log in if a session has been idle for more than 15 minutes.

Security

The management tool is protected by the following security features:

- **Allowed IP address:** You can configure a list of subnets from which access to the management tool is permitted.
- **Active interfaces:** You can enable or disable access to the management tool for each of the following:
  - Port 1
  - Port 2 (on products that have a second Ethernet port)
  - Wireless port
  - VPN
  - VLAN/GRE/Mesh

**Note**

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

Web server

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

- **Secure web server port:** Specify a port number for the service controller to use to provide secure HTTPS access to the management tool. Default is 443. Before reaching the management tool login page, you must accept a security certificate. The default certificate provided with the AP will trigger a warning message on most browsers because it is self-signed. To remove this warning message, you must replace the default certificate. See About certificate warnings on page 6-17.

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

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

Web inactivity logout

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

SNMP

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

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

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

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

**Contact**
Contact information for the AP.

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

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

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

The AP supports the following MIB II notifications:
- coldStart
- linkUp
- linkDown
- authenticationFailure

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

**v1/v2c communities**

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

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

**v3 users**

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

**Username**
The SNMP v3 username.
Security
Security protocol defined for the user. Authentication type and encryption type are separated by a slash. For example, MD5/DES indicates MD5 authentication and DES encryption.

Access level
Type of access assigned to the user:

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

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

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

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

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

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

Security
Use these settings to control access to the SNMP interface.

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

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

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

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


Configuring the SOAP server

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

**Server settings**

**Secure HTTP (SSL/TLS)**

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

**Using client certificate**

When enabled, the use of a X.509 client certificate is mandatory for SOAP clients.
HTTP authentication
When enabled, access to the SOAP interface is available via HTTP with the specified username and password.

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

Security
Use these settings to control access to the SOAP interface.

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

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

Security considerations

- The SOAP server is configured for SSL/TLS mode, and the use of a X.509 client certificate is mandatory for SOAP clients.

- The SOAP server is configured to trust all client certificates signed by the default Colubris SOAP CA installed on the AP.

- Users should generate and install their own SOAP CA private key/public key certificate to protect their devices from unauthorized access. This is important because the default SOAP CA and a valid client certificate are provided as an example to all customers. (See Managing certificates on page 6-12.)
CLI

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

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

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

Configuring CLI support

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

Secure shell access

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

Connectivity and login credentials for SSH connections use the same settings as defined for management tool managers on the Management > Management tool page.

- SSH connections to the CLI can be made on any active interface. Support for each interface must be explicitly enabled under Management tool > Security.
- The login credentials for SSH connections are the same as those defined under Management tool > Manager account.

Note: SSH logins always use the local manager username and password, even if Administrative user authentication is set to use an external RADIUS server.

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

- OpenSSH
- Tectia
- SecureCRT
- Putty
System time

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

1. Set timezone & DST as appropriate.


3. Select set date & time (time servers) and then select the desired time server. Add other servers if desired. The AP contacts the first server in the list. If the server does not reply, the AP tries the next server and so on.

4. Select Set date & time (time servers) and then select the desired time server. Add other servers if desired. The AP contacts the first server in the list. If the server does not reply, the AP tries the next server and so on. By default, the list contains two ntp vendor zone pools that are reserved for HP ProCurve Networking devices. By using these pools, you will get better service and keep from overloading the standard ntp.org server. For more information visit: www.pool.ntp.org.

5. Select Save and verify that the date and time is updated accurately. A working Internet connection on Port 1 is required.

**Note**

If access to the Internet is not available to the AP, you can temporarily set the time manually with the Set date & time (manually) option. However, It is important to configure a reliable time server on the AP.
**LEDs**

Use this option to control operation of the status lights on the AP after the AP has successfully started up and become fully operational.

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

The following settings are available:

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

---

**Country**

The Country page is not available on APs delivered with a fixed country setting. The country for which the AP is configured to operate is displayed on the management tool home page.

Select Management > Country and select the desired country.

**Caution**

Do not change Country to a country other than the one in which the AP operates. Failing to heed this caution may violate the regulatory compliance of the AP and engage your responsibility/liability for operating in your country.
Security

Contents

Using a RADIUS server........................................................................................................6-2
  Configuring a RADIUS client profile on the AP..........................................................6-2
Configuring user accounts on a RADIUS server .................................................................6-5
Configuring administrative accounts on a RADIUS server........................................6-11
Colubris AV-Pair attribute values......................................................................................6-12

Managing certificates........................................................................................................6-12
  Trusted CA certificate store ..................................................................................6-13
  Certificate and private key store .............................................................................6-14
  Certificate usage .....................................................................................................6-16
  About certificate warnings ....................................................................................6-17
Using a 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validating manager login credentials.</td>
<td>Authenticating administrative credentials using an external RADIUS server on page 5-4.</td>
</tr>
<tr>
<td>Validating user login credentials for 802.1X or MAC authentication types.</td>
<td>Wireless protection on page 2-11. MAC-based authentication on page 2-14.</td>
</tr>
<tr>
<td>Storing custom configuration settings for each user.</td>
<td>Configuring user accounts on a RADIUS server on page 6-5.</td>
</tr>
<tr>
<td>Storing accounting information for each user.</td>
<td>Accounting support is enabled under Wireless protection on page 2-11 or MAC-based authentication on page 2-14.</td>
</tr>
</tbody>
</table>

Configuring a RADIUS client profile on the AP

The AP enables you to define a maximum of 16 RADIUS profiles. Each profile defines the settings for a RADIUS client connection. To support a client connection, you must create a client account on the RADIUS server. The settings for this account must match the profile settings you define on the 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.

Configuration procedure

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

3. Configure the profile settings according to the information provided below in *Configuration parameters on page 6-3.*

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 RADIUS server waits before access and accounting requests time out. If the server does not receive a reply within this interval, the AP switches between the primary and secondary RADIUS servers, if a secondary server is defined. A reply that is received after the retry interval expires is ignored.
Retry interval applies to access and accounting requests that are generated by the following:

- Manager access to the management tool
- MAC-based authentication of devices.

You can determine the maximum number of retries as follows:

- MAC-based authentication: Number of retries is infinite.
- 802.1X authentication: Retries are controlled by the 802.1X client software.

**Authentication method:** Select the default authentication method that the AP uses when exchanging authentication packets with the RADIUS server defined for this profile.

For 802.1X users, the authentication method is always determined by the 802.1X client software and is not controlled by this setting.

If traffic between the AP and the RADIUS server is not protected by a VPN, it is recommended that you use either EAP-MD5 or MSCHAP V2 (if supported by your RADIUS Server). PAP, MSCHAP V1, and CHAP are less secure protocols.

**NAS ID:** Specify the identifier for the network access server that you want to use for the AP. By default the serial number of the AP is used. The AP includes the NAS-ID attribute in all packets that it sends to the RADIUS server.

**Always try primary server first:** Enable this option if you want to force the AP to contact the primary server first.

Otherwise, the AP sends the first RADIUS access request to the last known RADIUS server that replied to any previous RADIUS access request. If the request times out, the next request is sent to the other RADIUS server if defined.

For example, assume that the primary RADIUS server was not reachable and that the secondary server responded to the last RADIUS access request. When a new authentication request is received, the AP sends the first RADIUS access request to the secondary RADIUS server.

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

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

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

**Primary/Secondary RADIUS server**

- **Server address:** Specify the IP address 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.
Configuring user accounts on a RADIUS server

This section presents all RADIUS attributes that are supported for user accounts.

Access Request attributes

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Admin login</th>
<th>802.1X</th>
<th>MAC</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acct-Session-Id</td>
<td></td>
<td>■</td>
<td>■</td>
<td>32-bit unsigned integer</td>
</tr>
<tr>
<td>Called-Station-Id</td>
<td></td>
<td>■</td>
<td>■</td>
<td>Called-Station-Id</td>
</tr>
<tr>
<td>Calling-Station-Id</td>
<td></td>
<td>■</td>
<td>■</td>
<td>Calling-Station-Id</td>
</tr>
<tr>
<td>EAP-Message</td>
<td>■</td>
<td>■</td>
<td></td>
<td>EAP-Message</td>
</tr>
<tr>
<td>Framed-MTU</td>
<td>■</td>
<td>■</td>
<td></td>
<td>Framed-MTU</td>
</tr>
<tr>
<td>Message-Authenticator</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>Message-Authenticator</td>
</tr>
<tr>
<td>NAS-Identifier</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>NAS-Identifier</td>
</tr>
<tr>
<td>NAS-Ip-Address</td>
<td></td>
<td>■</td>
<td>■</td>
<td>NAS-Ip-Address</td>
</tr>
<tr>
<td>NAS-Port</td>
<td></td>
<td>■</td>
<td>■</td>
<td>NAS-Port</td>
</tr>
<tr>
<td>NAS-Port-Type</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>NAS-Port-Type</td>
</tr>
<tr>
<td>Service-Type</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>Service-Type</td>
</tr>
<tr>
<td>State</td>
<td>■</td>
<td>■</td>
<td></td>
<td>State</td>
</tr>
<tr>
<td>User-Name</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>User-Name</td>
</tr>
<tr>
<td>User-Password</td>
<td></td>
<td>■</td>
<td></td>
<td>User-Password</td>
</tr>
<tr>
<td>Vendor-specific (Colubris)</td>
<td></td>
<td></td>
<td>■</td>
<td>Colubris-AVPair (SSID)</td>
</tr>
</tbody>
</table>

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 in the **Wireless protection** section of 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 in the **Wireless protection** section of 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. Present only when the authentication scheme on the **Security > RADIUS > Profile 1** page is set to PAP/SecurID. Or if MAC-authentication is enabled, the MAC address of the wireless client station.

- **EAP-Message** (string): As defined in RFC 2869. Only present when the authentication scheme on the **Security > RADIUS > Profile 1** page 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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Admin login</th>
<th>802.1X</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acct-Interim-Interval</td>
<td></td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Class</td>
<td></td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>EAP-Message</td>
<td>■</td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>Idle-Timeout</td>
<td></td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>MS-MPPE-Recv-Key</td>
<td></td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>MS-MPPE-Send-Key</td>
<td></td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>Session-Timeout</td>
<td>■</td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>Termination-Action</td>
<td></td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>Tunnel-Medium-Type</td>
<td></td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>Tunnel-Private-Group-ID</td>
<td></td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>Tunnel-Type</td>
<td></td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>Vendor-specific (Microsoft)</td>
<td></td>
<td>■</td>
<td>■</td>
</tr>
</tbody>
</table>

| 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, the 802.1X client is re-authenticated.

- **Termination-Action**: As defined by RFC 2865. If set to 1, customer traffic is not allowed during the 802.1X re-authentication.

- **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**
Access Reject RADIUS attributes are not supported.

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Admin login</th>
<th>802.1X</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-Message</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message-Authenticator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>802.1X</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acct-Input-Gigawords</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acct-Input-Octets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acct-Input-Packets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acct-Output-Gigawords</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acct-Output-Octets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>802.1X</td>
<td>MAC</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------</td>
<td>----</td>
</tr>
<tr>
<td>Acct-Output-Packets</td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>Acct-Session-Id</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Acct-Session-Time</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Acct-Status-Type</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Acct-Terminate-Cause</td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>Called-Station-Id</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Calling-Station-Id</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Class</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Framed-IP-Address</td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>Framed-MTU</td>
<td>■</td>
<td></td>
</tr>
<tr>
<td>NAS-Identifier</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>NAS-Port</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>NAS-Port-Type</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>User-Name</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Vendor-specific (Colubris)</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>SSID</td>
<td>■</td>
<td>■</td>
</tr>
</tbody>
</table>

**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 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. See Colubris AV-Pair attribute values on page 6-12.

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>
Colubris AV-Pair attribute values

Each Colubris AV-Pair value is specified using the following format: `<keyword>=<value>`

The following keywords and values are supported:

**Administrative role**

Use this AV-Pair value to identify the role of administrative accounts.

**Syntax**

```
web-administrative-role=role
```

Where:

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

---

**Managing certificates**

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

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

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

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

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

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

**ID**
A sequentially assigned number to help identify certificates with the same common name.

**Issued to**
Name of the certificate holder. Click the name to view the contents of the certificate.

**Current usage**
Lists the services that are currently using this certificate.

**CRL**
Indicates if a certificate revocation list is bound to the certificate. An X.509 certificate revocation list is a document produced by a certificate authority (CA) that provides a list of serial numbers of certificate that have been signed by the CA but that should be rejected.

**Delete**
Select to remove the certificate from the certificate store.

**Installing a new CA certificate**

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

2. Select **Install** to install a new CA certificate.

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

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

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

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).

Certificate and private key store

**Caution**

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

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

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

**ID**

A sequentially assigned number to help identify certificates with the same common name.
Issued to
Name of the certificate holder. Select the name to view the contents of the certificate.

Issued by
Name of the CA that issued the certificate.

Current usage
Lists the services that are currently using this certificate.

Delete
Select to remove the certificate from the certificate store.

Installing a new private key/public key certificate chain pair

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

The certificate you install must:

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

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

1. Specify the name of the certificate file or select **Browse** to choose one from a list. Certificates must be in PKCS #7 format.
2. Specify the **PKCS #12 password**.
3. Select **Install** to install the certificate.

Default installed private key/public key certificate chains
The wireless.colubris.com private key/public key certificate chain is installed by default. This certificate is used by the management tool and SOAP server.
When a web browser connects to the AP using SSL, the AP sends only its own SSL certificate to the browser. This means that if the certificate has been signed by an intermediate certificate authority, and if the web browser only knows about the root certificate authority that signed the public key certificate of the intermediate certificate authority, the web browser does not get the whole certificate chain it needs to validate the identity of the AP. Consequently, the web browser issues security warnings.

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

Consequently, the web browser issues security warnings.

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

An SNMP trap is sent to let you know when the AP SSL certificate is about to expire if you enable the Traps option on the Management > SNMP page and then click Configure traps and enable the Certificate about to expire trap option under Maintenance.

Certificate usage

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

<table>
<thead>
<tr>
<th>Service</th>
<th>Authenticate to peer using</th>
<th>Number of associated CAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Management Tool</td>
<td>wireless.columbia.com</td>
<td>0</td>
</tr>
<tr>
<td>SOAP Server</td>
<td>wireless.columbia.com</td>
<td>1</td>
</tr>
</tbody>
</table>

Service

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

Authenticate to peer using

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

Number of associated CAs

Number of CA certificates used by the service.
Changing the certificate assigned to a service

Select the service name to open the Certificate details page. For example, if you select Web management tool, you will see:

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

About certificate warnings

Access to the management tool must occur through a secure connection (SSL). Until a valid, trusted certificate is installed on the AP, certificate warnings will appear at login.

To continue to work with the management tool without installing a certificate, proceed as follows: At the security certificate prompt, in Microsoft Internet Explorer 7, select Continue to this website; in Firefox 2, select Accept this certificate temporarily for this session and OK.

To eliminate these warnings you can purchase a valid SSL certificate (from a source such as Verisign) that will work with the default configuration of your Web browser, and install it on the AP.
Local mesh

Contents

Key concepts.................................................................................................................7-2
Benefits...................................................................................................................7-2

Local mesh terminology ..............................................................................................7-2
Static local mesh links ..........................................................................................7-2
Dynamic local mesh links.....................................................................................7-3

Local mesh profiles......................................................................................................7-5
Configuring a local mesh profile .........................................................................7-6

Configuration considerations ...................................................................................7-12
Single radio vs. multiple radios..............................................................................7-12
Using 802.11a for local mesh..............................................................................7-13
Maximum range ...................................................................................................7-13

Quality of service .......................................................................................................7-13

Configuration summary.............................................................................................7-14

Sample local mesh deployments..............................................................................7-14
RF extension ........................................................................................................7-14
Building-to-building connections ........................................................................7-15
Dynamic networks ..............................................................................................7-15
Key concepts

Benefits

The local mesh feature replaces the need for Ethernet cabling between APs, enabling expanded Wi-Fi coverage through the use of wireless bridges to transport network traffic in hard-to-wire or outdoor areas.

Key local mesh features include:

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

- **Provides fall-back operation to recover from node failure**. In a properly designed implementation, redundant paths can be provided. If a node fails, the mesh will automatically reconfigure itself to maintain connectivity.

- **Maintains network integrity when using DFS channels**. In accordance with the 802.11h standard, dynamic frequency selection (DFS) detects the presence of certain radar devices on a channel and automatically switches the network node to another channel if such signals are detected. 802.11h is intended to resolve interference issues with military radar systems and medical devices.

**Note**

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

Local mesh terminology

Static local mesh links

The following illustration and table define terms that are used in this guide when discussing the static local mesh feature.
Local mesh
Local mesh terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>The AP that you are currently configuring to support a static link.</td>
</tr>
<tr>
<td>Remote</td>
<td>The AP that to which the static link will connect.</td>
</tr>
<tr>
<td>Link</td>
<td>The wireless connection between a local and remote AP.</td>
</tr>
</tbody>
</table>

Dynamic local mesh links

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>An AP that is configured to support local mesh connections.</td>
</tr>
<tr>
<td>Root node</td>
<td>The root node is configured in <strong>Master</strong> mode and provides access to the ground network.</td>
</tr>
<tr>
<td>Alternate master node</td>
<td>A node that is configured in <strong>Alternate master</strong> mode which enables it to make upstream and downstream connections.</td>
</tr>
<tr>
<td>Slave node</td>
<td>A node that is configured in <strong>Slave</strong> mode which enables it to make upstream connections only.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ground network</td>
<td>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.</td>
</tr>
<tr>
<td>Mesh</td>
<td>A series of nodes that connect to form a network. Each mesh is identified by a unique mesh ID.</td>
</tr>
<tr>
<td>Link</td>
<td>The wireless connection between two nodes.</td>
</tr>
<tr>
<td>Downstream link</td>
<td>A link that transports data away from the ground network.</td>
</tr>
<tr>
<td>Upstream link</td>
<td>A link that transports data towards the ground network.</td>
</tr>
<tr>
<td>Peer</td>
<td>Any two connected nodes are peers. In the diagram, AP 1 is the peer of both AP 2 and AP 3.</td>
</tr>
</tbody>
</table>

### 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:

\[
\text{Score} = \text{SNR} - (\text{Number of hops} \times \text{SNR cost of each hop})
\]

If a node loses its upstream link, it automatically discovers and connects to another available node.

### Operating channel

If a mesh operates on a dynamic frequency selection (DFS) channel, the master node selects the operating channel. If another node detects radar and switches channels, that node reports the channel switch to the master node, which initiates a channel switch for the nodes connected to it. This allows the local mesh to converge on a specific channel.
A node that uses a DFS channel and that loses connection with its master, scans channels to find a master on another channel, which can be a new master or the same master.

If the local mesh does not operate on a DFS channel, configure the radios in one of the following ways:

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

---

**Local mesh profiles**

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

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Upstream link</th>
<th>Downstream link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master</td>
<td>None.</td>
<td>Up to nine links with alternate master or slave nodes.</td>
</tr>
<tr>
<td>Alternate master</td>
<td>A single link to a master node or alternate master node.</td>
<td>Up to eight links with alternate master or slave nodes.</td>
</tr>
<tr>
<td>Slave</td>
<td>A single link to a master node or alternate master node.</td>
<td>None.</td>
</tr>
</tbody>
</table>

When a dynamic profile is active, the AP constantly scans and tries to establish links as defined by the profile.
To view or add profiles select **Wireless > Local mesh**.

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

**Configuring a local mesh profile**

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

**Enabled/Disabled**
Specify if the profile is enabled or disabled. The profile is only active when enabled.

**Name**
Name of the profile.

**Use**
Select the interface to use for this link.

**Speed**
*(Static links only)*
Sets the speed the link will operate at. For load balancing you may want to limit the speed of a link when connecting to multiple destinations.

**Security**
Enable this option to secure data transmitted on the wireless link. The APs on both sides of the wireless link must be configured with the same security options.

**WEP**
Enables WEP to secure traffic on the wireless link.
Specify the encryption key the node will use to encrypt/decrypt all data it sends and receives. The key is 128 bits long and must be specified as 26 hexadecimal digits.

**TKIP**
Enables TKIP encryption to secure traffic on the link.
The node uses the key you specify in the PSK field to generate the TKIP keys that encrypt the wireless data stream.
Specify a key that is between 8 and 64 ASCII characters in length. It is recommended that the key be at least 20 characters long, and be a mix of letters and numbers.

**AES/CCMP**
Enables AES with CCMP encryption to secure traffic on the link. This is the most secure method.
The node uses the key you specify in the PSK field to generate the keys that encrypt the wireless data stream.
Specify a key that is between 8 and 64 ASCII characters in length. It is recommended that the key be at least 20 characters long and be a mix of letters and numbers.

**Policy manager**
The policy manager controls global configuration settings that apply to all nodes that are part of the local mesh.
For proper operation you should configure only one node as the policy manager. Setting more than one node as the policy manager will prevent policies from being properly implemented.

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

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

**Enforce node limit**

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

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

**Addressing**

**Static**

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

**Remote MAC address**

MAC address of the radio on the remote AP on which the link will be established.

**Local MAC address**

MAC address of the radio on this AP on which the link will be established.

**Dynamic**

Use this option to create dynamic local mesh installations.

**Mode**

Three different roles can be assigned to a node: master, alternate master, or slave. The role assigned to a node, governs how the node will establish upstream or downstream links with its peers. The available configuration settings change depending on the role that is selected.
- **Master:** The master is the root node that provides the upstream connection to the *ground network* that the other nodes want to reach. The master will only create downstream links to alternate master or slave nodes.

![Dynamic interface](image)

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

![Dynamic interface](image)
**Alternate Master:** An alternate master node must first establish an upstream link with a master or alternate master node before it can establish downstream link with an alternate master or slave node.

**Mesh ID**
Unique number that identifies a series of nodes that can connect together to form a local mesh network.

**Minimum SNR**
*Alternate master or slave nodes*
This node will only connect with other nodes whose SNR is above this setting (in dB).

**SNR cost per hop**
*Alternate master or slave nodes*
This value is an estimate of the cost of a hop in terms of SNR. It indicates how much SNR a node is willing to sacrifice to connect to node one hop closer to the root node, because each hop has an impact on performance, especially when using a single radio.

**Allowed downtime**
The maximum time (in seconds) that a link can remain idle before the link actually gets deleted. When a slave (or alternate master) looses its link to its master, the discovery phase is re-initiated.

**Maximum links**
*Master or alternate master nodes only*
The maximum number of upstream and downstream links that this node can support.
**Initial discovery time**

*(Alternate master or slave nodes)*

Amount of time that will be taken to discover the best available master node. The goal of this setting is to delay discovery until all the nodes in the surrounding area have had time to startup, making the identification of the best master more accurate. If this period is too short, a slave may connect to the first master it finds, not necessarily the best.

**Maximum links**

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

**Promiscuous mode**

*(Alternate master or slave nodes)*

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

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

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

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

**Preserve master link across reboots**

*(Alternate master or slave nodes)*

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

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

Update mesh ID from server
(Master nodes only)

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

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

Restart Discovery
(Alternate master or slave nodes)

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

---

Configuration considerations

Single radio vs. multiple radios

Simultaneous AP and local mesh

A radio can be configured to simultaneously support wireless clients and the creation of one or more local meshes. Although this offers flexibility it does have several limitations as follows:

- It reduces overall throughput since the total available bandwidth is shared between the local meshes and wireless users.
- It limits you to using the same radio options for both wireless clients and local meshes.

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

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

Using 802.11a for local mesh

It is recommended that 802.11a is 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) band for other applications such as local mesh.
- 802.11a provides more channels and more non-overlapping channels than 802.11b/g.
- Assuming an optimal implementation, 802.11a supports up to 54 Mbps for data throughput, providing a fat pipe for traffic exchange.
- Keep in mind that there are limitations inherent in using 802.11a, most notably shorter reach when compared to 2.4 GHz-based technology. Even so, 802.11a is a good choice in general.

Maximum range

The Maximum range setting on the Wireless > Radio(s) page can be used to fine tune internal timeout settings to account for the distance that a local mesh link spans. For normal operation, the timeout is optimized for links of less than 1 km.

Note

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 serve local wireless users, 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.)

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 local mesh links.

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 bridge on queue 2 even if the QoS setting on the bridge is VSC-based Low (queue 4).
Configuration summary

- 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.
- Daisy-chaining of nodes dramatically reduces throughput (which is typically divided by two for each hop) especially when one or more of the following are true:
  - Nodes provide both upstream and downstream links on the same radio.
  - Nodes share a radio with AP functionality.

Sample local mesh deployments

RF extension

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

In this scenario, a wireless bridge is used to extend coverage of the wireless network. Both APs are equipped with omni-directional antennas, enabling them to deliver both AP capabilities and wireless bridging using local mesh capabilities.
Building-to-building connections

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

Dynamic networks

In this scenario, a service 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.
Local mesh
Sample local mesh deployments

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

Contents

Config file management........................................................................................................8-2
  Manual configuration file management........................................................................8-2
  Scheduled operations.....................................................................................................8-3

Software updates..............................................................................................................8-4
  Performing an immediate software update.................................................................8-5
  Performing a scheduled update....................................................................................8-5

Licenses.............................................................................................................................8-6
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, automatically, or with a tool like cURL. Select Maintenance > Config file management.

Manual configuration file management

The following options are available for manual configuration file management.

Backup configuration

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

Before you install new software, you should always back up your current configuration. Select Backup to start the process. You are prompted for the location in which to save the configuration file.

If you specify a Password, the configuration file is protected by encrypting sensitive fields (example, passwords, secrets, and certificates) with a key based on the password. See also Restore configuration below.

Note

Even without a password, the certificates are still encrypted but with a key that is identical on all devices.
The local username and password for the manager are not saved to the backup configuration file. If you upload a configuration file, the current username and password are not overwritten.

**Note**

**Reset configuration**

See *Resetting to factory defaults on page B-1*.

**Restore configuration**

The **Restore configuration** group box enables you to reload a previously saved backup configuration file.

This feature enables you to maintain several configuration files with different settings, which can be useful if you must frequently alter the configuration of the AP or if you are managing several APs from a central site.

Use the following steps to restore a saved configuration file.

1. Select **Maintenance > Config file management**. The **Config file management** page opens.

2. In the **Restore configuration** group box under **Manual restore**, select **Browse** to navigate to and select the configuration file that you want to restore.

3. If the configuration file is protected with a password (see *Backup configuration*) you must supply the correct password to restore the complete configuration. If you supply an invalid password, all settings are restored except the certificates.

4. To upload the selected file to the AP, select **Restore**.

The AP automatically restarts when the upload is complete.

**Scheduled operations**

The **Scheduled operations** group box enables you to schedule unattended backups or restorations of the AP configuration file. See also *Performing a scheduled update on page 8-5*.

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

1. Select **Maintenance > Config file management**. The **Config file management** page opens.

2. At lower right, select the **Scheduled operations** checkbox.

3. Under **Operation**, select **Backup** or **Restore**.

4. Under **Day of week**, select **Everyday**, or select a specific day of the week on which to perform the backup or restoration.
5. Under **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. Under **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

7. To confirm that the specified **URL** is correct, select **Validate**.

8. To commit the schedule that you have configured, select **Save**.

---

**Software updates**

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

- Before updating be sure to check for update issues in the Release Notes.
- Even though configuration settings are preserved during software updates, it is recommended that you backup your configuration settings before updating. See Manual configuration file management on page 8-2.
- At the end of the update process, the AP automatically restarts, causing all users to be disconnected. Once the AP resumes operation, all users must reconnect. To minimize network disruption, use the scheduled install option to have updates performed outside of peak usage hours.
- When using a service controller in conjunction with one or more autonomous APs, you must (1) always update the service controller before updating the APs, and (2) never load an earlier software version on the APs than is installed on the service controller.

Performing an immediate software update

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

Performing a scheduled update

The AP can automatically retrieve and install software from a local or remote web site identified by its URL.

To schedule software installation, follow this procedure:

1. Enable Scheduled install.
2. For Day of week select a specific day or Everyday and set Time of day.
3. For URL, specify an ftp or http address like this:
   - ftp://username:password@192.168.132.11/newfirmware.cim
4. Validate the URL.
5. To commit the schedule, select Save.
6. 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 current. If it is not, the download stops and the software is not updated at this time.
Licenses

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

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

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

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

Work with licenses as follows:

- To temporarily deactivate all licenses, select Deactivate. Later, select Activate to reactivate them.
- To remove all licenses, select Remove and then at the prompt, select OK.
  
  **Note:** Before removing licenses, be sure to first backup the license file to your hard drive, using the Backup button.

- To order a new feature license, provide all information in the License ordering information box to your vendor.
- To install a license file, Browse to the file and then select Install License.
- To backup all licenses into a single file, select Backup.
Factory reset considerations

After a factory reset, factory-installed licenses are automatically re-activated but user-installed licenses remain in a deactivated state until manually activated. This is done to ensure a true factory-default reset.

To activate all user-installed licenses, select the Activate button.
Regulatory information

Contents

Notice for U.S.A ................................................................. A-2
Notice for Canada ........................................................................ A-3
Notice for the European Community ........................................ A-3
Supported External Antennas .................................................. A-5
Notice for Brazil ......................................................................... A-6
Notice for Japan .......................................................................... A-6
Notice for Taiwan ....................................................................... A-6
Notice for Korea .................
Notice for U.S.A.

Manufacturer's FCC Declaration of Conformity Statement

Manufacturer: Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1185 USA
Phone: 650-857-1501

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

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

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

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

This device is restricted to indoor use when using the 5.15-5.25 GHz band (Channels 36, 40, 44 and 48).

Warning

Exposure to Radio Frequency Radiation

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

This device complies with the limits for a Class B digital device and conforms to Industry Canada standard ICES-003. Products that contain a radio transmitter comply with Industry Canada standard RSS210 and are labeled with an IC approval number.

Cet appareil numérique de la classe B est conforme à la norme ICES-003 de Industry Canada. La radio sans fil de ce dispositif est conforme à la certification RSS 210 de Industry Canada et est étiquetée avec un numéro d'approbation IC.

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

This device has been designed to operate with the antennas listed in this section, having a maximum gain of 5.6 dBi. Antennas not included in this list or having a gain greater that 5.6 dBi are strictly prohibited for use with this device. The required impedance is 50 ohms.

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

This device is restricted to indoor use when using the 5.15-5.25 GHz band (Channels 36, 40, 44 and 48).

Notice for the European Community

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

Countries of Operation & Conditions of Use

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

Note

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

- This device may be operated indoors or outdoors in all EU and EFTA countries using the 2.4 GHz band (Channels 1 - 13), except where noted below.

- In **France**, this device may use the entire 2400 - 2483.5 MHz band (Channels 1 through 13) for indoor applications. For outdoor use, only the 2400 - 2454 MHz frequency band (Channels 1 through 9) may be used. For the latest requirements, see http://www.art-telecom.fr.

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

**5 GHz Operation**

- This device requires the user or installer to properly enter the **current country of operation** in the 5 GHz Radio Configuration Window,

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

- This device employs a **radar detection feature** required for European Community and EFTA country operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community or EFTA country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.

- This device is restricted to **indoor** use when operated in EU and EFTA countries using the 5.15-5.35 GHz band (Channels 36, 40, 44, 48, 52, 56, 60 and 64). See the table below for the allowed 5 GHz channels in each band.

**Operation Using 5 GHz Channels in the European Community**

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

<table>
<thead>
<tr>
<th>Frequency Band (MHz)</th>
<th>Allowed Channels</th>
<th>Usage</th>
<th>Maximum EIRP (mW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5150 - 5250</td>
<td>36, 40, 44, 48</td>
<td>Indoor use only</td>
<td>200</td>
</tr>
<tr>
<td>5250 - 5350</td>
<td>52, 56, 60, 64</td>
<td>Indoor use only</td>
<td>200</td>
</tr>
</tbody>
</table>
## Regulatory information

### Frequency

<table>
<thead>
<tr>
<th>Frequency Band (MHz)</th>
<th>Allowed Channels</th>
<th>Usage</th>
<th>Maximum EIRP (mW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5470 - 5725</td>
<td>100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140</td>
<td>Indoor or outdoor use</td>
<td>1000</td>
</tr>
</tbody>
</table>

### Disposal of Waste Equipment by Users in Private Household in the European Union

This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

### Supported External Antennas

The following table lists the available antennas for the HP ProCurve Wireless Access Points covered by this guide.

<table>
<thead>
<tr>
<th>Product Number</th>
<th>Antenna Type</th>
<th>Antenna Band (GHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2.4</td>
</tr>
<tr>
<td>J9401A</td>
<td>Omni</td>
<td>2.5 dBi</td>
</tr>
<tr>
<td>N/A*</td>
<td>Omni</td>
<td>5.6 dBi</td>
</tr>
</tbody>
</table>

* This antenna is included with MSM310-R, MSM313-R and MSM323-R

**Caution**

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

All HP ProCurve 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 ProCurve 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.
Notice for Brazil
Aviso aos usuários no Brasil Este equipamento opera em caráter secundário, isto é, não tem direito à proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Notice for Japan

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。
1  この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
2  万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した後、下記連絡先にご連絡頂き、混信回避のための処置等（例えば、バーティションの設置など）についてご相談して下さい。
3  その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先：日本ヒューレット・パッカード株式会社  TEL：0120－014121

Notice for Taiwan

DGT LPD (Low Power Device) Statement

低功率電波輻射性電機管理辦法

第十四條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
第十七條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
Notice for Korea

(warning for wireless equipment)

당해 무선설비는 운용 중 전파혼선 가능성이 있음
# Resetting to factory defaults

## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>B-2</td>
</tr>
<tr>
<td>Using the reset button</td>
<td>B-2</td>
</tr>
<tr>
<td>Using the management tool</td>
<td>B-2</td>
</tr>
<tr>
<td>Factory defaulting ruggedized products</td>
<td>B-4</td>
</tr>
</tbody>
</table>
Introduction

To force an AP into its factory default state, follow the procedures in this section.

Caution

Resetting an AP to factory defaults deletes all configuration settings, resets the manager username and password to admin, enables the DHCP client on the LAN port(s). If no DHCP server assigns an address to the AP, its address defaults to 192.168.1.1.

Note

Some of the techniques provided in this appendix cause the AP to be forced back into its default controlled mode. If desired, after performing the factory reset, switch the AP back into autonomous mode as described in the product Quickstart.

Licenses are retained after a factory reset. See *Factory reset considerations on page 8-7*.

Using the reset button

Note

Not applicable to ruggedized APs.

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

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

Using the management tool

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

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

1. Select *Maintenance > Config file management*. 

---

B-2
2. Under **Reset configuration**, click **Reset**.

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

1. Select **Maintenance > System**.
2. Under **Factory reset**, click **Reset to Factory Default**.
Factory defaulting ruggedized products

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

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

You need the following additional items:

- The factory default script file. on the HP ProCurve manuals page at:  
  www.procurve.com/manuals, look under MSM310-R and MSM320-R Outdoor Access Points for Factory Default Scripts. 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 ProCurve support personnel for loading special software files.
To reset a ruggedized product to factory defaults, follow this procedure:

1. Disconnect any cable from the AP.

2. Disconnect power from the PoE injector.

3. Configure your computer LAN port with a static IP address of **192.168.1.2** and a subnet mask of **255.255.255.0**.

4. Use a Cat 5 Ethernet crossover cable to connect your computer LAN port directly to the PoE injector **Data In** port.

5. Connect a Cat 5 Ethernet cable from the PoE injector **Data and Power Out** port directly to the AP.

6. Open a command line session on the computer.

7. In the folder containing the script, specify the script name including its language identifier and the factory parameter like this:
   
   ```
   MSMRemote-en factory
   ```

   Press **Enter** to execute the script.

8. Power on the PoE injector. The script performs the reset and confirms success with a message like this:

   ```
   Your "R" product has been successfully factory reset!
   ```

9. Once the factory reset completes, perform the procedure found in the *Initial software configuration* section of the AP Quickstart.
Resetting to factory defaults
Factory defaulting ruggedized products