



ProCurve MSM317 Access Device

Installation and Getting Started Guide



Power over Ethernet

HP ProCurve MSM317 Access Device

Installation and Getting Started Guide

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

Publication Number

5992-5495

May 2009

Applicable Products

MSM317 Access Device (US: J9422A, WW: J9423A)

MSM710 Access Controller	J9328A
MSM710 Mobility Controller	J9325A
MSM730 Access Controller	J9329A
MSM730 Mobility Controller	J9326A
MSM750 Access Controller	J9330A
MSM750 Mobility Controller	J9327A
MSM760 Access Controller	J9421A
MSM760 Mobility Controller	J9420A
MSM765zl Mobility Controller	J9370A

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, 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 1-8](#).

Contents

1 Introduction

About this guide	1-2
Products covered.....	1-2
HP ProCurve Product Naming.....	1-2
Important terms.....	1-3
Conventions	1-4
Management tool	1-4
Warnings and cautions	1-5
Commands and program listings	1-5
Introducing the MSM317 Access Device	1-6
Key features.....	1-7
Safety information.....	1-8
Professional Installation Required	1-8
Servicing	1-8
HP ProCurve Networking support.....	1-9
Before contacting support.....	1-9
Getting started.....	1-9
Online documentation	1-9

2 Installation

Hardware overview	2-2
External interfaces and status lights.....	2-2
External interfaces	2-2
Status lights	2-3
Punch-down block wiring.....	2-5
Integrated switch.....	2-5
Reset button	2-6
Using the reset button.....	2-6
Power	2-6
Faceplate and trim panel.....	2-7
Installation	2-7

Removal	2-8
Radio and antennas	2-8
Installing the MSM317	2-9
Checking status after installation	2-9
Connecting cables to the MSM317	2-9
Additional configuration.....	2-9

3 Configuration

Important.....	3-2
Radio configuration.....	3-2
Switch port configuration.....	3-2
Provisioning the MSM317.....	3-3
Directly provisioning the MSM317	3-3
Connectivity page	3-5
Discovery page	3-6
Configuring the switch ports	3-7
Switch ports list page	3-7
Port configuration page	3-8
Port settings	3-9
Port name.....	3-9
Flow control	3-9
Power over Ethernet	3-9
Quality of service.....	3-9
Default traffic priority	3-10
Priority lookup	3-11
DiffServ (Differentiated Services)	3-11
Rate limiting	3-11
Ingress rate	3-12
Egress rate	3-12
MAC filter	3-12
To define a MAC address list.....	3-12
VLAN	3-14
Port type.....	3-14
VLAN ID	3-15
Quarantine VLAN	3-16
Allow dynamic VLAN assignment.....	3-16

VSC binding	3-18
Binding to an access-controlled VSC	3-19
Binding to a non-access-controlled VSC	3-26
Authentication	3-28
802.1X	3-29
MAC-based.....	3-29
RADIUS	3-29
Viewing status information	3-30
AP details	3-30
Wireless clients.....	3-31
Port statistics.....	3-31
Bridge port statistics	3-32

A Regulatory information

Notice for U.S.A.	A-2
Notice for Canada.....	A-3
Notice for the European Community.....	A-3
Disposal of Waste Equipment by Users in Private Household in the European Union	A-4
Notice for Brazil.....	A-4
Notice for Japan.....	A-5
Notice for Korea	A-5
Notice for Taiwan	A-5

Introduction

Contents

About this guide	1-2
Products covered.....	1-2
HP ProCurve Product Naming.....	1-2
Important terms.....	1-3
Conventions	1-4
Introducing the MSM317 Access Device	1-6
Key features.....	1-7
Safety information.....	1-8
Servicing	1-8
HP ProCurve Networking support.....	1-9
Getting started	1-9
Online documentation	1-9

About this guide

This guide explains how to install, configure, and operate the MSM317 Access Device using both its provisioning tool and the management tool of an MSM7xx Controller.

Products covered

The guide applies to the following products:

- MSM317 Access Device (J9422A) USA version
- MSM317 Access Device (J9423A) Worldwide version

This guide also provides information on configuring the MSMS317 with the following products:

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

HP ProCurve Product Naming

As of October 1st, 2008, Colubris Networks was acquired by HP ProCurve. HP ProCurve has begun integrating the Colubris product line into the HP ProCurve Networking product portfolio (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 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 product names are as follows:

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

Important terms

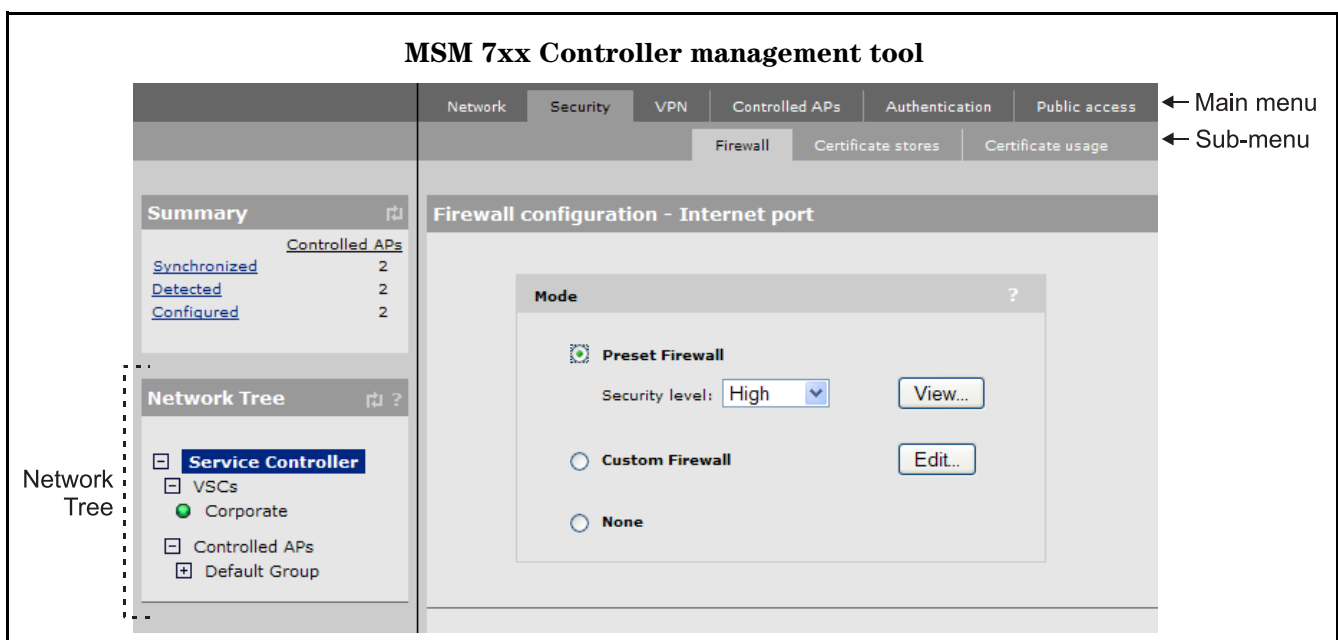
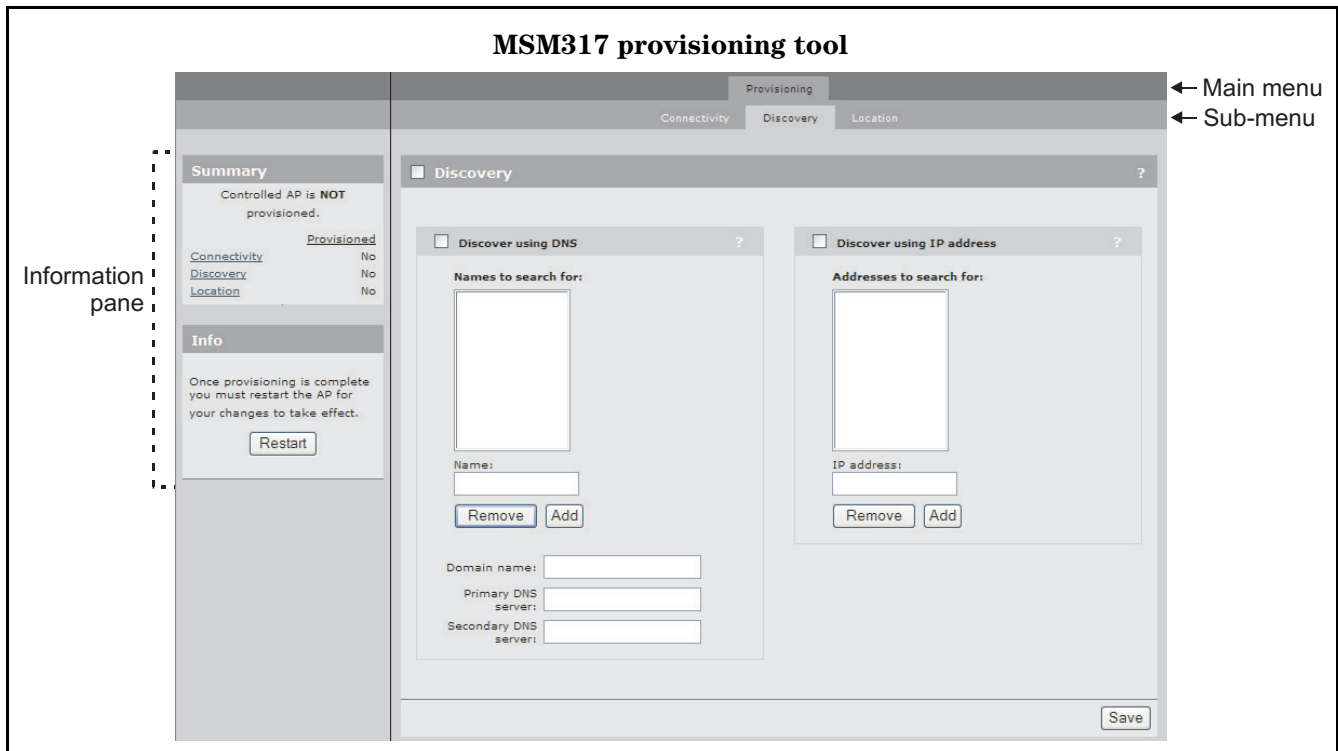
The following terms are used in this guide.

Term	Description
MSM AP	Refers to any HP ProCurve Networking MSM3xx or MSM4xx Access Point. Specific model references are used where appropriate.
MSM 7xx Controller	Refers to any HP ProCurve Networking MSM7xx Controller, including both Access Controller and Mobility Controller variants.

Conventions

Management tool

This guide uses specific syntax when directing you to interact with the provisioning tool interface on the MSM317 and the management tool interface on an MSM7xx Controller. Refer to the following images for identification of key user-interface elements and then the table below for sample directions:



Example instructions in this guide	What to do in the user interface
Select Service Controller >> Security > Firewall .	<i>On the MSM7xx</i> In the Network Tree select the Service Controller element, then on the main menu select Security , and then select Firewall on the sub-menu. All elements to the left of the double angle brackets >> are found in the Network Tree.
Select Service Controller > VSCs > [VSC name] >> Configuration .	<i>On the MSM7xx</i> Expand the Service Controller branch (click its + symbol), expand the VSCs branch, select a [VSC name], and select Configuration on the main menu.
Select Provisioning > Discovery .	<i>On the MSM317</i> On the main menu select Provisioning , and then select Discovery on the sub-menu.
For Password specify secret22 .	<i>On the MSM7xx and MSM317</i> In the Password field enter the text secret22 exactly as shown.

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:

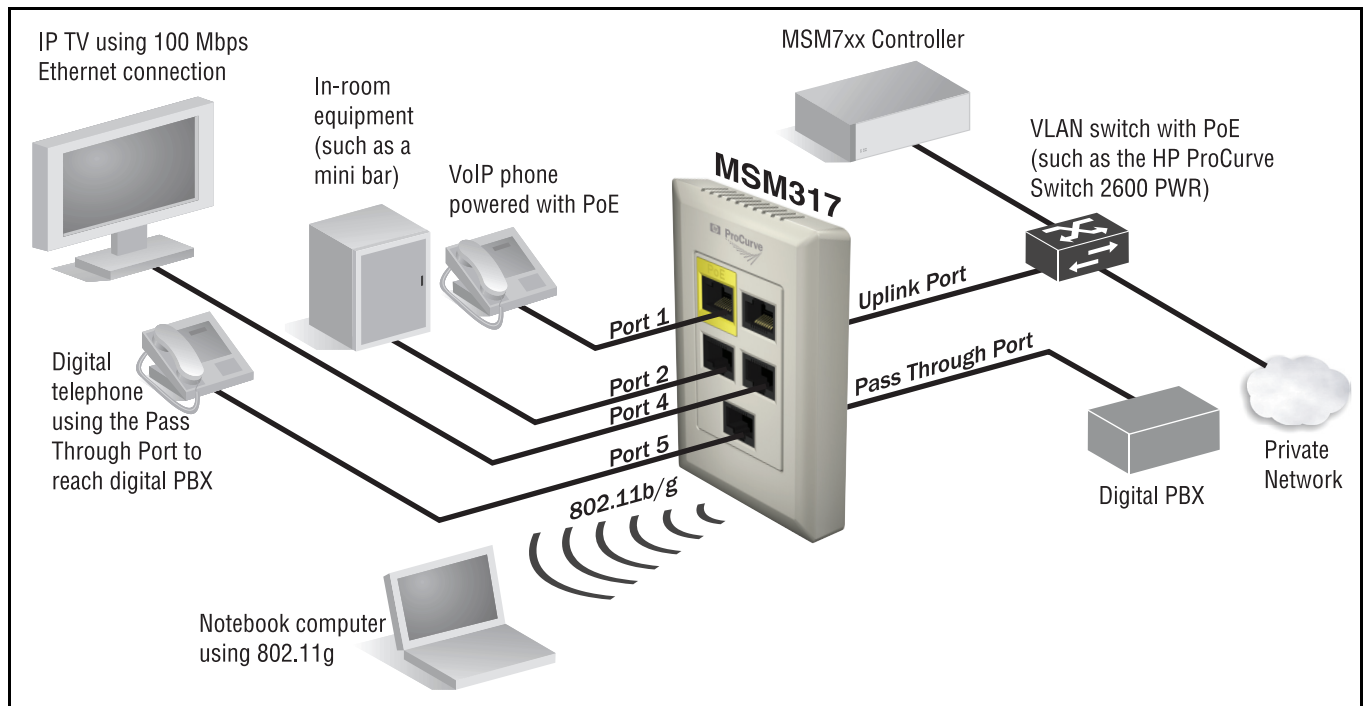
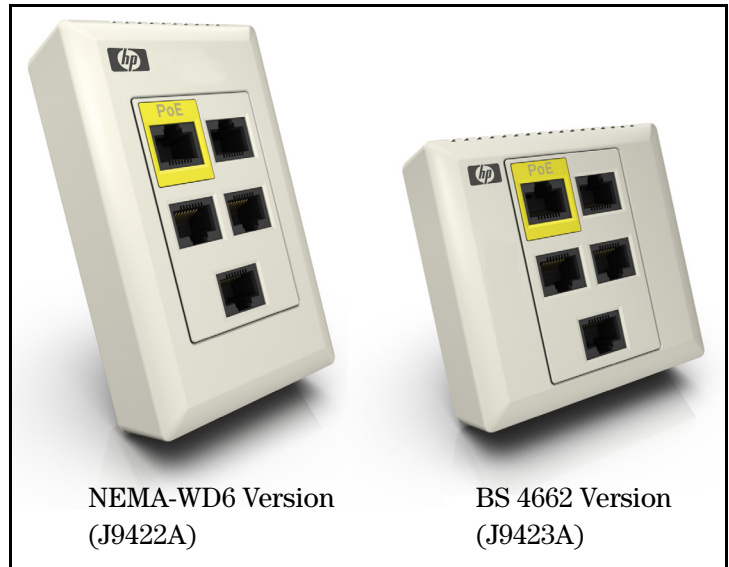
Example	Description
<code>use-access-list</code>	Command name. Specify it as shown.
<code>ip_address</code>	Items in italics are parameters for which you must supply a value.
<code>ssl-certificate=URL [%s]</code>	Items enclosed in square brackets are optional. You can either include them or not. Do not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

Introducing the MSM317 Access Device

The MSM317 Access Device revolutionizes the way wireless and wired IP-based services are delivered to hospitality and residential properties. The MSM317 integrates wired and wireless connectivity into a small unit that can be quickly and discretely installed in a standard wall box. The MSM317 provides four Ethernet ports, a 2.4GHz 802.11b/g wireless access point, and a pass-through RJ-45 connection for service and user connectivity. One of the Ethernet ports can be

configured as an IEEE 802.3af-compliant PoE (power over Ethernet) port to enable service devices such as IP telephones to be powered directly from the MSM317. The MSM317 requires a single powered cable drop to unlock its utility and, through the reduction in cabling, switch ports, and power-sourcing equipment, the MSM317 represents the best value for the delivery of next generation voice, data, and entertainment services.

A wide variety of devices can be connected to the MSM317.



Key features

802.11b/g radio

- Software-controllable output power from 10mW to 100mW EIRP.
- Frequency bands: 2.412 to 2.462 GHz, 2.412 to 2.484 GHz.
- Operating channels configurable based on country regulations.
- 802.11b at 1, 2, 5.5, 11 Mbps.
- 802.11g at 6, 9, 12, 18, 24, 36, 48, 54 Mbps.
- Two integrated 2.4GHz directional antennas with diversity.

Pass Through port

- Unmanaged RJ-45 connection for service and user connectivity.

A non-blocking managed Layer 2 switch, featuring:

- Support for four 10/100 Mbps ports with Auto-MDX support.
- Rate limiting.
- IEEE 802.1Q VLANs.
- Four priority queues mapped to IEEE 802.1p or DiffServ.
- IEEE 802.1X for device authentication.

PoE support:

- Obtains system power via PoE.
- IEEE 802.3af -compliant power forwarding through designated PoE port.

Safety information

Take note of the following safety information during installation of the MSM317:

Warning

Professional Installation Required

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

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

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

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

- Communications wires and cables which are installed in building locations shall be listed CM type in accordance with ANSI/NFPA 70, the National Electrical Code (NEC), in particular Section 800.179 (Communications Wires and Cables).
- Conductors and equipment shall be installed in accordance with ANSI/NFPA 70, the National Electrical Code (NEC), in particular Section 725.133 (Installation of Conductors and Equipment in Cables, Compartments, Cable Trays, Enclosures, Manholes, Outlet Boxes, Device Boxes, and Raceways for Class 2 and Class 3 Circuits).
- Wiring methods and materials shall be in accordance with NFPA 70, the National Electrical Code (NEC), in particular Section 725.130.
- The MSM317 does not have a power switch. It is powered-on when the Uplink port is plugged into a PoE power source.
- The MSM317 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.
- It is normal for the rear metal cover of the MSM317 to get hot during operation. The cover is a heat sink and is used to dissipate the heat generated by the MSM317.

Servicing

There are no user-serviceable parts inside HP ProCurve 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 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:

Collect this information	Where to find it
Product identification.	On the MSM317.
Software version.	On the MSM7xx Controller, select the MSM317 under Controlled APs in the Network Tree , then select Overview > AP details .
Network topology map, including the addresses assigned to all relevant devices.	Your network administrator.

Getting started

Get started with your MSM317 by following the directions in the next chapter of this guide.

Online documentation

For the latest documentation, visit the HP ProCurve Networking manuals Web page at: www.procurve.com/manuals.

Installation

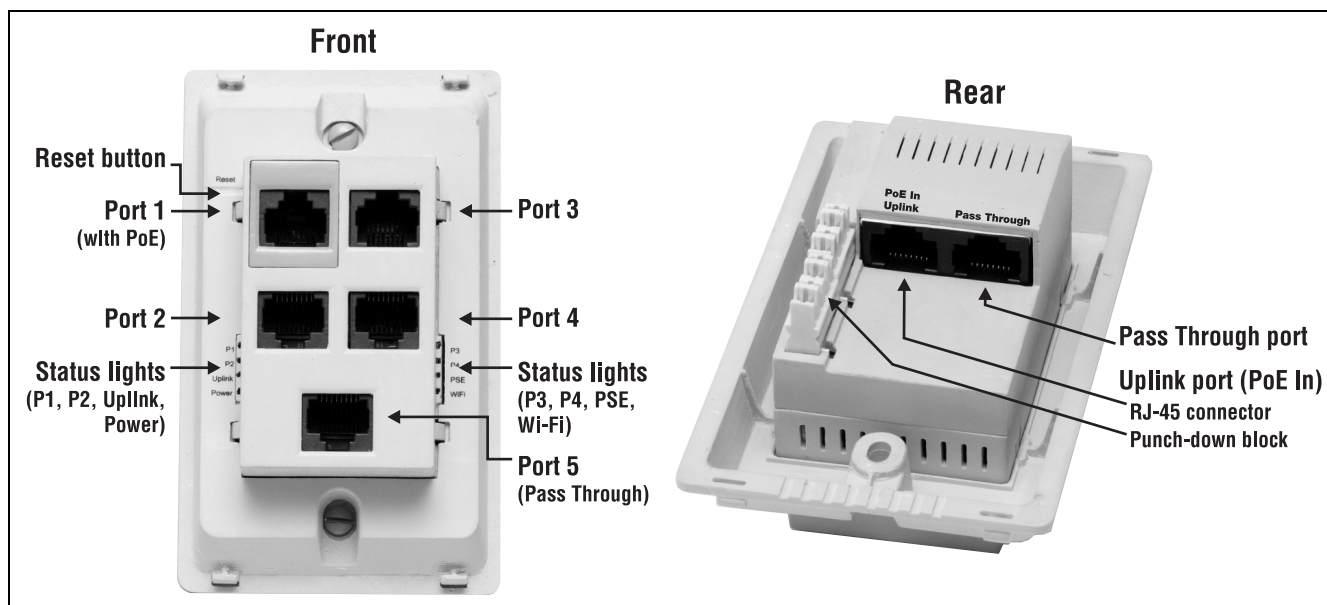
Contents

Hardware overview	2-2
External interfaces and status lights.....	2-2
Punch-down block wiring.....	2-5
Integrated switch.....	2-5
Reset button	2-6
Power	2-6
Faceplate and trim panel	2-7
Radio and antennas	2-8
Installing the MSM317	2-9
Checking status after installation.....	2-9
Connecting cables to the MSM317	2-9
Additional configuration.....	2-9

Hardware overview

This section provides detailed descriptions of the MSM317 hardware and its functionality.

External interfaces and status lights



External interfaces

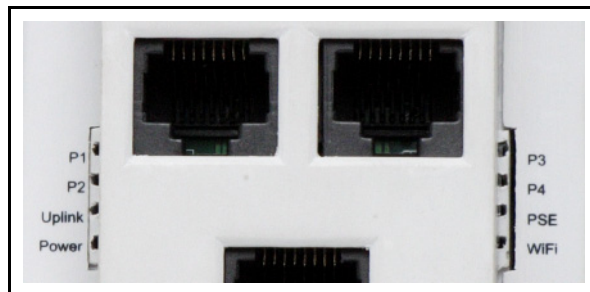
The MSM317 features the following external interfaces:

Front interfaces	Description
Port 1, 2, 3, 4	<ul style="list-style-type: none">■ Auto-sensing 10/100 Mbps Ethernet port with RJ-45 connector.■ Managed by the MSM317.■ Port 1 provides PoE for use by devices such as a VoIP phone.■ Any IP address that is assigned to the Uplink port is also assigned to Ports 1, 2, 3, and 4.
Port 5	<ul style="list-style-type: none">■ Port with RJ-45 connector.■ Not managed by the MSM317.■ Traffic on this port is hard-wired to the Pass Through port on the rear of the MSM317 and is not handled by the internal Ethernet switch.

Rear interfaces	Description
Uplink port (RJ-45 or punch-down block)	<ul style="list-style-type: none"> ■ Auto-sensing 10/100 Mbps Ethernet port with both an RJ-45 connector and punch-down block. Only one connector can be used at a time. ■ Managed by the MSM317. ■ Ports 1, 2, 3, and 4 are connected to the Uplink port by way of the internal Ethernet switch. ■ The Uplink port is used to connect the MSM317 to a network through which it can receive power from a PoE power source and establish a management tunnel with an MSM7xx Controller. Traffic from devices connected to Ports 1 to 4, and the wireless port, also reaches the network through the Uplink port. ■ By default, this port is configured as a DHCP client. If no DHCP server assigns an address to this port on startup, the IP address for the Uplink port defaults to 192.168.1.1. ■ The wireless port is bridged to the Uplink port (as a result it shares the same IP address).
Pass Through port	<ul style="list-style-type: none"> ■ Port with an RJ-45 connector. Hard-wired to port 5. ■ Not managed by the MSM317.

Status lights

The status lights are located to the left of Port 2 and to the right of Port 4. When the MSM317 is fully installed, the status lights are not visible because they are covered by the trim panel.



The status lights provide the following information while the MSM317 attempts to discover and establish a management tunnel with an MSM7xx Controller. See *Working with Controlled APs* in the *MSM7xx Controllers Management and Configuration Guide* for more information about the discovery process.

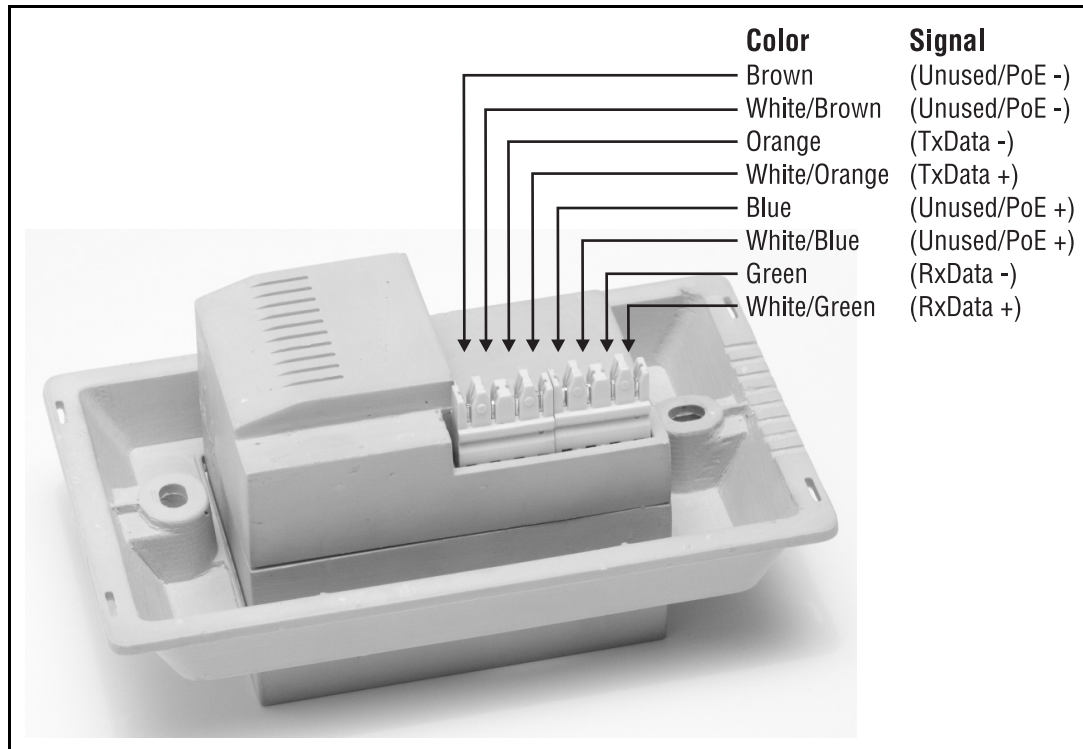
Behavior	Description
Power light blinks once every two seconds.	The MSM317 is starting up.
Power light blinks once per second.	The MSM317 is looking for an IP address, or building the list of VLANs on which to perform discovery. (To enable local provisioning, the provisioning tool Login page is available until discovery occurs. See Directly provisioning the MSM317 on page 3-3 .)
Power, Uplink, and P2 lights blink in sequence, from bottom to top.	The MSM317 has obtained an IP address and is attempting to discover an MSM7xx Controller.
Power light is On. Uplink and P2 lights blink alternately.	The MSM317 has found an MSM7xx Controller and is attempting to establish a management tunnel with it.
Power and Uplink lights blink alternately and quickly. P2 light is off.	The MSM317 has received a discovery reply from two or more MSM7xx Controllers with the same priority setting. The MSM317 is unable to connect with either controller until the priority conflict is resolved.
Power and Uplink lights blink slowly.	The MSM317 is attempting to establish an Ethernet connection on the Uplink port.

Once the discovery process is complete, and the MSM317 has established a secure management tunnel to a MSM7xx Controller, the lights provide the following information:

Light	State	Description
P1, P2, P3, P4, Uplink	On	Ethernet link is established.
	Off	Port is not connected.
	Blinking	Port is sending or receiving data.
PSE	On	PoE is enabled on Port 1.
	Off	PoE is disabled on Port 1.
Power	On	The MSM317 is powered on.
Wi-Fi	Blinking	The radio is transmitting or receiving data.

Punch-down block wiring

The punch-down block connector is wired as follows:



Caution

Do not connect both the Punch-down block and the Uplink port to a network. Only one connection can be used at a time.

To ensure good connections when using the punch-down block:

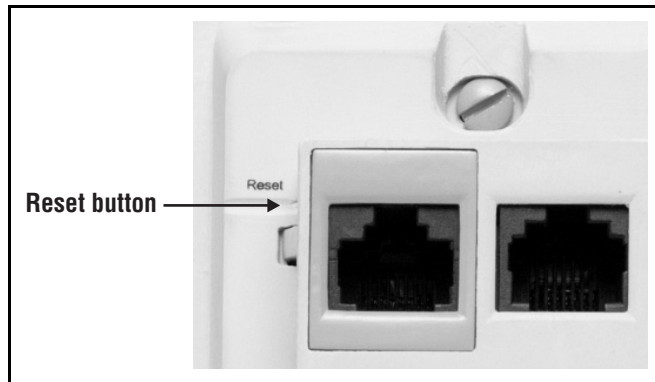
- Use solid conductor cables instead of stranded cables.
- Install cables into the individual Punch-down connectors using a 110-style tool.

Integrated switch

Ports 1 to 4 and the Uplink port are connected to the built-in Ethernet switch. Each port on the switch can be a member of a VLAN. These port-based VLANs let you reduce broadcast traffic and increase network security. Packets are forwarded only between ports that belong to the same VLAN. Thus, all ports carrying traffic for a particular subnet address should be configured on the same VLAN.

Reset button

The reset button is located to the left of Port 1. When the MSM317 is fully installed, the reset button is covered by the trim panel to prevent tampering.



Using the reset button

- **To restart the MSM317:** Use the end of a paper clip to press and quickly release the button. This is equivalent to power-cycling the MSM317.
- **To reset the MSM317 to factory defaults:** Use the end of a paper clip to press and hold the reset button until the status lights to the left of Port 2 (Power, Uplink, P2) blink three times, then release the button.

Note

Resetting the MSM317 to factory defaults deletes all configuration/provisioning settings and enables the DHCP client on the Uplink port. If no DHCP server assigns an address to the MSM317 on startup, the IP address for the Uplink port defaults to 192.168.1.1.

Power

The MSM317 receives power through the Uplink port (either via the RJ-45 connector or Punch-down block). The Ethernet connection to this port must be a standard 10/100 link delivered over category 5 (or better) structured cabling.

- The Uplink port must be connected to an 802.3af compliant power source.
- Port 1 supports an 802.3af Class 1 or Class 2 device (drawing a maximum of 6.49W). If a device requiring more power than defined by Class 2 is connected, power to the device is shut down.

Caution

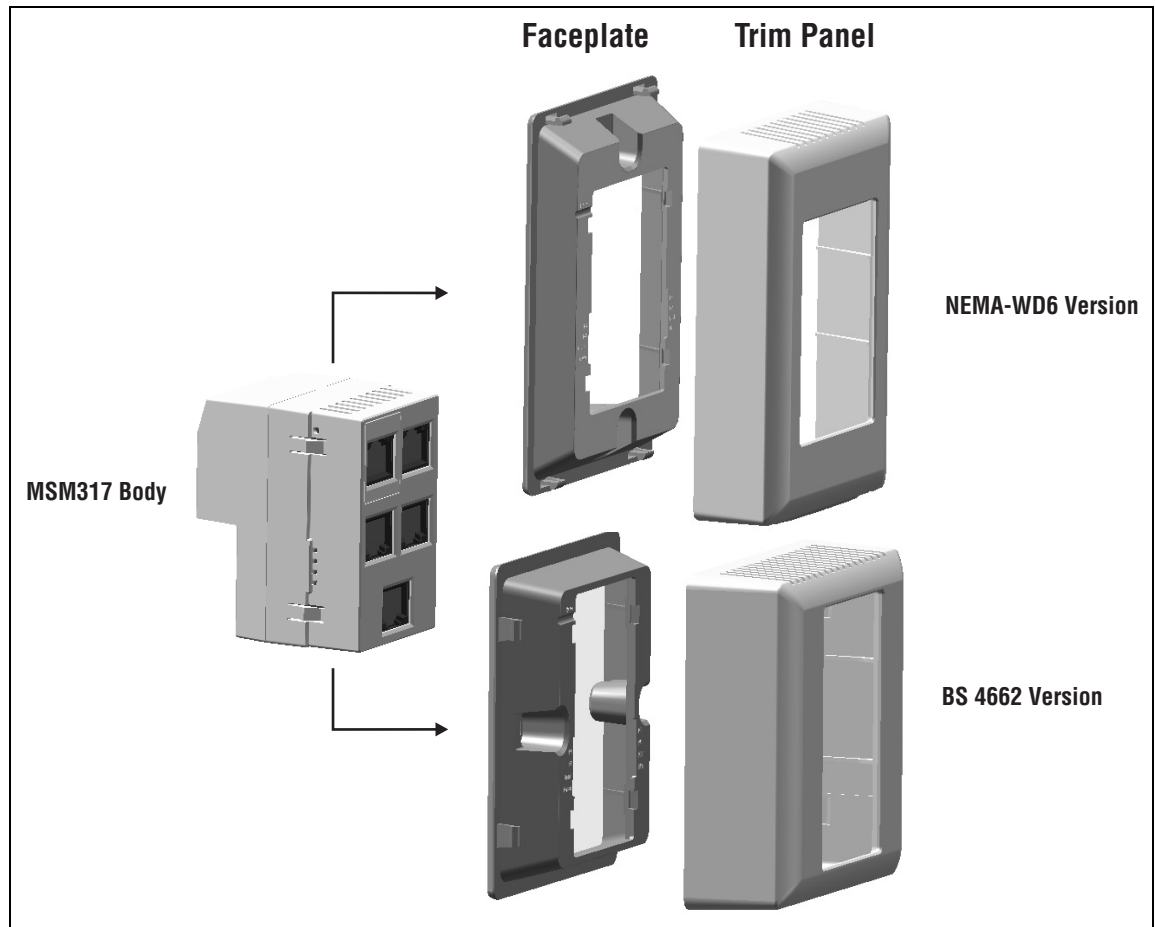
The MSM317 will be powered off by the PoE power source if there is an over-current situation.

The HP ProCurve Switch 2610 series features several models with PoE support that can be used in conjunction with the MSM317 to build a cost-effective wireless networking infrastructure.

Faceplate and trim panel

The MSM317 includes the following faceplates and trim panels:

- US faceplate and trim panel designed to fit a single-gang electrical outlet box (conforming to NEMA-WD6), with a minimum depth of 1.4 inches.
- International faceplate and trim panel designed to fit a single-gang electrical outlet box (conforming to BS 4662), with a minimum depth of 35mm.



Installation

Place the faceplate over the front of the MSM317 and press firmly to snap it into place. The trim panel snaps into place on top of the faceplate.

Removal

To remove the faceplate, slightly push in two tabs on one side of the MSM317 body with a small flat screwdriver. To remove the trim panel, pry off the trim panel with a small flat screwdriver.



Radio and antennas

The MSM317 contains a single 802.11b/g radio with integrated dual 2.4 GHz antennas supporting transmit/receive diversity. The radio can create a single wireless cell with power output in the range of 10mW to 100mW EIRP. Output power of the radio is software-controllable using the management tool on the MSM7xx Controller to which the MSM317 is connected.

The polar pattern for the antennas projects to the front of the MSM317 with minimum radiation to the rear. This permits two MSM317s to be installed back-to-back in adjacent rooms with reduced interference.

Installing the MSM317

Install the MSM317 as directed in the *MSM317 Access Device Installation Guide* provided with the unit and available online. The Installation Guide describes how to physically install a factory-default MSM317 in an electrical outlet box and make basic connections. For most installations, installing a factory-default MSM317 is sufficient, as the MSM317 will automatically discover and connect with an MSM7xx Controller after it is powered on. For routed network topologies however, provisioning of the MSM317 may be required before installation to ensure that the discovery process is successful. See [Provisioning the MSM317 on page 3-3](#).

Note

The MSM317 operates in *controlled mode* (autonomous mode is not supported). This means it must establish a network connection with an MSM7xx Controller before it can become fully operational. For more information, see *Working with controlled APs* in the *MSM7xx Controllers Management and Configuration Guide*.

Checking status after installation

During installation, the Uplink port must be connected to a network with a PoE power source and an MSM7xx Controller. If the network, PoE source, and MSM7xx Controller are all active, the status lights can be observed to verify that the MSM317 is operating correctly. See [Status lights on page 2-3](#).

Connecting cables to the MSM317

After installation is complete, connect equipment to the MSM317 as follows:

- Connect equipment that requires PoE to Port 1.
- Connect other equipment to Ports 2, 3, or 4.
- Connect equipment that will use the pass-through feature (such as a digital telephone) to Port 5.

Additional configuration

For detailed information on how to configure and manage the MSM317, see [Chapter 3: Configuration](#) in this guide and also *Working with controlled APs* in the *MSM7xx Controller Management and Configuration Guide*.

Configuration

Contents

Important.....	3-2
Radio configuration.....	3-2
Switch port configuration.....	3-2
Provisioning the MSM317.....	3-3
Directly provisioning the MSM317	3-3
Configuring the switch ports	3-7
Switch ports list page.....	3-7
Port configuration page	3-8
Port settings	3-9
Quality of service.....	3-9
Rate limiting	3-11
MAC filter	3-12
VLAN	3-14
VSC binding.....	3-18
Authentication	3-28
Viewing status information	3-30

Important

The MSM317 operates in controlled mode only. This means that except for locally provisioned settings (explained in [Directly provisioning the MSM317 on page 3-3](#)), the MSM317 is configured using the management tool on an MSM7xx Controller.

For a complete discussion on how to operate the MSM7xx management tool and manage controlled APs, see the *MSM7xx Controllers Management and Configuration Guide*.

Note

Until the MSM317 has established a management tunnel with an MSM7xx Controller, no user traffic is supported on Ports 1, 2, 3, 4, the Uplink port, and the wireless port. However, Port 5 and the Pass Through port are always fully operational.

Radio configuration

The MSM317 is part of the HP ProCurve MSM family of wireless networking products. As such, it shares many of the same wireless configuration options available on other MSM APs, and is configured in the same way when connected to an MSM7xx Controller. See the *MSM7xx Controllers Management and Configuration Guide* for radio configuration details.

Switch port configuration

The MSM317 switch ports provide unique capabilities that are not addressed in the *MSM7xx Controllers Management and Configuration Guide*. For details on switch port configuration, see [Configuring the switch ports on page 3-7](#).

Note

The MSM317 does not support STP (Spanning-Tree Protocol) on Ports 1 to 4.

Provisioning the MSM317

Provisioning is the means by which you change the factory default IP addressing method and controller discovery settings on the MSM317. These settings apply to the MSM317 Uplink port only.

Note

Provisioning settings are retained when the MSM317 is restarted or power cycled, but are removed when the MSM317 is reset to factory defaults.

Provisioning is generally not required when deploying the MSM317 in simple (unrouted layer 2) network topologies. However, it is required when the MSM317:

- does not have layer 2 connectivity to an MSM7xx Controller and it is not possible to control the DNS or DHCP server configuration. For example, when the MSM317 is on a different subnet than the MSM7xx Controller and routing is required to reach it.
- needs to be deployed with a static IP address assigned to the Uplink port.
- To accelerate the discovery process on networks with a large number of VLANs, or when many VLANs are connected to many service controllers.

For more information on how provisioning and discovery work, see *Working with Controlled APs* in the *MSM7xx Controllers Management and Configuration Guide*.

Provisioning can be done in two ways:

- **Use an MSM7xx Controller to provision the MSM317.** This method enables multiple MSM317s to be provisioned at the same time, with the same settings (does not support setting a static IP address, however). For complete details, see *Working with Controlled APs* in the *MSM7xx Controllers Management and Configuration Guide*.
- **Directly provision the MSM317:** In its factory default state, the MSM317 provides a provisioning menu with the same options that are available when using an MSM7xx Controller to provision the MSM317. If you want to assign a static IP to the MSM317, you must use this method. For complete details, see the next section.

Directly provisioning the MSM317

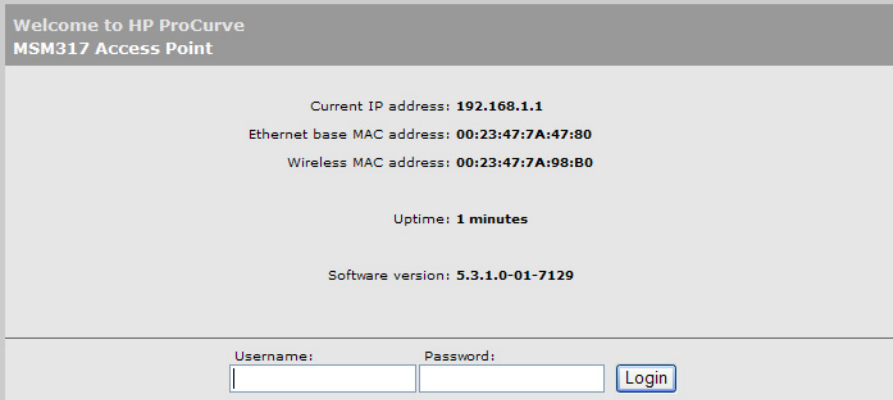
Note

- **Direct provisioning of the MSM317 can only be done when the MSM317 is in its factory-default state**, meaning that it has not been provisioned or has not discovered an MSM7xx Controller since last being reset to factory defaults. To force an MSM317 into its factory-default state, see [Reset button on page 2-6](#).
 - If you are provisioning multiple MSM317s, do not connect them all to the same PoE switch if no DHCP server is present, since they all default to the same IP address (192.168.1.1).
-

1. Configure your computer to use a static IP address in the range **192.168.1.2** to **192.168.1.254** with a subnet mask of **255.255.255.0**. Set the default gateway to **192.168.1.1**, and the DNS server to **192.168.1.1**.

For example, in Windows XP, use **Control Panel > Network Connections > Local Area Connection > Properties > Internet Protocol (TCP/IP) > Properties** to define these settings.

2. Use a standard Ethernet cable to connect your computer to Port 1, 2, 3, or 4 on the MSM317.
3. Power on the MSM317 by connecting an Ethernet cable from a PoE power source to the Uplink port on the rear of the MSM317.
4. Initially, the Power light will blink once every two seconds. Wait until it blinks once per second before proceeding to the next step.
5. Open a web browser (at least Microsoft Internet Explorer 7.0 or Mozilla Firefox 2.0) on your computer and specify the address: **https://192.168.1.1**.
6. At the security certificate prompt proceed as follows:
 - In Microsoft Internet Explorer 7, select **Continue to this website**.
 - In Firefox 2, select **Accept this certificate temporarily for this session** and **OK**.
7. On the **Login** page, specify **admin** for both **Username** and **Password** and then select **Login**.



Welcome to HP ProCurve
MSM317 Access Point

Current IP address: **192.168.1.1**
Ethernet base MAC address: **00:23:47:7A:47:80**
Wireless MAC address: **00:23:47:7A:98:B0**

Uptime: **1 minutes**

Software version: **5.3.1.0-01-7129**

Username: Password:

The provisioning tool home page opens.

You are in controlled mode. [Click here for more information.](#)

Welcome to HP ProCurve
MSM317 Access Point

Current IP address: **192.168.1.1**
Ethernet base MAC address: **00:23:47:7A:47:80**
Wireless MAC address: **00:23:47:7A:98:B0**

Uptime: **2 minutes**

Software version: **5.3.1.0-01-7129**
Hardware revision: **ZZ-ZZ-ZZZZ-ZZ:42**
Serial number: **TW8501X09A**
Operational mode: **Controlled**

[Provision...](#) [Restart](#)

8. Click **Provision** at the bottom of the home page and provision the MSM317 via settings on the **Connectivity** and **Discovery** pages. This is discussed in detail in the following sections.

Connectivity page

Enable provisioning of Connectivity here.

☒ **Connectivity**

Interface

☒ No VLAN
☐ VLAN ID:

Assign IP address via

☒ DHCP client
☐ Static

Static IP settings

IP address:
Mask:
Default gateway:

Use the Connectivity page to define addressing settings for the Uplink port.

Interface

Set the **VLAN ID** that will be used on the Uplink port for management traffic. This VLAN is only used for the discovery of an MSM7xx Controller and does not apply to user traffic sent on Ports 1 to 4 or the Uplink port. To apply a VLAN to a port for user traffic, see [VLAN on page 3-14](#).

Assign IP address via

Select how the MSM317 will obtain an IP address for the Uplink port.

- **DHCP client:** Enable this option to have the Uplink port act as a DHCP client and request an IP address from a DHCP server. The MSM317 sends DHCP requests on the specified VLAN if defined. If no VLAN is defined, the request is sent untagged.
- **Static:** Select this option to manually assign an IP address to the Uplink port.

Static IP settings

When you select **Static** for **Assign IP address via**, configure addressing settings as follows:

- **IP address:** Specify the IP address that you want to assign to the Uplink port.
- **Address mask:** Specify the appropriate subnet mask for the IP address you specified.
- **Default gateway:** Specify the IP address of the default gateway.

Discovery page

Enable provisioning of Discovery here.

☒ Discovery ?

☒ Discover using DNS ?

Names to search for:

controller-1
controller-2

Name:

Domain name:

Primary DNS server:

Secondary DNS server:

☐ Discover using IP address ?

Addresses to search for:

IP address:

Use the Discovery page to provision the method that the MSM317 uses to discover an MSM7xx Controller.

Discover using DNS

When this option is enabled, the MSM317 attempts to connect with an MSM7xx Controller using the host names in the order that they appear in the list. The MSM317 appends each host name with the specified **Domain name**. For example, the screen image above shows the MSM317 configured to search using the following names:

- controller-1.mydomain.com
- controller-2.mydomain.com

If you define a name that contains a dot, then the domain name is not appended. For example, if the name in the search list is **controller.yourdomain.com**, then no domain name is appended.

If the MSM317 is operating as a DHCP client, the DHCP server will generally return a domain name when it assigns an IP address to the MSM317. If you leave the **Domain name** field on this page blank, then the DHCP-assigned domain name is appended to the specified names instead.

Discover using IP address

When this option is enabled the MSM317 attempts to discover an MSM7xx Controller using the IP addresses in the order that they appear in this list.

Configuring the switch ports

This section explains how to configure the switch ports using the management tool on an MSM7xx Controller. This section assumes that you are familiar with the operation of the MSM7xx management tool. If not, see the *MSM7xx Controllers Management and Configuration Guide*.

Switch ports list page

This page lists all supported ports on the switch, indicates if the ports are enabled, and lists their VLAN number (if assigned). To define settings for a port, click the port name in the table.

Switch ports <input checked="" type="checkbox"/> Inherited ?			
Port	Name	Enabled	VLAN
1	Switch port 1	Yes	-
2	Switch port 2	Yes	-
3	Switch port 3	Yes	-
4	Switch port 4	Yes	-

To reach this page on the MSM7xx Controller do the following:

1. In the **Network tree** select **Service Controller**, then select **Controlled APs**.
2. In the right pane select **Configuration**, then select **Switch ports**.

Port configuration page

Ports 1 to 4 each have their own configuration page. The following screen shows the configuration page for Port 1. Configuration settings for the other ports are identical, except for the **Power over Ethernet** option which is only available on Port 1. To configure a port, select its name in the list.

Enable/disable the port here. (Available on Port 1 only.)

☒ Port 1

Port settings

Port name: Switch port 1

☒ Flow control

☐ Power over Ethernet

Quality of service

Default traffic priority: Normal

☐ Priority lookup: 802.1p + DSCP

Rate limiting

☐ Ingress rate: 128K bps

Traffic: All

☐ Egress rate: 128K bps

Traffic: All

☐ MAC filter

Available MAC lists:

Allow port access using these MAC lists:

VLAN

Port type: Untagged

☐ VLAN ID: 1

☐ Quarantine VLAN: 1

☐ Allow dynamic VLAN assignment

☐ VSC binding

VSC: HP ProCurve

Authentication

☐ 802.1X

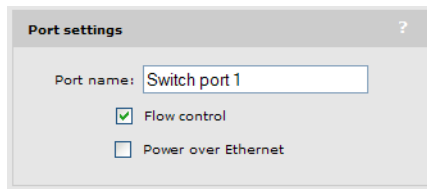
☐ MAC-based

RADIUS: <No RADIUS defined>

Cancel Save

Each configuration option on this page is discussed in detail in the sections that follow.

Port settings



Port name

Friendly name assigned to the port.

Flow control

When this option is enabled, the MSM317 uses Ethernet flow control when exchanging traffic with a connected device.

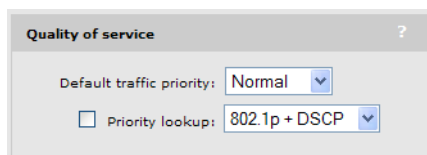
If you are using the **Rate limiting** option to limit ingress traffic you should enable flow control. This will ensure that a client device does not send traffic in excess of the ingress limit (providing that the client device supports flow control). Excess traffic is dropped when the **Rate limiting** option is enabled.

Power over Ethernet

(Only available on Port 1)

Enables power forwarding on Port 1 allowing a PoE device to be powered when connected to this port. See [Power on page 2-6](#).

Quality of service



The quality of service (QoS) feature provides a number of different mechanisms to prioritize traffic from the switch ports when it is forwarded on the Uplink port. This is useful when the MSM317 handles traffic from multiple devices that have different data flow requirements.

Four egress traffic queues are defined on the Uplink port. In order of priority, the queues are:

Queue	Priority setting
1	Very-high
2	High
3	Normal
4	Low

Note

These queues are also used by traffic from the wireless network. To see how QoS is implemented for wireless traffic, see the *MSM7xx Controllers Management and Configuration* guide.

Default traffic priority

Use this option to specify the priority (queue) that the MSM317 will assign to traffic in certain cases. The following tables summarize how traffic is classified.

If the *Priority lookup* option is disabled:

QoS marking on incoming traffic	Queue to which traffic is assigned	Is a VLAN defined on the port?	QoS marking applied to traffic exiting the Uplink port
DiffServ	Queue defined by the Default traffic priority setting.	Yes	DiffServ marking is preserved plus corresponding 802.1p marking added.
		No	DiffServ marking is preserved.
802.1p		Yes	802.1p marking is replaced by Default traffic priority.
		No	802.1p marking is preserved.
No QoS marking		Yes	Remarked as 802.1p based on Default traffic priority setting.
		No	No QoS marking.

If the *Priority lookup* option is enabled:

QoS marking on incoming traffic	Queue to which traffic is assigned	Is a VLAN defined on the port?	QoS marking on traffic exiting the Uplink port
No QoS marking or a marking that does not match the configured Priority lookup.	Queue defined by the Default traffic priority setting.	Yes	Remarked as 802.1p based on the Default traffic priority setting.
		No	Original QoS marking is preserved.
802.1p	Queue defined by the 802.1p Priority lookup.	Yes	802.1p marking is preserved.
		No	Unmarked. 802.1p marking is removed.
DiffServ	Queue defined by the DiffServ Priority lookup.	Yes	DiffServ marking is preserved plus corresponding 802.1p marking is added.
		No	DiffServ marking is preserved.
802.1p + DiffServ	Queue defined by the 802.1p Priority lookup.	Yes	Both 802.1p and DiffServ markings are preserved.
		No	DiffServ marking is preserved.

Priority lookup

Enable this option to classify ingress traffic based on 802.1p, DiffServ, or both.

802.1p

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

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

DiffServ (Differentiated Services)

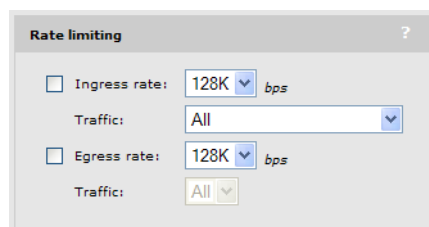
This mechanism classifies traffic based on the value of the Differentiated Services (DS) codepoint field in IPv4 and IPv6 packet headers (as defined in RFC2474). The codepoint is composed of the six most significant bits of the DS field.

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

802.1p + DiffServ

When this option is selected, both methods are used with 802.1p taking priority.

Rate limiting



The screenshot shows a 'Rate limiting' configuration window. It contains two sections: 'Ingress rate' and 'Egress rate'. Each section has a checkbox, a text input field with a dropdown arrow, and a unit 'bps'. The 'Ingress rate' checkbox is checked, and its value is '128K'. The 'Egress rate' checkbox is also checked, and its value is '128K'. Below each rate setting is a 'Traffic:' label followed by a dropdown menu. Both dropdown menus are set to 'All'.

This option lets you control the speed at which traffic can be sent/received on the port.

Ingress rate

Set the maximum rate at which this port will accept ingress traffic. Traffic in excess of the set rate is dropped. When using this option you should enable **Flow control**. This will ensure that a client device does not send traffic in excess of the ingress limit. (Providing that the client device supports flow control.)

Traffic

Select the type of traffic to which rate limiting applies: **Broadcast**, **Broadcast and multicast**, or **All** (broadcast, multicast, and unicast).

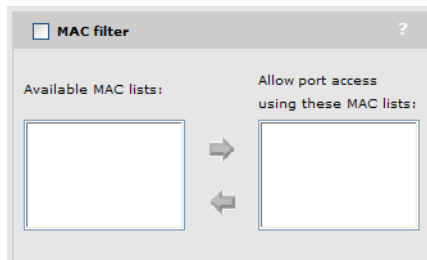
Egress rate

Set the maximum rate at which this port will send traffic. This rate applies to all outgoing traffic (broadcast, multicast, and unicast). Traffic in excess of the set rate is delayed.

Traffic

Indicates the type of traffic to which egress rate limiting applies. It is set to **All** (broadcast, multicast, and unicast), and cannot be changed.

MAC filter



This option lets you control port access based on client station MAC addresses. Addresses are checked against one or more lists stored on the MSM7xx Controller. If the MAC address of a connected device appears in any selected list, then the device is permitted to send and receive traffic on the port.

To define a MAC address list

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

To configure a new MAC address list, do the following:

1. Open the management tool on the MSM7xx Controller.
2. In the **Network tree** select **Service Controller**.
3. In the right pane select **Authentication**, then select **MAC lists**.

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

The screenshot shows the 'Add/Edit MAC list' configuration window. It has a title bar with the text 'Add/Edit MAC list'. Inside the window, there are two main sections. The first section, labeled 'Global', contains a 'Name:' label followed by an empty text input field. The second section, labeled 'MAC list', contains two input fields: 'MAC address:' and 'Mask:', each followed by an empty text box. To the right of the 'Mask:' input field is an 'Add' button. Below these input fields is a large, empty rectangular list box. At the bottom of the 'MAC list' section is a button labeled 'Remove Selected Entry'. At the very bottom of the window, there are two buttons: 'Cancel' on the left and 'Save' on the right.

5. Under **Global**, specify a name to identify the MAC address list.

6. Under **MAC list**, specify the MAC address and mask that you want to match, then select **Add**. For example:

- The following definition matches a single MAC address:

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

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

By changing the last digit of the mask, the definition now matches a range of MAC addresses from **00:03:52:07:2B:40** to **00:03:52:07:2B:4F**:

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

Mask = FF:FF:FF:FF:FF:F0

- The following definition matches all the devices with the mac prefix (OUI) of **00:03:52**:

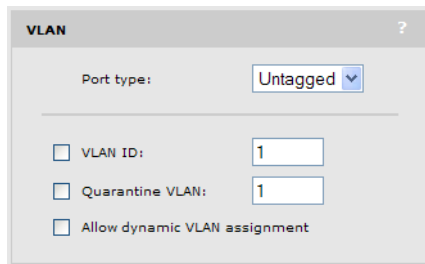
MAC address = 00:03:52:00:00:00

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

7. Repeat step 6 until you have defined all needed entries.

8. Select **Save**.

VLAN



This option lets you define a VLAN on the port.

Port type

The port can be configured as tagged or untagged. This affects how traffic is sent and received on the port only. It does not determine if traffic is tagged or untagged when sent on the Uplink port. Possible settings and their effects are as follows:

Port type	Incoming traffic (client device to MSM317)	Outgoing traffic (MSM317 to client device)
Untagged	Only untagged traffic is accepted.	All outgoing traffic on the port is sent untagged.
Tagged	Only traffic tagged with the same VLAN ID configured on the port is accepted.	Outgoing traffic on the port is automatically tagged with the VLAN ID configured on the port.

For example:

VLAN settings	Incoming traffic	Outgoing traffic	Uplink port
Port type = Untagged VLAN ID = 20	Only untagged traffic is accepted.	Outgoing traffic on the port is untagged.	Traffic is sent/received on VLAN 20.
Port type = Tagged VLAN ID = 20	Only traffic tagged with VLAN 20 is accepted.	Outgoing traffic on the port is tagged with VLAN 20.	Traffic is sent/received on VLAN 20.
Port type = Untagged VLAN ID = 20 Dynamically assigned VLAN = 30	Only untagged traffic is accepted.	Outgoing traffic on the port is untagged.	Traffic is sent/received on VLAN 30 for users that have a dynamically assigned VLAN, and on VLAN 20 for all other users.
Port type = Tagged * VLAN ID = 20 Dynamically assigned VLAN = 30	Only traffic tagged with VLAN 30 is accepted.	Outgoing traffic on the port is tagged with VLAN 30.	Traffic is sent/received on VLAN 30.

* Although the last configuration illustrated in the preceding table is supported, it is not recommended. Dynamic VLANs should generally only be enabled on untagged ports.

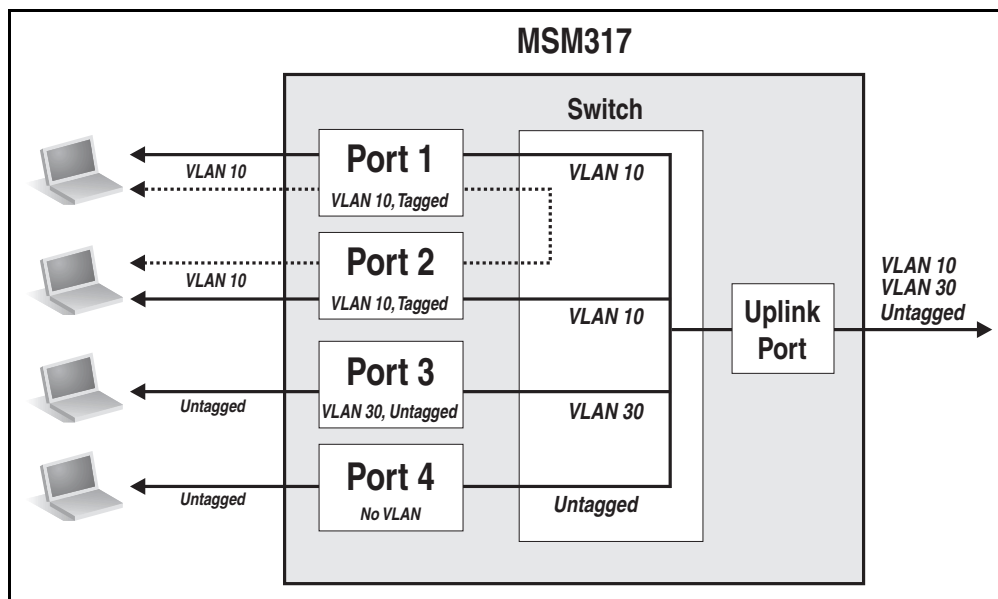
VLAN ID

Defines the VLAN ID for the port. In their default configuration, Ports 1 to 4 and the Uplink port belong to the default VLAN (VLAN 0). This places all ports on the switch onto one physical broadcast domain. (No tagging is applied for the default VLAN however.)

Ports 1 to 4 can be removed from the default VLAN and assigned to their own VLAN. The Uplink port however, is always a member of all defined VLANs. If a VLAN is defined on any port, it is also automatically defined on the Uplink port. In this way, the Uplink port is always connected to Ports 1 to 4.

VLAN example

The following diagram illustrates how traffic is handled by the switch when VLANs are assigned to one or more ports.



- Port 1 and Port 2 are configured with VLAN 10. This connects the two ports allowing traffic to be switched between them (as shown by the dotted line). Both ports are configured as *Tagged*, which means that outgoing traffic on these ports is tagged with VLAN 10, and incoming traffic must also be tagged with VLAN 10. In addition, traffic from these ports is also switched on the Uplink port. Traffic on the Uplink port is always tagged with the configured VLAN ID, which in this case is 10.
- Port 3 is configured with VLAN 30, and is untagged. This means that incoming and outgoing traffic on this port has no VLAN ID. In addition, traffic from this port is also switched on the Uplink port. Traffic on the Uplink port is always tagged with the configured VLAN ID, which in this case is 30.
- Port 4 has no VLAN assigned and is configured as Untagged. Therefore, traffic is forwarded on the Uplink port untagged. Port 4 will only accept incoming traffic that is untagged.

Note

- Port 5 is not shown in this diagram. It is an unmanaged port. Traffic on Port 5 is hard-wired to the Pass Through port on the rear of the MSM317 and is not handled by the switch.
 - The punch-down block is not shown in this diagram. It provides the same type of connection as the Uplink port. Only one can be used at a time.
-

Quarantine VLAN

When this option is enabled, users that fail to be authenticated still gain access to the port. However, all user traffic is forced onto the specified quarantine VLAN.

Allow dynamic VLAN assignment

When this option is enabled, a VLAN that is dynamically assigned to a user will override the VLAN settings for the port.

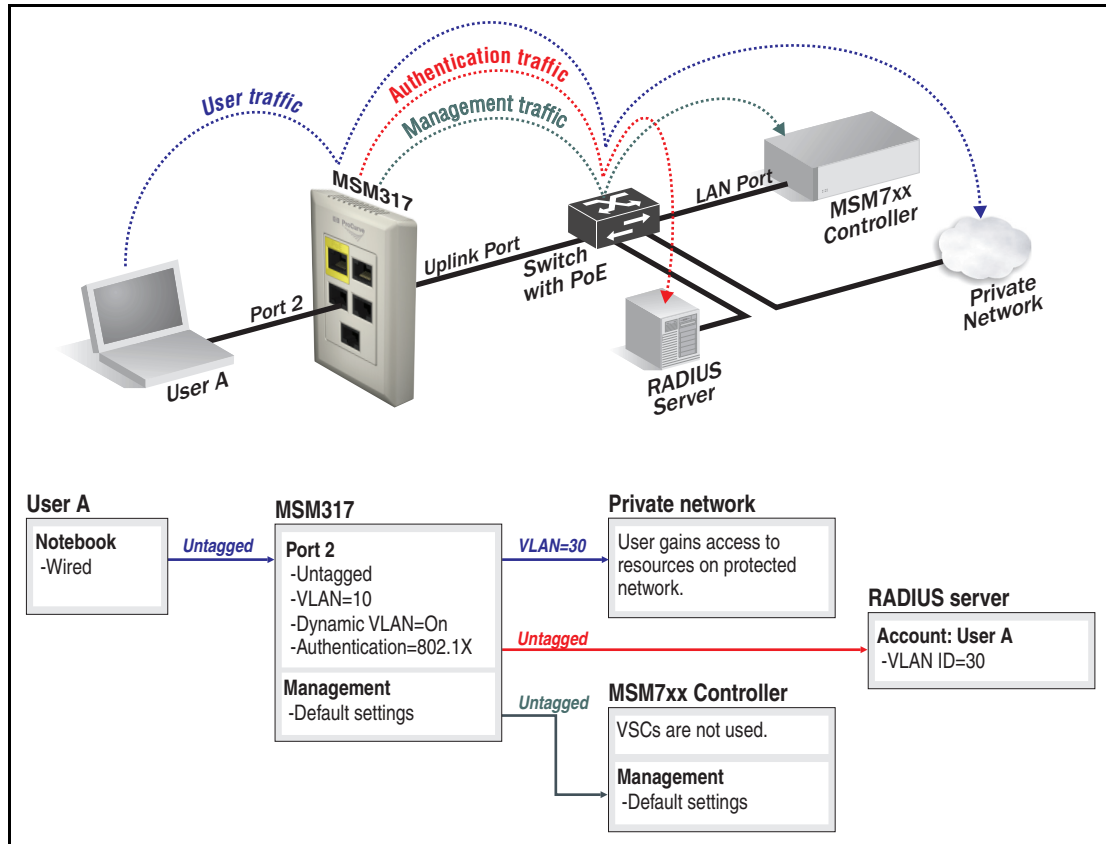
Dynamic VLANs are assigned by setting an attribute in a user's RADIUS account or in a local user account on the MSM7xx Controller. (See the *MSM7xx Controllers Management and Configuration Guide* for more information on configuring user attributes.)

Note

When this option is enabled, the port cannot be bound to an access-controlled VSC.

The following examples illustrate how dynamic VLANs are applied in different scenarios: when not binding to a VSC, and when binding to a non-access-controlled VSC.

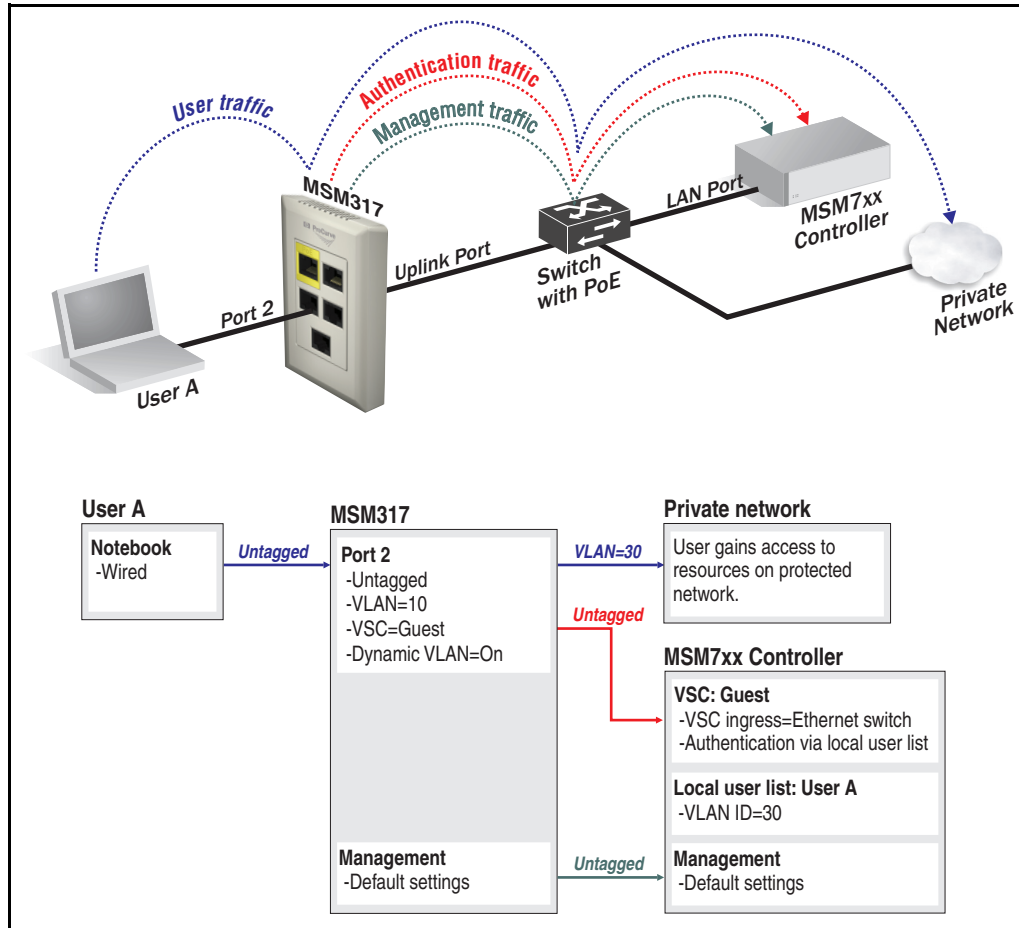
Example 1: When not binding to a VSC



In this scenario, the authentication option is enabled on Port 2, with the credentials for user A being validated against the RADIUS server attached to the switch. Authentication traffic is sent untagged to the RADIUS server. (The RADIUS server must be on the same VLAN, or no VLAN, as the MSM7xx Controller.)

A dynamic VLAN (30) is defined in the user's RADIUS account. Once the user is authenticated, this VLAN overrides the port-assigned VLAN, resulting in the user's traffic being sent on VLAN 30 by the MSM317. In this scenario, the MSM7xx Controller is used purely to configure and manage the MSM317. It does not handle user traffic or authentication traffic.

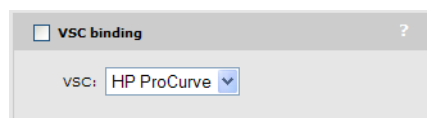
Example 2: When binding to a non-access-controlled VSC



In this scenario, Port 2 is bound to a non-access-controlled VSC named **Guest**. This VSC is configured to provide 802.1X authentication with the login credentials for user A validated against the local user list stored on the MSM7xx Controller.

A local account is created for user A with an egress VLAN ID of 30. Once user A is authenticated, this VLAN overrides the port-assigned VLAN, resulting in the user's traffic being sent on VLAN 30.

VSC binding



Use this option to bind a port to a VSC. This applies settings from the VSC to the port. The type of settings that are applied depend on the type of VSC: access-controlled or non-access-controlled.

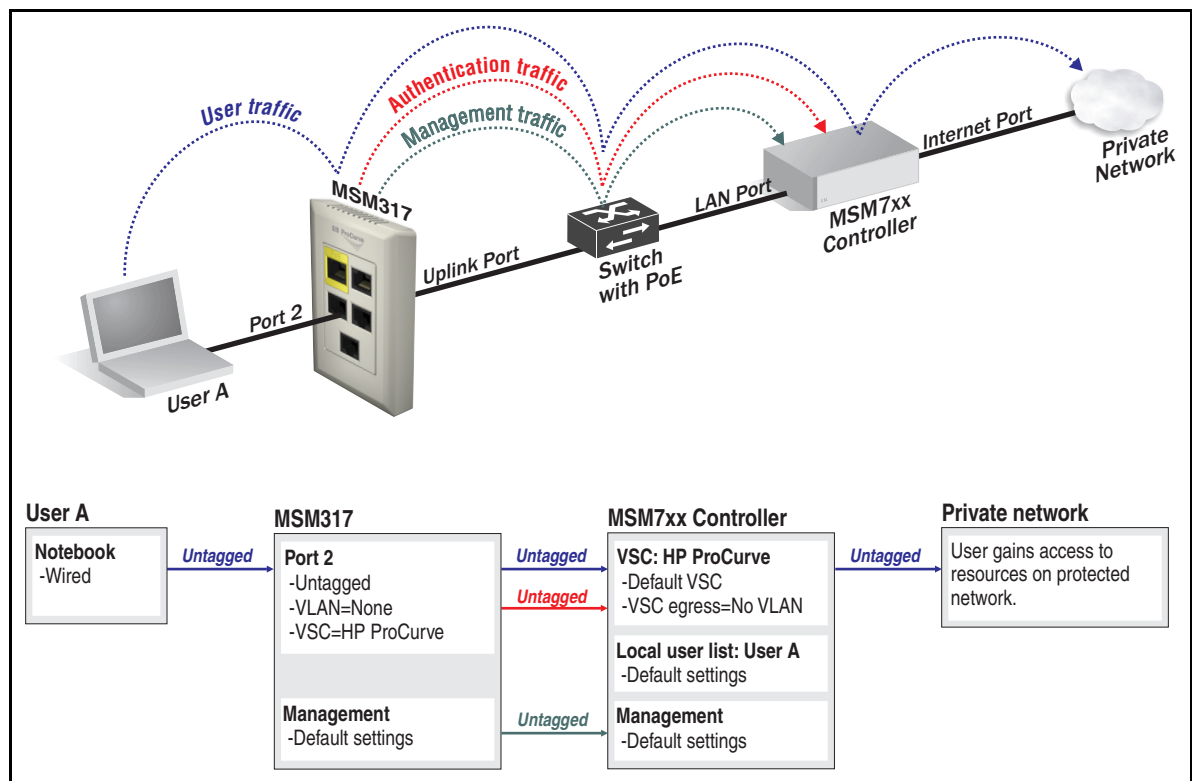
Binding to an access-controlled VSC

When a port is bound to an access-controlled VSC, the MSM7xx Controller is used for authentication and access control, and all non-wireless VSC features are applied to the switch port.

- When binding to an access-controlled VSC, other than the default VSC, a VLAN must be assigned to both the port and the VSC to ensure that user traffic is handled correctly.
- When the default VSC is used, no VLAN definitions are required because untagged traffic on the MSM7xx Controller's LAN port is automatically handled by the default VSC.

The following examples illustrate various ways of binding to an access-controlled VSC.

Example 1: Binding to the default VSC

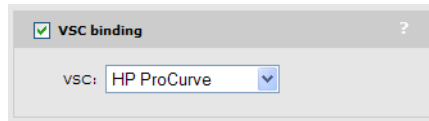


In this scenario, Port 2 is bound to the VSC named **HP ProCurve** (which is the default VSC). Authentication occurs using the local user accounts on the MSM7xx Controller (via 802.1X or HTML-based logins). Once authenticated, user A gains access to resources on the private network according to the configuration of the MSM7xx Controller's public access interface feature. No VLANs are assigned in this example, therefore user traffic is forwarded untagged from the MSM317 to the MSM7xx Controller and is automatically assigned to the default VSC.

Configuration

Configuring the switch ports

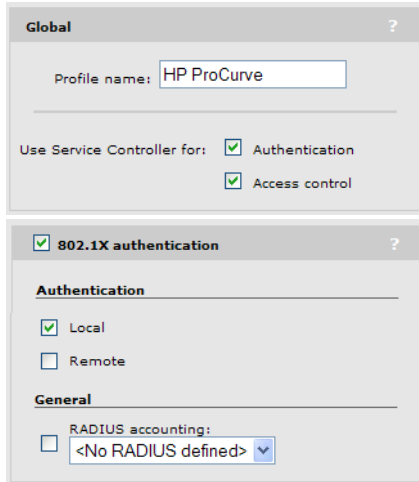
Key configuration settings for Port 2 are as follows:



☒ **VSC binding** ?

VSC: HP ProCurve

Key configuration settings for the VSC are as follows:



Global ?

Profile name: HP ProCurve

Use Service Controller for: ☒ Authentication ☒ Access control

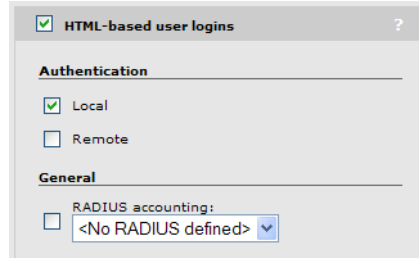
☒ **802.1X authentication** ?

Authentication

☒ Local ☐ Remote

General

☐ RADIUS accounting: <No RADIUS defined>



☒ **HTML-based user logins** ?

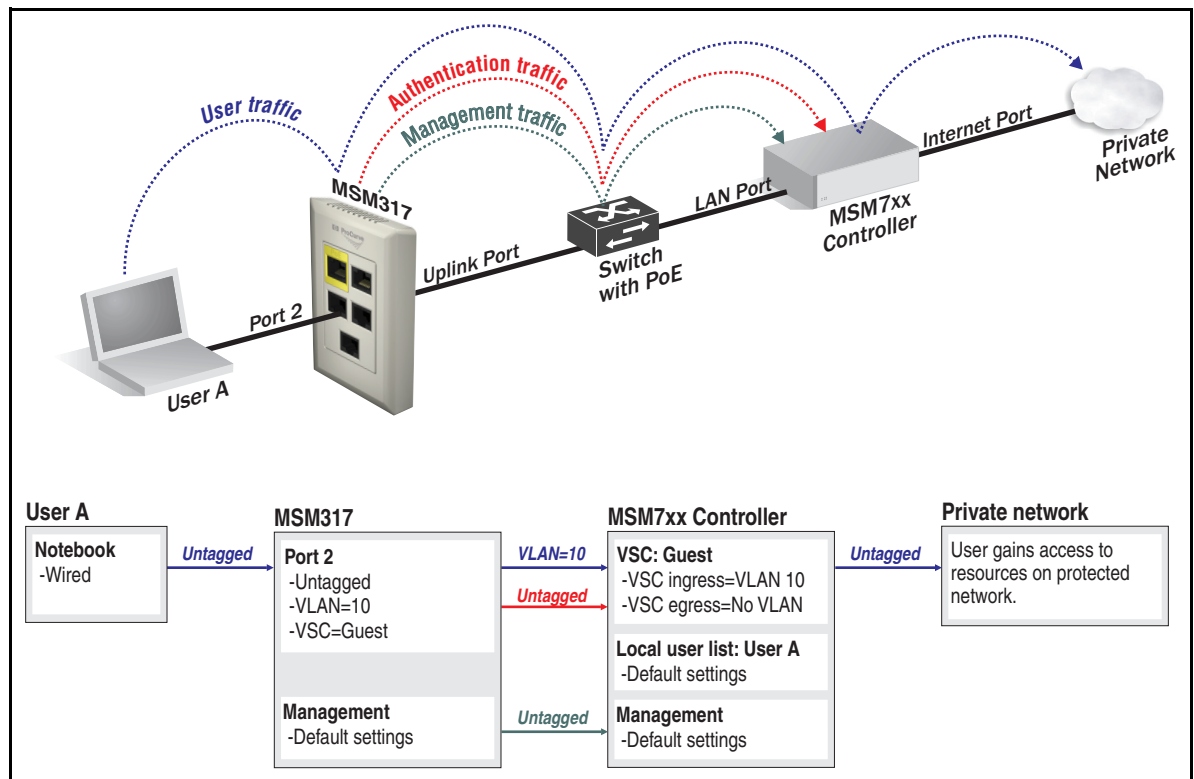
Authentication

☒ Local ☐ Remote

General

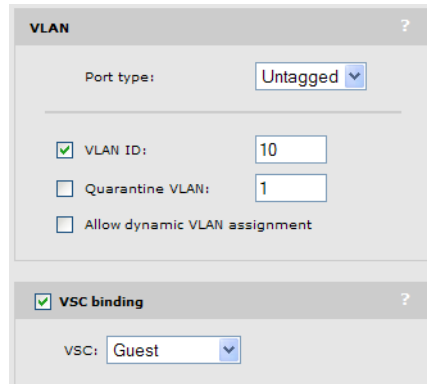
☐ RADIUS accounting: <No RADIUS defined>

Example 2: Binding to a specific VSC



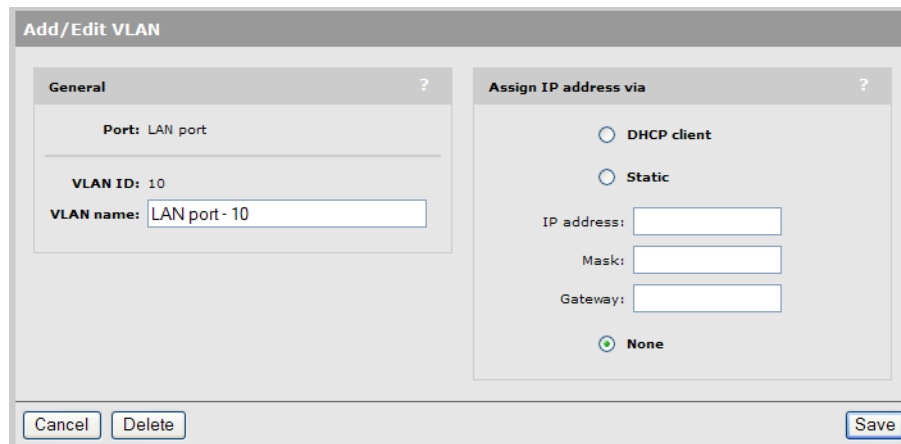
In this scenario, Port 2 is bound to the VSC named **Guest**. Authentication occurs using the local user accounts on the MSM7xx Controller (via 802.1X or HTML-based logins). Once authenticated, user A gains access to resources on the private network according to the configuration of the public access interface feature on the MSM7xx Controller. Since the **Guest** VSC is not the default VSC, a VLAN definition must be assigned to the port to ensure that user traffic is properly routed from the MSM317 to the VSC on the MSM7xx Controller.

Key configuration settings for Port 2 are as follows:



The image shows a 'VLAN' configuration dialog box. It has a title bar with a question mark icon. Inside, there's a 'Port type:' dropdown menu set to 'Untagged'. Below this, there are three checkboxes: 'VLAN ID:' (checked) with a text input field containing '10', 'Quarantine VLAN:' (unchecked) with a text input field containing '1', and 'Allow dynamic VLAN assignment' (unchecked). At the bottom, there's a 'VSC binding' section with a checked checkbox and a 'VSC:' dropdown menu set to 'Guest'.

Configuration of the VLAN on the MSM7xx Controller is as follows:



The image shows an 'Add/Edit VLAN' dialog box with two main sections. The 'General' section on the left has a 'Port:' dropdown set to 'LAN port', a 'VLAN ID:' text input field containing '10', and a 'VLAN name:' text input field containing 'LAN port - 10'. The 'Assign IP address via' section on the right has three radio buttons: 'DHCP client' (unselected), 'Static' (unselected), and 'None' (selected). Below these are text input fields for 'IP address:', 'Mask:', and 'Gateway:'. At the bottom of the dialog are 'Cancel', 'Delete', and 'Save' buttons.

Since the VLAN is only used to route traffic to the appropriate VSC on the MSM7xx Controller, it does not require an IP address.

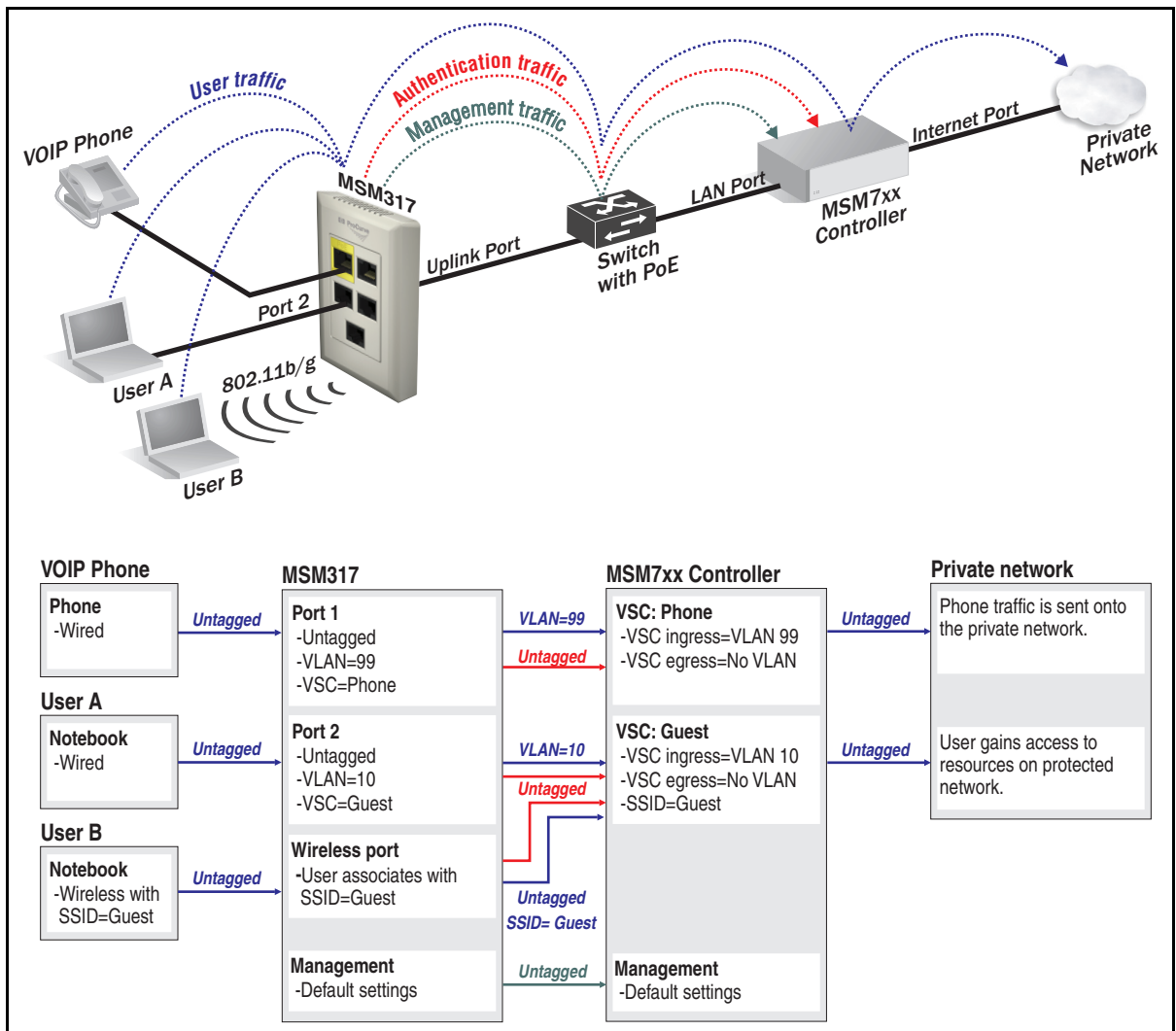
Key configuration settings for the VSC are as follows:

Global
Profile name: HP ProCurve
Use Service Controller for: ☒ Authentication
☒ Access control

VSC ingress mapping
☒ SSID
☒ VLAN LAN port- 10

☒ 802.1X authentication
Authentication
☒ Local
☐ Remote
General
☐ RADIUS accounting:
<No RADIUS defined>

Example 3: Binding to multiple VSCs



In this scenario, the MSM317 provides access for three types of users as follows:

VOIP phone

An in-room IP phone is connected to Port 1, which is bound to the VSC named **Phone**. Authentication occurs using the phone's MAC address via the local user accounts on the MSM7xx Controller. Since the **Phone** VSC is not the default VSC, a VLAN definition must be assigned to the port to ensure that phone traffic is properly routed from the MSM317 to the **Phone** VSC on the MSM7xx Controller.

Key configuration settings for Port 2 are as follows:

The image shows a 'VLAN' configuration window. Under 'Port type', 'Untagged' is selected. Under 'VLAN ID', '99' is entered. 'Quarantine VLAN' is set to '1'. 'Allow dynamic VLAN assignment' is unchecked. In the 'VSC binding' section, 'Phone' is selected from the dropdown menu.

Configuration of the VLAN on the MSM7xx Controller is as follows:

The image shows an 'Add/Edit VLAN' window. In the 'General' tab, 'Port' is 'LAN port', 'VLAN ID' is '99', and 'VLAN name' is 'LAN port - 99'. In the 'Assign IP address via' tab, 'DHCP client' and 'Static' are unselected, and 'None' is selected. The 'IP address', 'Mask', and 'Gateway' fields are empty.

Key configuration settings for the VSC are as follows:

The image shows two VSC configuration windows. The first window, 'Global', has 'Profile name' set to 'Phone'. Under 'Use Service Controller for:', both 'Authentication' and 'Access control' are checked. The second window, 'MAC-based authentication', has 'Local' checked under 'Authentication'. Under 'General', 'RADIUS accounting' is unchecked and set to '<No RADIUS defined>'.

User A

Wired guests, as illustrated by user A, connect to Port 2, which is bound to the VSC named **Guest**. Authentication occurs using the local user accounts on the MSM7xx Controller. Once authenticated, user A gains access to resources on the private network according to the configuration of the public access interface feature on the MSM7xx Controller. Since the **Guest** VSC is not the default VSC, a VLAN definition must be assigned to the port to ensure that user traffic is properly routed from the MSM317 to the VSC on the MSM7xx Controller.

Key configuration settings for Port 2 are as follows:

VLAN ?

Port type: Untagged

☒ VLAN ID: 10

☐ Quarantine VLAN: 1

☐ Allow dynamic VLAN assignment

☒ **VSC binding** ?

VSC: Guest

Configuration of the VLAN on the MSM7xx Controller is as follows:

Add/Edit VLAN

General ?

Port: LAN port

VLAN ID: 10

VLAN name: LAN port - 10

Assign IP address via ?

☐ DHCP client

☐ Static

IP address:

Mask:

Gateway:

☒ None

Cancel Delete Save

Key configuration settings for the VSC are as follows:

Global ?

Profile name: Guest

Use Service Controller for: ☒ Authentication ☒ Access control

VSC ingress mapping ?

☒ SSID

☒ VLAN: LAN port - 10

☒ **802.1X authentication** ?

Authentication

☒ Local ☐ Remote

General

☐ RADIUS accounting: <No RADIUS defined>

User B

Wireless guests, illustrated by user B, connect to the MSM317 radio using the SSID **Guest**. This SSID is defined in the VSC named **Guest** which is bound to the MSM317 using **Controlled APS > [AP group] >> VSC bindings** on the MSM7xx Controller. (There is no option on the MSM317 to bind a VSC to the wireless port.) Authentication occurs using the local user accounts on the MSM7xx Controller. Once authenticated, the user gains access to resources on the private network according to the configuration of the MSM7xx Controller's public access interface feature. The SSID assigned to the VSC is used to route traffic from the MSM317 to the VSC on the MSM7xx Controller, therefore no VLAN is required. For more information on binding VSCs for wireless users, see the *MSM7xx Controllers Management and Configuration Guide*.

The configuration settings for the VSC are identical to those done in the previous section (Wired guests), except for the wireless-related settings which are shown below:

The screenshot shows a configuration window titled "Virtual AP" with a question mark icon. It contains two main sections: "WLAN" and "Wireless clients".

WLAN Section:

- Name (SSID):
- DTIM count:
- ☒ Broadcast name (SSID)
- ☐ Advertise TX power

Wireless clients Section:

- Max clients per radio:
- Allow traffic between: wireless clients

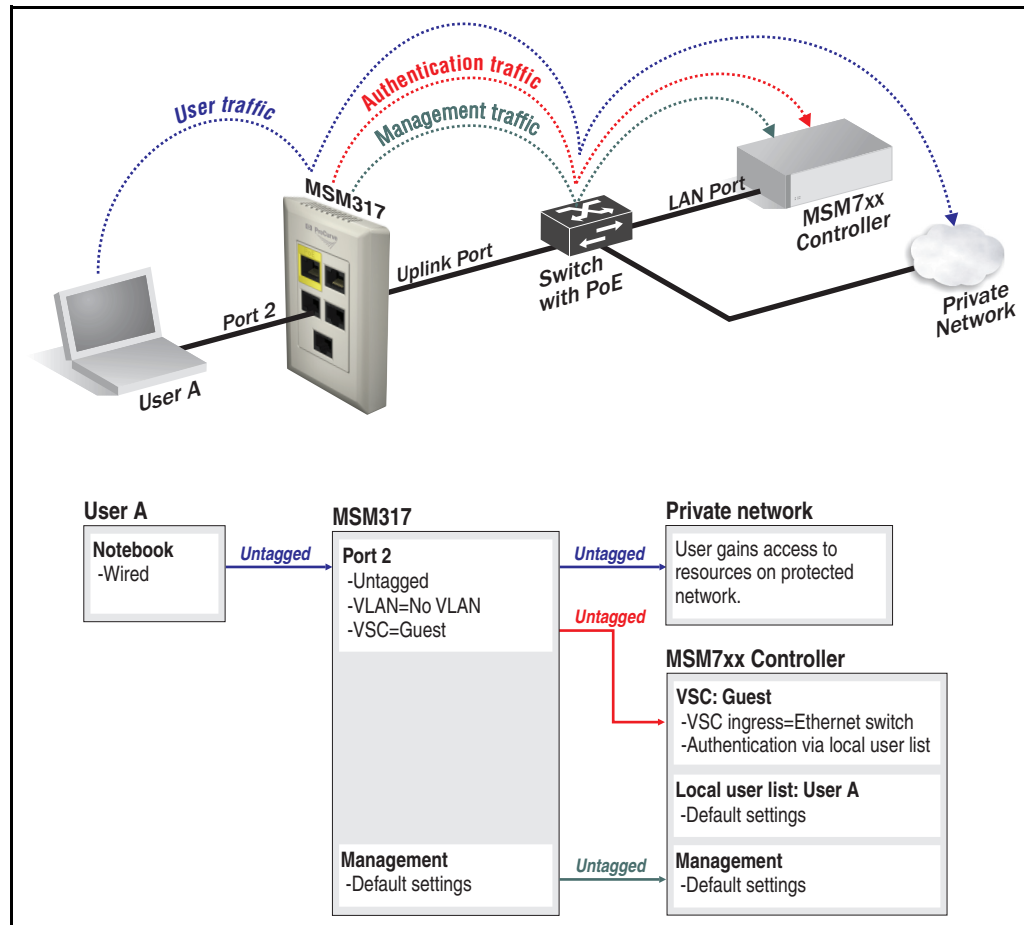
Below these sections are three expandable sections, each with a plus icon in a box:

- Client data tunnel**
- Quality of service**
- Allowed wireless rates**

Binding to a non-access-controlled VSC

When a port is bound to a non-access-controlled VSC, the MSM7xx Controller is used for authentication tasks only. Authentication can occur by checking the user's MAC address or via 802.1X. Access control must then be performed by another device on the network, or not at all.

Example 1: Binding to a specific VSC



In this scenario, Port 2 is bound to the VSC named **Guest**. Since this is a non-access-controlled VSC, the port is mapped directly to the VSC ingress on the MSM7xx Controller with the Ethernet switch option. Authentication occurs via the local user accounts on the MSM7xx Controller (via 802.1X or MAC-based). Once authenticated, user A gains direct access to any resources on the private network.

Key configuration settings for Port 2 are as follows:

☒ VSC binding ?

VSC:

Guest

Key configuration settings for the VSC are as follows:

Global ?

Profile name:

Guest

Use Service Controller for:

☒ Authentication

☐ Access control

VSC ingress mapping ?

☐ SSID

☒ Ethernet Switch

802.1X authentication ?

Authentication

☒ Local

☐ Remote

General

☐ RADIUS accounting:

<No RADIUS defined>

MAC-based authentication ?

Authentication

☒ Local

☐ Remote

General

☐ RADIUS accounting:

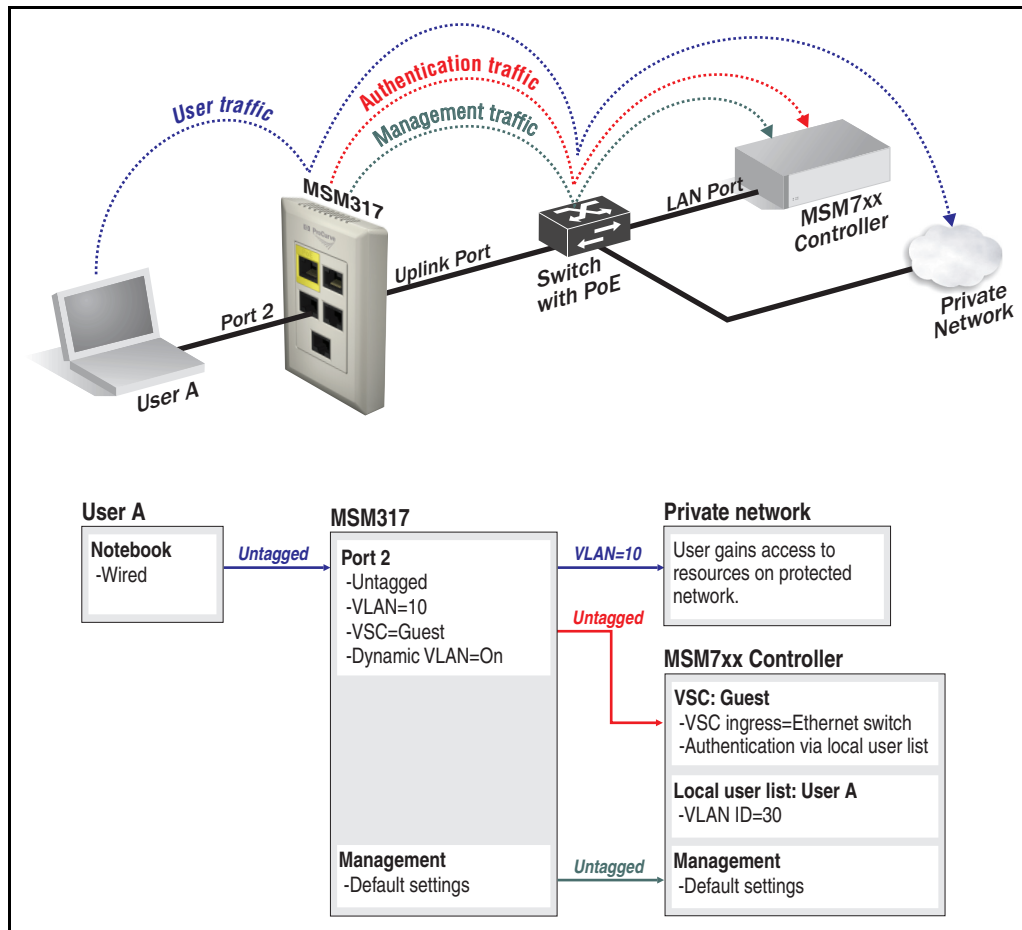
<No RADIUS defined>

3-27

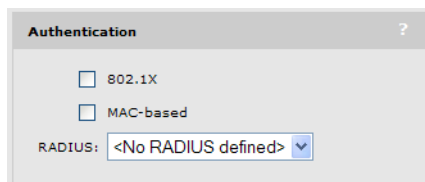
Configuration

Configuring the switch ports

If the private network is operating on a VLAN, you can assign a VLAN to Port 2. In the following scenario, once authenticated, the user gains direct access to any resources on the private network using VLAN 10.



Authentication



This option is only available if the **VSC binding** option is not enabled.

Authentication can be enabled on Ports 1 to 4, allowing access to the ports to be controlled using the MAC address of a client station or via 802.1X. If a client station fails to authenticate, access to the port is blocked unless the **Quarantine VLAN** option (under **VLAN**) is enabled, in which case access is enabled but all traffic is forced onto the specified quarantine VLAN.

If both authentication options are enabled at the same time, then:

- 802.1X takes priority for client stations that are 802.1X enabled. If 802.1X authentication fails, MAC authentication is not checked and the client station fails to authenticate.
- MAC authentication takes priority for client stations that are not 802.1X enabled. If MAC authentication fails, then the client station fails to authenticate.

Note

Only one authenticated MAC address is supported per port. This means if multiple devices are connect to a port via a hub, only one device (or user) can gain access at a time.

802.1X

This option enables support for client stations with 802.1X client software that uses EAP-TLS, EAP-TTLS, EAP-SIM, PEAP, or any other transparent EAP method. Encryption is not supported.

802.1X logins are authenticated via an external RADIUS server defined by the RADIUS profile selected for **RADIUS**.

MAC-based

This option lets you control access based on a client station's MAC address. Addresses are authenticated via an external RADIUS server defined by the RADIUS profile selected for **RADIUS**.

To successfully authenticate a client station, an account must be created on the RADIUS server with both username and password set to the MAC address of the client station. The MAC address must be defined as 12 hexadecimal numbers, with the values "a" to "f" in lowercase. For example, **0003520a0f01**.

RADIUS

Select the RADIUS profile that will be used for 802.1X and MAC-based authentication. RADIUS profiles are defined on the RADIUS profiles page. To open this page:

1. In the **Network tree** select **Service Controller**.
2. In the right pane select **Authentication**, then select **RADIUS profiles**.

Viewing status information

The MSM7xx management tool provides a number of pages where you can view MSM317 status information. To access these pages, first select the MSM317 in the **Network Tree**. (Initially, the MSM317 will appear in the Default group and its name will be the product serial number. To make the MSM317 easier to identify in the following screen images, it has been renamed to MSM317-1.)

Note

For detailed descriptions of each page shown in the following sections, see the online help.

AP details

To view global information about the MSM317, select **Overview > AP details**. For example:

The screenshot displays the MSM317-1 Overview and Details pages. The Overview page shows a table with one entry, MSM317-1, with a status of 'Synchronized'. The Details page provides comprehensive information about the access point, organized into several sections:

- Diagnostic information:** The AP is up and running, offers wireless services and had its firmware and configuration settings successfully updated by the service controller.
- Configured information:**

Access point name:	MSM317-1
Access point location:	n/a
Access point contact:	n/a
Group name:	MSM317
- Networking information - AP:**

Control channel:	Port 1
VLAN identifier:	Untagged
MAC address:	00:23:47:7a:17:00
IP address:	192.168.1.13
IP netmask:	255.255.255.0
IP gateway:	192.168.1.1
Connectivity:	L2
- Networking information - Service controller:**

Discovered on interface:	LAN port
VLAN ID:	Untagged
- Licensing information:**

Integrated license(s):	None
Needed license(s):	None
Valid license(s):	None
Violated license(s):	None
- Maintenance information:**

Serial number:	TW8501X00V
Ethernet base MAC:	00:23:47:7a:17:00
Platform:	MSM317
Boot revision:	Boot 13.6 (Nov 15 2008 - 01:12:53)
Hardware revision:	n/a
Firmware revision:	5.3.1.0-01-7129
- Wireless information:**

Operating mode:	AP only
Wireless mode:	802.11b/g
Channel selection:	Automatic
Current channel:	Channel 10, 2.457GHz
- Security information:**

Authorization status:	Authorized
Authorization method:	Discovered
Connected since:	Fri Apr 24 14:14:53 2009








Wireless clients

To see a list of all wireless clients connected to the MSM317 and related status information, select **Overview > Wireless clients**. For example:

AP: MSM317-1 Wireless clients ?									
Number of associated client stations: 1									
AP name	Radio	MAC address	IP address	SSID	Security	Duration	Signal	Noise	SNR
MSM317-1	1	00:1d:4f:31:81:cf	192.168.1.21	MSM317	Authorized	04:00:13	-74	-99	25

Port statistics

To see statistics for each port on the MSM317, select **Status > Ports**. For example:

AP: MSM317-1 Port statistics ?										
Ethernet statistics										
Port	Receive			Transmit			Collisions	Ether Speed	Ether Duplex	
	Frames	Dropped	Errors	Frames	Dropped	Errors				
 Data tunnel	45	0	0	0	0	0	0	N/A	N/A	
 Switch port 1	0	0	0	0	0	0	0	Disc.	Disc.	
 Switch port 2	0	0	0	0	0	0	0	Disc.	Disc.	
 Switch port 3	0	0	0	0	0	0	0	Disc.	Disc.	
 Switch port 4	0	0	0	0	0	0	0	Disc.	Disc.	
 Uplink Port	17388	0	0	17839	0	0	0	100Mbps	Full	
 Wireless port	2008	16	4602212	35284	0	19638	0	N/A	N/A	

Bridge port statistics

To see the traffic forwarding tables for the bridge and the switch ports, select **Status > Ports**. For example:

AP: MSM317-1 | Bridge status

?

	Wireless	Uplink port
State:	Forwarding	Forwarding
ID:	8001	8002

Spanning Tree Protocol

Spanning Tree Protocol:	enabled		
Bridge ID:	8000.0023477a1700		
Designated root:	8000.0023477a1700		
Root path cost:	0		
Max age:	20.00	(bridge)	20.00
Hello time:	2.00	(bridge)	2.00
Forward delay:	0.00	(bridge)	0.00
Topology change flag:	No	(detected)	No

AP: MSM317-1 | Bridge forwarding table

?

Port	MAC address	VSC ID	VLAN	Authorized?	Local?	Aging
Uplink Port	00:23:47:7a:17:00	-	-	Yes	Yes	0ms
Uplink Port	00:03:52:04:9d:b1	-	-	Yes	No	190ms
Uplink Port	00:03:52:08:02:47	-	-	Yes	No	670ms
Uplink Port	00:03:52:01:5c:77	-	-	Yes	No	33500ms
Uplink Port	00:03:52:bf:70:4a	-	-	Yes	No	20970ms
Wireless port	00:1d:4f:31:81:cf	1	-	Yes	No	66810ms
Wireless port	00:23:47:7a:18:00	-	-	Yes	Yes	0ms

AP: MSM317-1 | Switch forwarding table

?

Port	MAC address	VSC ID	VLAN	Authorized?	Local?	Aging
Uplink Port	00:03:52:01:5c:77	-	-	Yes	No	25000ms
Uplink Port	00:03:52:04:9d:b1	-	-	Yes	No	0ms
Uplink Port	00:03:52:08:02:47	-	-	Yes	No	0ms
Uplink Port	00:03:52:bf:70:4a	-	-	Yes	No	25000ms

Regulatory information

Contents

Notice for U.S.A.....	A-2
Notice for Canada	A-3
Notice for the European Community	A-3
Notice for Brazil	A-4
Notice for Japan	A-5
Notice for Taiwan.....	A-5
Notice for Korea.....	A-5

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.

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.

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.

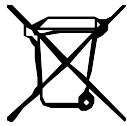
Note

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.

- This device may be operated indoors or outdoors in all EU and EFTA countries using the 2.4GHz 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-telcom.fr>.

L'utilisation de cet équipement (2.4GHz 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 à 2483.5MHz (Chaîne 1-13). Pour une utilisation en environnement extérieur, vous devez utiliser les fréquences comprises entre 2400 à 2454-MHz (Chaîne 1-9). Pour les dernières restrictions, voir <http://www.art-telecom.fr>.

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.

Caution

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. Unauthorized 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上、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、パ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 Korea

(warning for wireless equipment)

당해 무선설비는 운용 중 전파혼선 가능성이 있음

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。

Technology for better business outcomes

To learn more, visit www.hp.com/go/procurve/

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP will not be liable for technical or editorial errors or omissions contained herein.



May 2009

Manual Part Number
5992-5495