HP V-M200 802.11n Access Point

Management and Configuration Guide

HP V-M200 802.11n Access Point

Management and Configuration Guide

Publication Number

5998-0296
August 2010

Applicable Products

	WW	USA
V-M200 802.11n Access Point	J9468A	J9467A

Trademark Credits

Disclaimer

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

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

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

Warranty

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

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

Open Source Software Acknowledgement Statement

This software incorporates open source components that are governed by the GNU General Public License (GPL), version 2. In accordance with this license, HP 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: HP Networking Support

Roseville, CA 95747 USA

Safety

Before installing and operating this product, please read *Safety information on page 1-5*.

Hewlett-Packard Company

8000 Foothills Boulevard
Roseville, California 95747
www.hp.com/networking

Contents

1 Introduction

2 Using Quick Setup

4 Working with wireless communities

5 Wireless configuration

6 Configuring network settings and VLANs

7 Authentication services

8 Creating WDS links

1

Introduction

Contents

About this guide

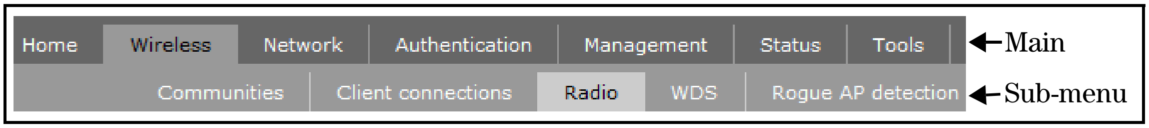
This guide explains how to install, configure, and operate the HP V-M200 802.11n Access Point.

Conventions

The following conventions are used in this guide.

Management tool

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



Example directions in this guide	What to do in the user interface
Select **Wireless > Radio**.	Select **Wireless** on the main menu, and then select **Radio** on the sub-menu.
For **Password** specify **secret22**.	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.

Introducing the HP V-M200 802.11n Access Point

Geared towards small and medium-sized businesses (SMBs), the HP V-M200 802.11n Access Point offers next-generation 802.11n technology, superior bandwidth, and multiple operating modes.

The V-M200 is an 802.11n MIMO (multiple input, multiple output) access point that provides extended coverage and enhanced throughput for both legacy 802.11a/b/g and newer 802.11n clients. The V-M200 dispenses multiple network services, delivers high-performance client access, and offers ease of deployment.

Since SMBs often lack the IT resources of large companies, and their network security may not be strong enough to protect the integrity of their business data, the V-M200 is designed to offer robust and consistent security through the following authentication and encryption standards:

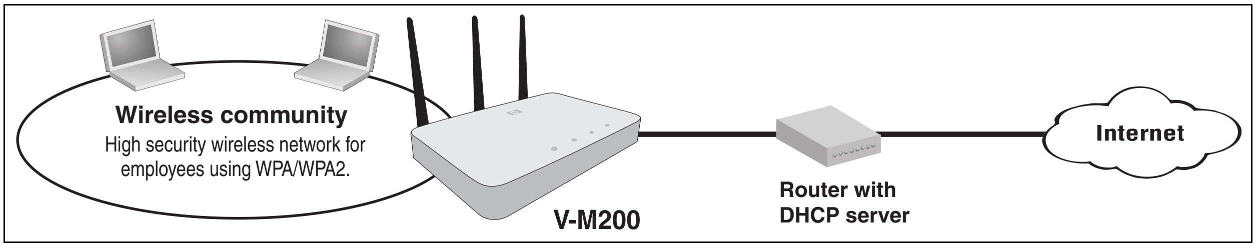
- Wi-Fi Protected Access (WPA and WPA2)
- Extensible Authentication Protocol (EAP) Types, including EAP-MD5, EAP-TLS, EAP-TTLS, PEAPv0, PEAPv1, and EAP-FAST

These authentication and encryption certifications support IEEE 802.1X for user-based authentication, Temporal Key Integrity Protocol (TKIP) for WPA encryption, and Advanced Encryption Standard (AES) for WPA2 encryption.

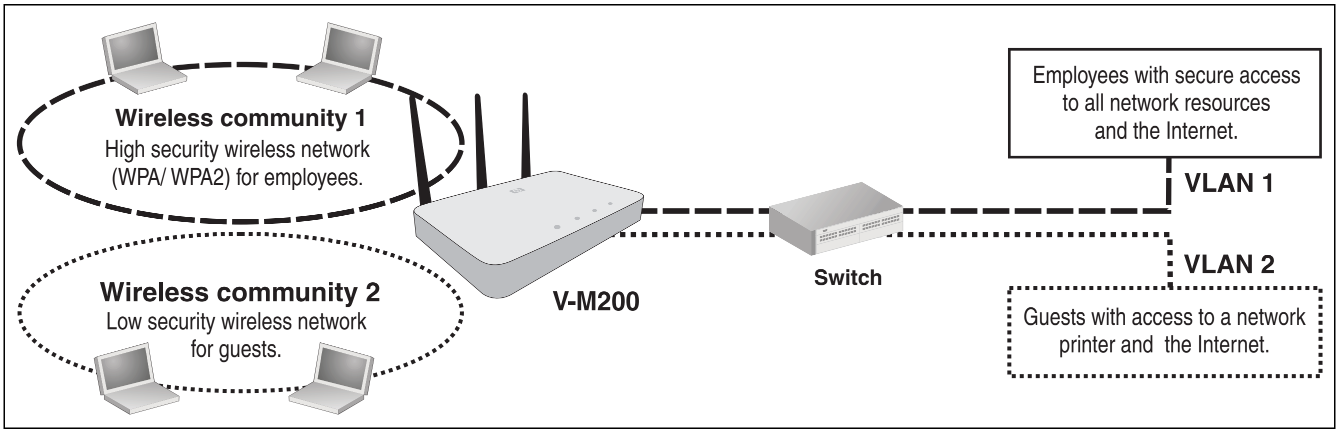
The V-M200 is managed through its easy-to-use Web-based management tool, and it can be easily deployed and integrated into an existing LAN infrastructure.

Sample deployments

In a small office, the V-M200 can be directly connected to a broadband router (DSL or cable) to provide wireless networking for all employees. In the following scenario, employees can share data and resources with each other and access the Internet at the same time.


Wireless community
High security wireless network for employees using WPA/WPA2.
V-M200
Router with DHCP server
Internet

With its wireless community feature, the V-M200 can be configured to provide up to four separate wireless networks (all on the same wireless channel), each with its own configuration settings for security, quality of service, VLAN support, and more.

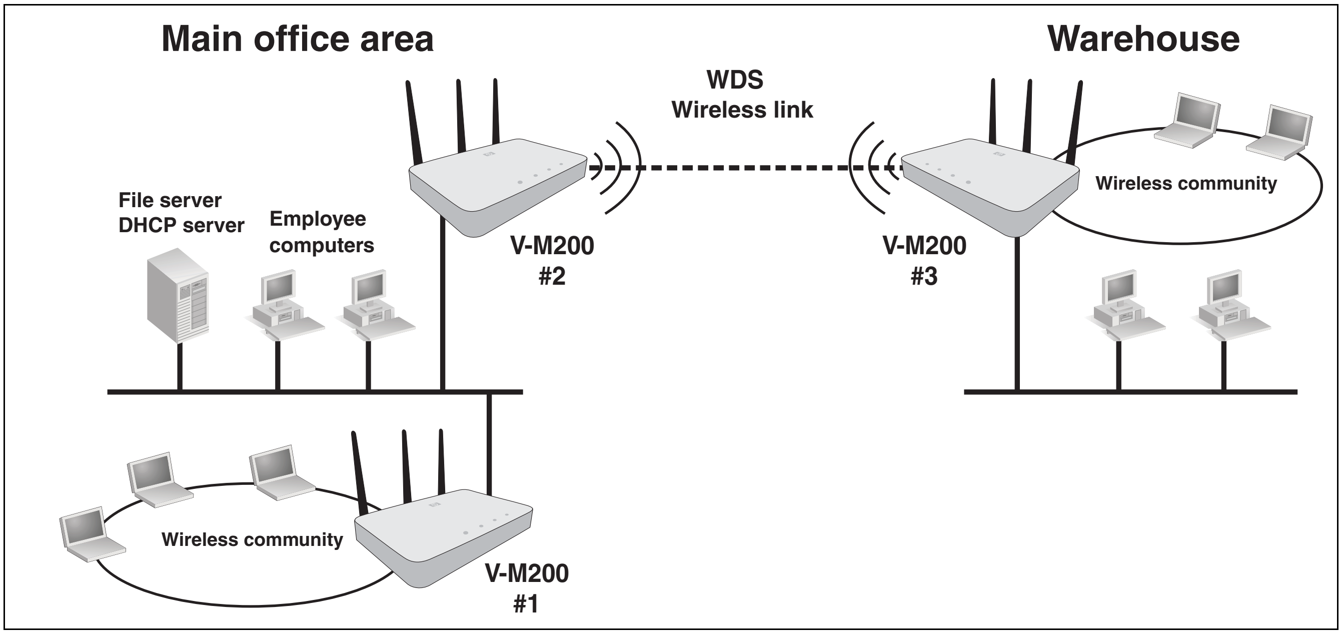

Wireless community 1
High security wireless network (WPA/ WPA2) for employees.
Wireless community 2
Low security wireless network for guests.
V-M200
Switch
Employees with secure access to all network resources and the Internet.
VLAN 1
VLAN 2
Guests with access to a network printer and the Internet.

In this scenario, employees connect to wireless community 1, which is protected with WPA/ WPA2. All employee traffic exits the V-M200 on VLAN 1, providing access to private resources on the company network, as well as the Internet.

Guests connect to wireless community 2, which is protected with WEP. All guest traffic exits the V-M200 on VLAN 2, providing access only to the Internet. In addition, wireless traffic from guests is given a lower priority than employee traffic.

For offices that already have a wired networking infrastructure, the V-M200 is easily integrated to provide wireless networking. It can also be used to extend the reach of the network to areas that are difficult or impossible to reach with traditional cabling.

In the following scenario, V-M200 #1 provides wireless network services to the employees in the main office. While V-M200 #2 and V-M200 #3 use the Wireless Distribution System (WDS) to create a wireless link between the main office network and a small network in a warehouse. WDS eliminates the need to run cabling, allowing for fast and easy deployment.



Key features

- **Radio:** Supports IEEE 802.11a, 802.11b, 802.11g, and 802.11n (2.4 GHz /5 GHz).
- **Automatic channel selection**: Auto-selects RF channel and transmit power.
- **Wireless communities**: Allows you to create up to four different wireless networks (on the same channel), each with its own configuration settings, including network name, user authentication, encryption, quality of service, and more.
- **Power over Ethernet (PoE)**: Supports 802.3af PoE as a powered device (PD), so that it can be mounted where power outlets are not readily available.
- **Authentication and encryption**: Enforces client authorization based on user credentials (802.1X/EAP), or hardware identifiers (MAC address, WEP key).
- **Intrusion detection**: Detects rogue APs by scanning the radio frequency (RF) space for unauthorized APs at specific intervals to protect the network.
- **Wireless Distribution System (WDS)**: Provides point-to-point bridging to extend the network to places where Ethernet infrastructure is not available.
- **Ethernet port**: Provides a single 10/100/1000 Mbps IEEE 802.3 Ethernet port for connection to a wired network.

Safety information

Warning

Important information to read before installing

See the HP V-M200 802.11n Access Point Quickstart for installation instructions. Prior to installing or using the V-M200, make sure that the installation plans are in compliance with RF and other regulations, such as building and wiring codes, safety, channel, indoor/outdoor restrictions, and license requirements for the intended country of use. 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: Make sure that proper surge protection and grounding precautions are taken according to local electrical code. Failure to do so may result in personal injury, fire, equipment damage, or a voided warranty. The HP hardware warranty provides no protection against damage caused by static discharge or a power surge.

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. At least Cat 5e cabling is required.

Country of use: In some regions, you are prompted to select the country of use during setup. Once the country has been set, the V-M200 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 V-M200 is powered-on when its Ethernet port is plugged into a PoE power source or when an external power supply is connected.
- The V-M200 and all interconnected equipment must be installed indoors within the same building, 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 Networking products. Any servicing, adjustment, maintenance, or repair must be performed only by trained service personnel.

HP Networking support

The HP Web site, **www.hp.com/networking/support** 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 Networking support, you first should collect the following information:

Collect this information	Where to find it
Product identification.	On the bottom of the product.
Software version.	The V-M200 management tool Login page.
Network topology map, including the addresses assigned to all relevant devices.	Your network administrator.

Getting started

Get started with your V-M200 by following the directions in the *HP V-M200 802.11n Access Point Quickstart*.

Online documentation

For the latest documentation, visit the HP Networking support Web page at: **www.hp.com/networking/support** and select **Manuals**.

2

Using Quick Setup

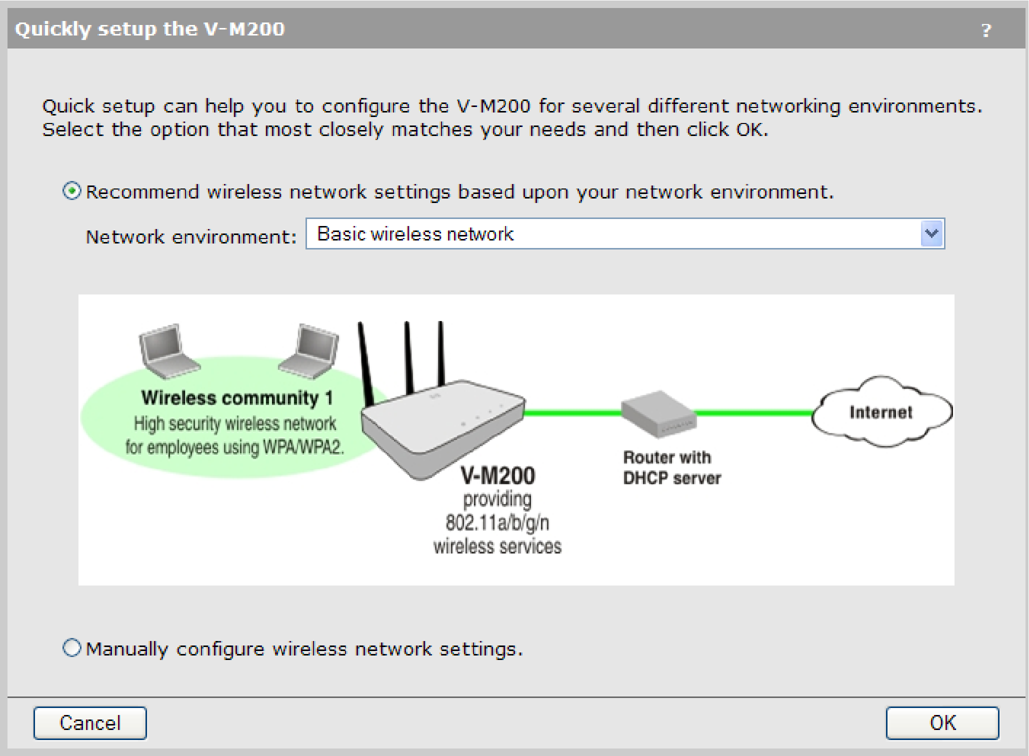
Contents

Overview

Quick Setup provides an easy way to quickly configure settings on the V-M200 for several different networking scenarios. Just pick the scenario that most closely resembles your installation and fill in the appropriate fields to get going.

Automatically running Quick Setup the first time you login

The first time you login to the management tool (see the *HP V-M200 802.11n Access Point Quickstart* for first time login procedure), the Quick Setup home page is automatically presented at the end of the startup sequence. This page lets you choose one of four configuration scenarios to use as the basis for your setup.



Quickly setup the V-M200 ?

Quick setup can help you to configure the V-M200 for several different networking environments.
Select the option that most closely matches your needs and then click OK.

● Recommend wireless network settings based upon your network environment.

Network environment: Basic wireless network

○ Manually configure wireless network settings.

See the following sections for a description of each scenario:

- *Basic wireless network on page 2-3*
- *Multiple wireless networks on page 2-7*
- *Multiple wireless networks with wired VLANS on page 2-12*
- *Multiple wireless networks with RADIUS authentication on page 2-18*.

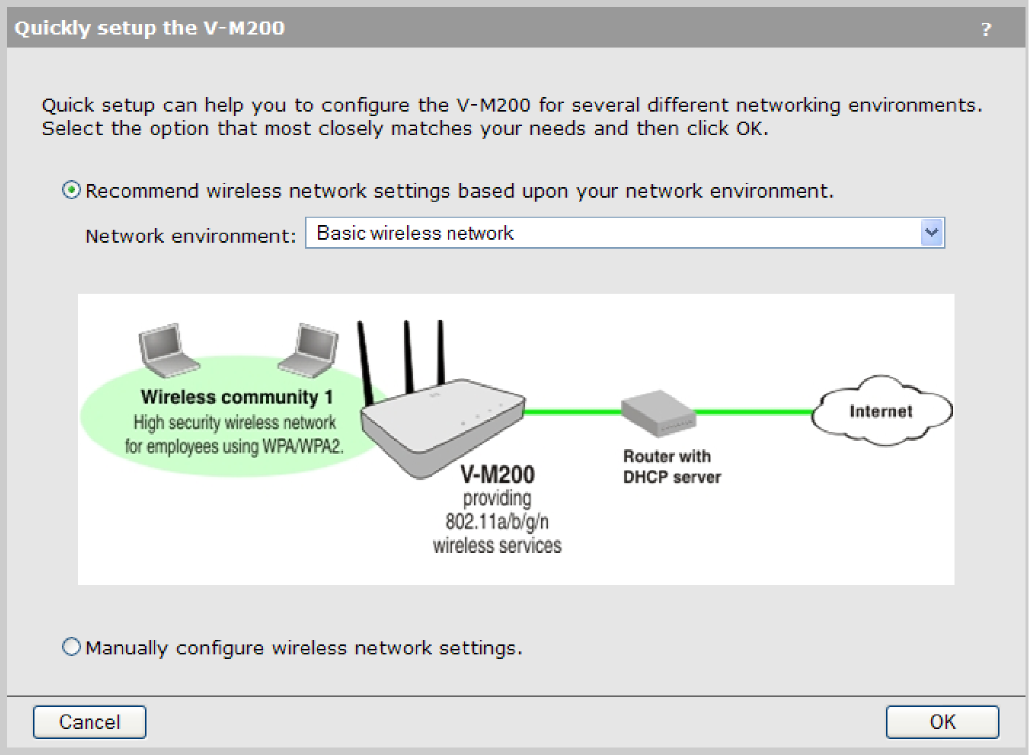
Manually running Quick Setup after your first login

If you manually launch Quick Setup by selecting **Home > Quick Setup**, you will see the Quick Setup global settings page instead of the Quick Setup home page. See *Global settings page on page 2-20*.

Basic wireless network

See also the HP V-M200 802.11n Access Point Quickstart which describes the configuration procedure for a basic wireless network.

Choose this option if you want to create a single wireless network to provide wireless connectivity for your users. This option can be used to connect the V-M200 directly to a broadband router or to an existing wired network, using either static IP addressing or DHCP.



Quickly setup the V-M200 ?

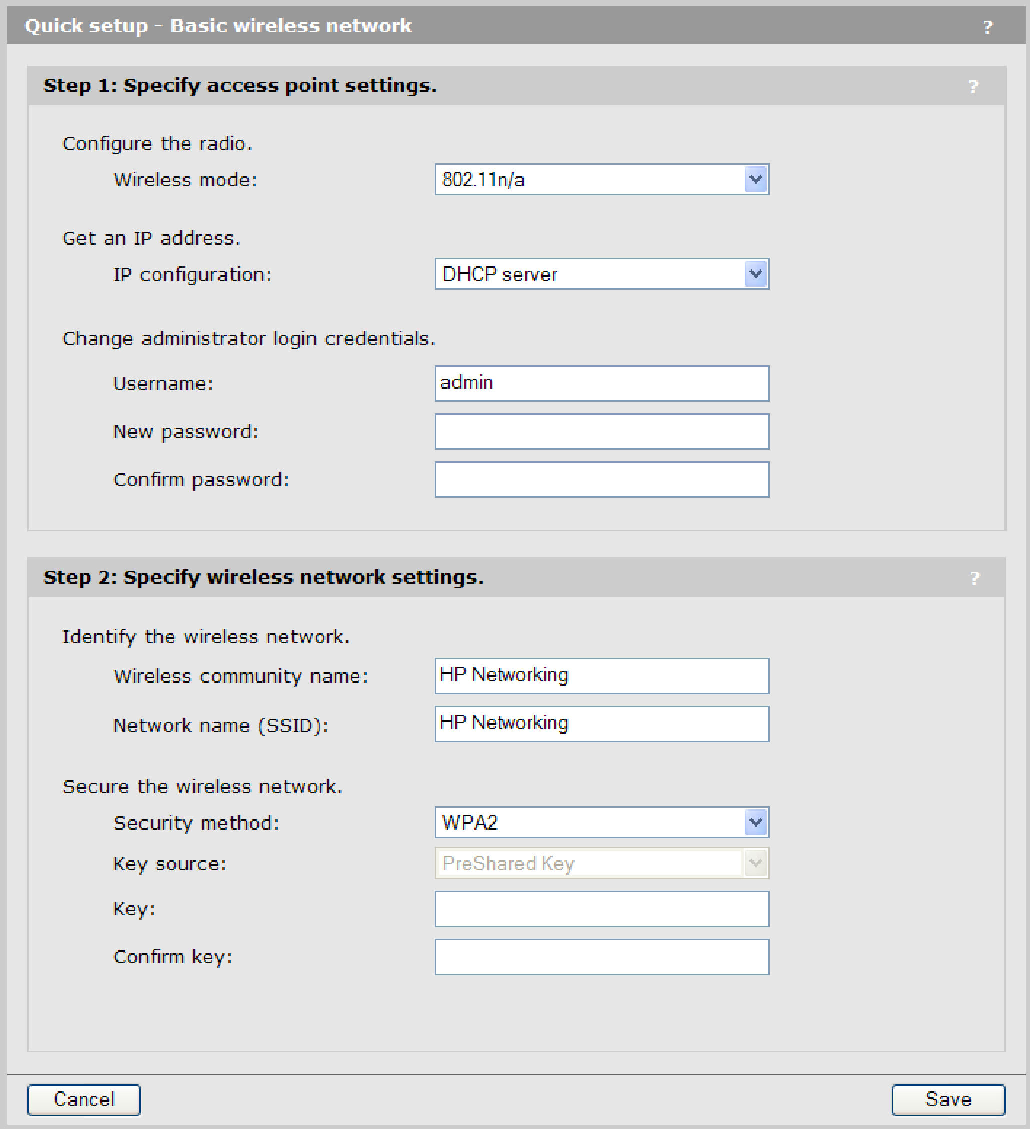
Quick setup can help you to configure the V-M200 for several different networking environments. Select the option that most closely matches your needs and then click OK.

● Recommend wireless network settings based upon your network environment.

Network environment: Basic wireless network

○ Manually configure wireless network settings.

Click **OK** to display the configuration page for the scenario.



Quick setup - Basic wireless network

Step 1: Specify access point settings.

Configure the radio.

Wireless mode: 802.11n/a

Get an IP address.

IP configuration: DHCP server

Change administrator login credentials.

Username: admin

New password:

Confirm password:

Step 2: Specify wireless network settings.

Identify the wireless network.

Wireless community name: HP Networking

Network name (SSID): HP Networking

Secure the wireless network.

Security method: WPA2

Key source: PreShared Key

Key:

Confirm key:

Step 1: Specify wireless network settings

For a complete description of all settings see:

- *Step 1: Configure access point settings on page 2-21*.
- The online help for this section.

Step 2: Specify wireless network settings

Identify the wireless network

Use this section to define names for the wireless community.

Community name

Specify a name to identify the community on the V-M200.

Network name (SSID)

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

By default, the V-M200 will broadcast this name so that wireless users can see it when they try to connect to the wireless network.

Secure the wireless network

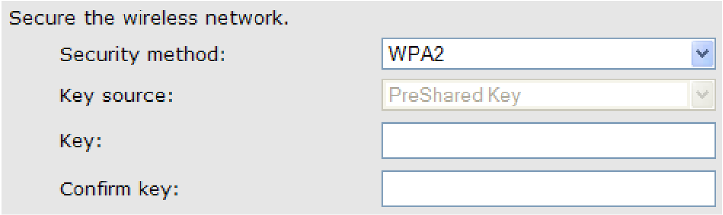
Use this section to define security settings for the wireless network.

Security method

Choose the method that will be used to protect wireless transmissions. Refer to the sections that follow for configuration details.

WPA, WPA2, WPA or WPA2

Wi-Fi Protected Access (WPA) is a security protocol that provides for both encryption of the wireless data stream (via TKIP or AES/CCMP) and authentication of wireless users (via 802.1X/EAP).



Secure the wireless network.

Security method: WPA2

Key source: PreShared Key

Key:

Confirm key:

The following versions are supported:

Version	Description
WPA	WPA with TKIP encryption. WPA cannot be used when the radio operating mode supports 802.11n.
WPA2	WPA2 (802.11i) with CCMP encryption. If all your clients are WPA2, select this option for the maximum possible security.
WPA or WPA2	Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time. Some legacy WPA clients may not work if this mode is selected. This mode is slightly less secure than using the pure WPA2 mode.

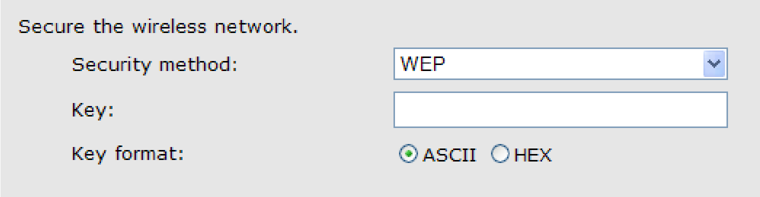
Key source

This scenario only supports the use of a **PreShared key**.

- **Key:** The V-M200 uses the key you specify in this field to generate the TKIP or AES/CCMP keys that are used to encrypt the wireless data stream. This key must be configured by each user in their WPA software. Specify a key that is between 8 and 63 alphanumeric characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers. The double quote character (") should not be used.

WEP

This is the least secure method of protecting wireless transmissions. WEP is provided to so you can support client stations that do not have WPA software.



Secure the wireless network.

Security method: WEP

Key:

Key format: ● ASCII ○ HEX

Note WEP cannot be used when the radio operating mode supports 802.11n.

Key

The number of characters you specify for the key determines the level of encryption.

- For 40-bit encryption, specify 5 ASCII characters or 10 hexadecimal digits.
- For 128-bit encryption, specify 13 ASCII characters or 26 hexadecimal digits.

When encryption is enabled, wireless stations that do not support encryption cannot communicate with the V-M200. The definition for each encryption key must be the same on the V-M200 and all client stations.

Key format

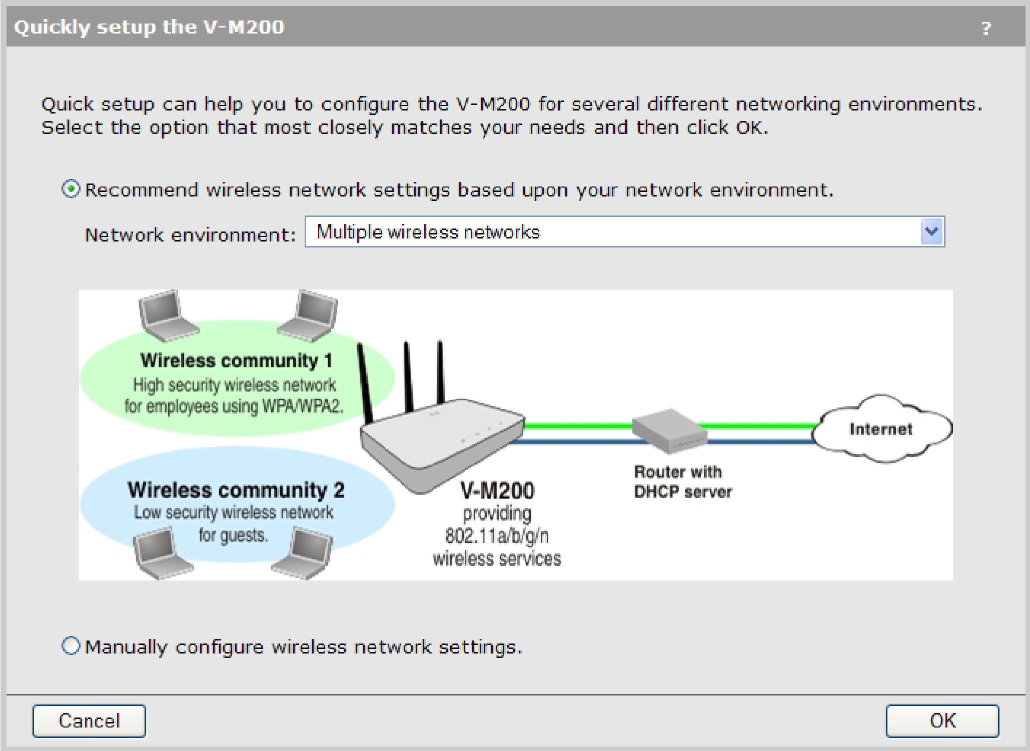
Select the format used to specify the encryption key:

- **ASCII:** ASCII keys are much weaker than carefully chosen HEX keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client stations support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.
- **HEX:** Your keys should only include the following characters: 0-9, a-f, A-F.

Multiple wireless networks

Choose this option if you want to create multiple wireless networks to support users with different networking requirements. For example, you could create two wireless networks, one for employees and one for guests. The guest network could be given a lower priority so employee traffic is never delayed due to excessive guest traffic.

This option can be used to connect the V-M200 to a network using either static IP addressing or DHCP.



Quickly setup the V-M200

Quick setup can help you to configure the V-M200 for several different networking environments. Select the option that most closely matches your needs and then click OK.

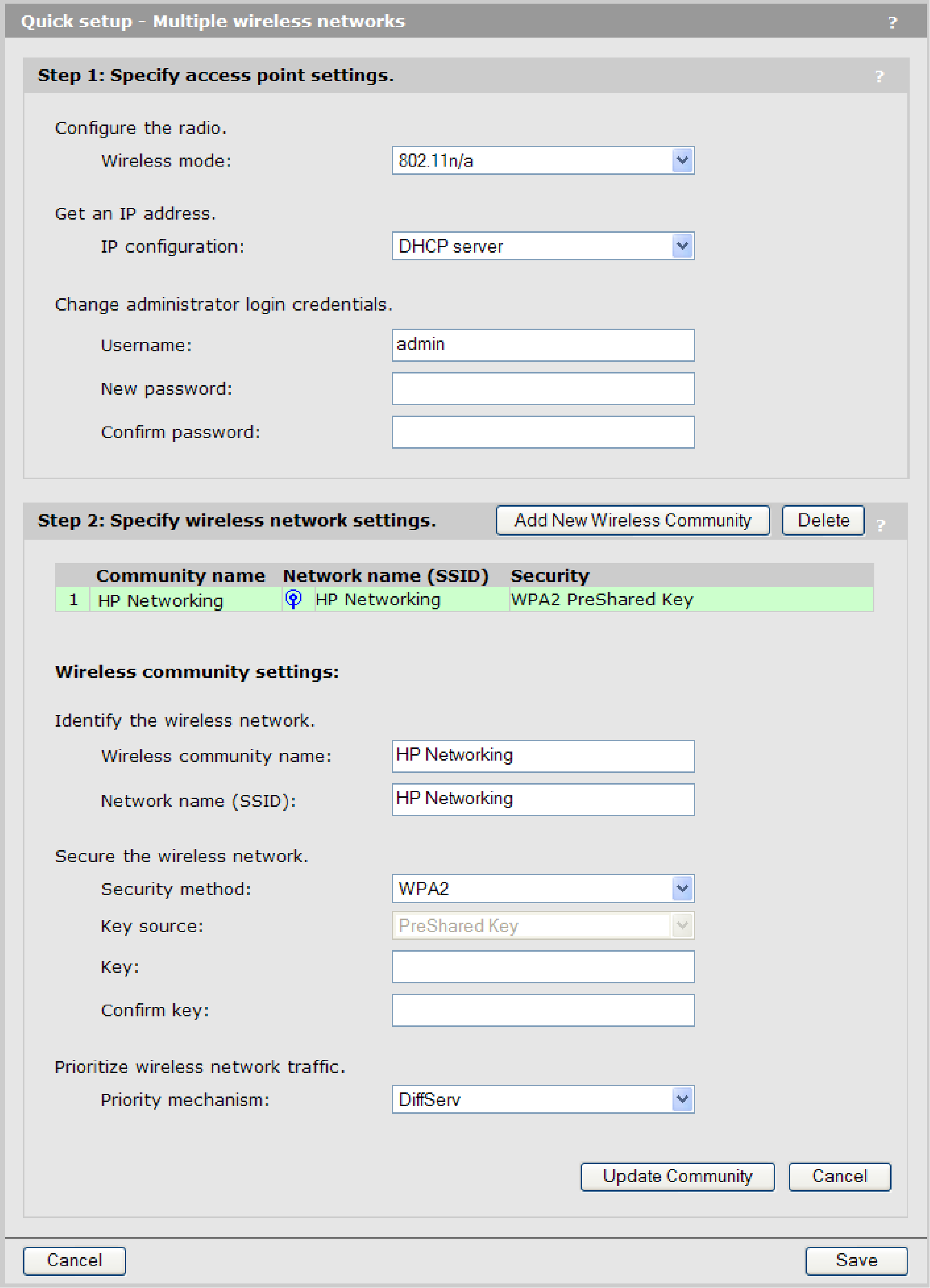
● Recommend wireless network settings based upon your network environment.

Network environment: Multiple wireless networks

○ Manually configure wireless network settings.

?
Wireless community 1
High security wireless network for employees using WPA/WPA2.
Wireless community 2
Low security wireless network for guests.
V-M200
providing 802.11a/b/g/n wireless services
Router with DHCP server
Internet
Cancel
OK

Click **OK** to display the configuration page for the scenario.



Quick setup - Multiple wireless networks
?

Step 1: Specify access point settings.

Configure the radio.

Wireless mode:	802.11n/a

Get an IP address.

IP configuration:	DHCP server

Change administrator login credentials.

Username:	admin
New password:	
Confirm password:	

Step 2: Specify wireless network settings.

Add New Wireless Community
Delete

	Community name	Network name (SSID)	Security
1	HP Networking	HP Networking	WPA2 PreShared Key

Wireless community settings:

Identify the wireless network.

Wireless community name:	HP Networking
Network name (SSID):	HP Networking

Secure the wireless network.

Security method:	WPA2
Key source:	PreShared Key
Key:	
Confirm key:	

Prioritize wireless network traffic.

Priority mechanism:	DiffServ

Step 1: Specify wireless network settings

For a complete description of all settings see:

- *Step 1: Configure access point settings on page 2-21*.
- The online help for this section.

Step 2: Specify wireless network settings

Buttons

Add New Wireless Community

Select this button to add a new wireless community to the table. The V-M200 supports up to four wireless communities. After you add a new community, configure its settings using the fields under **Wireless community settings**. Select **Update Community** when you are done.

Delete

Select this button to delete the selected wireless community. (The one that is currently being edited.) If the community is configured to use a RADIUS server for WPA authentication, the RADIUS profile created when the community was added is also deleted if it is not being used by another wireless community.

Update Community

Select this button to update the community with your configuration settings. The settings are not saved until you select the **Save** button.

Cancel

Select this button to discard your settings.

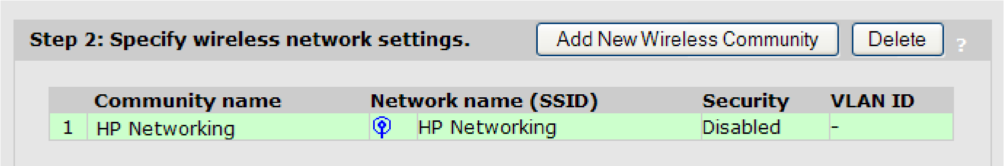
Save

Select this button to save your settings.

Wireless community table

This table lists all wireless communities that are defined on the V-M200. The V-M200 supports up to four wireless communities. Each wireless community defines the settings for a distinct wireless network with its own configuration settings.

To edit the settings for a community, select the community in the table, then configure the fields under **Wireless community settings**. Select **Update Community** when you are done.



Step 2: Specify wireless network settings.

	Community name	Network name (SSID)	Security	VLAN ID
1	HP Networking	HP Networking	Disabled	-

Wireless community settings

The following sections present the settings for the selected wireless community.

Identify the wireless network

Use this section to define names for the wireless community.

Community name

Specify a name to identify the community on the V-M200.

Network name (SSID)

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

By default, the V-M200 will broadcast this name so that wireless users can see it when they try to connect to the wireless network.

Secure the wireless network

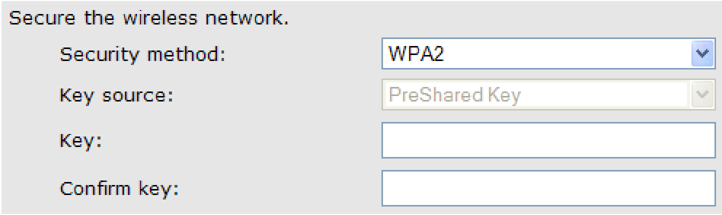
Use this section to define security settings for the wireless network.

Security method

Choose the method that will be used to protect wireless transmissions. Refer to the sections that follow for configuration details.

WPA, WPA2, WPA or WPA2

Wi-Fi Protected Access (WPA) is a security protocol that provides for both encryption of the wireless data stream (via TKIP or AES/CCMP) and authentication of wireless users (via 802.1X/EAP).



Secure the wireless network.

Security method: WPA2

Key source: PreShared Key

Key:

Confirm key:

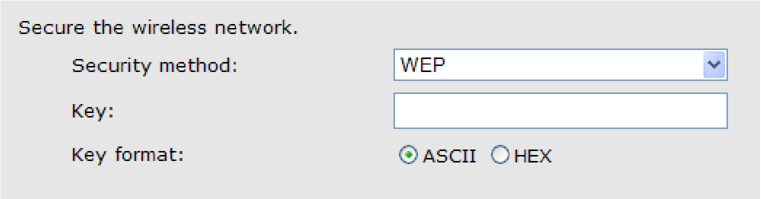
The following versions are supported:

Version	Description
WPA	WPA with TKIP encryption. WPA cannot be used when the radio operating mode supports 802.11n.
WPA2	WPA2 (802.11i) with CCMP encryption. If all your clients are WPA2, select this option for the maximum possible security.
WPA or WPA2	Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time. Some legacy WPA clients may not work if this mode is selected. This mode is slightly less secure than using the pure WPA2 mode.

Key source
This scenario only supports the use of a **PreShared key**.

- **Key:** The V-M200 uses the key you specify in this field to generate the TKIP or AES/CCMP keys that are used to encrypt the wireless data stream. This key must be configured by each user in their WPA software. Specify a key that is between 8 and 63 alphanumeric characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers. The double quote character (”) should not be used.

WEP
This is the least secure method of protecting wireless transmissions. WEP is provided to so you can support client stations that do not have WPA software.



Secure the wireless network.

Security method: WEP

Key:

Key format: ● ASCII ○ HEX

Note WEP cannot be used when the radio operating mode supports 802.11n.

Key
The number of characters you specify for the key determines the level of encryption.

- For 40-bit encryption, specify 5 ASCII characters or 10 hexadecimal digits.
- For 128-bit encryption, specify 13 ASCII characters or 26 hexadecimal digits.

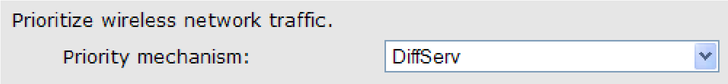
When encryption is enabled, wireless stations that do not support encryption cannot communicate with the V-M200. The definition for each encryption key must be the same on the V-M200 and all client stations.

Key format
Select the format used to specify the encryption key:

- **ASCII:** ASCII keys are much weaker than carefully chosen HEX keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client stations support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.
- **HEX:** Your keys should only include the following characters: 0-9, a-f, A-F.

Prioritize wireless network traffic

The quality of service (QoS) feature provides a number of different mechanisms to prioritize wireless traffic sent to wireless client stations.



Prioritize wireless network traffic.

Priority mechanism: DiffServ

This is useful when you have defined multiple wireless communities and want to ensure a specific level of service for each one.

For example, if you have two communities, one for employees and one for guests, you might want to make the employee traffic higher priority so that employee traffic is never delayed due to excessive guest traffic.

Priority mechanism

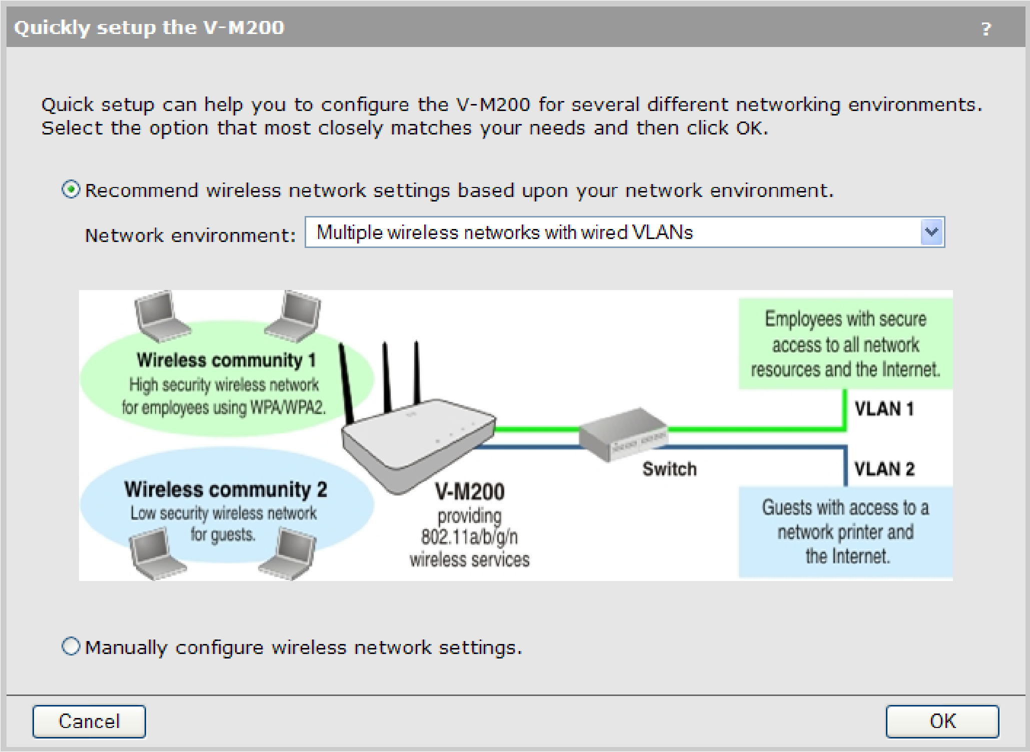
By default, Diffserv is used. Unless you have specific requirements you can leave this setting. For a complete description of all options, see *Quality of service (QoS) on page 4-15*.

Multiple wireless networks with wired VLANS

Choose this option if you want to:

- Create multiple wireless networks to support users with different requirements.
- Map the traffic from each wireless network to a specific VLAN.

This option can be used to connect the V-M200 to a network using either static IP addressing or DHCP.



Quickly setup the V-M200

Quick setup can help you to configure the V-M200 for several different networking environments. Select the option that most closely matches your needs and then click OK.

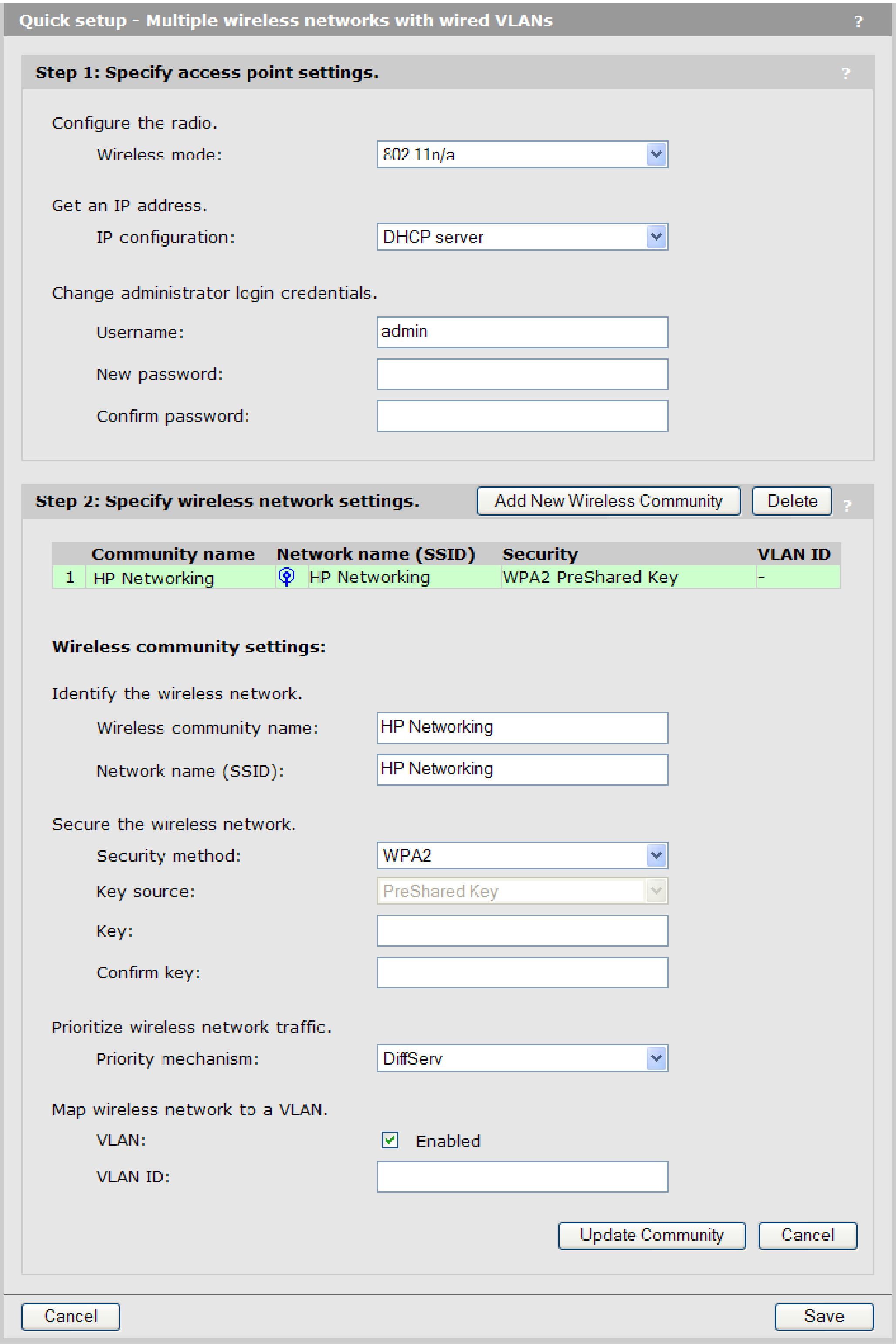
● Recommend wireless network settings based upon your network environment.

Network environment: Multiple wireless networks with wired VLANs

Wireless community 1
High security wireless network for employees using WPA/WPA2.
Wireless community 2
Low security wireless network for guests.
V-M200
providing 802.11a/b/g/n wireless services
Switch
Employees with secure access to all network resources and the Internet.
VLAN 1
VLAN 2
Guests with access to a network printer and the Internet.

○ Manually configure wireless network settings.

Click **OK** to display the configuration page for the scenario.



Quick setup - Multiple wireless networks with wired VLANs

Step 1: Specify access point settings.

Configure the radio.

Wireless mode:	802.11n/a

Get an IP address.

IP configuration:	DHCP server

Change administrator login credentials.

Username:	admin
New password:	
Confirm password:	

Step 2: Specify wireless network settings.

	Community name	Network name (SSID)	Security	VLAN ID
1	HP Networking	HP Networking	WPA2 PreShared Key	-

Wireless community settings:

Identify the wireless network.

Wireless community name:	HP Networking
Network name (SSID):	HP Networking

Secure the wireless network.

Security method:	WPA2
Key source:	PreShared Key
Key:	
Confirm key:	

Prioritize wireless network traffic.

Priority mechanism:	DiffServ

Map wireless network to a VLAN.

VLAN:	☑ Enabled
VLAN ID:	

Step 1: Specify wireless network settings

For a complete description of all settings see:

- *Step 1: Configure access point settings on page 2-21*.
- The online help for this section.

Step 2: Specify wireless network settings

Buttons

Add New Wireless Community

Select this button to add a new wireless community to the table. The V-M200 supports up to four wireless communities. After you add a new community, configure its settings using the fields under **Wireless community settings**. Select **Update Community** when you are done.

Delete

Select this button to delete the selected wireless community. (The one that is currently being edited.) If the community is configured to use a RADIUS server for WPA authentication, the RADIUS profile created when the community was added is also deleted if it is not being used by another wireless community.

Update Community

Select this button to update the community with your configuration settings. The settings are not saved until you select the **Save** button.

Cancel

Select this button to discard your settings.

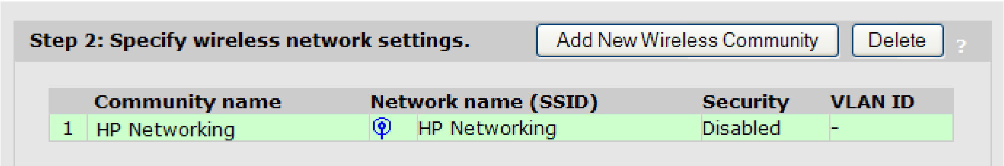
Save

Select this button to save your settings.

Wireless community table

This table lists all wireless communities that are defined on the V-M200. The V-M200 supports up to four wireless communities. Each wireless community defines the settings for a distinct wireless network with its own configuration settings.

To edit the settings for a community, select the community in the table, then configure the fields under **Wireless community settings**. Select **Update Community** when you are done.


Step 2: Specify wireless network settings.
Add New Wireless Community
Delete
?

	Community name	Network name (SSID)	Security	VLAN ID
1	HP Networking	HP Networking	Disabled	-

Wireless community settings

The following sections present the settings for the selected wireless community.

Identify the wireless network

Use this section to define names for the wireless community.

Community name

Specify a name to identify the community on the V-M200.

Network name (SSID)

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

By default, the V-M200 will broadcast this name so that wireless users can see it when they try to connect to the wireless network.

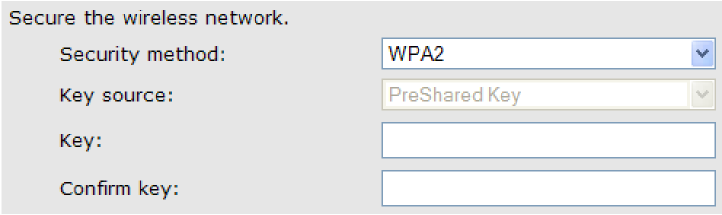
Secure the wireless network

Use this section to define security settings for the wireless network.

Security method

Choose the method that will be used to protect wireless transmissions. Refer to the sections that follow for configuration details.

WPA, WPA2, WPA or WPA2
Wi-Fi Protected Access (WPA) is a security protocol that provides for both encryption of the wireless data stream (via TKIP or AES/CCMP) and authentication of wireless users (via 802.1X/EAP).



Secure the wireless network.

Security method: WPA2

Key source: PreShared Key

Key:

Confirm key:

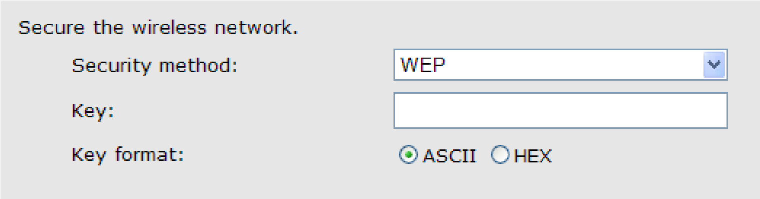
The following versions are supported:

Version	Description
WPA	WPA with TKIP encryption. WPA cannot be used when the radio operating mode supports 802.11n.
WPA2	WPA2 (802.11i) with CCMP encryption. If all your clients are WPA2, select this option for the maximum possible security.
WPA or WPA2	Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time. Some legacy WPA clients may not work if this mode is selected. This mode is slightly less secure than using the pure WPA2 mode.

Key source
This scenario only supports the use of a **PreShared key**.

- **Key:** The V-M200 uses the key you specify in this field to generate the TKIP or AES/CCMP keys that are used to encrypt the wireless data stream. This key must be configured by each user in their WPA software. Specify a key that is between 8 and 63 alphanumeric characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers. The double quote character (") should not be used.

WEP
This is the least secure method of protecting wireless transmissions. WEP is provided to so you can support client stations that do not have WPA software.



Secure the wireless network.

Security method: WEP

Key:

Key format: ● ASCII ○ HEX

Note WEP cannot be used when the radio operating mode supports 802.11n.

Key
The number of characters you specify for the key determines the level of encryption.

- For 40-bit encryption, specify 5 ASCII characters or 10 hexadecimal digits.
- For 128-bit encryption, specify 13 ASCII characters or 26 hexadecimal digits.

When encryption is enabled, wireless stations that do not support encryption cannot communicate with the V-M200. The definition for each encryption key must be the same on the V-M200 and all client stations.

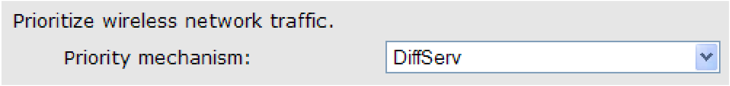
Key format

Select the format used to specify the encryption key:

- **ASCII:** ASCII keys are much weaker than carefully chosen HEX keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client stations support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.
- **HEX:** Your keys should only include the following characters: 0-9, a-f, A-F.

Prioritize wireless network traffic

The quality of service (QoS) feature provides a number of different mechanisms to prioritize wireless traffic sent to wireless client stations.



Prioritize wireless network traffic.

Priority mechanism: DiffServ

This is useful when you have defined multiple wireless communities and want to ensure a specific level of service for each one.

For example, if you have two communities, one for employees and one for guests, you might want to make the employee traffic higher priority so that employee traffic is never delayed due to excessive guest traffic.

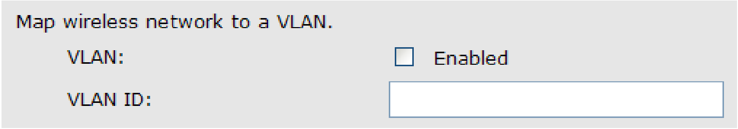
Priority mechanism

By default, Diffserv is used. Unless you have specific requirements you can leave this setting. For a complete description of all options, see *Quality of service (QoS) on page 4-15*.

Map wireless network to a VLAN

Use this option to bind the wireless community to a specific VLAN on the Ethernet port. All traffic sent by the wireless community will be assigned to the VLAN you specify when it exits the Ethernet port. The VLAN is not used for wireless traffic.

If you do not set a VLAN, traffic is sent untagged.



Map wireless network to a VLAN.

VLAN: □ Enabled

VLAN ID:

VLAN

Select this checkbox to enable VLAN support.

VLAN ID

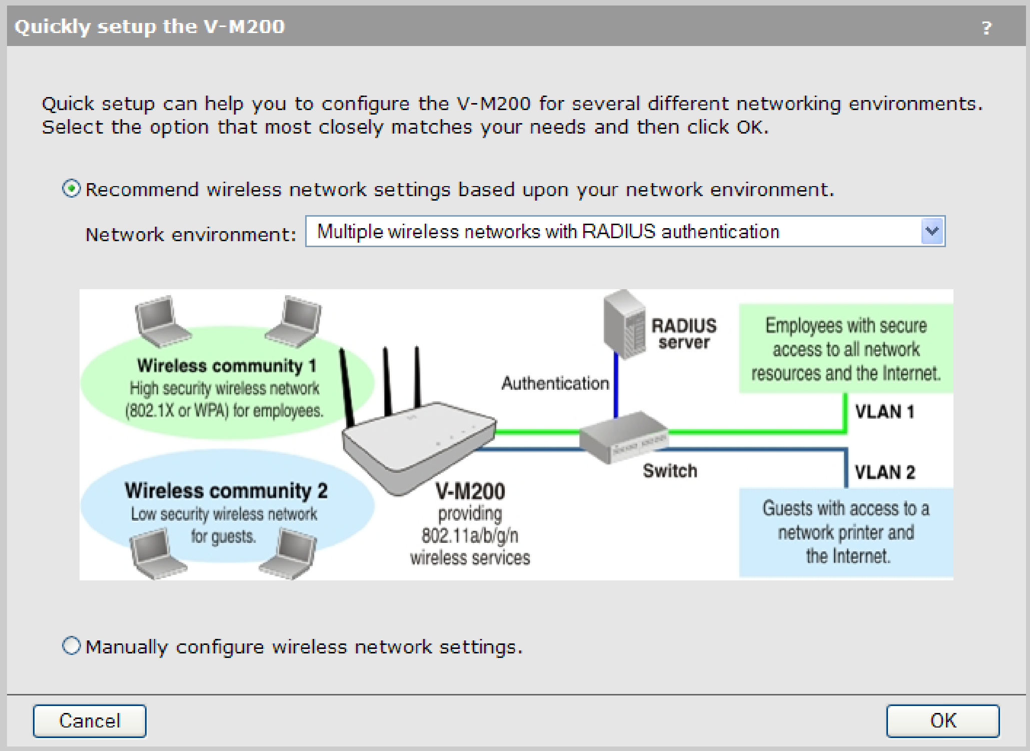
Specify the VLAN ID to assign to this community.

Multiple wireless networks with RADIUS authentication

Choose this option if you want to:

- Create multiple wireless networks to support users with different requirements.
- Map the traffic from each wireless network to a specific VLAN.
- Authenticate user login credentials using a third-party RADIUS server.

This option can be used to connect the V-M200 to a network using either static IP addressing or DHCP.



Quickly setup the V-M200

Quick setup can help you to configure the V-M200 for several different networking environments. Select the option that most closely matches your needs and then click OK.

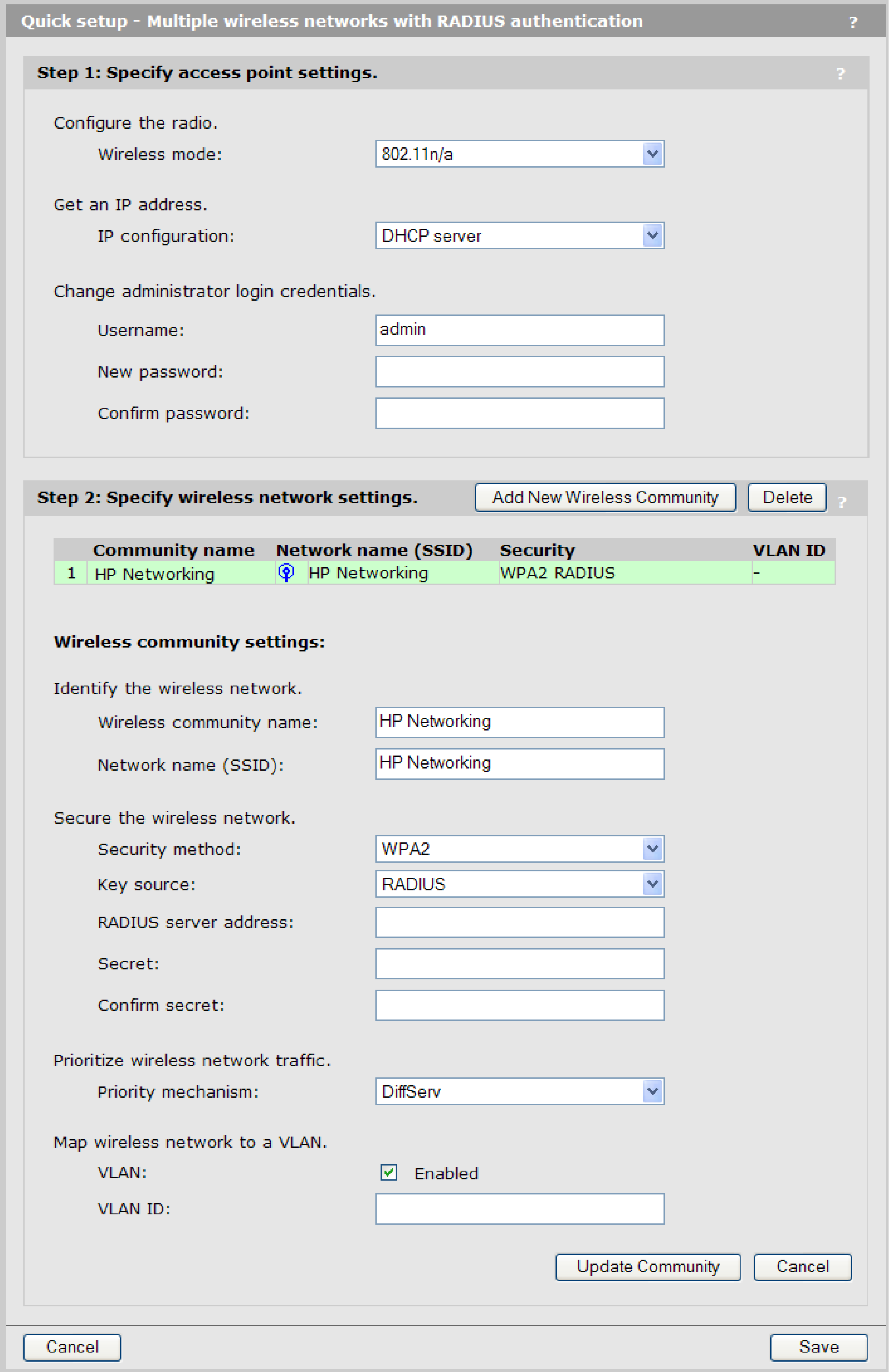
● Recommend wireless network settings based upon your network environment.

Network environment: Multiple wireless networks with RADIUS authentication

○ Manually configure wireless network settings.

?
Wireless community 1
High security wireless network (802.1X or WPA) for employees.
Wireless community 2
Low security wireless network for guests.
V-M200
providing
802.11a/b/g/n
wireless services
Authentication
RADIUS server
Switch
Employees with secure access to all network resources and the Internet.
VLAN 1
VLAN 2
Guests with access to a network printer and the Internet.
Cancel
OK

Click **OK** to display the configuration page for the scenario.



Quick setup - Multiple wireless networks with RADIUS authentication

Step 1: Specify access point settings.

Configure the radio.

Wireless mode:	802.11n/a

Get an IP address.

IP configuration:	DHCP server

Change administrator login credentials.

Username:	admin
New password:	
Confirm password:	

Step 2: Specify wireless network settings.

	Community name	Network name (SSID)	Security	VLAN ID
1	HP Networking	HP Networking	WPA2 RADIUS	-

Wireless community settings:

Identify the wireless network.

Wireless community name:	HP Networking
Network name (SSID):	HP Networking

Secure the wireless network.

Security method:	WPA2
Key source:	RADIUS
RADIUS server address:	
Secret:	
Confirm secret:	

Prioritize wireless network traffic.

Priority mechanism:	DiffServ

Map wireless network to a VLAN.

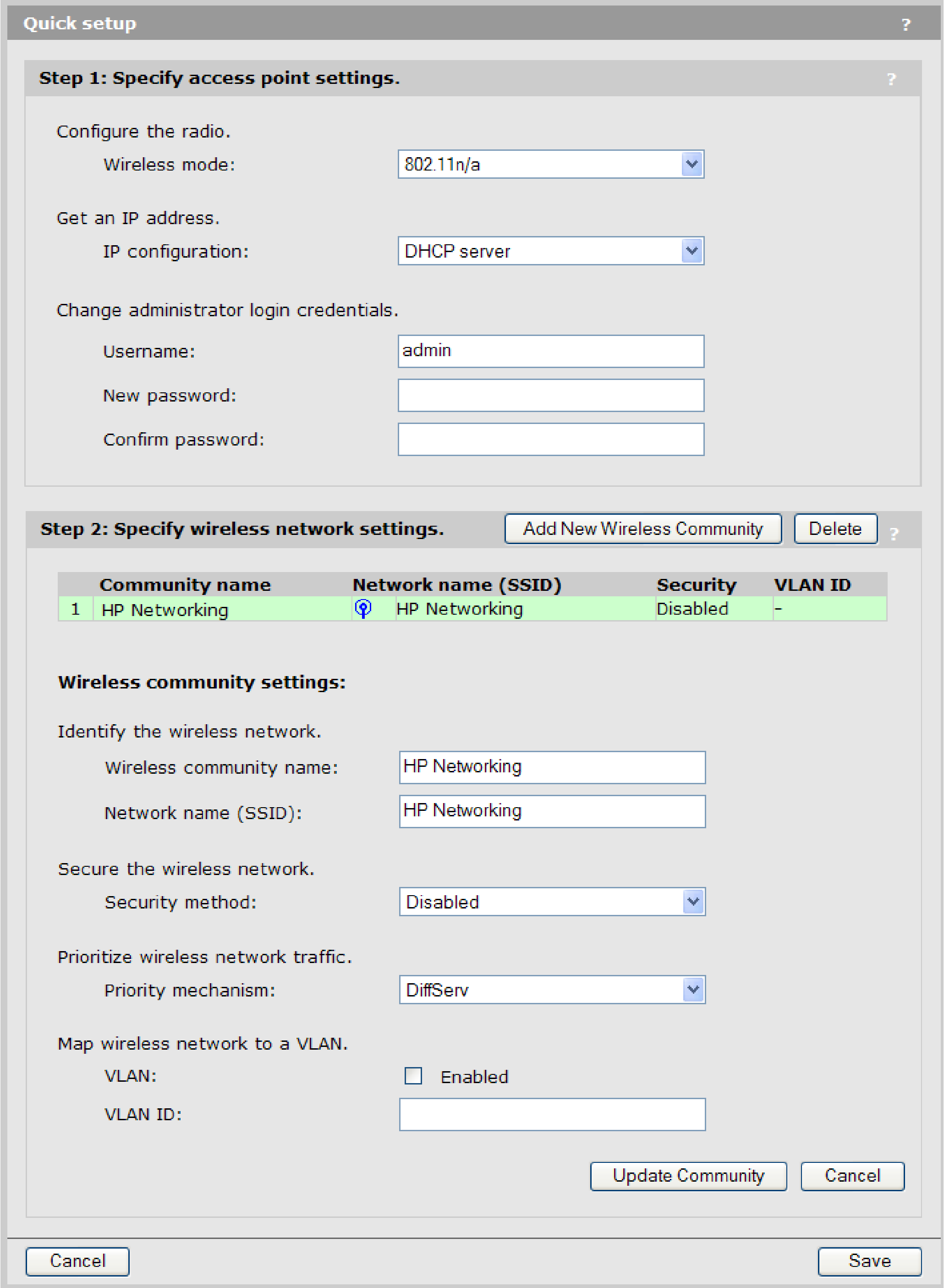
VLAN:	☑ Enabled
VLAN ID:	

For a complete description of all settings see:

- *Global settings page on page 2-20*.
- The online help for this page.

Global settings page

If you manually launch Quick Setup by selecting **Home > Quick setup**, you will see the Quick Setup global settings page. This page shows all the settings that are supported by all Quick Setup scenarios. See the sections that follow for complete descriptions of each setting.



Step 1: Specify access point settings.

Configure the radio.

Wireless mode: 802.11n/a

Get an IP address.

IP configuration: DHCP server

Change administrator login credentials.

Username: admin

New password:

Confirm password:

Step 2: Specify wireless network settings.

	Community name		Network name (SSID)	Security	VLAN ID
1	HP Networking		HP Networking	Disabled	-

Wireless community settings:

Identify the wireless network.

Wireless community name: HP Networking

Network name (SSID): HP Networking

Secure the wireless network.

Security method: Disabled

Prioritize wireless network traffic.

Priority mechanism: DiffServ

Map wireless network to a VLAN.

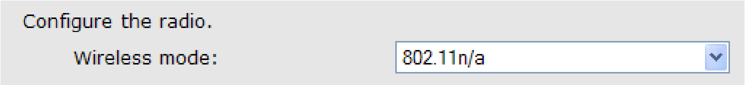
VLAN: ☐ Enabled

VLAN ID:

Step 1: Configure access point settings

Configure the radio

Use this section to set the radio operating mode.



Configure the radio.

Wireless mode: 802.11n/a

Wireless mode

Select the mode that best supports the wireless client stations at your location.

Supported wireless modes are determined by the regulatory domain (country) in which the V-M200 is configured to operate. Available options may include one or more of the following:

- **802.11n (5 GHz):** (Pure 802.11n) Supports up to 300 Mbps in the 802.11n 5 GHz frequency band.
- **802.11n/a:** (Compatibility mode.) Supports up to 270 Mbps for 802.11n and 54 Mbps for 802.11a in the 5 GHz frequency band.
- **802.11n (2.4 GHz):** (Pure 802.11n) Supports up to 144.4 Mbps in the 802.11n 2.4 GHz frequency band.
- **802.11n/g:** (Compatibility mode.) Supports up to 130 Mbps for 802.11n and 54 Mbps for 802.11g in the 2.4 GHz frequency band. Only use this setting when support for 802.11g is necessary.
- **802.11n/b/g:** (Compatibility mode.) Up to 130 Mbps for 802.11n, 54 Mbps for 802.11g, and 11 Mbps for 802.11b in the 2.4 GHz frequency band. Only use this setting when support for 802.11b is necessary.
- **802.11b**: Supports up to 11 Mbps in the 2.4 GHz frequency band.
- **802.11b/g**: Supports up to 11 and 54 Mbps in the 2.4 GHz frequency band.
- **802.11g**: Supports up to 54 Mbps in the 2.4 GHz frequency band.
- **802.11a**: Supports up to 54 Mbps in the 5 GHz frequency band.

Note

- In **802.11n (2.4)** and **802.11n (5 GHz)** modes, the V-M200 does not permit non-802.11n clients to associate. Also in these modes, the V-M200 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 (a/b/g) APs operating on the same channel, but provides the best throughput for the V-M200 and its 11n clients.
- In **802.11n/a, 802.11n/g, 802.11n/b/g** modes, the V-M200 permits both 802.11n and legacy clients (a/b/g) to associate. The V-M200 uses protection mechanisms (RTS/CTS or CTS-to-self) when sending 11n data to prevent disruption to legacy (a/b/g) clients associated on the same channel.

Get an IP address

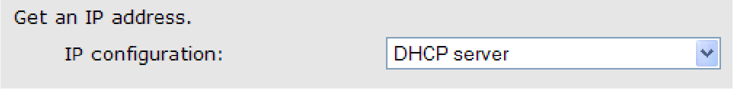
Use this section to configure how an IP address is assigned to the V-M200.

IP configuration

Select the method that will be used to assign an IP address to the Ethernet port on the V-M200.

DHCP server

The V-M200 will operate as a DHCP client and automatically obtain an IP address from a DHCP server on the network connected to the Ethernet port. If no DHCP server is found, the IP address 192.168.1.1 is assigned to the Ethernet and wireless ports.

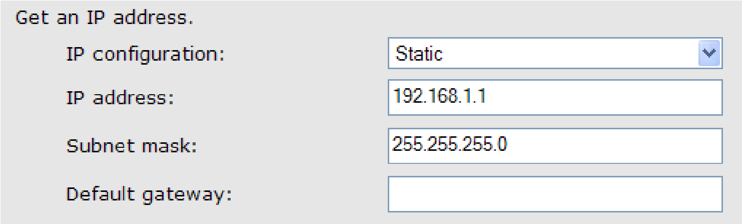


Get an IP address.

IP configuration:	DHCP server

Static

You must manually specify the IP address, subnet mask, and default gateway to assign to the Ethernet port. By default, the address **192.168.1.1** is assigned.



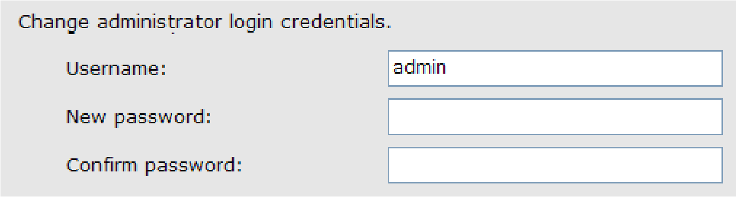
Get an IP address.

IP configuration:	Static
IP address:	192.168.1.1
Subnet mask:	255.255.255.0
Default gateway:	

- **IP address:** Specify the IP address you want to assign to the Ethernet port in the format: **n.n.n.n**, where **n** is a number between 1 and 255.
- **Subnet mask:** Specify the appropriate subnet mask for the IP address you specified in the format: **n.n.n.n**, where **n** is a number between 1 and 255.
- **Default gateway:** Specify the IP address of the default gateway in the format: **n.n.n.n**, where **n** is a number between 1 and 255. This is generally the address of the device on the wired network that provides access to the Internet.

Change administrator login credentials

Use these settings to change the username and password for the manager account. If you leave the **Username** and **Password** fields blank and then select **Save**, no change is made to the current manager username and password.



Change administrator login credentials.

Username:	admin
New password:	
Confirm password:	

Username

Specify a new login name for the V-M200 manager account. By default, the username is set to **admin**.

New password
Confirm password

Specify a new password for the V-M200 manager account. By default, the password is set to **admin**.

Passwords must be 6 to 16 printable ASCII characters in length, and contain at least 4 different characters. Passwords are case sensitive. Space characters and double quotes (“) cannot be used.

Step 2: Specify wireless network settings

Buttons

Add New Wireless Community

Select this button to add a new wireless community to the table. After you add a new community, configure its settings using the fields under **Wireless community settings**. Select **Add Community** when you are done.

Delete

Select this button to delete the selected wireless community. (The one that is currently being edited.) If the community is configured to use a RADIUS server for WPA or 802.1X authentication, the RADIUS profile created when the community was added is also deleted if it is not being used by another wireless community.

Update Community

Select this button to update the community with your configuration settings. The settings are not saved until you select the **Save** button.

Cancel

Select this button to discard your settings.

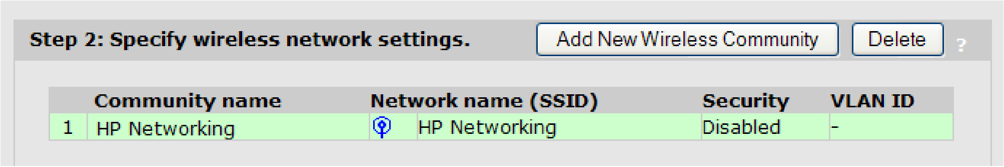
Save

Select this button to save your settings.

Wireless community table

This table lists all wireless communities that are defined on the V-M200. The V-M200 supports up to four wireless communities. Each wireless community defines the settings for a distinct wireless network with its own configuration settings.

To edit the settings for a community, select the community in the table, then configure the fields under **Wireless community settings**. Select **Update Community** when you are done.



Step 2: Specify wireless network settings.

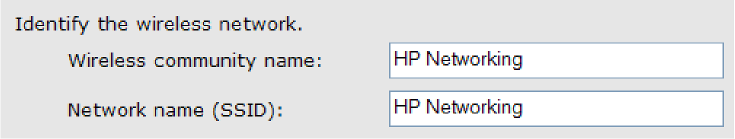
	Community name	Network name (SSID)	Security	VLAN ID
1	HP Networking	HP Networking	Disabled	-

Wireless community settings

The following sections present the settings for the selected wireless community.

Identify the wireless network

Use this section to define names for the wireless community.



Identify the wireless network.

Wireless community name:	HP Networking
Network name (SSID):	HP Networking

Community name

Specify a name to identify the community on the V-M200.

Network name (SSID)

Specify a name to uniquely identify the wireless network associated with this community.

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

Secure the wireless network

Use this section to define security settings for the wireless network.

Security method

Choose the method that will be used to protect wireless transmissions. Refer to the sections that follow for configuration details.

WPA, WPA2, WPA or WPA2

Wi-Fi Protected Access (WPA) is a security protocol that provides for both encryption of the wireless data stream (via TKIP or AES/CCMP) and authentication of wireless users (via 802.1X/EAP).The following versions are supported:

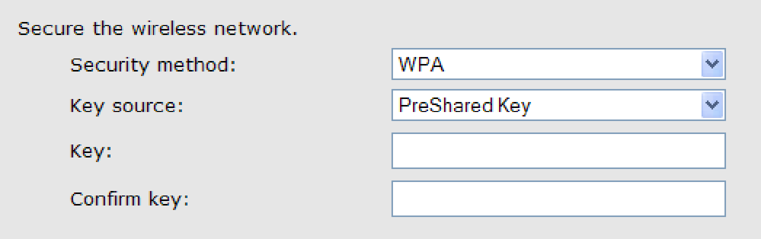
Version	Description
WPA	WPA with TKIP encryption.
WPA2	WPA2 (802.11i) with CCMP encryption. If all your clients are WPA2, select this option for the maximum possible security.
WPA or WPA2	Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time. Some legacy WPA clients may not work if this mode is selected. This mode is slightly less secure than using the pure WPA2 mode.

Note WPA cannot be used when the radio operating mode supports 802.11n.

Key source

This option determines how the WPA encryption keys are generated.

- **PreShared Key**: The V-M200 uses a statically defined key to encrypt traffic. To connect to this community, wireless users must configure their WPA software with this key.



Secure the wireless network.

Security method: WPA

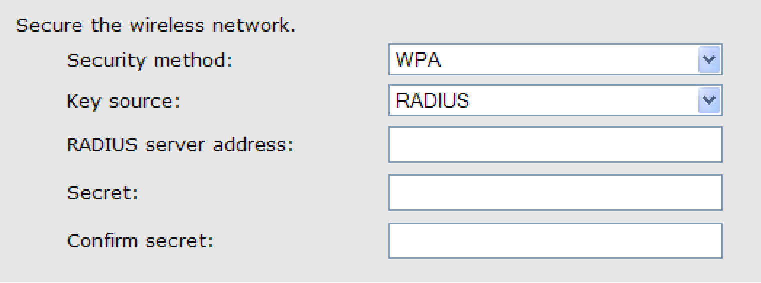
Key source: PreShared Key

Key:

Confirm key:

- **Key:** The V-M200 uses the key you specify in this field to generate the TKIP or AES/CCMP keys that are used to encrypt the wireless data stream. Since this is a static key, it is not as secure as the RADIUS option. Specify a key that is between 8 and 63 alphanumeric characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers. The double quote character (”) should not be used.

- **RADIUS**: The V-M200 retrieves the key from the RADIUS server and uses it to generate the TKIP or AES/CCMP keys that are used to encrypt the wireless data stream. The key is dynamically generated by the RADIUS server each time the user logs in. Communication with the RADIUS server occurs via 802.1X using the EAP protocol specified by the user's WPA client software.



Secure the wireless network.

Security method: WPA

Key source: RADIUS

RADIUS server address:

Secret:

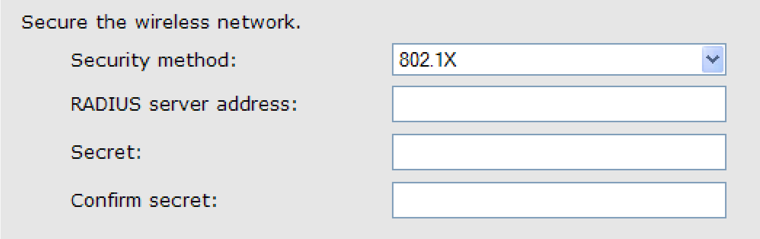
Confirm secret:

When you select this option, a RADIUS profile is created with the same name as the wireless community. To customize the settings for this RADIUS profile, select **Authentication > RADIUS profiles**. See *Using a third-party RADIUS server on page 7-2*.

  - **RADIUS server address:** Specify the IP address of the RADIUS server.
  - **Secret / Confirm secret:** Specify the secret (password) that V-M200 will use when communicating with the RADIUS server. The shared secret is used to authenticate all packets exchanged with the server to prove that they originate from a valid/trusted source.

802.1X

802.1X provides for user authentication via a third-party RADIUS server. By default, user traffic is not encrypted. To enable encryption, you need to edit the wireless community (select **Wireless > Communities**) and enable WEP encryption for 802.1X.



Secure the wireless network.

Security method: 802.1X

RADIUS server address:

Secret:

Confirm secret:

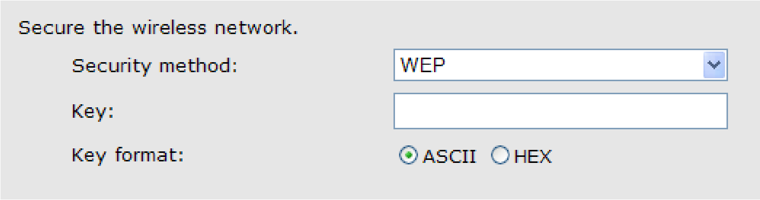
RADIUS server address

Specify the IP address of the RADIUS server.

Secret/Confirm secret

Specify the secret (password) that V-M200 will use when communicating with the RADIUS server. The shared secret is used to authenticate all packets exchanged with the server to prove that they originate from a valid/trusted source.

WEP
This is the least secure method of protecting wireless transmissions. WEP provides encryption only, no user authentication.


Secure the wireless network.

Security method: WEP

Key:

Key format: ● ASCII ○ HEX

Note WEP cannot be used when the radio operating mode supports 802.11n.

Key
The number of characters you specify for the key determines the level of encryption.

- For 40-bit encryption, specify 5 ASCII characters or 10 hexadecimal digits.
- For 128-bit encryption, specify 13 ASCII characters or 26 hexadecimal digits.

When encryption is enabled, wireless stations that do not support encryption cannot communicate with the V-M200. The definition for each encryption key must be the same on the V-M200 and all client stations.

Key format
Select the format used to specify the encryption key:

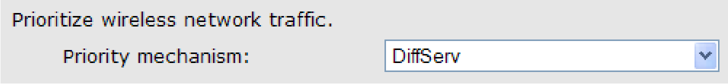
- **ASCII:** ASCII keys are much weaker than carefully chosen HEX keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client stations support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.
- **HEX:** Your keys should only include the following characters: 0-9, a-f, A-F.

Prioritize wireless network traffic

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 you have defined multiple wireless communities and want to ensure a specific level of service for each one.

For example, if you have two communities, one for employees and one for guests, you might want to make the employee traffic higher priority so that employee traffic is never delayed due to excessive guest traffic.


Prioritize wireless network traffic.

Priority mechanism: DiffServ

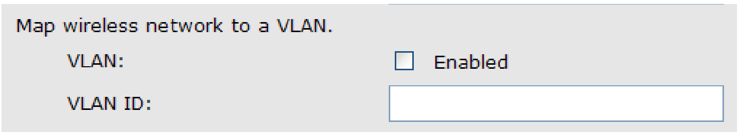
Priority mechanism

For a complete description of all options, see *Quality of service (QoS) on page 4-15*.

Map wireless network to a VLAN

Use this option to bind the wireless community to a specific VLAN on the Ethernet port. All traffic sent by the wireless community will be assigned to the VLAN you specify when it exits the Ethernet port. The VLAN is not used for wireless traffic.

If you do not set a VLAN, traffic is sent untagged.



Map wireless network to a VLAN.

VLAN: □ Enabled

VLAN ID:

A VLAN can be assigned on a per-user basis by setting an attribute in the user's RADIUS account (when using RADIUS-based authentication). RADIUS assigned VLANs take precedence over those assigned to the wireless community. For example, if the community has an Ethernet VLAN of 10, and a user receives a VLAN of 20 via RADIUS, all traffic for this user exits the Ethernet port on VLAN 20. Traffic for other users exits on VLAN 10.

See *Working with VLANs on page 6-4* for information on using this feature.

VLAN

Select this checkbox to enable VLAN support.

VLAN ID

Specify the VLAN ID to assign to this community.

3

Managing the V-M200

Contents

Management tool

The V-M200 is configured and monitored via its Web-based management tool at address **https://<*V-M200-ip-address*>** where **<*V-M200-ip-address*>** is the IP address assigned to the V-M200. Use Microsoft Internet explorer 7/8 or Firefox 3.x.

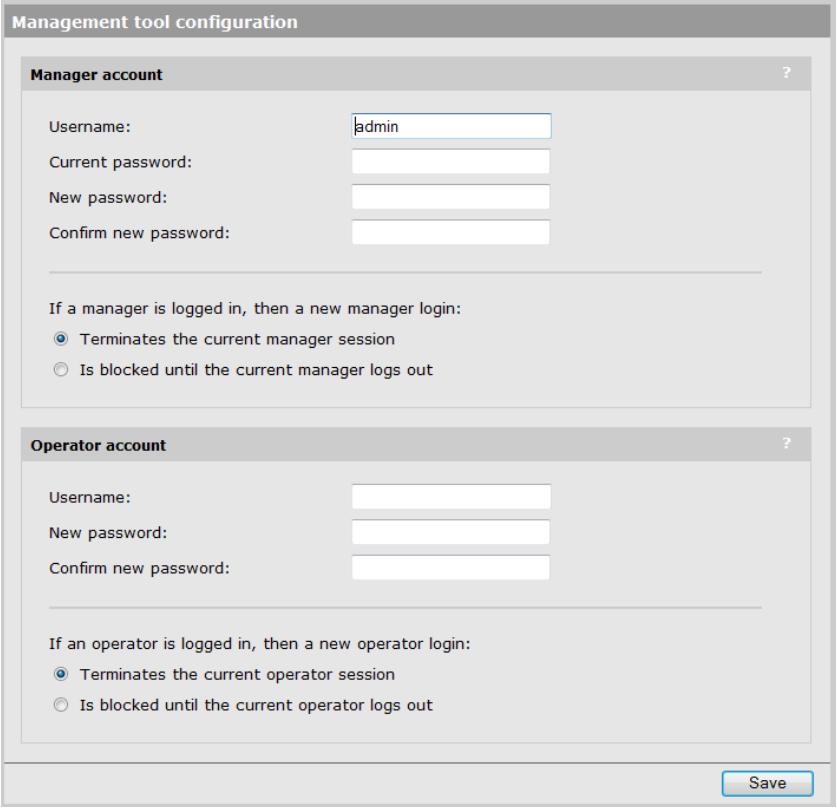
For information on launching the management tool for the first time, see the *HP V-M200 802.11n Access Point Quickstart*.

Note

A security certificate warning is displayed the first time you connect to the management tool. This is normal. Select whatever option is needed in your Web browser to continue to the management tool. The security warning will not appear again unless you change the IP address of the V-M200.

Customizing management tool settings

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



Management tool configuration

Manager account

Username: admin
Current password:
New password:
Confirm new password:

If a manager is logged in, then a new manager login:
● Terminates the current manager session
○ Is blocked until the current manager logs out

Operator account

Username:
New password:
Confirm new password:

If an operator is logged in, then a new operator login:
● Terminates the current operator session
○ Is blocked until the current operator logs out

About the manager and operator accounts

Two types of administrator accounts are available: manager and operator.

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

The management tool has an automatic **inactivity logout timer** that is set to five minutes. If a manager or operator is idle for five minutes, then they are automatically logged out.

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

Manager settings

- **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 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.

Operator settings

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

Passwords

Passwords must be 6 to 16 printable ASCII characters in length, with at least 4 different characters. Passwords are case sensitive. Space characters and double quotes (“) cannot be used.

Note

If you leave **Username** and **Password** fields blank and then select **Save**, no change is made to the current username and password.

Caution

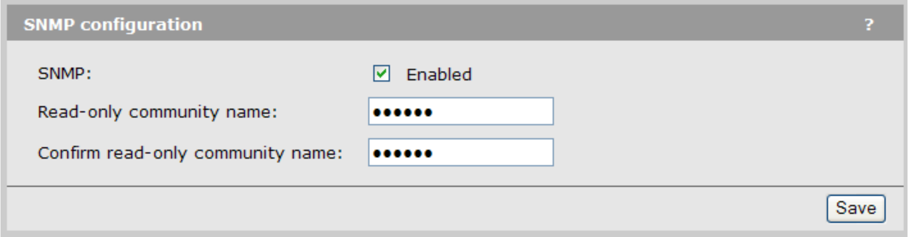
If you forget the manager password, the only way to access the manager account is to reset the V-M200 to factory default settings. For information see *Appendix B: Resetting to factory defaults on page B-1*.

SNMP

The V-M200 provides a robust SNMP v1/v2 implementation supporting both industry-standard MIB II objects as well as HP-specific MIBs.

Configuring the SNMP agent

Select **Management > SNMP** to open the SNMP agent configuration page.



SNMP configuration ?

SNMP: ☑ Enabled

Read-only community name: ••••••

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

SNMP

Use this checkbox to enable/disable the SNMP agent. By default, the SNMP agent is enabled. If you disable the agent, the V-M200 will not respond to SNMP requests.

Read-only community name

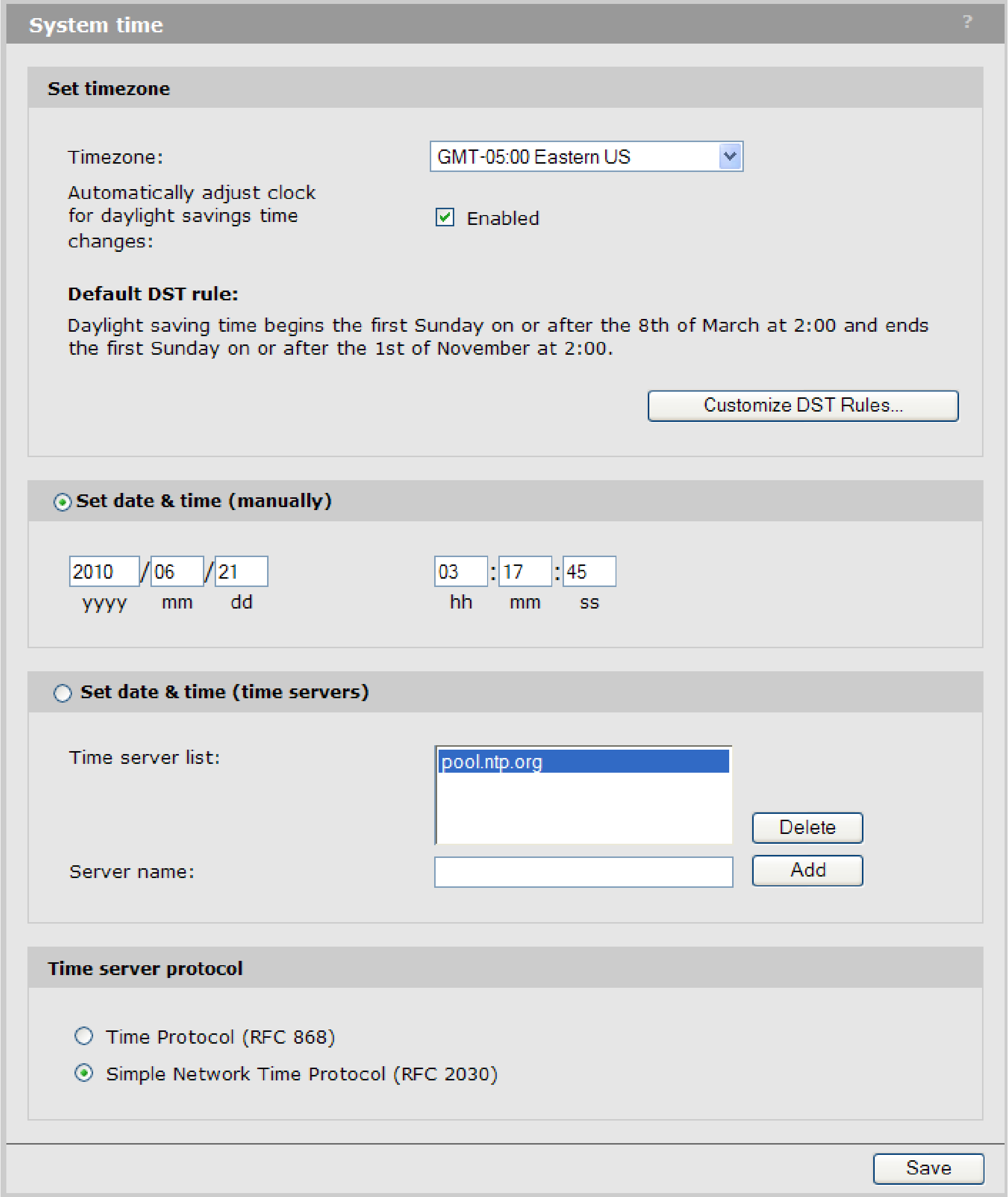
This is the password that controls read-only access to SNMP information on the V-M200. A network management program must supply this name when attempting to get SNMP information from the V-M200. By default, the name is set to **public**.

System time

Correct system time is important for proper operation of the V-M200, especially when using the logs to troubleshoot.

Configuring the system time

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



System time ?

Set timezone

Timezone: GMT-05:00 Eastern US

Automatically adjust clock for daylight savings time changes: ☑ Enabled

Default DST rule:

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

Customize DST Rules...

● **Set date & time (manually)**

2010 / 06 / 21 — yyyy mm dd

03 : 17 : 45 — hh mm ss

○ **Set date & time (time servers)**

Time server list: pool.ntp.org

Delete

Server name:

Add

Time server protocol

○ Time Protocol (RFC 868)

● Simple Network Time Protocol (RFC 2030)

Save

Set timezone

Select the timezone for your area and enable support for daylight savings time if required. If the rules for daylight savings time are different in your area, click **Customize DST Rule** to make the appropriate changes.

Set date & time (manually)

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

Set date and time (time servers)

(A working Internet connection is required to use this option.)

Select this option to have the V-M200 periodically contact a network time server to update its internal clock.

By default, the list contains **pool.ntp.org**, which is a large, virtual cluster of timeservers providing reliable NTP service.

When multiple servers are defined, the V-M200 contacts the first server in the list. If the server does not reply, the V-M200 tries the next server, and so on.

Time server protocol

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

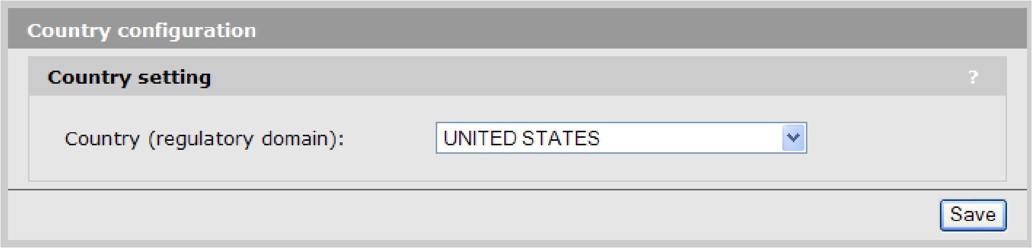
Country

Note The country page is not available on V-M200s delivered with a fixed country setting.

The country of operation, also known as the regulatory domain, determines the availability of certain wireless settings on the V-M200.

Once the country has been set, the V-M200 automatically limits the available wireless channels, channel width, and adjusts the radio power level in accordance with the regulations of the selected country.

To configure country settings, select **Management > Country.**



Country (regulatory domain): UNITED STATES

Caution Incorrectly selecting the country may result in illegal operation and may cause harmful interference to other systems. Please ensure that the V-M200 is operating in accordance with channel, power, indoor/outdoor restrictions, and license requirements for the intended country. If you fail to heed this caution, you may be held liable for violating the local regulatory compliance.

Note

- In some regions, you are prompted to select the country of use during setup.
- The currently selected country (regulatory domain) is displayed on the management tool home page.

4

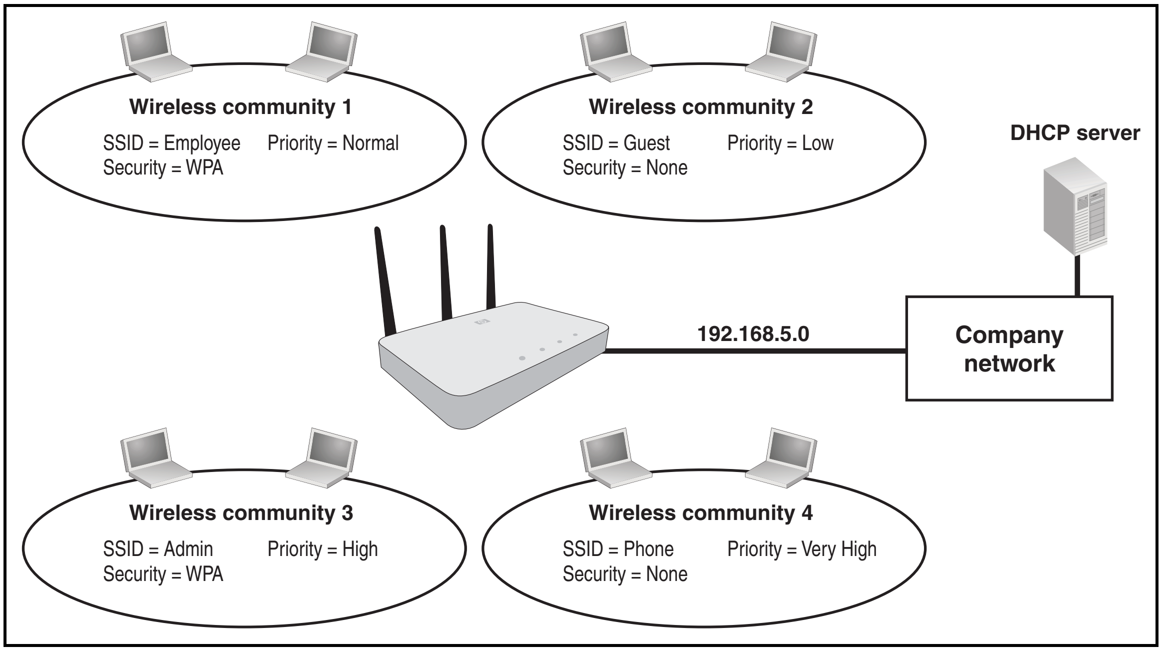
Working with wireless communities

Contents

Overview

The V-M200 allows you to create up to four wireless communities. Each wireless community defines the settings for a distinct wireless network, with its own network name (SSID), settings for wireless protection, user authentication, VLANs, quality of service, and more.

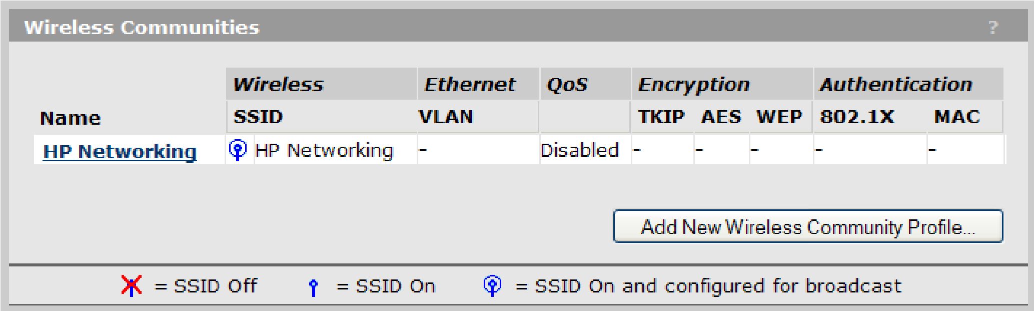
For example, in the following scenario, four wireless communities are defined. Each wireless community is configured with a different wireless network name (SSID), and the priority of user traffic is set to different levels using the QoS feature.



Even though multiple wireless communities are in use, all wireless users are on the same network (192.168.5.0). This means that all wireless users can reach resources on the corporate network. However, communication between wireless users may or may not be possible depending on the configuration settings defined for each wireless community.

Managing wireless communities

Wireless communities are managed on the Wireless communities page, which you open by selecting **Wireless > Communities**.



Wireless Communities ?

	Wireless	Ethernet	QoS	Encryption			Authentication	
Name	SSID	VLAN		TKIP	AES	WEP	802.1X	MAC
HP Networking	⊚ HP Networking	-	Disabled	-	-	-	-	-

Add New Wireless Community Profile...

✗ = SSID Off ⫯ = SSID On ⊚ = SSID On and configured for broadcast

You can define up to four wireless communities.

- To edit an existing community, click its name in the list.
- To add a new community, click **Add New Wireless Community Profile**.

In both cases, the Add/Edit Wireless Community page opens providing access to all configuration options. (See *Wireless community configuration options on page 4-4* for details.)

About the default wireless community

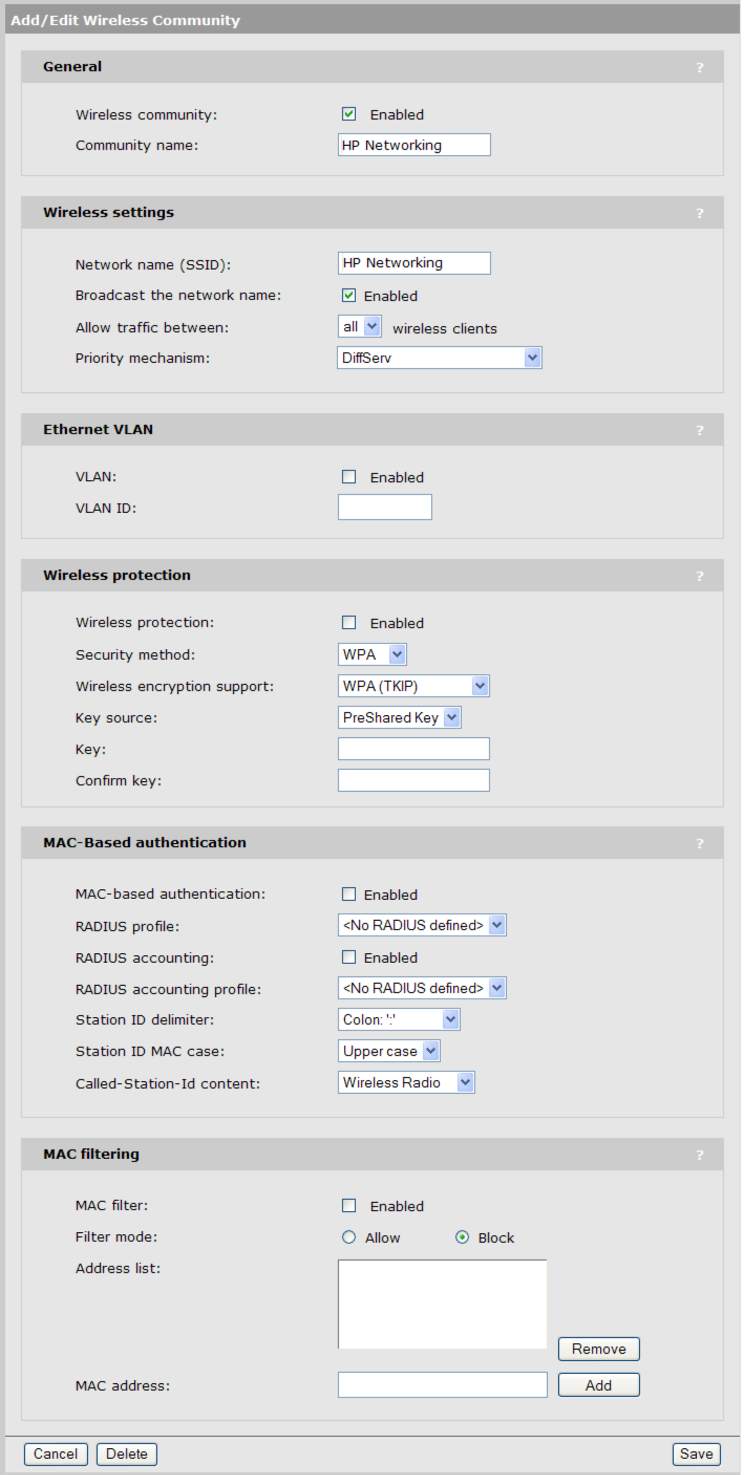
By default, a single wireless community is defined. It is named **HP Networking**, which is also its network name (SSID).

Caution

The default wireless community does not have any security or authentication options enabled. To protect the wireless network from malicious third-party wireless users, it is strongly recommended that you enable some form of wireless protection on the default wireless community.

Wireless community configuration options

Wireless community settings are configured using the Add/Edit Wireless Community page. If you edit the default wireless community (HP Networking) you will see these settings.



Add/Edit Wireless Community

General

Wireless community:	☑ Enabled
Community name:	HP Networking

Wireless settings

Network name (SSID):	HP Networking
Broadcast the network name:	☑ Enabled
Allow traffic between:	all wireless clients
Priority mechanism:	DiffServ

Ethernet VLAN

VLAN:	□ Enabled
VLAN ID:	

Wireless protection

Wireless protection:	□ Enabled
Security method:	WPA
Wireless encryption support:	WPA (TKIP)
Key source:	PreShared Key
Key:	
Confirm key:	

MAC-Based authentication

MAC-based authentication:	□ Enabled
RADIUS profile:	<No RADIUS defined>
RADIUS accounting:	□ Enabled
RADIUS accounting profile:	<No RADIUS defined>
Station ID delimiter:	Colon: ':'
Station ID MAC case:	Upper case
Called-Station-Id content:	Wireless Radio

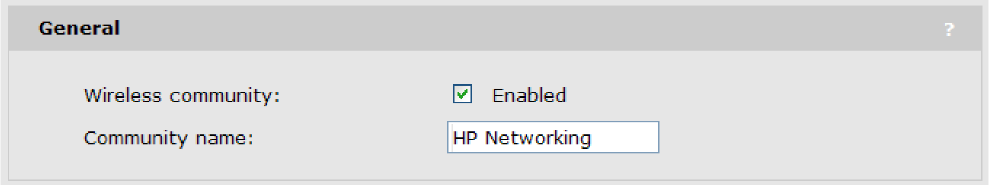
MAC filtering

MAC filter:	□ Enabled
Filter mode:	○ Allow ● Block
Address list:	
MAC address:	

The following sections describe all wireless community configuration options and explain how they can be used.

General

Controls general settings for the wireless community.



General ?

Wireless community: ☑ Enabled

Community name: HP Networking

Wireless community

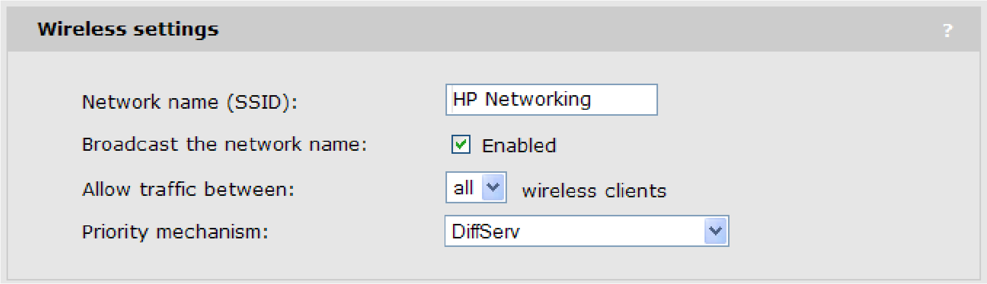
Select this checkbox to enable the wireless community. Once enabled, wireless users can connect to the wireless network defined by the community.

Community name

Define a name to identify the community on the V-M200.

Wireless settings

Configures the wireless network created by the wireless community.



Wireless settings ?

Network name (SSID): HP Networking

Broadcast the network name: ☑ Enabled

Allow traffic between: all wireless clients

Priority mechanism: DiffServ

Network name (SSID)

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

Broadcast the network name

This option controls whether the network name (SSID) is broadcast to all wireless users or not.

- When enabled, it means that the wireless network will be visible to wireless users when they scan the wireless neighborhood. 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.
- When disabled, it means that the network is not visible to scans and that wireless users must manually specify the network name (SSID) to successfully connect to the network.

Allow traffic between All/No wireless clients

This option controls the exchange of traffic between wireless users. The following settings are available:

- **All:** Wireless users connected to the same community can communicate with each other over the wireless network.
- **No:** Wireless users cannot communicate with each other over the wireless network.

Communication between users on different wireless communities

Communication between wireless users who are connected to different wireless communities can only occur if the users are assigned to the same VLAN.

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

- Unicast traffic exchanged between wireless communities is controlled by the setting of the receiving community.
- Multicast traffic exchanged between wireless communities is always controlled by the setting of the sending community.

The following table summarizes all possible scenarios:

Sender	Receiver	Unicast traffic	Multicast traffic
All	All	Allowed	Allowed
All	No	Blocked	Allowed
No	All	Blocked	Blocked
No	No	Blocked	Blocked

For example, if two communities have the following settings, then all wireless users on both communities can communicate with each other.

- **Allow traffic between wireless clients** set to **all**.
- **Ethernet VLAN** set to the same value on both communities.

By assigning VLAN attributes on a per-user basis via RADIUS (*VLAN assignment via RADIUS on page 6-5*), you can enable communication between specific users only.

Priority mechanism

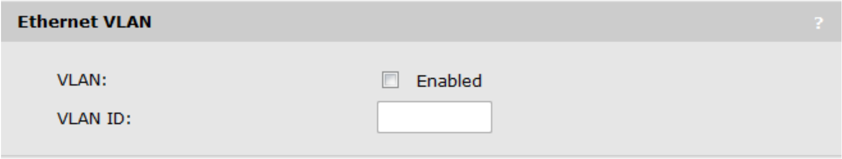
The quality of service (QoS) feature provides a number of different mechanisms to prioritize wireless traffic sent to wireless client stations. This is useful when you have defined multiple wireless communities and want to ensure a specific level of service for each one.

For example, if you have two communities, one for employees and one for guests, you might want to make the employee traffic higher priority so that employee traffic is never delayed due to excessive guest traffic.

See *Quality of service (QoS) on page 4-15* for more information on using this feature.

Ethernet VLAN

Use this option to bind the wireless community to a specific VLAN on the Ethernet port. All traffic sent/received on the Ethernet port by the wireless community will be assigned to the VLAN you specify.



Ethernet VLAN

VLAN: □ Enabled

VLAN ID:

If you do not set a VLAN, traffic is sent untagged. However, a VLAN can still be assigned on a per-user basis by setting an attribute in the user's RADIUS account (when using RADIUS-based authentication).

See *Working with VLANs on page 6-4* for information on using this feature.

Wireless protection

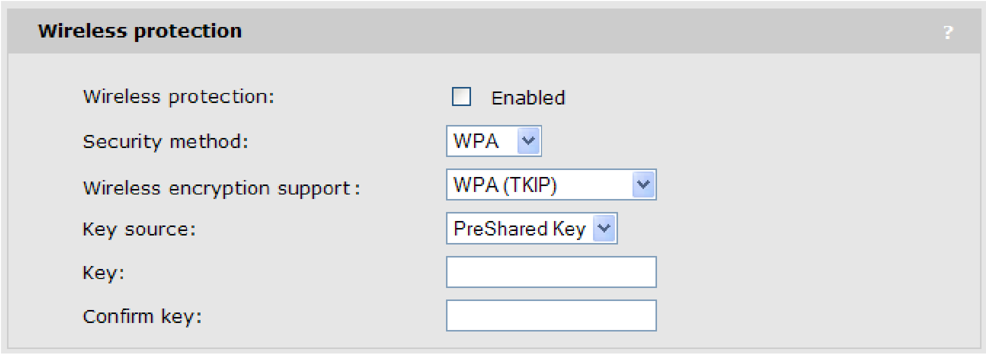
The V-M200 provides several methods to protect wireless transmissions from eavesdropping and to safeguard network access from unauthorized users. To choose the method that best meets the needs of your network, refer to the sections that follow.

WPA

Wi-Fi Protected Access (WPA) is a security protocol that provides for both encryption of the wireless data stream (via TKIP or AES/CCMP) and authentication of wireless users using an third-party RADIUS server (via 802.1X/EAP).

The WPA options you see change depending on the setting of **Key source**.

Key source set to **PreShared Key**



Wireless protection

Wireless protection: □ Enabled

Security method: WPA

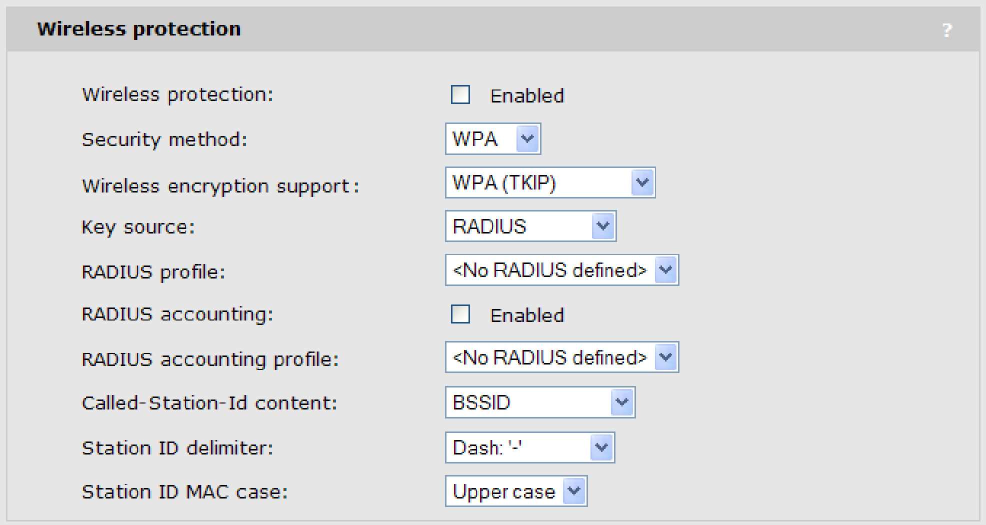
Wireless encryption support: WPA (TKIP)

Key source: PreShared Key

Key:

Confirm key:

Key source set to **RADIUS**



Wireless protection ?

Wireless protection:	□ Enabled
Security method:	WPA
Wireless encryption support:	WPA (TKIP)
Key source:	RADIUS
RADIUS profile:	<No RADIUS defined>
RADIUS accounting:	□ Enabled
RADIUS accounting profile:	<No RADIUS defined>
Called-Station-Id content:	BSSID
Station ID delimiter:	Dash: '-'
Station ID MAC case:	Upper case

Security method

- **WPA (TKIP)**: WPA with TKIP encryption. Original version of the standard. Still supported by many legacy clients.
- **WPA2 (AES/CCMP)**: WPA2 (802.11i) with AES/CCMP encryption. More secure than WPA (TKIP). If all your users have WPA2 client software, select this option for the maximum possible security.
- **WPA or WPA2**: Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time. Some legacy WPA clients may not work if this mode is selected. This mode is slightly less secure than using the WPA2 (AES/CCMP) mode.

Note WPA (TKIP) cannot be used when the radio operating mode supports 802.11n.

Key source

This option determines how the WPA encryption keys are generated and whether 802.1X authentication is used.

- **PreShared Key**: The V-M200 uses the key you specify in the **Key** field to generate the TKIP or AES/CCMP keys that are used to encrypt the wireless data stream. Since this is a static key, it is not as secure as the RADIUS option. Specify a key that is between 8 and 63 alphanumeric characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers. The double quote character (") should not be used.

- **RADIUS**: The V-M200 retrieves the key from the RADIUS server and uses it to generate the TKIP or AES/CCMP keys that are used to encrypt the wireless data stream. The key is dynamically generated by the RADIUS server each time the user logs in. Communication with the RADIUS server occurs via 802.1X using the EAP protocol specified by the user's WPA client software.

  If you select the **RADIUS** option, you need to configure the following settings:

  - **RADIUS profile:** Select the RADIUS profile to use. The profile defines the settings that are used by the V-M200 to communicate with the RADIUS server. RADIUS profiles are defined by selecting **Authentication > RADIUS profiles**. For more information, see *Using a third-party RADIUS server on page 7-2*.

  - **RADIUS accounting:** Enable this option to have the V-M200 generate a RADIUS START/STOP and interim request for each user. The V-M200 respects the RADIUS interim-update-interval attribute if it is present inside the RADIUS access accept response for the authentication.

  - **RADIUS accounting profile:** Select the RADIUS profile to use for accounting requests. The profile defines the settings that are used by the V-M200 to communicate with the RADIUS server. RADIUS profiles are defined by selecting **Authentication > RADIUS profiles**. For more information, see *Using a third-party RADIUS server on page 7-2*.

  - **Called-Station-ID content:** Select the value that the V-M200 will return as the called station ID.

    - **Port 1**: MAC address of the Ethernet port on the V-M200.

    - **Wireless radio**: MAC address of the wireless port on the V-M200.

    - **BSSID**: Basic service set ID of the wireless network defined by this community.

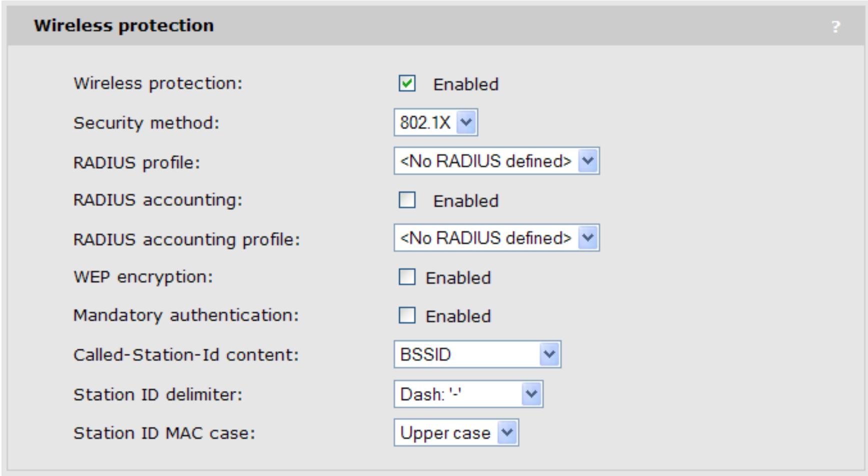
    - **MAC address:SSID:** The MAC address of the V-M200 followed by a colon followed by the SSID of the wireless community to which the client station is connected.

  - **Station ID delimiter:** Select the one-character delimiter that will be used to format both the calling station ID and the called station ID attributes in RADIUS packets. By default, a dash (-) is used.

  - **Station ID MAC case:** Select the case applied to the station ID.

802.1X

802.1X enables you to authenticate wireless clients via user accounts stored on a third-party RADIUS server.



Wireless protection

Wireless protection:	☑ Enabled
Security method:	802.1X
RADIUS profile:	<No RADIUS defined>
RADIUS accounting:	□ Enabled
RADIUS accounting profile:	<No RADIUS defined>
WEP encryption:	□ Enabled
Mandatory authentication:	□ Enabled
Called-Station-Id content:	BSSID
Station ID delimiter:	Dash: '-'
Station ID MAC case:	Upper case

Caution

802.1X is purely a protocol for user authentication. Using 802.1X without enabling the **WEP encryption** option results in wireless traffic being **unencrypted**. Therefore, for security reasons, use of 802.1X without enabling WEP encryption is not recommended.

Supported 802.1X protocols

The following EAP protocols are supported by the V-M200. Other EAP protocols may also work, but have not been tested. The 802.1X protocol that is used is always determined by the configuration of the user's 802.1X client software and is not configured on the V-M200.

- EAP-MD5: Extensible Authentication Protocol Message Digest 5. Offers minimum security. Not recommended.
- EAP-TLS: Extensible Authentication Protocol Transport Layer Security. Provides strong security based on mutual authentication. Requires both client and server-side certificates.
- EAP-TTLS: Extensible Authentication Protocol Tunnelled Transport Layer Security. Provides excellent security with less overhead than TLS, as client-side certificates can be used, but are not required.
- PEAPv0: Protected Extensible Authentication Protocol. One of the most supported implementations across all client platforms. Uses MSCHAPv2 as the inner protocol.
- PEAPv1: Protected Extensible Authentication Protocol. Alternative to PEAPv0 that permits other inner protocols to be used.
- EAP-FAST: Extensible Authentication Protocol Flexible Authentication via Secure Tunneling). Can use a pre-shared key instead of server-side certificate.

For more detailed information, see the appropriate Internet Engineering Task Force (IETF) Request for Comments (RFC) for each protocol.

802.1X settings

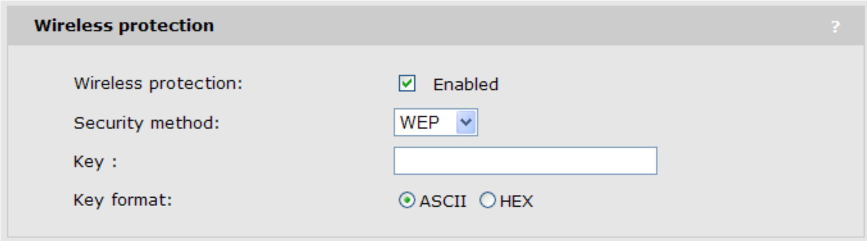
If you select the **802.1X** option, the following settings are configurable:

- **RADIUS profile:** Select the RADIUS profile to use. RADIUS profiles are defined by selecting **Authentication > RADIUS profiles**. The profile defines the settings that are used by the V-M200 to communicate with the RADIUS server. RADIUS profiles are defined by selecting **Authentication > RADIUS profiles**. For more information, see *Using a third-party RADIUS server on page 7-2*.
- **RADIUS accounting:** Enable this option to have the V-M200 generate a RADIUS START/ STOP and interim request for each user. The V-M200 respects the RADIUS interim-update-interval attribute if it is present inside the RADIUS access accept response for the authentication.
- **RADIUS accounting profile:** Select the RADIUS profile to use for accounting requests. The profile defines the settings that are used by the V-M200 to communicate with the RADIUS server. RADIUS profiles are defined by selecting **Authentication > RADIUS profiles**. For more information, see *Using a third-party RADIUS server on page 7-2*.
- **WEP encryption:** Enable the use of dynamic WEP keys for all 802.1X sessions. Dynamic key rotation occurs on key 1, which is the broadcast key. Key 0 is the pair-wise key. It is automatically generated by the V-M200. To configure the key change interval, select **Authentication > 802.1X**.
- **Called-Station-ID content:** Select the value that the V-M200 will return as the called station ID.
  - **Port 1**: MAC address of the Ethernet port on the V-M200.
  - **Wireless radio**: MAC address of the wireless port on the V-M200.
  - **BSSID**: Basic service set ID of the wireless network defined by this community.
  - **MAC address:SSID:** The MAC address of the V-M200 followed by a colon followed by the SSID of the wireless community to which the client station is connected.
- **Station ID delimiter:** Select the one-character delimiter that will be used to format both the calling station ID and the called station ID attributes in RADIUS packets. By default, a dash (-) is used.
- **Station ID MAC case:** Select the case applied to the station ID.

Note Global settings for 802.1X are configured by selecting **Authentication > 802.1X**. See ***Global 802.1X settings on page 7-11***.

WEP

WEP enables you to encrypt wireless transmissions, but does not provide for user authentication. WEP is not as secure as WPA.



Wireless protection

Wireless protection:	☑ Enabled
Security method:	WEP
Key :	
Key format:	● ASCII ○ HEX

Note WEP cannot be used when the radio operating mode supports 802.11n.

Key

The number of characters you specify for the key determines the level of encryption.

- For 40-bit encryption, specify 5 ASCII characters or 10 HEX digits.
- For 128-bit encryption, specify 13 ASCII characters or 26 HEX digits.

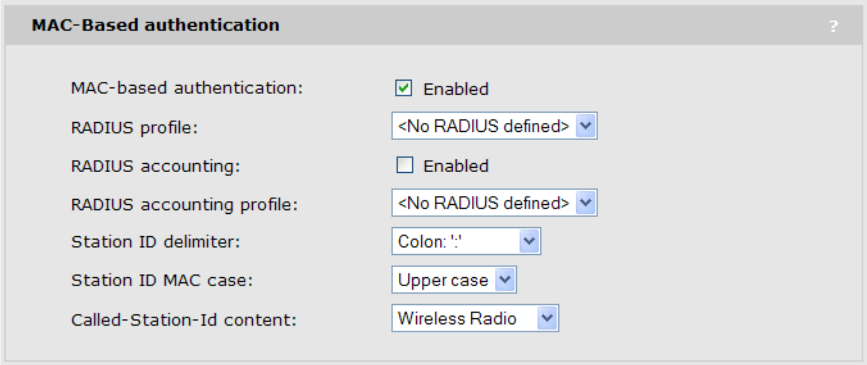
Key format

Select the format used to specify the encryption key. The definition for the encryption key must be the same on the V-M200 and all client stations.

- **ASCII:** ASCII keys are much weaker than carefully chosen HEX keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client stations support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.
- **HEX:** Your keys should only include the following characters: 0-9, a-f, A-F.

MAC-based authentication

This feature enables you to authenticate wireless users based on the MAC address of their wireless device. Authentication occurs via a third-party RADIUS server.



MAC-Based authentication

MAC-based authentication:	☑ Enabled
RADIUS profile:	<No RADIUS defined>
RADIUS accounting:	□ Enabled
RADIUS accounting profile:	<No RADIUS defined>
Station ID delimiter:	Colon: ':'
Station ID MAC case:	Upper case
Called-Station-Id content:	Wireless Radio

Note

- When both this option and the MAC filtering option are enabled, MAC filtering occurs first.
- MAC-based authentication cannot be enabled at the if Wireless protection is set to WPA/WPA2 with RADIUS.

To successfully authenticate a user, an account must be created on the RADIUS server with both username and password set to the MAC address of the user's wireless device.

The MAC address sent by the V-M200 (in the RADIUS REQUEST packet) for both username and password is **12 hexadecimal numbers, with the values "a" to "f" in lowercase**. For example, 0003520a0f01.

The RADIUS server will reply to the REQUEST with either an ACCEPT or REJECT RADIUS RESPONSE packet. In the case of an ACCEPT, the RADIUS server can return the session-timeout RADIUS attribute (if configured for the account). This attribute indicates the amount of time, in seconds, that the authentication is valid for. When this period expires, the V-M200 will re-authenticate the user.

MAC-based authentication

Select this checkbox to enable MAC-based authentication.

RADIUS profile

Select the RADIUS profile to use for authentication.The profile defines the settings that are used by the V-M200 to communicate with the RADIUS server. RADIUS profiles are defined by selecting **Authentication > RADIUS profiles**. For more information, see *Using a third-party RADIUS server on page 7-2*.

RADIUS accounting

Enable this option to have the V-M200 generate a RADIUS START/STOP and interim request for each user. The V-M200 respects the RADIUS interim-update-interval attribute if it is present inside the RADIUS access accept response for the authentication.

RADIUS accounting profile

Select the RADIUS profile to use for accounting. The profile defines the settings that are used by the V-M200 to communicate with the RADIUS server. RADIUS profiles are defined by selecting **Authentication > RADIUS profiles**. For more information, see *Using a third-party RADIUS server on page 7-2*.

Station ID delimiter

Select the one-character delimiter that will be used to format both the calling station ID and the called station ID attributes in RADIUS packets. By default, a colon (:) is used.

Station ID MAC case

Select the case applied to the station ID.

Called-Station-ID Content

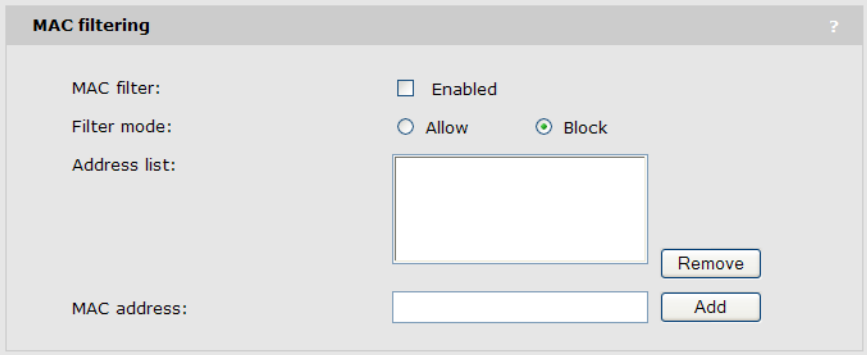
Select the value that the V-M200 will return as the called station ID.

- **Port 1**: MAC address of the Ethernet port on the V-M200.
- **Wireless Radio**: MAC address of the wireless port on the V-M200.
- **BSSID**: Basic service set ID of the wireless network defined by this community.
- **MAC address:SSID:** The MAC address of the V-M200 followed by a colon followed by the SSID of the wireless community to which the client station is connected.

MAC filtering

This feature enables you to control access to the wireless network based on the MAC address of a user's wireless device. You can either block access or allow access, depending on your requirements.

Note MAC filtering occurs before any other authentication method.



MAC filtering

MAC filter: □ Enabled

Filter mode: ○ Allow ● Block

Address list:

MAC address:

MAC filter

Select this checkbox to enable the MAC filter.

Filter mode

- **Allow**: Only users whose MAC addresses appear in the MAC address list can connect to the wireless network created by this community.
- **Block**: Users whose MAC address appear in the MAC address list are blocked from accessing the wireless network created by this community.

Address list

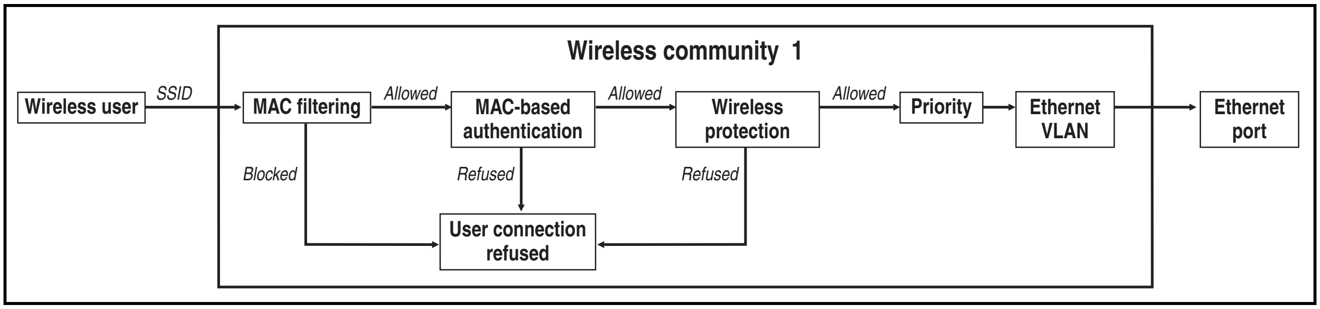
List of defined MAC addresses. Up to 64 MAC addresses are supported. To delete an address, select it in the list and click **Delete**.

MAC address

To add a MAC address, specify six pairs of hexadecimal digits separated by colons and click **Add**. For example: 00:00:00:0a:0f:01.

Wireless community data flow

The following diagram illustrates the order in which the wireless community features act upon incoming data from a wireless user.



For a detailed description of each feature, see *Wireless community configuration options on page 4-4*.

Quality of service (QoS)

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

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

Outgoing wireless traffic on a wireless community 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.

To see how traffic is marked based on QoS settings, see *Upstream/downstream traffic marking on page 4-17*.

Regardless of the priority mechanism that is selected, traffic that cannot be classified by a priority mechanism is assigned to queue 3.

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

802.1p

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

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

Community Based priority

This mechanism enables you to assign a single priority level to all traffic on a wireless community. If you enable the community based priority mechanism, it takes precedence regardless of the priority mechanism supported by associated client stations. For example, if you set **Community Based Low** priority, then all clients connected to this community have their traffic set at low priority.

Queue	Community Based priority value
1	Community Based Very-high
2	Community Based High
3	Community Based Normal
4	Community Based Low

Diffserv (Differentiated Services)

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

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

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 V-M200 and then forwarded onto the wired network (via the Ethernet port) by the V-M200.

Mechanism	**INCOMING TRAFFIC** Wireless traffic sent from wireless client stations to the V-M200	**OUTGOING TRAFFIC** Traffic sent by the V-M200 to the wired network
		L2 marking
802.1p	WMM	802.1p (requires an Ethernet VLAN to be defined on the wireless community).
Community Based	WMM Non-WMM	If an egress VLAN is defined for the wireless community, then 802.1p and IP DSCP are set to reflect the Community Based priority setting. If no egress VLAN is defined for the wireless community, then the 802.1p header is not added, and only IP DSCP is set to reflect the Community Based priority setting.
DiffServ	DiffServ	None

Downstream traffic marking

This table describes the marking applied to traffic received from the wired network (via the Ethernet port) by the V-M200 and then sent to connected wireless client stations.

Mechanism	**INCOMING TRAFFIC** Traffic received from the wired network	**OUTGOING TRAFFIC** Wireless traffic sent from the V-M200 to wireless client stations	
		WMM Client	**Non-WMM Client**
802.1p	802.1p	WMM + HPQ (WMM marking done according to the rules for the mechanism.)	HPQ (hardware priority queueing)
Community Based	All traffic on the community		
DiffServ	DiffServ		

Although the WMM specification refers to 802.1D and not 802.1p, this guide uses the term 802.1p because it is more widely recognized. (The updated IEEE 802.1D: ISO/IEC 15802-3 (MAC Bridges) standard covers all parts of the Traffic Class Expediting and Dynamic Multicast Filtering described in the IEEE 802.1p standard.)

5

Wireless configuration

Contents

Wireless coverage

As a starting point for planning your network, you can assume that when operating at high power, the V-M200 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, you should always perform a site survey to determine the optimal settings and location for the V-M200.

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

Factors limiting wireless coverage

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

Interference

Interference is caused by other APs or devices that operate in the same frequency band as the V-M200 and can substantially affect throughput. Several tools are available to diagnose interference problems as they occur.

- Select **Wireless > Rogue AP detection** to view detailed information about all wireless APs operating in the immediate area so that you can effectively set the operating frequencies. This feature also makes it easy for you to find rogue APs. See *Detecting rogue APs on page 5-13*.
- 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.

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, the V-M200s 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. The V-M200 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 V-M200 to serve users on different floors in a concrete building. Such installations require a separate V-M200 on each floor.

Configuring overlapping wireless cells

When the radio is operating in the 2.4 GHz band, 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.

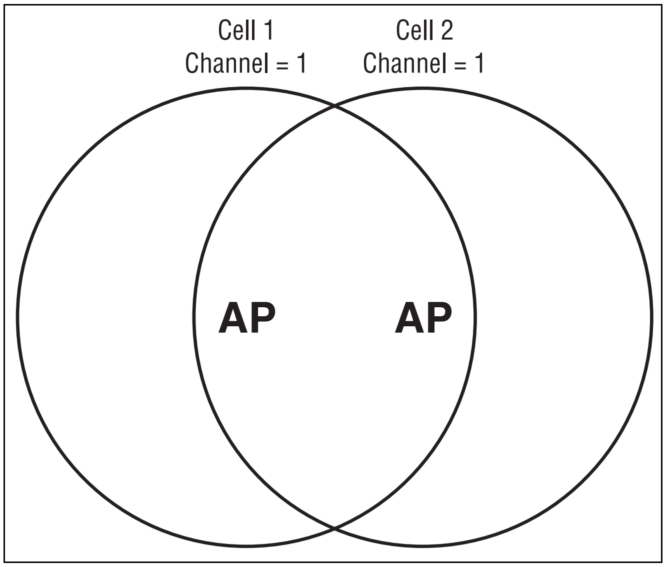
Note Overlapping channels do not occur when the radio is operating in the 5 GHz band. All 5 GHz channels are non-overlapping.

Performance degradation and channel separation

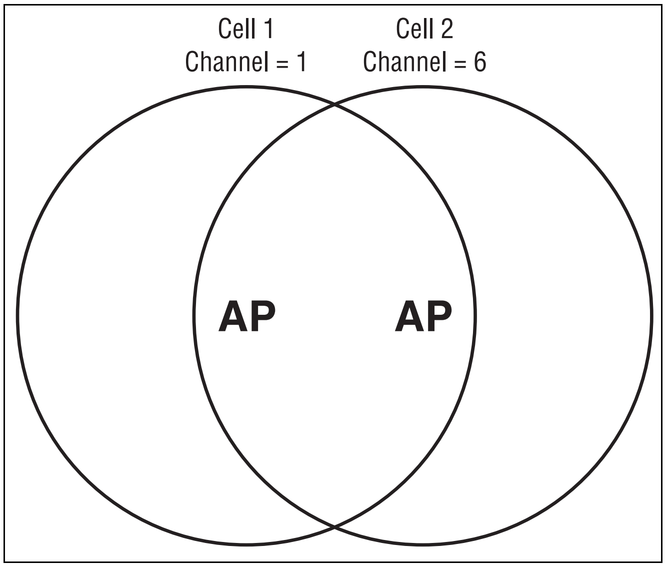
When two wireless cells operating on the same frequency overlap, throughput can be reduced in both cells. Reduced throughput occurs because a wireless user that is attempting to transmit data defers (delays) transmission if another station is transmitting. In a network with many users and much traffic, 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.



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 V-M200 to transmit at the same time.



Selecting channels

For optimal performance when operating in the 2.4 GHz band, 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.

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 > Rogue AP detection** 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 V-M200 supports the following 14 channels in the 2.4 GHz band.

Channel	Frequency
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442

Channel	Frequency
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2477

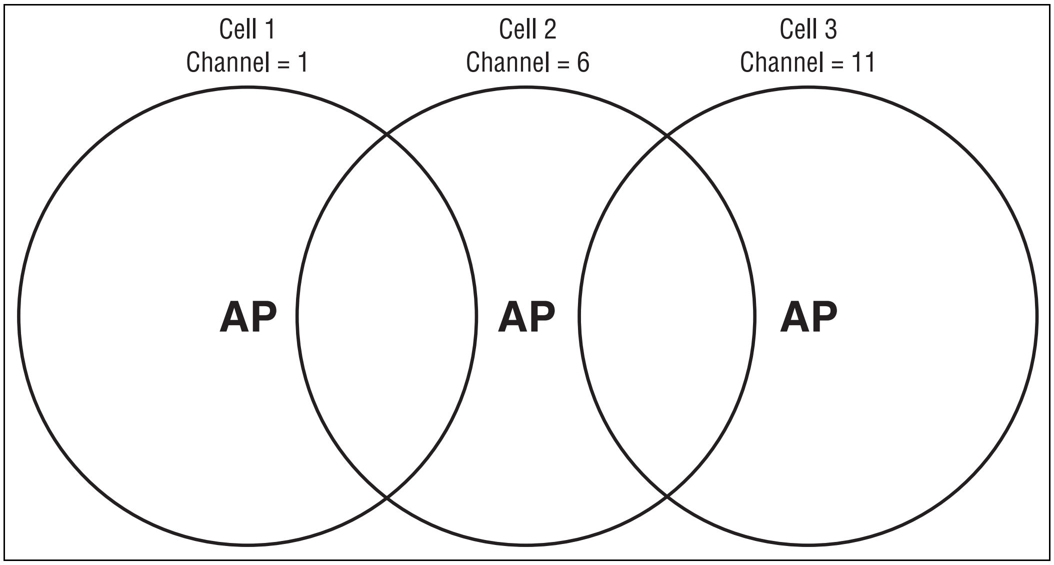
However, the number of channels available for use in a particular country are determined by the regulations defined by the local governing body. The following table shows the number of channels that are available in North America and Europe.

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

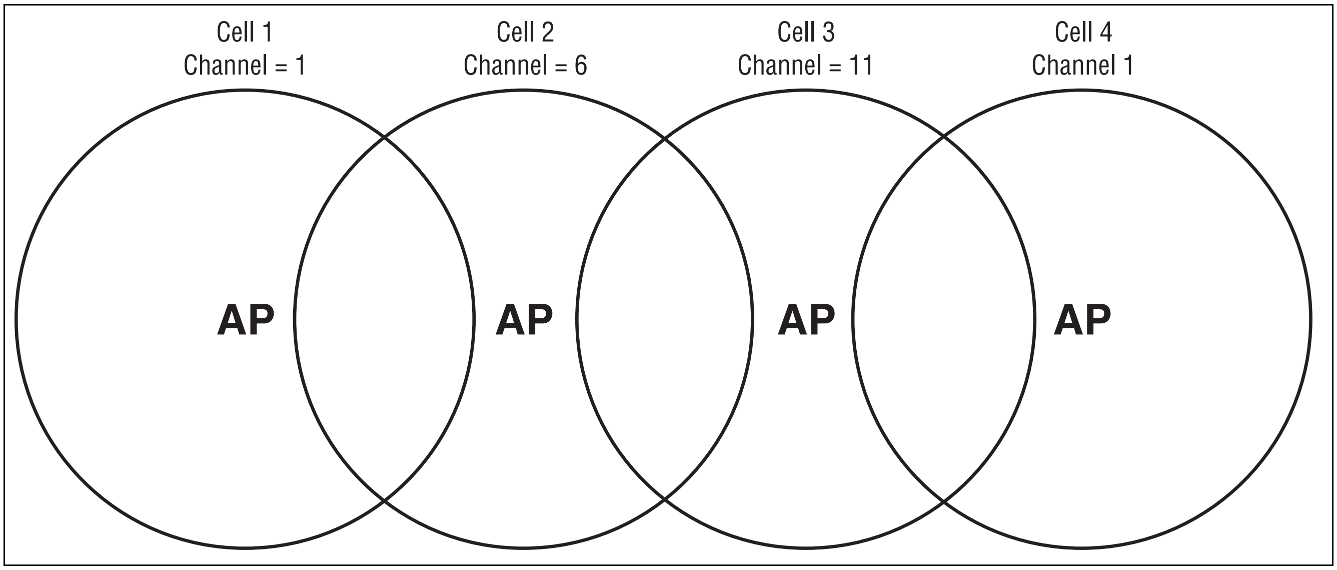
Since the minimum recommended separation between overlapping channels is 25 MHz (five cells) the recommended maximum number of overlapping cells you can have in most regions is three. The following table gives examples relevant to North America and Europe for channels in the 2.4 GHz band.

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

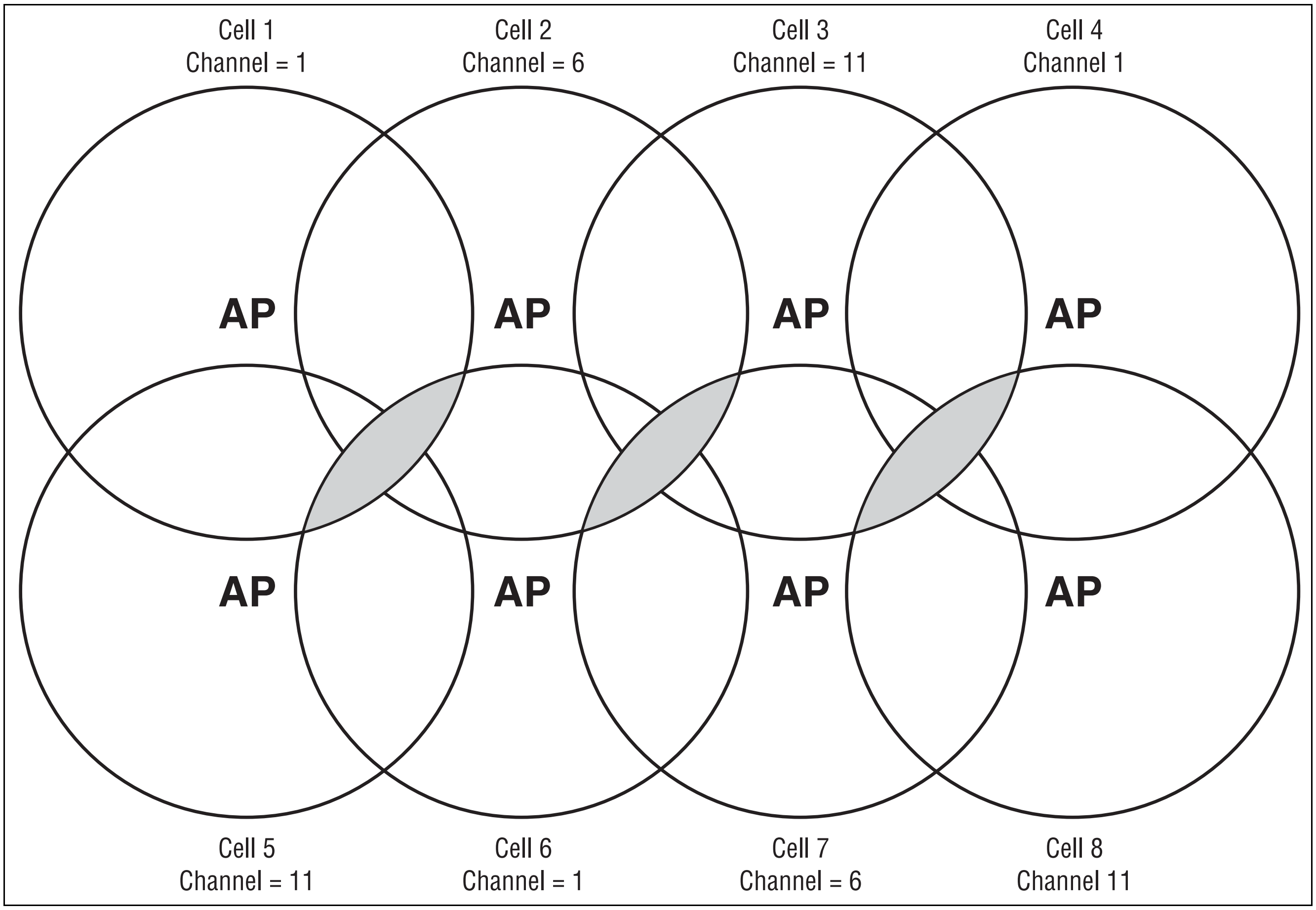
In North America, you can reduce transmission delays by using different operating frequencies as shown in the following figure.



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



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



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.

Supporting legacy wireless clients

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

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

802.11n clients face the same problem as described for 802.11g clients. 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. The 802.11n clients can achieve maximum data rates only when the legacy clients are not present.

Available 802.11n modes

Supported wireless modes are determined by the regulatory domain. Available options may include one or more of the following:

- **802.11n (5 GHz):** (Pure 802.11n) Up to 300 Mbps in the 802.11n 5 GHz frequency band.
- **802.11n/a:** (Compatibility mode.) Up to 270 Mbps for 802.11n and 54 Mbps for 802.11a in the 5 GHz frequency band.
- **802.11n (2.4 GHz):** (Pure 802.11n) Up to 144.4 Mbps in the 802.11n 2.4 GHz frequency band.
- **802.11n/g:** (Compatibility mode.) Up to 130 Mbps for 802.11n and 54 Mbps for 802.11g in the 2.4 GHz frequency band. Only use this setting when support for 802.11g is necessary.
- **802.11n/b/g:** (Compatibility mode.) Up to 130 Mbps for 802.11n, 54 Mbps for 802.11g, and 11 Mbps for 802.11b in the 2.4 GHz frequency band. Only use this setting when support for 802.11b is necessary.

Note The V-M200 Radio 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 refers to these two modes as Pure-N. When the V-M200 radio is in either of these modes, it will not allow non-802.11n clients to associate. Legacy clients can see the V-M200, and may attempt to associate, but they will be rejected. The V-M200 makes this determination based on the supported rate set that the client presents during its association request. If the client's rate does not match the 802.11n rate, it is not allowed to associate.

In these modes, the V-M200 will not use protection when sending HT frames to associated clients. If legacy V-M200s 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 V-M200 will still signal associated clients to use protection when they send data. The V-M200 does this via a field in the beacons that it sends. So clients sending data to the V-M200 will use protection, but data sent from the V-M200 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. The V-M200 does not support this preamble and therefore does not support Greenfield mode.

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 the V-M200 radio. 802.11n/b/g supports 802.11n and 802.11b/g clients in the 2.4 GHz spectrum. In either of these modes, the V-M200 allows both 802.11n and legacy clients to associate. The V-M200 advertises protection in the beacon when legacy clients are associated or operating on the same channel. This alerts the associated 802.11n clients to use protection when transmitting. The V-M200 also uses protection when necessary while sending HT data.

When to use these modes: these compatibility modes should be used when legacy clients are present in the network. HP recommends 802.11n/a or 802.11 n/b/g as the typical operating mode. 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 V-M200 does not advertise 1, 2, 5.5 and 11 Mbps as supported rates in its beacons or Probe-Responses. The V-M200 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

When operating in the 5 GHz band, the V-M200 enables you 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 width channel is that the available bandwidth is doubled leading to much higher throughput.

When operating in the 2.4 Ghz band, a channel width of 20 MHz is automatically selected and cannot be changed.

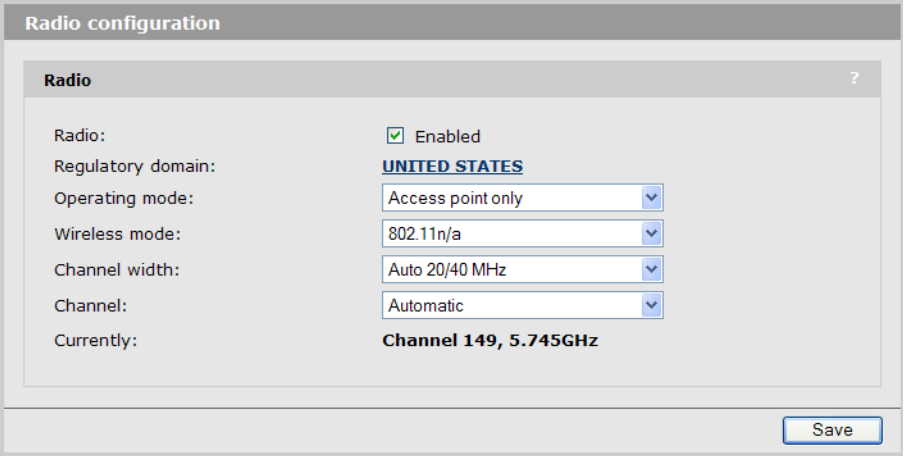
When operating in the 5 GHz band, the **Auto 20/40 MHz** option should be used as the channel width.

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

When Auto 20/40 MHz is selected, the V-M200 radio 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.

Radio configuration

To define configuration settings for the V-M200 radio, select **Wireless > Radi**o to open the Radio configuration page.



Radio configuration

Radio

Radio:	☑ Enabled
Regulatory domain:	UNITED STATES
Operating mode:	Access point only
Wireless mode:	802.11n/a
Channel width:	Auto 20/40 MHz
Channel:	Automatic
Currently:	Channel 149, 5.745GHz

Radio

Select this checkbox to activate the radio.

Regulatory domain

Note This option is not available on V-M200s delivered with a fixed country setting.

Indicates the geographical region in which the V-M200 operates. To change the domain, click the domain name or select **Management > Country**.

Caution Wireless radios are governed by different regulatory standards depending on the region in which they are installed. By setting the regulatory domain, the V-M200 will only allow you to configure wireless settings in accordance with the regulations in the selected domain. Therefore, the settings that are available on this page may not include all options that are described in this section. Please ensure that the V-M200 is operating in accordance with channel, power, indoor/outdoor restrictions and license requirements for the intended country.

Operating mode

Select the operating mode. Available options are:

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

Wireless mode

Select the mode that best supports the wireless client stations at your location.

Supported wireless modes are determined by the regulatory domain (country). Available options may include one or more of the following.

- **802.11n (5 GHz):** (Pure 802.11n) Supports up to 300 Mbps in the 802.11n 5 GHz frequency band.
- **802.11n/a:** (Compatibility mode) Supports up to 270 Mbps for 802.11n and 54 Mbps for 802.11a in the 5 GHz frequency band.
- **802.11n (2.4 GHz):** (Pure 802.11n) Supports up to 144.4 Mbps in the 802.11n 2.4 GHz frequency band.
- **802.11n/g:** (Compatibility mode) Supports up to 130 Mbps for 802.11n and 54 Mbps for 802.11g in the 2.4 GHz frequency band. Only use this setting when support for 802.11g is necessary.
- **802.11n/b/g:** (Compatibility mode) Supports up to 130 Mbps for 802.11n, 54 Mbps for 802.11g, and 11 Mbps for 802.11b in the 2.4 GHz frequency band. Only use this setting when support for 802.11b is necessary.
- **802.11b**: Supports up to 11 Mbps in the 2.4 GHz frequency band.
- **802.11b/g**: Supports up to 11 and 54 Mbps in the 2.4 GHz frequency band.
- **802.11g**: Supports up to 54 Mbps in the 2.4 GHz frequency band.
- **802.11a**: Supports up to 54 Mbps in the 5 GHz frequency band.

Note

In **802.11n (2.4 GHz)** and **802.11n (5 GHz)** modes, the V-M200 does not permit non-802.11n clients to associate. Also in this mode, the V-M200 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 V-M200 and its 802.11n clients.

In **802.11n/a**, **802.11n/g**, and **802.11n/b/g** modes, the V-M200 permits both 802.11n and legacy clients (802.11a/b/g) to associate. The V-M200 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.

For more information, refer to *802.11n best practices on page 5-7*.

Channel width

(Only applicable when **Wireless mode** includes some type of 802.11n support.)

(Only configurable when **Wireless mode** is set to **802.11n (5 GHz)** or **802.11n/a**. For all other 802.11n modes, **Channel width** is set to **20 MHz** and cannot be changed.)

Select the **Channel width** that will be used for 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. This option reduces the number of unoccupied channels available to neighboring APs.

Note

Although some 802.11n clients only support 20 MHz channels, they can still associate with a V-M200 configured for **Auto 20/40 MHz**.

Channel

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

Use the **Automatic** option to have the V-M200 select the best available channel.

If setting the channel manually, for optimal performance when operating in 2.4 GHz modes, select a channel that is different from other wireless APs that operate in neighboring cells by at least by five channel numbers (25 MHz). For example, if another AP is operating on channel 1, set the V-M200 to channel 6 or higher. Select **Wireless > Rogue AP detection**, and then select **Configure Access Point List** to view a list of APs currently operating in your area.

When operating in 802.11a or 802.11n (5 GHz) modes, interference between APs is not a consideration as all channels are non-overlapping.

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

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

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

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

Detecting rogue APs

You can use the **Rogue AP detection** feature to scan for other APs operating nearby and flag them as either *authorized APs* or *rogue APs*. This is useful for monitoring the installation of wireless access points in your company's work areas to ensure that new APs (which could be a security risk if improperly configured) are not deployed without your knowledge.

This feature can also be used to determine the operating frequencies of nearby APs for site planning purposes.

Note

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

Scanning modes

The way in which the V-M200 performs scanning depends on the configuration of the wireless radio (**Wireless > Radio** page). The following scanning modes are possible:

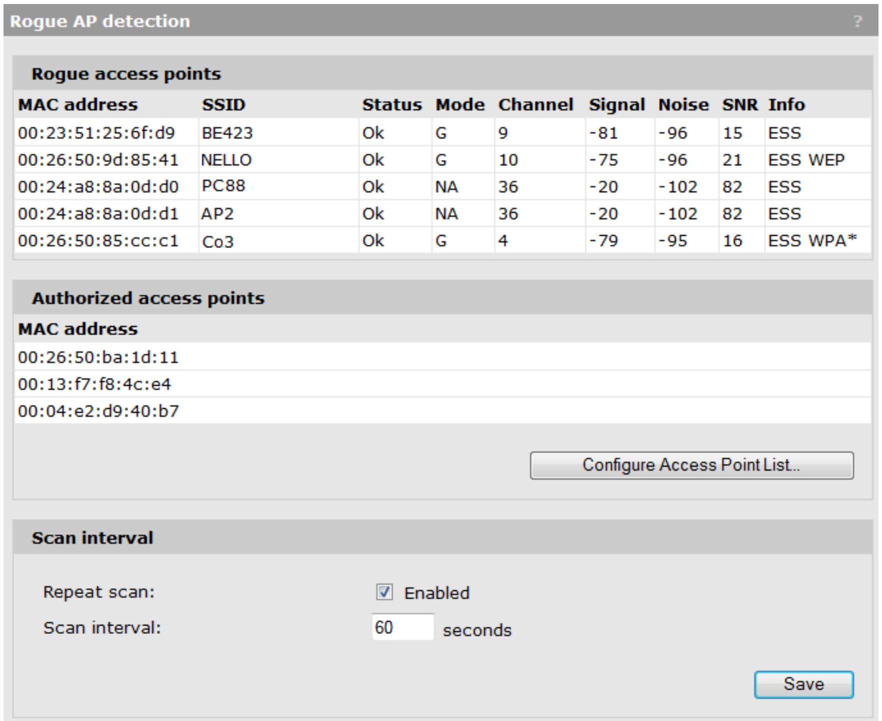
- **Monitor mode:** When the radio has its **Operating mode** set to **Monitor**, scanning occurs continuously. The scan switches to a new channel every 200 ms, sequentially covering all supported wireless modes and channels. Use this method to quickly obtain an overview of all APs in your area for site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

- **Automatic channel:** When the radio has its **Channel** set to **Automatic**, scanning is performed for all the channels in the currently selected **Wireless mode** when the V-M200 starts up.
- **Background scanning:** For any other radio configuration, scanning is controlled by the settings on the Rogue AP detection page. To enable scanning, select the **Repeat scan** checkbox and set the **Scan interval**. Scanning is performed for all the channels in the currently selected radio **Wireless mode**. One channel is scanned during each scan interval. By default, the scan interval is set to 600 seconds. This is done to minimize the impact on radio throughput.

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

Viewing scan results

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



Rogue AP detection

Rogue access points

MAC address	SSID	Status	Mode	Channel	Signal	Noise	SNR	Info
00:23:51:25:6f:d9	BE423	Ok	G	9	-81	-96	15	ESS
00:26:50:9d:85:41	NELLO	Ok	G	10	-75	-96	21	ESS WEP
00:24:a8:8a:0d:d0	PC88	Ok	NA	36	-20	-102	82	ESS
00:24:a8:8a:0d:d1	AP2	Ok	NA	36	-20	-102	82	ESS
00:26:50:85:cc:c1	Co3	Ok	G	4	-79	-95	16	ESS WPA*

Authorized access points

MAC address
00:26:50:ba:1d:11
00:13:f7:f8:4c:e4
00:04:e2:d9:40:b7

Scan interval

Repeat scan: ☑ Enabled

Scan interval: 60 seconds

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

Note

Rogue access points are not listed until you define at least one authorized access point as described under *Creating a list of authorized access points on page 5-15*.

Scanning for rogue APs

When the V-M200 discovers an AP during a scan it compares the MAC address of the AP against the list of authorized APs (which you must define). If the scanned AP does not appear in the list of authorized APs, it is displayed in the Rogue access points table.

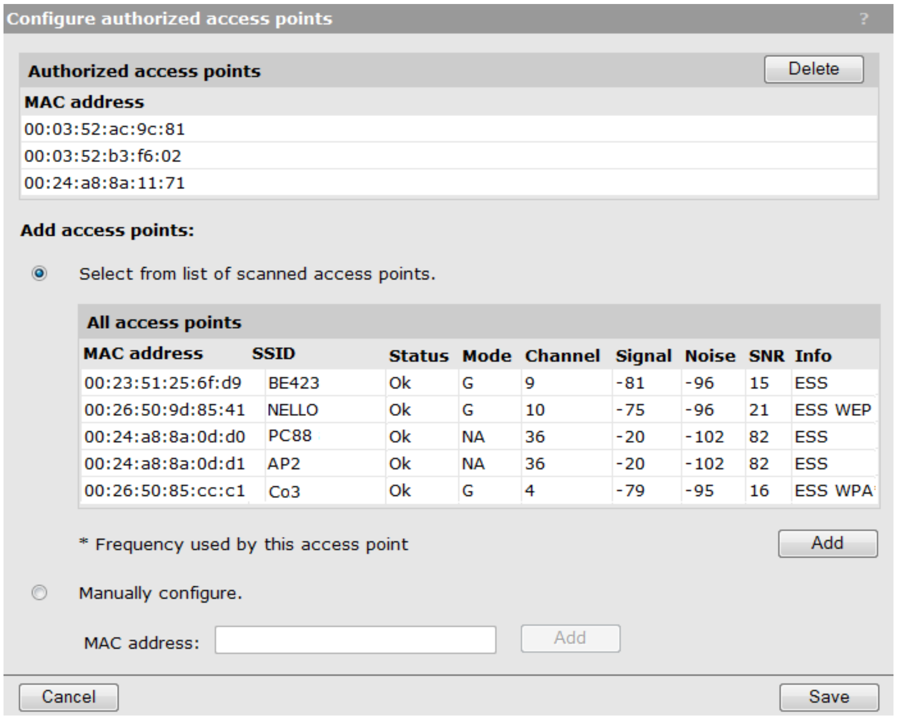
If the V-M200 is in background scanning mode, it will scan all channels in the currently selected radio operating mode approximately once every two hours (assuming the default scan interval of 600 seconds). This provides for continuous background monitoring for rogue APs.

Creating a list of authorized access points

The easiest way to create this list is automatically. However, this requires that the authorized APs are already operating and have been found by a scan. If not, then the list can be defined manually.

To create the list

1. Under the **Authorized access points** table, click **Configure Access Point List**.
2. Under **Add access points**, do the following for each access point you want to authorize:



Authorized access points
MAC address
00:03:52:ac:9c:81
00:03:52:b3:f6:02
00:24:a8:8a:11:71

Add access points:

● Select from list of scanned access points.

All access points

MAC address	SSID	Status	Mode	Channel	Signal	Noise	SNR	Info
00:23:51:25:6f:d9	BE423	Ok	G	9	-81	-96	15	ESS
00:26:50:9d:85:41	NELLO	Ok	G	10	-75	-96	21	ESS WEP
00:24:a8:8a:0d:d0	PC88	Ok	NA	36	-20	-102	82	ESS
00:24:a8:8a:0d:d1	AP2	Ok	NA	36	-20	-102	82	ESS
00:26:50:85:cc:c1	Co3	Ok	G	4	-79	-95	16	ESS WPA

* Frequency used by this access point

○ Manually configure.

MAC address:

- If the access points you want to add appear in the **All access points table:**
  1. Select the option **Select from list of scanned access points**.
  2. Select the access point in the **All access points table** that you want to authorize.
  3. Select **Add**. The MAC address for this access point is added to the **Authorized access points** table.

- To add access points that do not appear in the **All access points table:**
    1. Select the option **Manually configure**.
    2. Specify the **MAC address** of the access point that you want to authorize. The MAC address must be in the following format: 12 hexadecimal numbers separated by colons, with the values “a” to “f” in lowercase. For example: **00:03:520:a0:f01**.
    3. Select **Add**. The MAC address is added to the **Authorized access points** table.

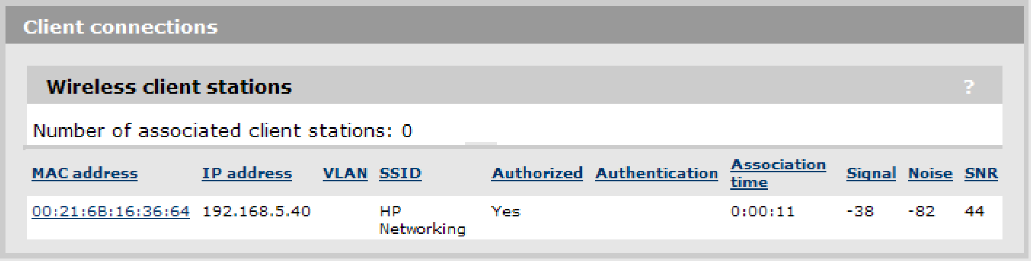
3. Select **Save** to return to the Rogue AP detection page. The Authorized access points table will show all the new APs that you added, and they will no longer appear in the Rogue access points table.

Viewing wireless information

The V-M200 provides several pages where you can view information related to wireless operation.

Viewing all connected wireless clients

Select **Wireless > Client** connections.



Client connections

Wireless client stations

Number of associated client stations: 0

MAC address	IP address	VLAN	SSID	Authorized	Authentication	Association time	Signal	Noise	SNR
00:21:6B:16:36:64	192.168.5.40		HP Networking	Yes		0:00:11	-38	-82	44

MAC address

The MAC address of the client station.

IP Address

The IP address assigned to the client station.

VLAN

The Ethernet VLAN assigned to the client station.

SSID

The SSID with which the client station is associated.

Authorized

- **Yes:** Client station has the right to transmit/receive traffic.

- **No:** Client station can only transmit/receive 802.1X packets.
- **Filtered:** Client traffic is blocked by the MAC filtering feature.

Authentication

Indicates how the client station was authenticated.

Association time

Indicates how long the client station has been associated with the V-M200.

Signal

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

Noise

Indicates how much background noise exists in the signal path between the client station and the V-M200. Noise is expressed in decibel milliwatt (dBm). The lower (more negative) the value, the weaker the noise.

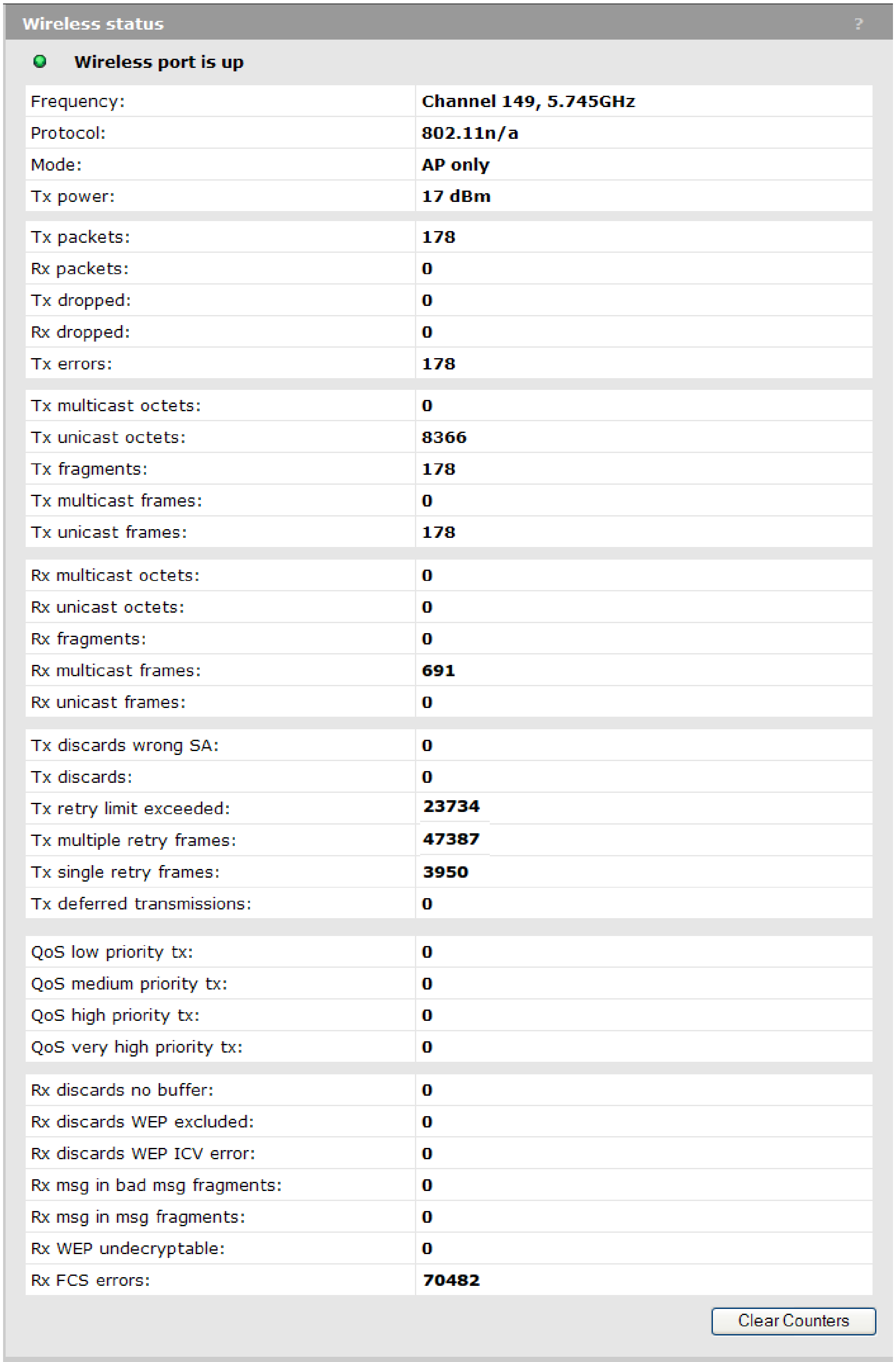
SNR

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

In most environments, SNR is a good indicator for the quality of the radio link between the client station and the V-M200. A higher SNR value means a better quality radio link.

Viewing wireless statistics for the radio

Select **Status > Wireless**.



● Wireless port is up

Frequency:	Channel 149, 5.745GHz
Protocol:	802.11n/a
Mode:	AP only
Tx power:	17 dBm
Tx packets:	178
Rx packets:	0
Tx dropped:	0
Rx dropped:	0
Tx errors:	178
Tx multicast octets:	0
Tx unicast octets:	8366
Tx fragments:	178
Tx multicast frames:	0
Tx unicast frames:	178
Rx multicast octets:	0
Rx unicast octets:	0
Rx fragments:	0
Rx multicast frames:	691
Rx unicast frames:	0
Tx discards wrong SA:	0
Tx discards:	0
Tx retry limit exceeded:	23734
Tx multiple retry frames:	47387
Tx single retry frames:	3950
Tx deferred transmissions:	0
QoS low priority tx:	0
QoS medium priority tx:	0
QoS high priority tx:	0
QoS very high priority tx:	0
Rx discards no buffer:	0
Rx discards WEP excluded:	0
Rx discards WEP ICV error:	0
Rx msg in bad msg fragments:	0
Rx msg in msg fragments:	0
Rx WEP undecryptable:	0
Rx FCS errors:	70482

Wireless port

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

Frequency

The current operating frequency.

Protocol

Identifies the wireless protocol used by the V-M200 to communicate with wireless users.

Mode

Current mode of operation.

Tx power

Current transmission power.

Tx packets

The total number of packets transmitted.

Rx packets

The total number of packets received.

Tx dropped

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

Rx dropped

The number of received packets that were dropped due to lack of resources on the V-M200. This should not occur under normal circumstances. A possible cause could be if many client stations are continuously transmitting small packets at a high data rate.

Tx errors

The total number of packets that could not be sent due to the following error: Rx retry limit exceeded.

Tx multicast octets

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

Tx unicast octets

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

Tx fragments

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

Tx multicast frames

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

Tx unicast frames

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

Rx multicast octets

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

Rx unicast octets

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

Rx fragments

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

Rx multicast frames

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

Rx unicast frames

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

Tx discards wrong SA

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

Tx discards

The number of transmit requests that were discarded to free up buffer space on the V-M200. This can be caused by packets being queued too long in one of the transmit queues, or because too many retries and defers occurred, or otherwise not being able to transmit (for example, when scanning).

Tx retry limit exceeded

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

Tx multiple retry frames

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

Tx single retry frames

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

Tx deferred transmissions

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

QoS low priority tx

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

QoS medium priority tx

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

QoS high priority tx

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

QoS very high priority tx

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

Rx discards no buffer

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

Rx discards WEP excluded

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

Rx discards WEP ICV error

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

Rx MSG in bad msg fragments

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

Rx MSG in msg fragments

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

Rx WEP undecryptable

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

Rx FCS errors

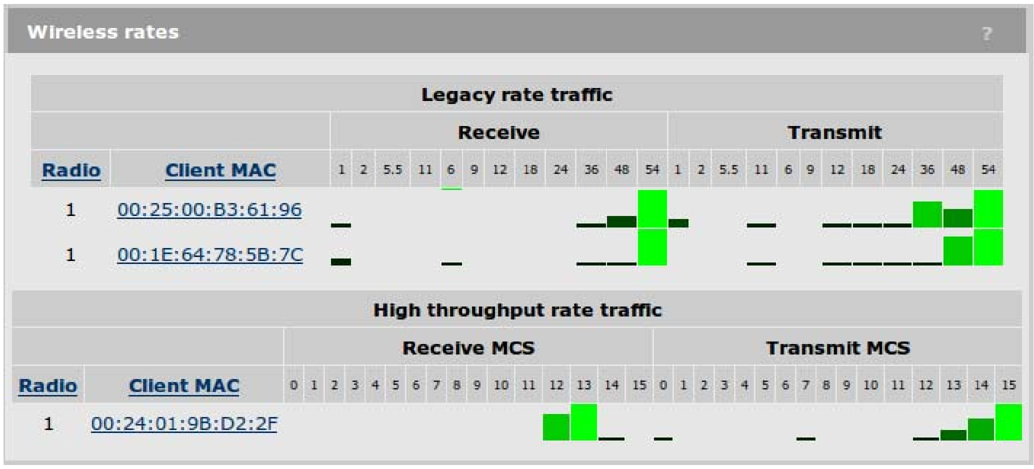
The number of MPDUs, considered to be destined for this station (Address matches), received with an FCS error. Note that this does not include data received with an incorrect CRC in the PLCP header. These are not considered to be MPDUs.

Clear counters

Click this button to reset all counters to zero.

Viewing throughput for wireless clients

Select **Status > Wireless rates**.



Legacy rate traffic

		Receive												Transmit											
Radio	Client MAC	1	2	5.5	11	6	9	12	18	24	36	48	54	1	2	5.5	11	6	9	12	18	24	36	48	54
1	00:25:00:B3:61:96																								
1	00:1E:64:78:5B:7C																								

High throughput rate traffic

		Receive MCS																Transmit MCS															
Radio	Client MAC	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	00:24:01:9B:D2:2F																																

This page indicates the volume of traffic sent and received at each data rate for each connected user.

- **Legacy rate traffic:** Displays information for clients using 802.11 a/b/g modes. The size of the bar indicates the amount of traffic sent at each rate.
- **High Throughput rate traffic:** Displays information for clients using 802.11n modes for each supported MCS (modulation coding scheme). The size of the bar indicates the amount of traffic sent at each MCS. For the V-M200, supported rates are as follows:

MCS	Data rate in Mbps based on channel width	
	20 MHz	40 MHz
0	6.50	13.50
1	13.00	27.00
2	19.50	40.50
3	26.00	54.00
4	39.00	81.00
5	52.00	108.00

MCS	Data rate in Mbps based on channel width	
	20 MHz	40 MHz
6	58.50	121.50
7	65.00	135.00
8	13.00	27.00
9	26.00	54.00
10	39.00	81.00
11	52.00	108.00
12	78.00	162.00
13	104.00	216.00
14	117.00	243.00
15	130.00	270.00

6

Configuring network settings and VLANs

Contents

Assigning an IP address to the V-M200

There are several ways to assign an IP address to the Ethernet port on the V-M200.

Automatically assigning an IP address (default method)

By default the V-M200 operates as a DHCP client. This means that if the network has a DHCP server, the V-M200 will automatically receive a new IP address in place of its default IP address (192.168.1.1) upon connecting to the network.

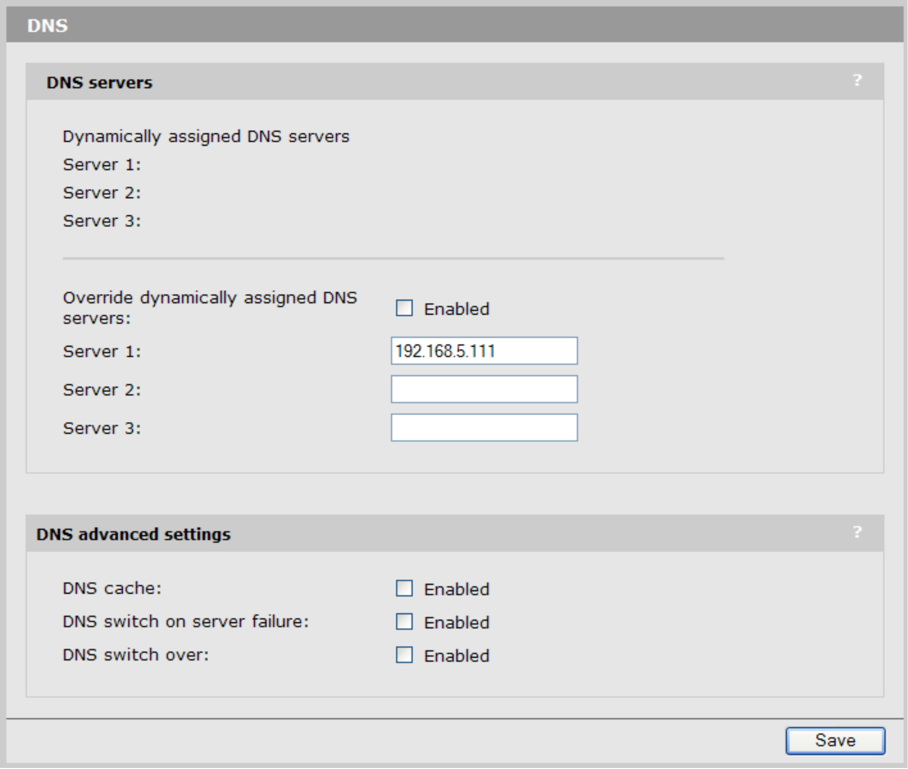
The DHCP server will assign an address from its pool of available addresses. You can find the IP address of the V-M200 by looking for its Ethernet base MAC address in the DHCP server log. The Ethernet MAC address is printed on the V-M200 label identified as **Ethernet Base MAC**, or listed on the management tool Home page as **Ethernet MAC address**.

To have the DHCP server assign a specific IP address to the V-M200, you need to pre-configure the DHCP to associate the IP address you want to use with the MAC address of the Ethernet port on the V-M200.

Manually assigning an IP address

You can manually assign an IP address to the Ethernet port. This requires that you also define the address of the DNS server and default gateway that are in use on your network.

1. Select **Network > DNS.** The DNS page opens.



DNS

DNS servers

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

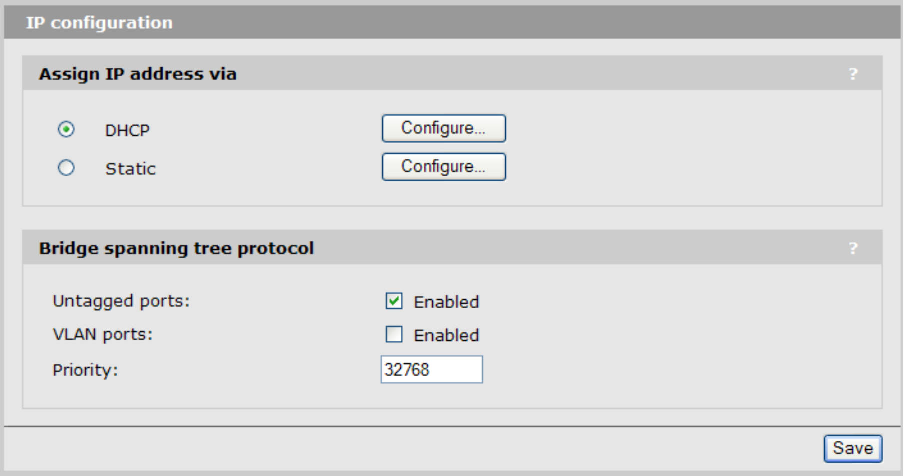
Override dynamically assigned DNS servers: □ Enabled
Server 1: 192.168.5.111
Server 2:
Server 3:

DNS advanced settings

DNS cache: □ Enabled
DNS switch on server failure: □ Enabled
DNS switch over: □ Enabled

Save

2. Select the checkbox next to **Override dynamically assigned DNS servers**.
3. Define an IP address for at least **Server 1**. Define values for **Server 2** and **Server 3** if available on your network.
4. Select the checkbox next to **DNS cache**.
5. Select **Save**.
6. Select **Network > IP**. The IP configuration page opens.



IP configuration

Assign IP address via

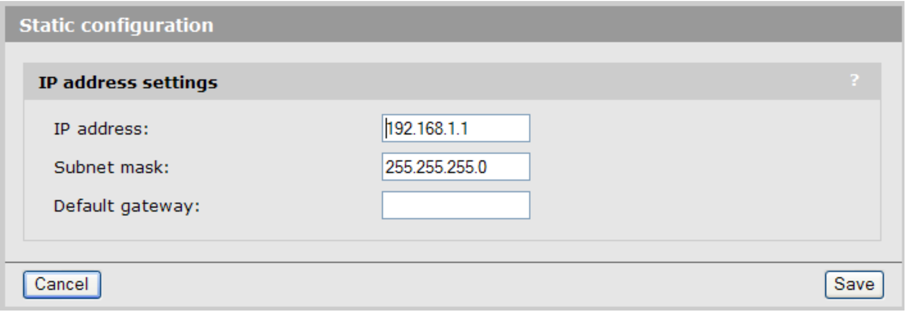
● DHCP [Configure...]
○ Static [Configure...]

Bridge spanning tree protocol

Untagged ports: ☑ Enabled
VLAN ports: □ Enabled
Priority: 32768

[Save]

7. Under **Assign IP address via**, select **Static** and then select **Configure**. The Static configuration page opens.



Static configuration

IP address settings

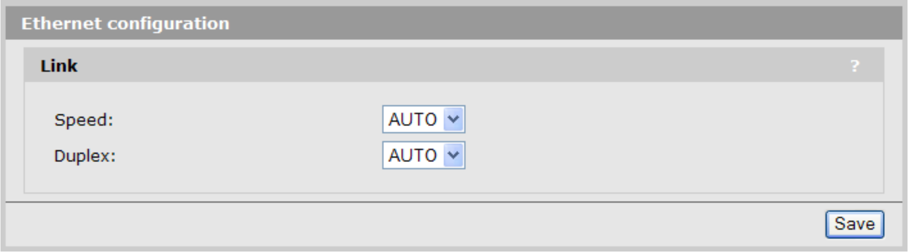
IP address: 192.168.1.1
Subnet mask: 255.255.255.0
Default gateway:

[Cancel] [Save]

8. Configure the following settings:
   - **IP address**: Set an address that is on the same subnet as the network to which the V-M200 will connect once installed. Respect any DHCP server-mandated static address ranges.
   - **Subnet mask**: Set the corresponding mask for the IP address.
   - **Default gateway**: Set the IP address of the gateway on the network.
9. Select **Save**. Your connection to the management tool will be lost.
10. You can now connect the Ethernet port on the V-M200 to your network.

Ethernet port link settings

If required, you can adjust the link settings by selecting **Network > Ethernet.**



Ethernet configuration

Link

Speed: AUTO

Duplex: AUTO

If you do not use the **Auto** setting for **Speed** or **Duplex**, make sure that the device to which the V-M200 is connected has a matching configuration. If there is a speed mismatch, the link will not be established. If there is a duplex mismatch, the link may be established but with transmission errors and reduced connectivity.

Speed

- **Auto:** Lets the V-M200 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 V-M200 automatically set duplex mode based on the type of equipment to which it is connected.
- **Full:** Forces the port to operate in full duplex mode.
- **Half:** Forces the port to operate in half duplex mode.

Working with VLANs

The V-M200 provides a robust and flexible VLAN implementation that enables you to group wireless clients by functionality, workgroup, or application rather than by their physical location.

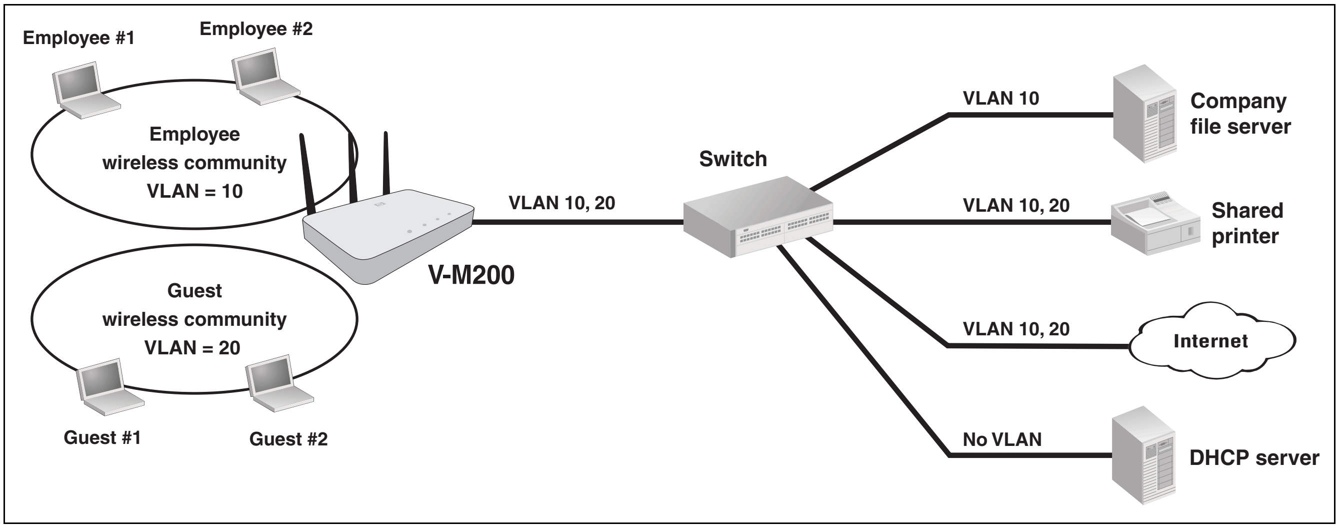
VLANs enable you to effectively send traffic from wireless users onto different logical segments on the same physical network connected to the Ethernet port.

VLANs can be assigned globally to all users on a wireless community, or individually on a per-user basis when using a RADIUS server for authentication. The following sections explain how to configure both options.

VLAN assignment via wireless community

The easiest way to assign user traffic to a VLAN is to configure the **Ethernet VLAN** setting in a wireless community (See *Ethernet VLAN on page 4-7*). This puts all the traffic from users that connect to the wireless community onto the specified VLAN via the V-M200 Ethernet port.

In the following scenario, two wireless communities are defined, each with its own VLAN.



- The Employee wireless community is configured with VLAN 10. All employee traffic exits the V-M200 on VLAN 10, providing access to the company file server, shared printer, and the Internet.
- The Guest wireless community is configured with VLAN 20. All guest traffic exits the V-M200 on VLAN20, providing access to the shared printer and the Internet.

Note

If two wireless communities are assigned to the same VLAN, wireless users may be able to communicate with each other. See *Communication between users on different wireless communities on page 4-6*.

VLAN assignment via RADIUS

VLANs can also be assigned on a per-user basis by setting VLAN attributes in a user's RADIUS account. To use this option you need to do the following:

- Configure a wireless community with **Security method** set to **WPA** or **802.1X**. If using WPA, **Key source** must be set to **RADIUS**. For configuration details, see *Wireless protection on page 4-7*.
- Configure a RADIUS profile to connect with the RADIUS server. For configuration details, see *Defining a RADIUS client profile on the V-M200 on page 7-2*.
- Define RADIUS user accounts with the appropriate VLAN attributes (Tunnel-Medium-Type, Tunnel-Private-Group-ID, and Tunnel-Type). For configuration details, see *Configuring user accounts on a RADIUS server on page 7-5*.

Note When a VLAN is defined in a user's RADIUS account it always overrides the Ethernet VLAN defined for a wireless community. This enables you to define an Ethernet VLAN setting for a community and then override it on a per-user basis as required.

Example

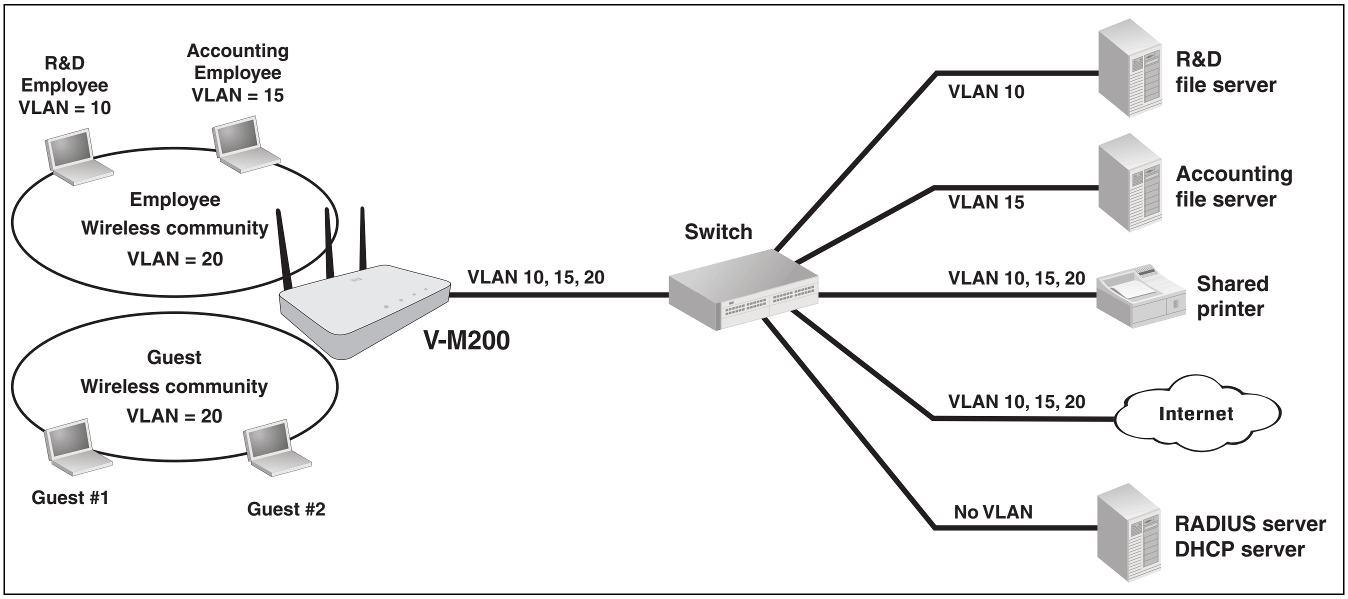
In the following scenario, RADIUS user accounts are configured to assign employees to different VLANs depending on the workgroup to which an employee belongs.

Employee wireless community

- R&D employees are assigned to VLAN 10 via attributes in their RADIUS account.
- Accounting employees are assigned to VLAN 15 via attributes in their RADIUS account.
- Employees without a VLAN assignment in their RADIUS account get assigned to the VLAN that is configured for the wireless community, which in this example is 20. This enables these employees to access the shared printer and the Internet.

Guest wireless community

- The Guest community does not use RADIUS. All traffic on the Guest community is assigned to VLAN 20, providing access to the shared printer and the Internet.



Bridging traffic between wireless communities with VLANs

When users on two different wireless communities are assigned to the same VLAN, they may be able to communicate with each other depending on the setting of the **Allow traffic between all/no wireless clients** option. See *Communication between users on different wireless communities on page 4-6* for details.

Discovery protocols

The V-M200 supports the Link Layer Discovery Protocol (LLDP) and the Cisco Discovery Protocol (CDP). These protocols provide a mechanism for the V-M200 to exchange information about its identity, capabilities, and interconnection with other devices on the network.

Information gathered via LLDP and CDP is stored in the V-M200 in a management information database (MIB) and can be retrieved with the simple network management protocol (SNMP).

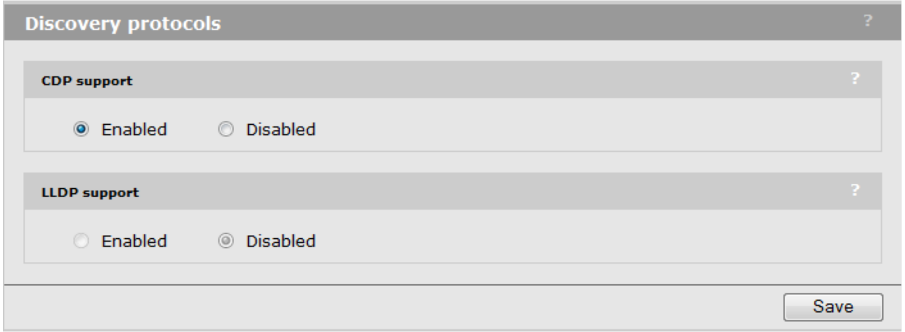
CDP

CDP (Cisco Discovery Protocol) provides a mechanism for the V-M200 to advertise information about itself to other devices on the wired network. This information is useful for network administration purposes and is sent on the Ethernet port and any active WDS links.

When the CDP support is enabled, the CDP settings are configured by default and cannot be changed.

To enable CDP support

1. Select **Network > Discovery protocols**.



Discovery protocols

CDP support

● Enabled ○ Disabled

LLDP support

○ Enabled ● Disabled

2. Select **Enabled** under **CDP support** and then select **Save**.

LLDP

The IEEE 802.1AB Link Layer Discovery Protocol (LLDP) provides a standards-based method for network devices to discover each other and exchange information about their capabilities. An LLDP device advertises itself to adjacent (neighbor) devices by transmitting LLDP data packets on all ports on which outbound LLDP is enabled, and reading LLDP advertisements from neighbor devices on ports that are inbound LLDP-enabled. An LLDP enabled port receiving LLDP packets inbound from neighbor devices stores the packet data in a Neighbor database (MIB).

LLDP information is used by network management tools to create accurate physical network topologies by determining which devices are neighbors and through which ports they connect.

LLDP operates at layer 2 and requires an LLDP agent to be active on each network interface that will send and receive LLDP advertisements. LLDP advertisements can contain a variable number of TLV (type, length, value) information elements. Each TLV describes a single attribute of a device.

When an LLDP agent receives information from another device, it stores the information locally in a special LLDP MIB (management information base). This information can then be queried by other devices via SNMP. For example, the HP Manager software retrieves this information to build an overview of a network and all its components.

Note LLDP information is only sent/received on the Ethernet port and active WDS links. LLDP information is not collected from wireless devices connected to an AP.

SNMP support

Support is provided for the following MIBs:

- LLDP MIB definition described in chapter 12 of the 802.1AB standard.
- Interfaces MIB (RFC 2863).

Supported LLDP TLVs

When the LLDP support is enabled, the LLDP agent supports the following mandatory and optional TLVs.

Mandatory TLVs

- **Chassis ID (Type 1):** The MAC address of the V-M200.
- **Port ID (Type 2):** The MAC address of the port on which the TLV will be transmitted.
- **Time to live (Type 3):** Defines the length of time that neighbors will consider LLDP information sent by this agent to be valid. Calculated by multiplying Transmit interval by the Multiplier.

Optional TLVs

- **Port description (Type 4):** A description of the port.
- **System name (Type 5):** Administrative name assigned to the device from which the TLV was transmitted.
- **System description (Type 6):** Description of the system, comprised of the following information: operational mode, hardware type, hardware revision, and firmware version.
- **System capabilities (Type 7):** Indicates the primary function of the device. Set to: **WLAN access point**.

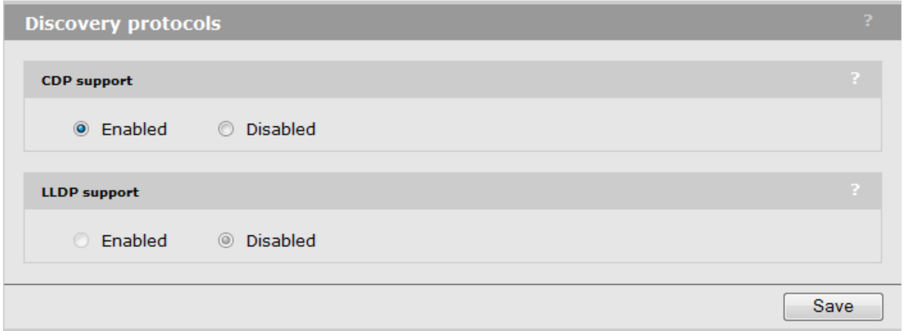
LLDP default settings

When the LLDP support is enabled, the values of the following LLDP settings are configured by default. You cannot change these values.

- **Transmit interval = 30 seconds.** The interval at which local LLDP information is updated and TLVs are sent to neighboring network devices.
- **Multiplier = 5 seconds.** The value of Multiplier is multiplied by the Transmit interval to define Time to live.
- **Time to live = 150 seconds.** Length of time that neighbors consider LLDP information sent by this agent to be valid. Time to live is calculated by multiplying Transmit interval by Multiplier.

Configuring LLDP support on the V-M200

LLDP settings are configured by selecting **Network > Discovery protocols**.


Discovery protocols

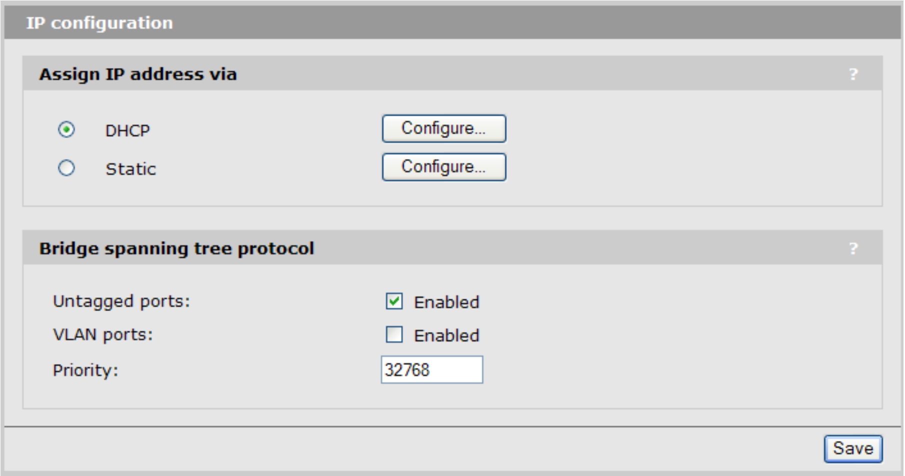
CDP support
● Enabled ○ Disabled

LLDP support
○ Enabled ● Disabled

To enable LLDP support, select **Enabled** under **LLDP support**.

Bridge spanning tree protocol

The V-M200 uses the Spanning-Tree Protocol (STP) to prevent undesirable loops from occurring in the network that may result in decreased throughput. Spanning tree is configured by selecting **Network > IP.**


IP configuration

Assign IP address via
● DHCP
○ Static

Bridge spanning tree protocol
Untagged ports: ☑ Enabled
VLAN ports: □ Enabled
Priority: 32768

Spanning tree can be enabled for:

- **Untagged ports:** Applies to all untagged traffic on the Ethernet port and active WDS links.
- **VLAN ports:** Applies to any traffic that has a VLAN assigned to it. VLANs can be assigned by setting the Ethernet VLAN option in a wireless community, or by setting a user-defined VLAN via RADIUS attributes.

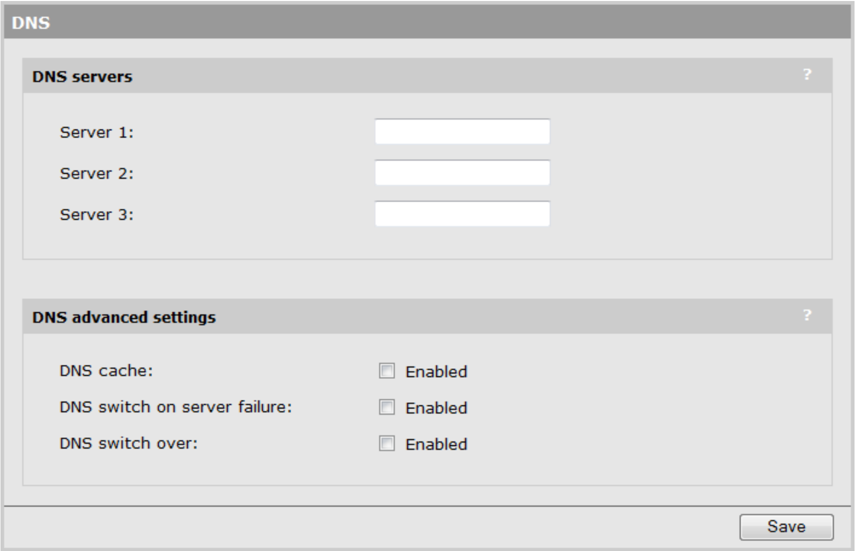
Priority

Sets the priority of the V-M200 within the spanning tree network. Generally, the bridge with lowest priority is designated as the root bridge of the spanning tree.

DNS server configuration

The V-M200 provides several options to customize DNS handling. To configure these options, select **Network > DNS.**

- If static IP addressing is being used, the following page is displayed allowing you to define up to three DNS servers.



DNS

DNS servers

Server 1:

Server 2:

Server 3:

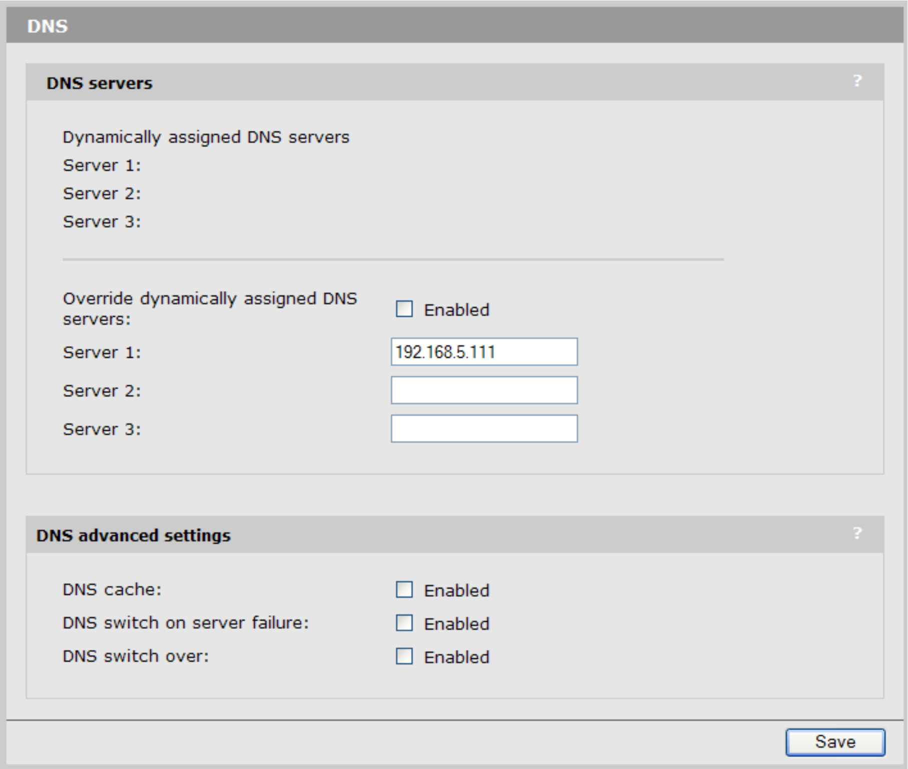
DNS advanced settings

DNS cache: □ Enabled

DNS switch on server failure: □ Enabled

DNS switch over: □ Enabled

- If DHCP IP addressing is being used, the following page is displayed. It shows the servers that have been dynamically assigned by the DHCP server. To manually assign your own DNS servers, select the **Override dynamically assigned DNS** option and then specify up to three DNS servers.



DNS

DNS servers

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

Override dynamically assigned DNS servers: ☐ Enabled
Server 1: 192.168.5.111
Server 2:
Server 3:

DNS advanced settings

DNS cache: ☐ Enabled
DNS switch on server failure: ☐ Enabled
DNS switch over: ☐ Enabled

DNS servers

- **Server 1**: Specify the IP address of the primary DNS server for the V-M200 to use.
- **Server 2**: Specify the IP address of the secondary DNS server for the V-M200 to use.
- **Server 3**: Specify the IP address of the tertiary DNS server for the V-M200 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 V-M200 restarts.

DNS switch on server failure

This setting controls how the V-M200 switches between the primary and secondary DNS servers.

- When enabled, the V-M200 switches servers if the current server replies with a DNS server failure message.
- When disabled, the V-M200 switches servers if the current server does not reply to a DNS request.

DNS switch over

This setting controls how the V-M200 switches back to the primary DNS server after it has switched to the secondary DNS server because the primary was unavailable.

- When enabled, the V-M200 switches back to the primary server after it becomes available again.
- When disabled, the V-M200 switches back to the primary server only if the secondary server becomes unavailable.

7

Authentication services

Contents

Using a third-party RADIUS server

The V-M200 can use third-party RADIUS servers to perform a number of authentication and configuration tasks, including the tasks shown in the table below.

Task	For more information see
Validating user login credentials for the WPA, 802.1X, or MAC-based authentication options.	*Wireless protection on page 4-7.* *MAC-based authentication on page 4-12*.
Storing custom configuration settings, such as a VLAN ID, for each user.	*Configuring user accounts on a RADIUS server on page 7-5*.
Storing accounting information for each user.	*Wireless protection on page 4-7* or *MAC-based authentication on page 4-12* for information on how to enable accounting support.

Defining a RADIUS client profile on the V-M200

The V-M200 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 V-M200.

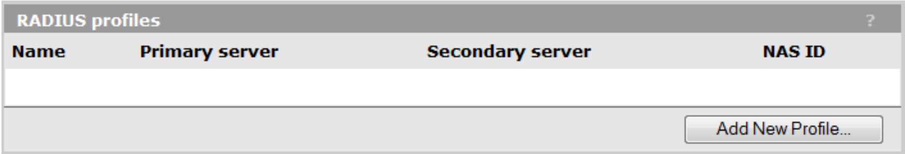
For backup redundancy, each profile supports a primary and secondary server.

The V-M200 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.

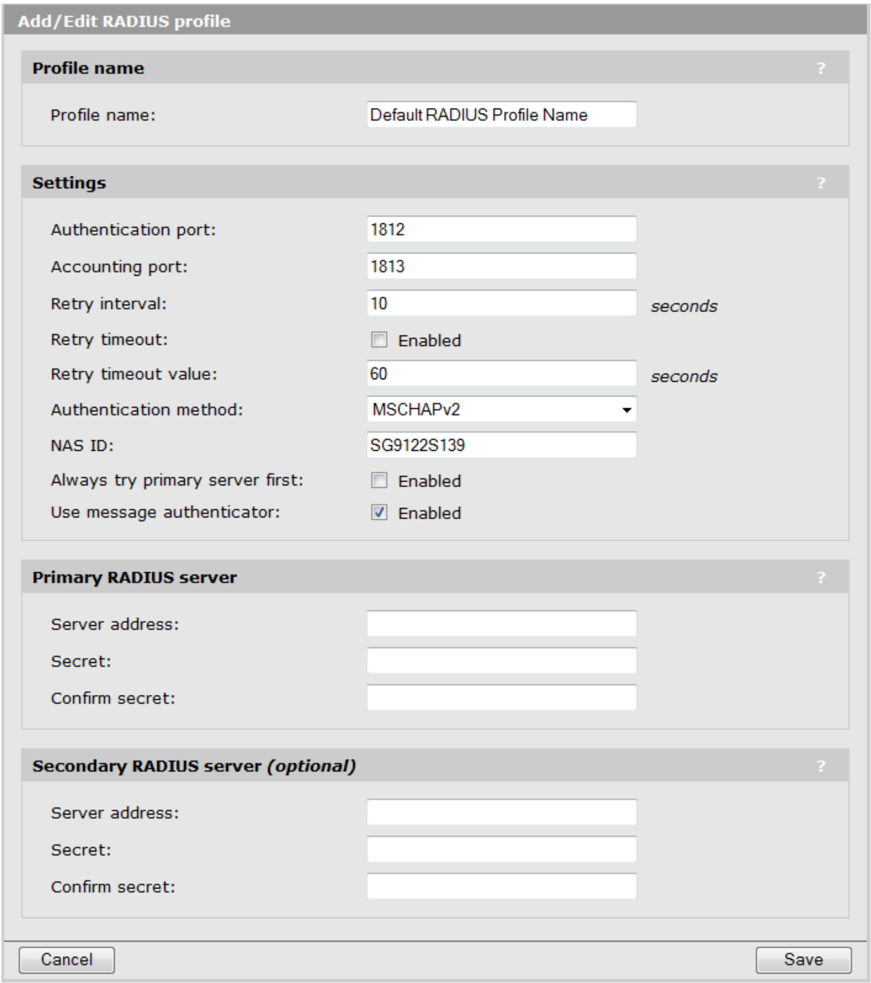
Note If you change a RADIUS profile to connect to a different server while users are active, all RADIUS traffic for active user sessions is immediately sent to the new server.

To define a RADIUS profile

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



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



Add/Edit RADIUS profile

Profile name

Profile name: Default RADIUS Profile Name

Settings

Authentication port: 1812

Accounting port: 1813

Retry interval: 10 *seconds*

Retry timeout: □ Enabled

Retry timeout value: 60 *seconds*

Authentication method: MSCHAPv2

NAS ID: SG9122S139

Always try primary server first: □ Enabled

Use message authenticator: ☑ Enabled

Primary RADIUS server

Server address:

Secret:

Confirm secret:

Secondary RADIUS server *(optional)*

Server address:

Secret:

Confirm secret:

3. Configure the profile settings as described in the following section.

4. Select **Save**.

Configuration settings

Profile name

Specify a name to identify the profile.

Settings

- **Authentication port:** Specify a port on the RADIUS server to use for authentication. By default RADIUS servers use port 1812.
- **Accounting port:** Specify a port on the RADIUS server to use for accounting. By default RADIUS servers use port 1813.

- **Retry interval:** Specify the number of seconds that the RADIUS server waits before access and accounting requests time out. If the server does not receive a reply within this interval, the V-M200 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:

  - 802.1x authentication.
  - MAC-based authentication.

  You can determine the maximum number of retries as follows:

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

- **Retry timeout:** When enabled, this option allows the V-M200 to drop accounting requests after retrying (every retry interval) for the specified **Retry timeout** value. When disabled, the V-M200 retries forever.
- **Retry timeout value:** Specify the amount of time (in seconds) between retries.
- **Authentication method:** Select the default authentication method that the V-M200 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 V-M200 and the RADIUS server is not protected by a VPN, it is recommended that you use either EAP-MD5 or MSCHAPv2 (if supported by your RADIUS Server). PAP, MSCHAPv1, and CHAP are less secure protocols.

- **NAS ID:** Specify the identifier for the network access server that you want to use for the V-M200. By default, the serial number of the V-M200 is used. The V-M200 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 V-M200 to contact the primary server first.

  Otherwise, the V-M200 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 V-M200 sends the first RADIUS access request to the secondary RADIUS server.

  If the secondary RADIUS server does not reply, the V-M200 retransmits the RADIUS access request to the primary RADIUS server. When two servers are configured, the V-M200 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 V-M200.

  Note: This option has no effect on 802.1X 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 V-M200 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. These attributes apply when a wireless community is configured to use WPA or 802.1X with RADIUS support.

Access Request attributes

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

Attribute	**WPA / 802.1X**	**MAC-based**	**Format**
Acct-Session-Id	✓	✓	32-bit unsigned integer
Called-Station-Id	✓	✓	Called-Station-Id
Calling-Station-Id	✓	✓	Calling-Station-Id
EAP-Message	✓	-	EAP-Message
Framed-MTU	✓	-	Framed-MTU
Message-Authenticator	✓	✓	Message-Authenticator
NAS-Identifier	✓	✓	NAS-Identifier
NAS-Ip-Address	✓	✓	NAS-IP-Address
NAS-Port	✓	✓	NAS-Port
NAS-Port-Type	✓	✓	NAS-Port-Type
Service-Type	✓	✓	Service-Type
State	✓		State
User-Name	✓	✓	User-Name
User-Password	-	✓	User-Password
Vendor-specific (Colubris) SSID	-	✓	Colubris-AVPair (SSID)

Descriptions

- **Acct-Session-Id** (32-bit unsigned integer): A unique accounting ID used to make it easy to match up records in a log file.
- **Called-Station-Id** (string): This value can be customized for each wireless community by setting the value of **Called-Station-ID content** (page *4-9*). The format can be customized for each wireless community by setting the value of **Station ID delimiter** and **Station ID MAC case** (page *4-9*)
- **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 can be customized for each wireless community by setting the value of **Station ID delimiter** and **Station ID MAC case** (page *4-9*).
- **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 **Authentication > RADIUS profiles** page for the RADIUS profile being used.
- **NAS-Ip-Address** (32-bit unsigned integer): The IP address of the port the V-M200 is using to communicate with the RADIUS server.
- **NAS-Port** (32-bit unsigned integer): A virtual port number starting at 1. Assigned by the V-M200.
- **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 method** on the **Authentication > RADIUS profiles** page is set to **PAP**. Or, if MAC-based authentication is being used, this is set to the MAC address of the wireless client station.
- **EAP-Message** (string): As defined in RFC 2869. Only present when the **Authentication method** on the **Authentication > RADIUS profiles** page is set to EAP-MD5.
- **Vendor-specific (Colubris-AVPair SSID)**: SSID of the wireless community to which the user is connected.

The Colubris-AVPair attribute conforms to RADIUS RFC 2865. You may need to define this attribute on your RADIUS server (if it is not already present) using the following values:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 0
- Attribute type: A string in the following format `<keyword>=<value>`

Access Accept attributes

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

Attribute	WPA / 802.1X	MAC-based
Acct-Interim-Interval	✓	✓
Class	✓	✓
EAP-Message	✓	-
Idle-Timeout	✓	-
MS-MPPE-Recv-Key	✓	-
MS-MPPE-Send-Key	✓	-
Session-Timeout	✓	✓
Termination-Action	✓	-
Tunnel-Medium-Type	✓	-
Tunnel-Private-Group-ID	✓	-
Tunnel-Type	✓	-
Vendor-specific (Microsoft) MS-MPPE-Recv-Key MS-MPPE-Send-Key	 ✓ ✓	 - -

Descriptions

- **Acct-Interim-Interval** (32-bit unsigned integer): When present, enables the transmission of RADIUS accounting requests of the **Interim Update** type. Specify the number of seconds between each transmission.
- **Class** (string): As defined in RFC 2865.
- **EAP-Message** (string): Note that the content will not be read, as the RADIUS Access Accept EAP-Message 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, user traffic is not allowed during the 802.1X re-authentication.
- **Tunnel-Medium-Type**: Used only when assigning a specific VLAN number to a user. In this case, it must be set to 802. The **tag** field for this attribute must be set to **0**.
- **Tunnel-Private-Group-ID**: Used only when assigning a specific VLAN number to a user. In this case it must be set to the VLAN ID. The **tag** field for this attribute must be set to **0**.
- **Tunnel-Type**: Used only when assigning a specific VLAN number to a user. In this case it must be set to VLAN. The **tag** field for this attribute must be set to **0**.
- **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.

Attribute	WPA / 802.1X	MAC-based
EAP-Message	✓	-
Message-Authenticator	✓	-
State	✓	-

Descriptions

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

Accounting Request attributes

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

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

Descriptions

- **Acct-Input-Gigawords** (32-bit unsigned integer): High 32-bit value of the number of octets/bytes received by the user. Only present when Acct-Status-Type is Interim-Update or Stop.
- **Acct-Input-Octets** (32-bit unsigned integer): Low 32-bit value of the number of octets/bytes received by the user. Only present when Acct-Status-Type is Interim-Update or Stop.

- **Acct-Input-Packets** (32-bit unsigned integer): Number of packets received by the user. Only present when Acct-Status-Type is Interim-Update or Stop.
- **Acct-Output-Gigawords** (32-bit unsigned integer): High 32-bit value of the number of octets/bytes sent by the user. Only present when Acct-Status-Type is Interim-Update or Stop. As defined in RFC 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 V-M200.
- **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.

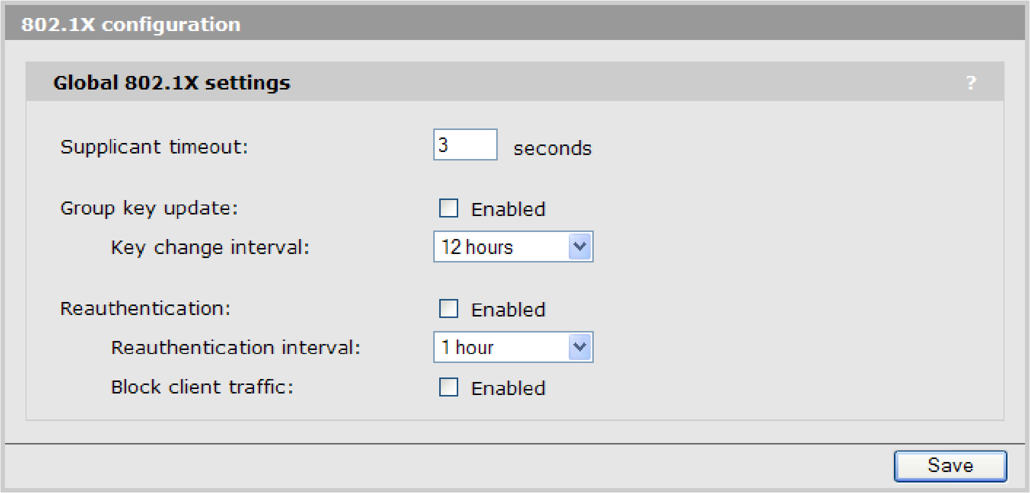
- **Called-Station-Id** (string): This value can be customized for each wireless community by setting the value of **Called-Station-ID content** (page *4-9*). The format can be customized for each wireless community by setting the value of **Station ID delimiter** and **Station ID MAC case** (page *4-9*)
- **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 can be customized for each wireless community by setting the value of **Station ID delimiter** and **Station ID MAC case** (page *4-9*).
- **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 V-M200).
- **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 **Authentication > RADIUS profiles** page for the profile being used.
- **NAS-Port** (32-bit unsigned integer): A virtual port number starting at 1. Assigned by the V-M200.
- **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 user 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>`

Global 802.1X settings

Global 802.1X settings are configured by selecting **Authentication > 802.1X**. These settings apply to all 802.1X connections in all wireless communities. This includes connections made with WPA/WPA2 when using a RADIUS server for authentication.



802.1X configuration

Global 802.1X settings

Supplicant timeout: 3 seconds

Group key update: □ Enabled

Key change interval: 12 hours

Reauthentication: □ Enabled

Reauthentication interval: 1 hour

Block client traffic: □ Enabled

Supplicant timeout

Specify the maximum length of time that the V-M200 will wait for a client station to respond to an EAPOL (Extensible Authentication Protocol over LAN) packet before resending it. (802.1X uses EAPOL for port access control.)

If client stations are configured to manually enter the 802.1X username or password or both, increase the value of the timeout to 15 to 20 seconds.

Group key update

Enable this option to force updating of 802.1X group keys at the selected **Key change interval**.

- **Key change interval**: Select the amount of time between updates to the group key.

Reauthentication

Enable this option to force 802.1X clients to reauthenticate.

- **Reauthentication interval:** Specify the interval at which client stations must reauthenticate.
- **Block client traffic:** When this option is disabled, client stations remain connected during reauthentication. Client traffic is blocked only when reauthentication fails. When this option is enabled, client traffic is blocked during reauthentication and is only reactivated if authentication succeeds.

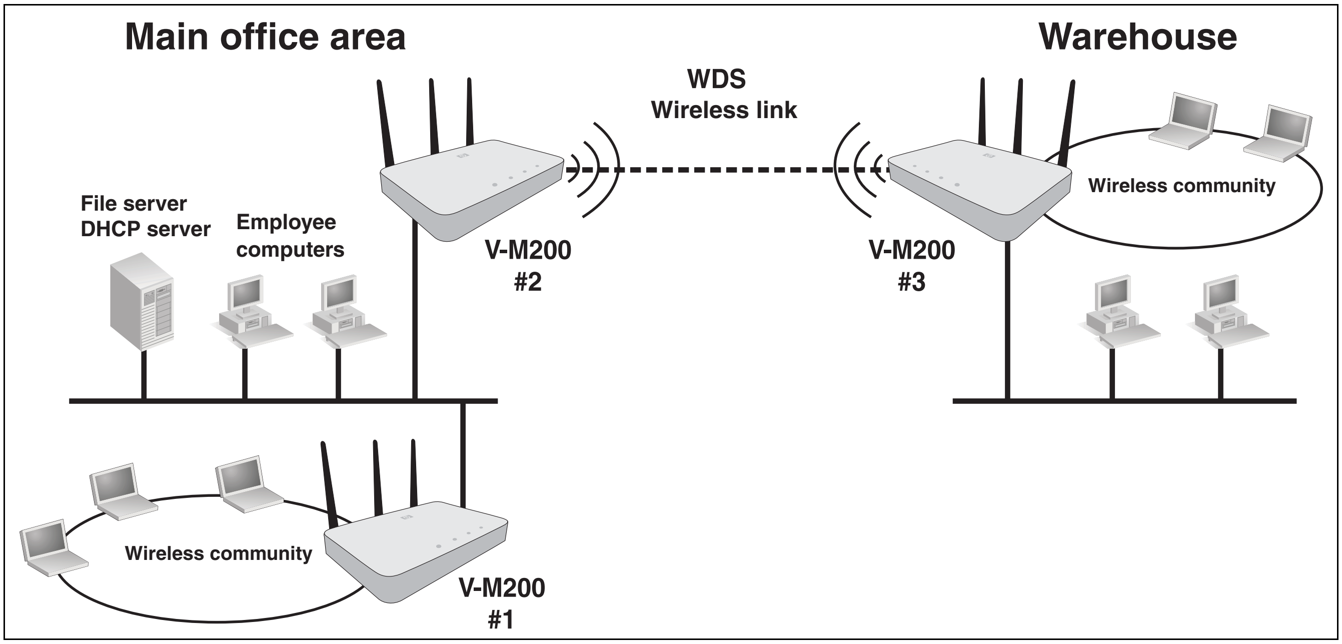
8

Creating WDS links

Contents

Key concepts

The Wireless Distribution System (WDS) feature enables you to create point-to-point wireless links between one or more V-M200s. These links create a wireless bridge that interconnects the networks connected to the Ethernet port on each V-M200. For example, V-M200 #2 and V-M200 #3 use the WDS to create a wireless link between the main office network and a small network in a warehouse.



WDS links provide an effective solution for extending network coverage in situations where it is impractical or expensive to run cabling. Each V-M200 can create up to three WDS links.

Configuration considerations

The following guidelines apply when you create a WDS link between two or more V-M200s.

- The radios on all V-M200s must be set to the same operating frequency and channel. This means that on the **Wireless > Radio** page under **Channel**, you cannot select **Automatic**.
- The Ethernet ports for all V-M200s must be connected to the same subnet, and each V-M200 must have a unique IP address.
- If AES/CCMP security is enabled, the same key must be defined on all V-M200s.
- Although the V-M200 can support up to three WDS links, only one link can be defined between any two V-M200s.

Simultaneous access point and WDS support

The V-M200 can be configured to simultaneously support wireless communities and one or more WDS links. Although this offers flexibility, it does have the following limitations:

- The total available bandwidth on the radio is shared between all WDS links and wireless users. This can result in reduced throughput if lots of traffic is being sent by both wireless users and the WDS links. You can use the QoS feature to prioritize traffic. See *Quality of service (QoS) on page 4-15* for details.
- The same radio options are used for both wireless clients and WDS links.

Using the 5 GHz band for WDS links

It is recommended that 802.11n or 802.11a in the 5 GHz band be used for WDS links whenever possible. This optimizes throughput and reduces the potential for interference.

Advantages

- 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 band for other applications such as WDS.
- 802.11a and 802.11n channels in the 5 GHz band are non-overlapping.
- Assuming an optimal implementation, 802.11a supports up to 54 Mbps and 802.11n supports up to 300 Mbps, providing a *fat pipe* for traffic exchange.

Limitations

- WDS links are not supported when the radio is configured in one of the following compatibility modes: **802.11n/a**, **802.11n/g**, or **802.11n/b/g**. Since the same radio options must be used for both wireless clients and WDS links, support for 802.11b/g clients is not possible.
- The 5 GHz band has a shorter reach when compared to the 2.4 GHz band. This could be a factor depending on the distance your WDS link span.

Quality of service

The WDS feature enables you to define a quality of service (QoS) setting that will govern how traffic is sent on all WDS links.

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

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

Traffic on a WDS link 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.

Note

When traffic is forwarded onto a WDS link from a wireless community, the QoS settings of the community take priority. For example, if you create a wireless community with a QoS setting of **Community Based High**, then traffic from this community will traverse the WDS link on queue 2, even if the QoS setting on the WDS link is **Low** (queue 4).

Priority mechanisms

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

802.1p

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

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

Very High, High, Normal, Low

These mechanisms enable you to assign a specific priority level to all traffic.

Queue	Priority value
1	Very High
2	High
3	Normal
4	Low

Diffserv (Differentiated Services)

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

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

Spanning-tree protocol

The Spanning-Tree Protocol (STP) can be used to prevent undesirable loops from occurring in the network that may result in decreased throughput. To enable STP for wireless links, see *Bridge spanning tree protocol on page 6-9*.

Discovery protocols

The V-M200 supports the Link Layer Discovery Protocol (LLDP) and the Cisco Discovery Protocol (CDP). These protocols provide a mechanism for the V-M200 to exchange information about its identity, capabilities, and interconnection with other devices on the network. When enabled, both protocols function across an active WDS links. See *Discovery protocols on page 6-7*.

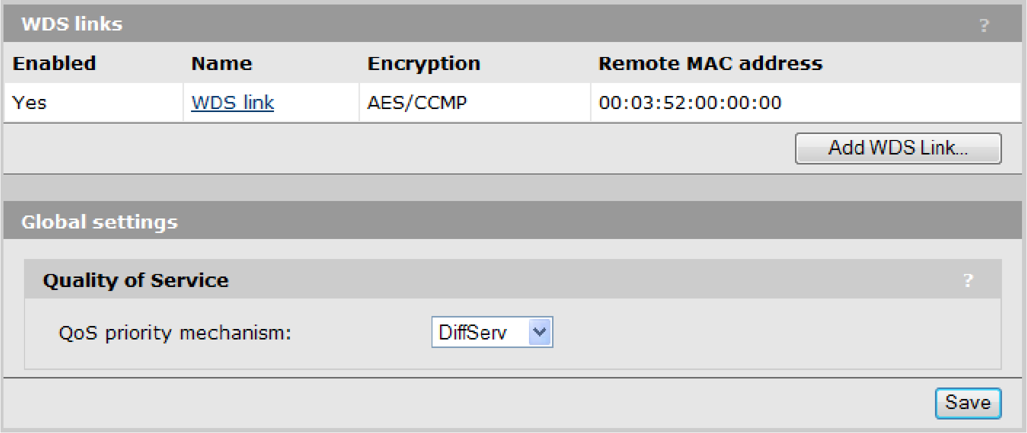
Configuration considerations

The following guidelines apply when you create a WDS link between two or more V-M200s.

- All radios must be set to the same operating frequency and channel. This means that on the **Wireless** > **Radio** page under **Channel,** you cannot select **Automatic.**
- The Ethernet ports for all V-M200s must be connected to the same subnet, and each V-M200 must have a unique IP address.
- If AES/CCMP security is enabled, the same key must be defined on all V-M200s.
- Although the V-M200 can support up to three WDS links, only one wireless link can be defined between any two V-M200s.

WDS configuration settings

To view or add a WDS link, select **Wireless > WDS.**



WDS links

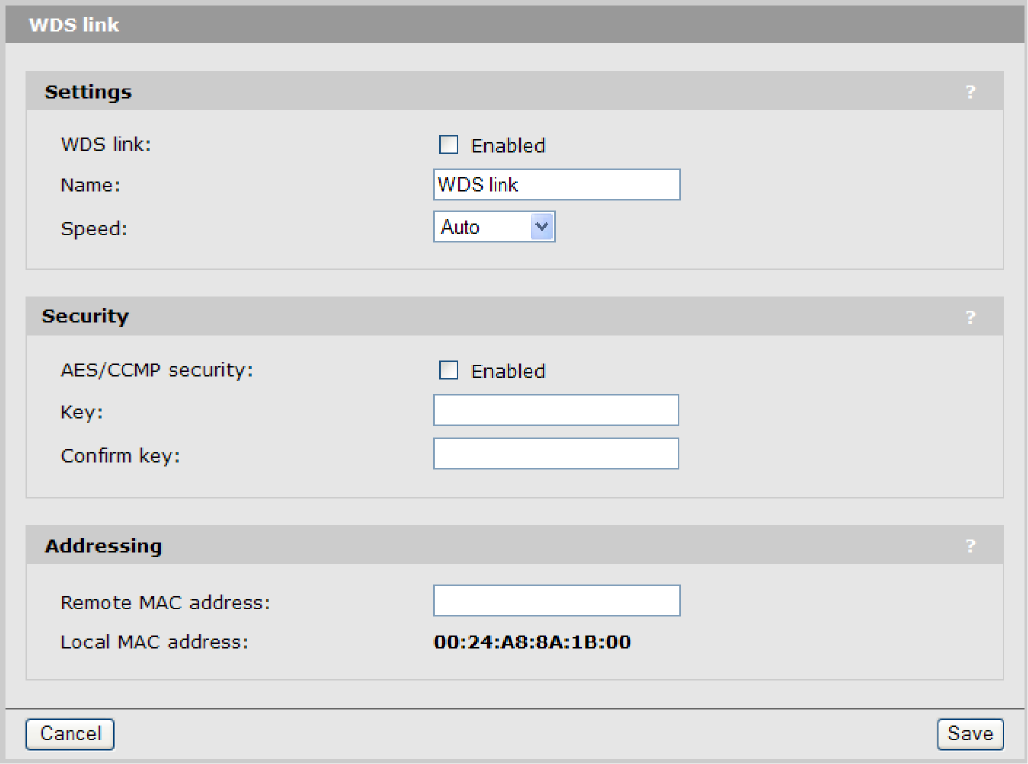
Enabled	Name	Encryption	Remote MAC address
Yes	WDS link	AES/CCMP	00:03:52:00:00:00

Global settings

Quality of Service

QoS priority mechanism: DiffServ

To configure a WDS link, select its name in the list. Or to add a WDS link, select **Add WDS Link**. In either case, the WDS link page opens.



WDS link

Settings

WDS link: □ Enabled

Name: WDS link

Speed: Auto

Security

AES/CCMP security: □ Enabled

Key:

Confirm key:

Addressing

Remote MAC address:

Local MAC address: **00:24:A8:8A:1B:00**

Settings

Enabled/Disabled

Specify if the WDS link is enabled or disabled. Once a link is enabled, it actively attempts to establish the WDS connection to the remote V-M200. To view the status of the WDS connection, select **Status > WDS**.

Name
Name of the WDS link.

Speed
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.

Select the **Auto** option to have the V-M200 automatically choose the speed that provides the best throughput (least number of errors).

Security

AES/CCMP security
Enables AES with CCMP encryption to secure traffic on the link. The V-M200 uses the key you specify in the **Key** field to generate the keys that encrypt the wireless data stream.

Specify a key that is between 8 and 63 ASCII characters in length. It is recommended that the key be at least 20 characters long and be a mix of letters and numbers.

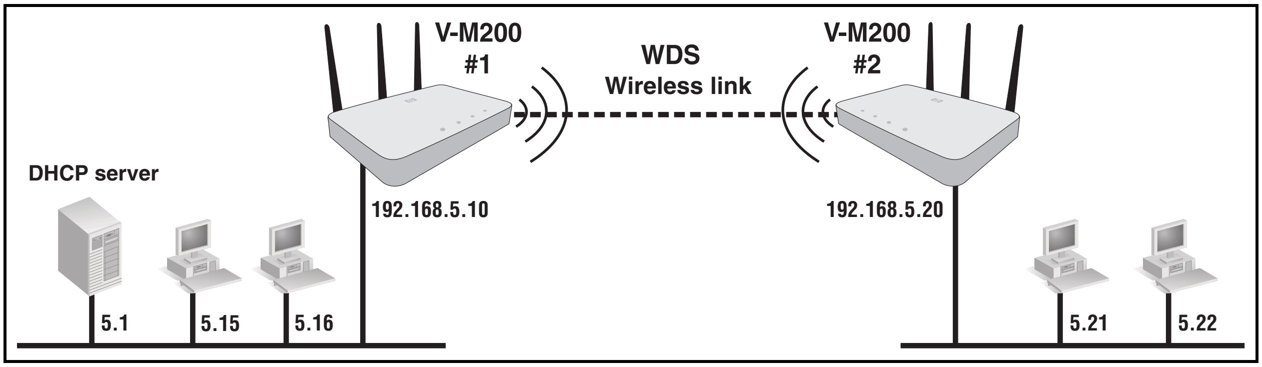
Addressing

Remote MAC address
Specify the MAC address of the wireless port on the remote <<PRODUCT-NAME>> to which this link will connect. The MAC address must be in the following format: 12 hexadecimal numbers, with the values “a” to “f” in lowercase. For example: 0003520a0f01.

Local MAC address
Shows the MAC address of the wireless port on the V-M200. This address needs to be entered on the V-M200 to which this link will connect.

Sample WDS deployment

This example shows you how to create a wireless link between two physically separate network segments.



This example assumes that both V-M200s have their IP addresses set and are connected to their respective networks as shown in the diagram.

A. Obtain the MAC address of V-M200 #2

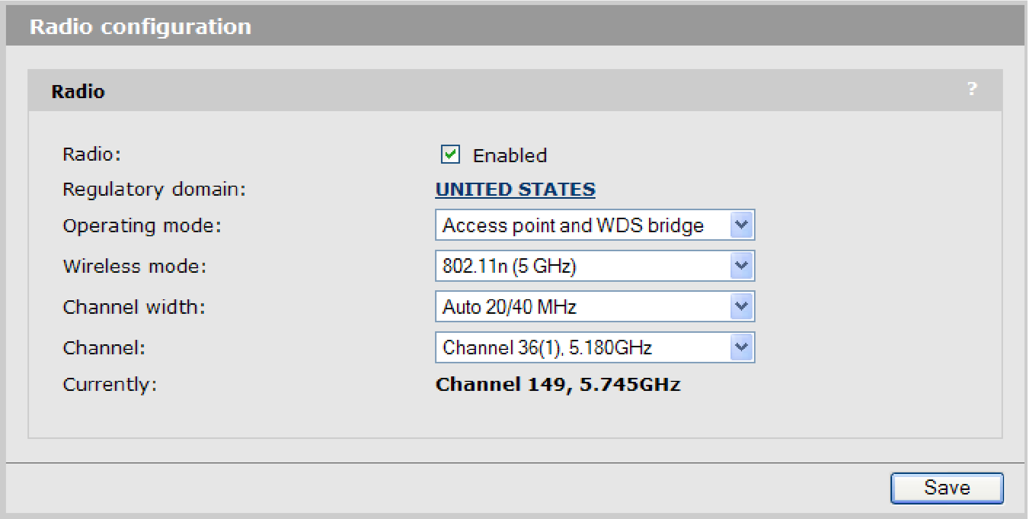
1. Connect to the management tool on V-M200 #2. Open the home page and write down its MAC address.

B. Setup the WDS link on V-M200 #1

2. Open the management tool on V-M200 #1.

3. Select **Wireless > Radio**. The Radio configuration page opens.

   - Enable the **Radio**.
   - Set **Operating mode** to **Access point and WDS bridge**.
   - Set **Wireless mode** to **802.11n (5 GHz)**.
   - Set **Channel** to **Channel 36**.
   - Select **Save**.



Radio configuration

Radio

Radio: ☑ Enabled

Regulatory domain: UNITED STATES

Operating mode: Access point and WDS bridge

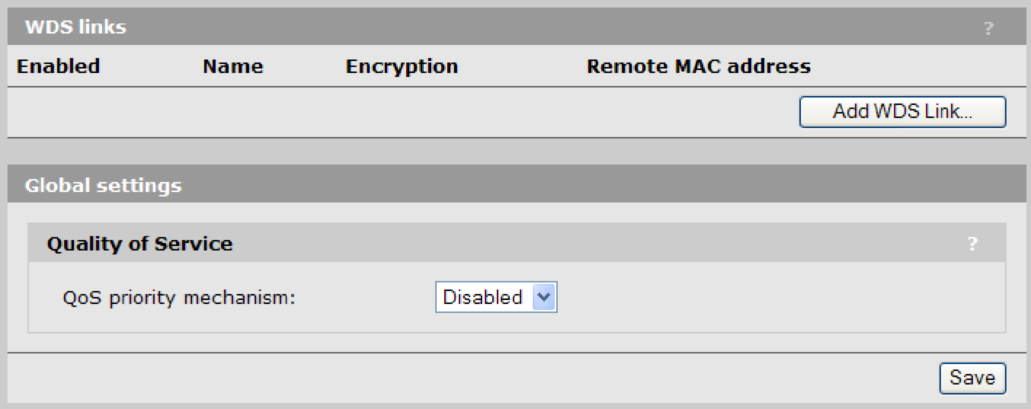
Wireless mode: 802.11n (5 GHz)

Channel width: Auto 20/40 MHz

Channel: Channel 36(1), 5.180GHz

Currently: **Channel 149, 5.745GHz**

4. Select **Wireless > WDS.**



WDS links

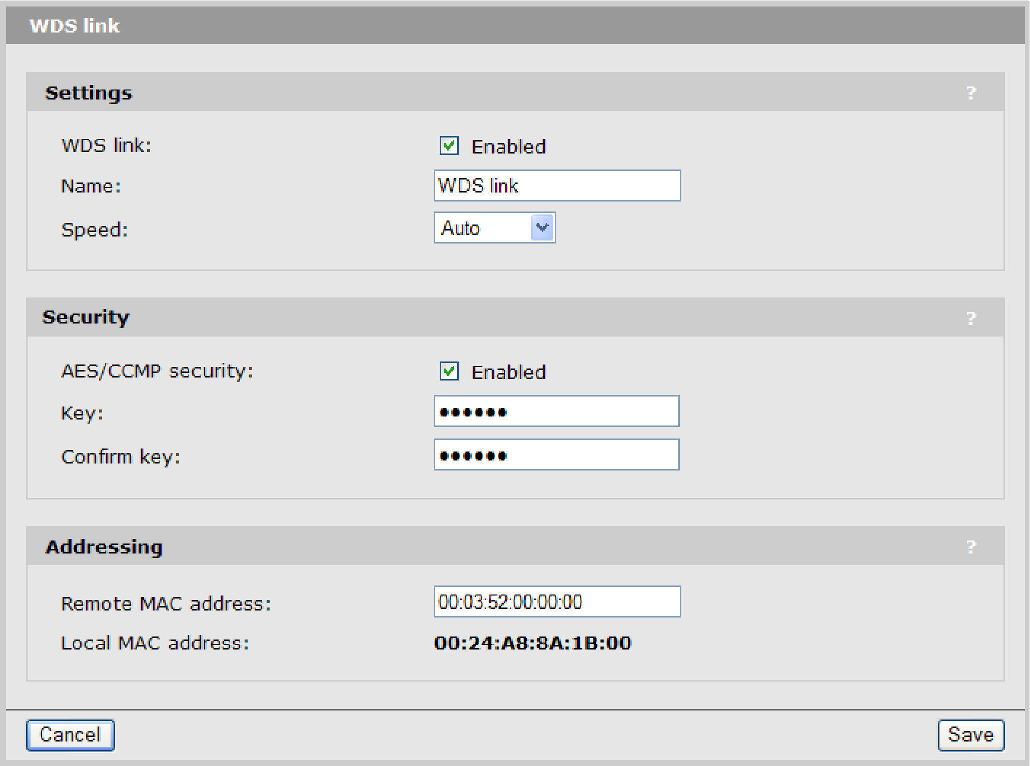
Enabled	Name	Encryption	Remote MAC address

Global settings

Quality of Service

QoS priority mechanism: Disabled

5. Select **Add WDS Link**.
    - Under **Security**:
        - Enable **security**.
        - Set **Key** to **a39xm2**.
    - Under **Addressing**:
        - Set **Remote MAC address** to the MAC address of V-M200 #2.
    - Select **Save**.



WDS link

Settings

WDS link: ☑ Enabled

Name: WDS link

Speed: Auto

Security

AES/CCMP security: ☑ Enabled

Key: ••••••

Confirm key: ••••••

Addressing

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

Local MAC address: **00:24:A8:8A:1B:00**

C. Setup the WDS link on V-M200 #2

Configuration settings on V-M200 #2 are similar to those defined on V-M200 #1.

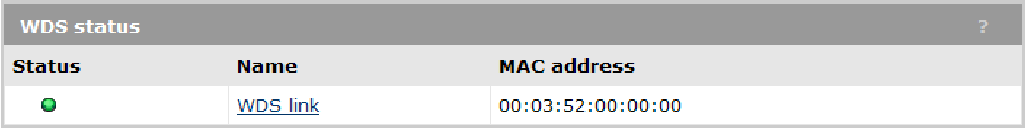
1. Open the management tool on the V-M200 #2.
2. Select **Wireless > Radio**. The Radio configuration page opens.
    - Enable the **Radio**.
    - Set **Operating mode** to **Access point and WDS bridge**.
    - Set **Wireless mode** to **802.11n (5 GHz)**.
    - Set **Channel** to **Channel 36**.
    - Select **Save**.
3. Select **Wireless > WDS.**

4. Select **Add WDS Link**.
   - Under **Security**:
     - Enable **AES/CCMP security**.
     - Set **Key** to **a39xm2**.
   - Under **Addressing**:
     - Set **Remote MAC address** to the MAC address of V-M200 #2.
   - Select **Save**.

D. Test the link and make performance adjustments

The WDS link should now be active.

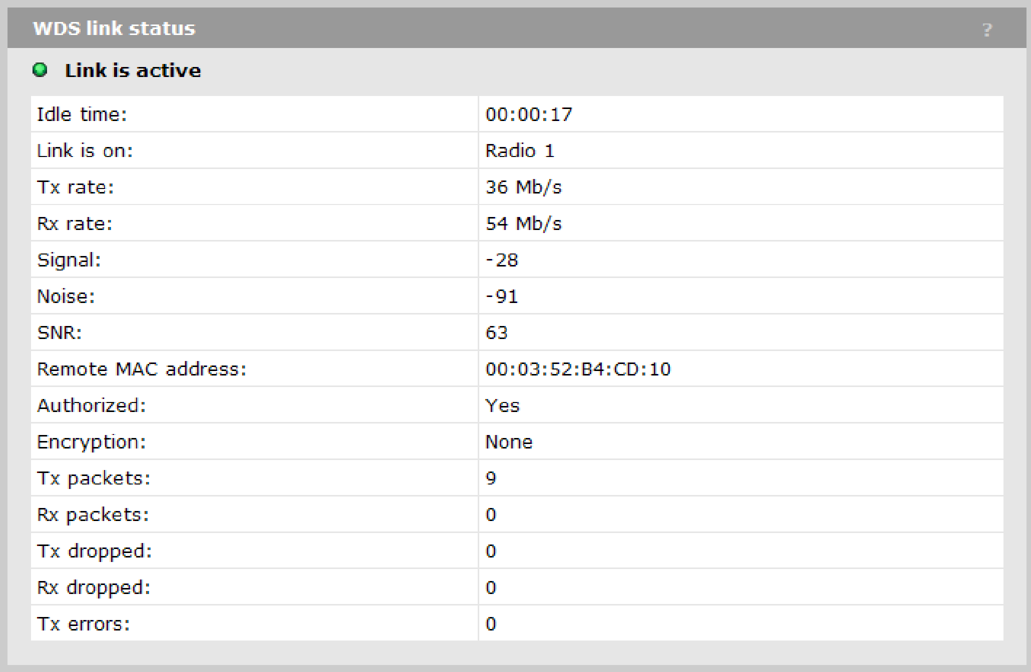
1. Select **Tools > Ping** on V-M200 #1 and ping the address of V-M200 #2 (192.168.5.20). If the ping succeeds, it means that the WDS link is working.
2. Select **Status > WDS**. The WDS status page opens.



WDS status ?

Status	Name	MAC address
●	WDS link	00:03:52:00:00:00

3. Select **WDS link** in the table. The WDS link status page opens.



WDS link status ?

● **Link is active**

Idle time:	00:00:17
Link is on:	Radio 1
Tx rate:	36 Mb/s
Rx rate:	54 Mb/s
Signal:	-28
Noise:	-91
SNR:	63
Remote MAC address:	00:03:52:B4:CD:10
Authorized:	Yes
Encryption:	None
Tx packets:	9
Rx packets:	0
Tx dropped:	0
Rx dropped:	0
Tx errors:	0

4. Use the **SNR** value as a guide to adjust the antennas to obtain the best possible **Tx Rate**. A higher SNR value means a better quality radio link.

   After each change, allow a minimum of two minutes for **Tx Rate** to report its new value.

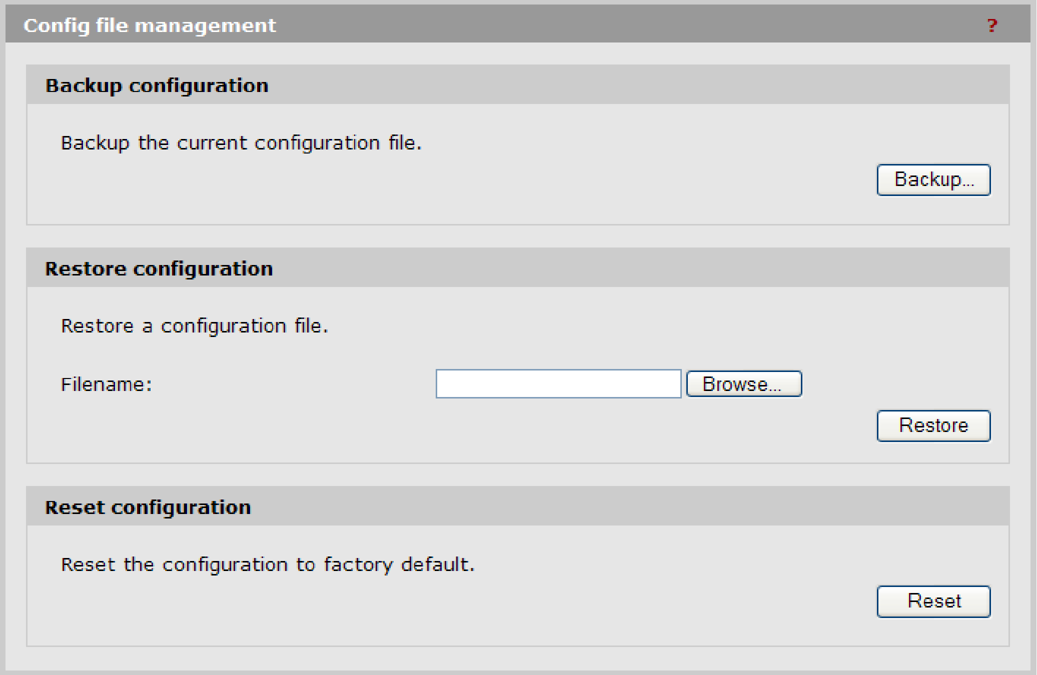
9

Maintenance

Contents

Config file management

The configuration file contains all the settings that customize the operation of the V-M200. You can save and restore the configuration file by selecting **Maintenance > Config file management**.



Config file management

Backup configuration

Backup the current configuration file.

Restore configuration

Restore a configuration file.

Filename:

Reset configuration

Reset the configuration to factory default.

Backup configuration

The **Backup configuration** feature enables you to back up your configuration settings so that they can be easily restored in case of failure.

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.

Note

The local username and password for the manager and operator accounts are not saved to the backup configuration file. If you restore a configuration file, the current manager and operator username and password are not overwritten.

Restore configuration

The **Restore configuration** feature enables you to load a previously saved configuration file. Use the following steps to restore a saved configuration file.

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

2. Under **Restore configuration,** select **Browse** to navigate to the configuration file that you want to restore.
3. To upload the selected file to the V-M200, select **Restore.**

Note

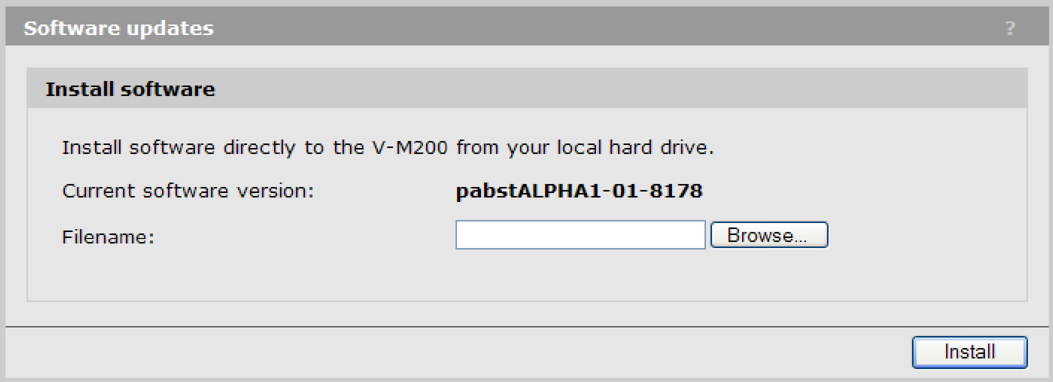
The V-M200 automatically restarts when the upload is completed.

Reset configuration

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

Software updates

To update the V-M200 software, select **Maintenance > Software updates**.



Install software directly to the V-M200 from your local hard drive.

Current software version: **pabstALPHA1-01-8178**

Filename:

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 back up your configuration settings before updating. See *Config file management on page 9-2*.
- At the end of the update process, the V-M200 automatically restarts, disconnecting all users. Once the V-M200 resumes operation, all users must reconnect.

To update the V-M200 software, **Browse** to the software file (with the extension *.cim*) and then select **Install**.

A

Regulatory statements

Contents

Industry Canada statement

This device complies with RSS-210 of the Industry Canada 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.

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:

1. Ce périphérique ne doit pas causer d'interférence et.
2. Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Conformité Européene — CE marking

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN60950-1: 2006 + A11: 2009

Safety of Information Technology Equipment

EN 50385: 2002

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 300 328 V1.7.1

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 893 V1.5.1

Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive

EN 301 489-1 V1.8.1

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V2.1.1

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for Broadband Data Transmission Systems

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

B

Resetting to factory defaults

Contents

Factory reset procedures

To force the V-M200 into its factory default state, follow the procedures in this section.

Caution Resetting the V-M200 to factory defaults deletes all configuration settings, resets the manager user name and password to **admin**, and enables the DHCP client on the Ethernet port. If no DHCP server assigns an address to the V-M200, its address defaults to 192.168.1.1.

Using the reset button

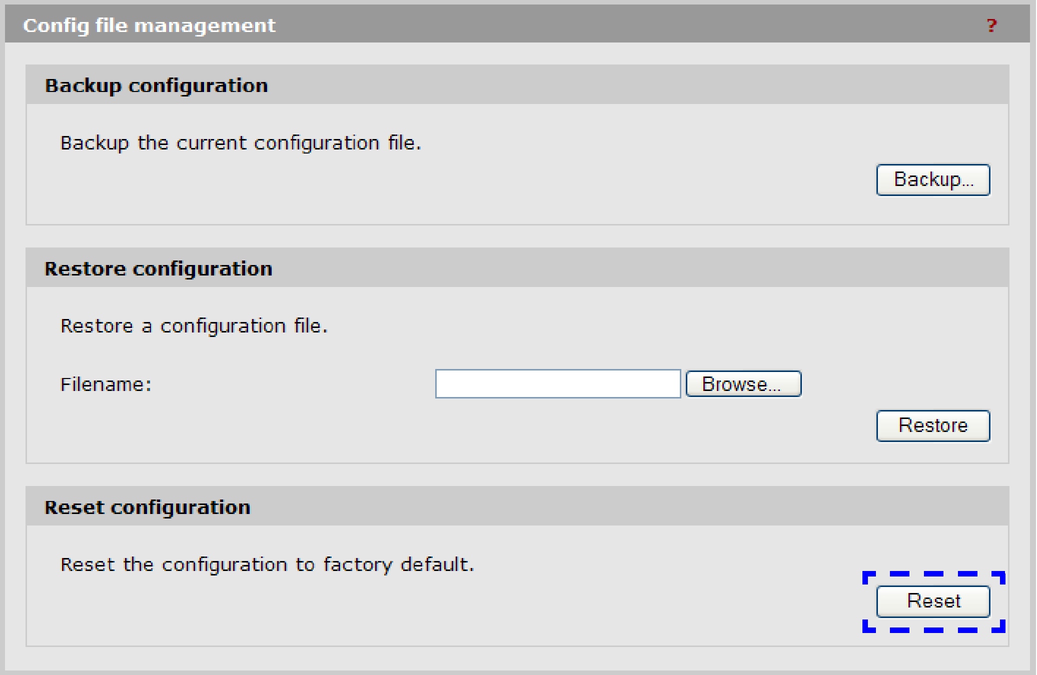
Using a tool such as a paper clip, press and hold the reset button for a few seconds until the status lights blink three times.

Note If you keep the reset button pressed for too long, the V-M200 will switch into maintenance mode as indicated by a rapid blinking of the status lights. If this occurs, power cycle the V-M200 and repeat the factory-default reset procedure.

Using the management tool

To reset the V-M200 to factory defaults, follow this procedure:

1. Launch the management tool (default https://192.168.1.1).
2. Select **Maintenance > Config file management**.
3. Under **Reset configuration**, click **Reset**.



Config file management

Backup configuration

Backup the current configuration file.

Restore configuration

Restore a configuration file.

Filename:

Reset configuration

Reset the configuration to factory default.

Technology for better business outcomes

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

August 2010

Manual Part Number
5998-0296