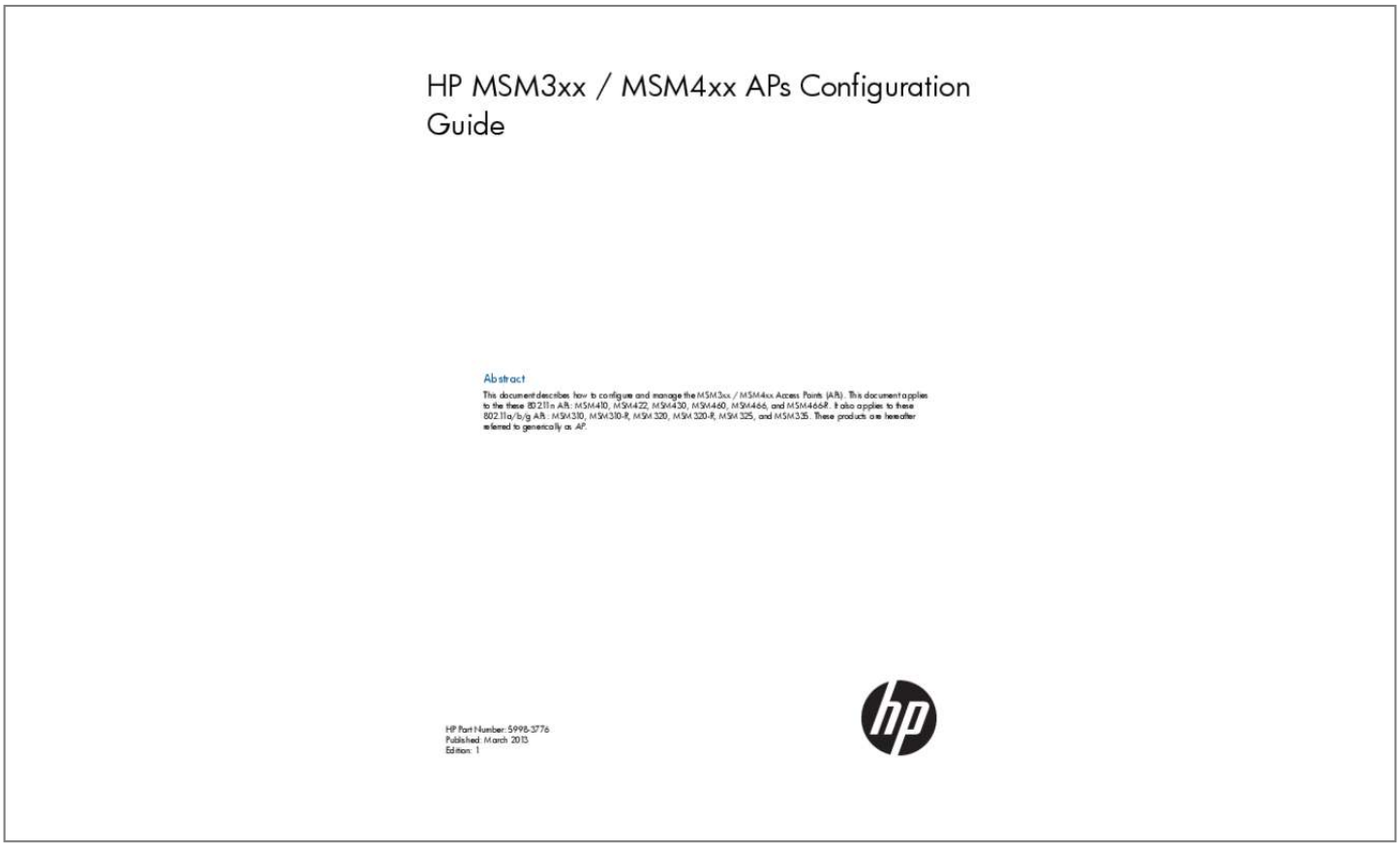

HP MSM3xx / MSM4xx APs Configuration Guide

Abstract

This document describes how to configure and manage the MSM3xx / MSM4xx Access Points (APs). This document applies to the these 802.11n APs: MSM410, MSM422, MSM430, MSM460, MSM466, and MSM466-R. It also applies to these 802.11a/b/g APs: MSM310, MSM310-R, MSM320, MSM320-R, MSM325, and MSM326. These products are hereafter referred to generically as AP.

HP Part Number: 5998-3776
Published: March 2013
Edition: 1

Manual abstract:

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein. Acknowledgments Windows® is a U.S. registered trademark of Microsoft Corporation. Warranty WARRANTY STATEMENT: See the warranty information sheet provided in the product box. Contents 1 Introduction...

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
..7 New in release 6.0.0.
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....7 2 Using the management tool....
.....
.....
.....

.....
.....
.....
.....

.....
.....
....8 Starting the management tool.
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
..109 Configuring a local mesh profile...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
110 Sample local mesh deploymen.....
.....
.....128 1n 802.1 1a/b/g antennas for MSM APs...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
....128 Radio power-level setting example.
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
....130 6 Contents 1 Introduction This guide explains how to configure and manage the HP MSM3xx/MSM4xx Access Points that are operating in autonomous mode.
For instructions on working with these APs when operating in controlled mode, see the MSM7xx Controllers Configuration Guide. New in release 6.0.0 Refer to the following sections for more information on the primary new and changed features in this release. New or changed in this release For information, see... Events. @@@@@@@This name can then be used to access the list wherever it is needed. New in release 6.

0.0 7 2 Using the management tool Starting the management tool Using Microsoft Internet Explorer 8+ or Mozilla Firefox 3+ (with SSL v3 support enabled), open page: https://192.168.1.1 and then log in. This assumes you are connected to the LAN port on the controller (ports 1, 2, 3, or 4 on the MSM720). About passwords: The default username and password is admin. New passwords must be 6 to 16 printable ASCII characters in length with at least 4 different characters. Passwords are case sensitive. Space characters and double quotes (") cannot be used.

Passwords must also conform to the selected security policy as described in "Passwords" (page 11). About the security warning: A security certificate warning is displayed the first time that you connect to the management tool. This is normal. Select whatever option is needed in your Web browser to continue to the management tool. The default certificate provided with the AP will trigger a warning message on most browsers because it is self-signed.
To remove this warning message, you must replace the default certificate. See "Managing certificates" (page 97). Setting up manager and operator accounts Two types of administrative user accounts are defined on the AP: manager and operator. • •The manager account provides full management tool rights. The operator account provides read-only rights plus the ability to disconnect wireless clients and perform troubleshooting.
To configure the accounts, select Management > Management tool. 8 Using the management tool Only one administrator (manager or operator) can be logged in at any given time. Options are provided to control what happens when an administrator attempts to log in while another administrator (or the same administrator in a different session) in already logged in. In every case, the manager's rights supersede those of an operator. Setting up manager and operator accounts 9 The following options can be used to prevent the management tool from being locked by an idle manager or operator: •Terminates the current manager session: When enabled, an active manager or operator session will be terminated by the login of another manager. This prevents the management tool from being locked by an idle session until the Account inactivity logout timeout expires. Is blocked until the current manager logs out: When enabled, access to the management tool is blocked until an existing manager logs out or is automatically logged out due to an idle session. An operator session is always terminated if a manager logs in. An active operator session cannot block a manager from logging in. •Terminates the current operator session: When enabled, an active operators session will be terminated by the login of another operator.

This prevents the management tool from being locked by an idle session until the Account inactivity logout timeout expires. Operator access to the management tool is blocked if a manager is logged in. An active manager session cannot be terminated by the login of an operator. An operator session is always terminated if a manager logs in. An active operator session cannot block a manager from logging in. •Login control: If login to the management tool fails five times in a row (bad username and/or password), login privileges are blocked for five minutes. Once five minutes expires, login privileges are once again enabled. However, if the next login attempt fails, privileges are again suspended for five minutes. This cycle continues until a valid login occurs. You can configure the number of failures and the timeout.
Account inactivity logout: By default, if a connection to the management tool remains idle for more than ten minutes, the controller automatically terminates the session.

You can configure the timeout. • • Administrative user authentication Login credentials can be verified using local account settings and/or an external RADIUS sever. This also affects how many accounts you can have. • • Local: Select this option to use a single manager and operator account. Configure the settings for these accounts under Manager account and Operator account. RADIUS: Using a RADIUS server enables you to have multiple manager and operator accounts, each with a unique login name and password. To setup this option, see "Authenticating manager logins using a third-party RADIUS server" (page 89). If both options are enabled, the RADIUS server is always checked first. 10 Using the management tool Passwords Passwords must be 6 to 16 printable ASCII characters in length with at least 4 different characters.

Passwords are case sensitive. Space characters and double quotes (") cannot be used. Passwords must also conform to the selected security policy as follows. • Follow FIPS 140-2 guidelines: When selected, implements the following requirements from the FIPS 140-2 guidelines: □ □ All administrator passwords must be at least six characters long. All administrator passwords must contain at least four different characters. For more information on these guidelines, refer to the Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules. • Follow PCI DSS 1.2 guidelines: When selected, implements the following requirements from the PCI DSS 1.2 guidelines: □ □ □ All administrator passwords must be at least seven characters long. All administrator passwords must contain both numeric and alphabetic characters.

The settings under Login control must be configured as follows: – – Lock access after nn login failures must be set to 6 or less. Lock access for nn minutes must be set to 30 minutes or more. □ The settings under Account inactivity logout must be configured as follows: – Timeout must be set to 15 minutes or less. For more information on these guidelines, refer to the Payment Card Industry Data Security Standard v1.2 document. Configuring management tool security Select Management > Management tool and configure the settings under Security. Allowed addresses Enables you to define a list of IP address from which to permit access to the management tool. To add an entry, specify the IP address and appropriate mask and select Add. When the list is empty, access is permitted from any IP address. For example: To allow access for a single computer with IP address 192.

168.1.209, specify: Configuring management tool security 1 1 IP address = 192.168.1.

209 Mask = 255.255.255.255 To allow access for several computers in the IP address range 192.168.

10.16 to 192.168.10.31, specify: IP address = 192.168.10.16 Mask = 255.255.255.

240 Active interfaces Select the interfaces through which access to the management tool will be permitted. (These settings also apply when SSH is used to access the command line interface.) Configuring the Login page message You can customize the message that is displayed at the top of the login page by selecting Management > Management tool and entering a new message under Login message. Configuring Auto-refresh Select Management > Management tool and configure the settings under Auto-Refresh. This option controls how often the AP updates the information in group boxes that show the auto-refresh icon in their title bar. Under Interval, specify the number of seconds between refreshes. Setting the system time Select Management > System time to open the System time page. This page enables you to configure the time server and time zone information. 1. 2.

12 Set timezone & DST as appropriate. Set Time server protocol, to Simple Network Time Protocol. Using the management tool 3. 4. Select Set date & time (time servers) and then select the desired time server.

Add other servers if desired. The AP contacts the first server in the list. If the server does not reply, the AP tries the next server and so on. By default, the list contains two ntp vendor zone pools that are reserved for HP networking devices. By using these pools, you will get better service and keep from overloading the standard ntp.

org server. For more information visit: www.pool.ntp.org. Select Save and verify that the date and time is updated accurately. A working Internet connection on Port 1 is required. NOTE: If access to the Internet is not available to the AP, you can temporarily set the time manually with the Set date & time (manually) option. However, It is important to configure a reliable time server on the AP. LEDs Select Management > LEDs to control operation of the status lights on the AP after the AP has successfully started up and become fully operational.

Until fully operational, status lights follow their normal behavior. This allows potential error conditions to be diagnosed. The following settings are available: • • • Normal: All status lights on the AP operate normally. Quiet: All status lights on the AP are turned off once the AP is fully operational. Awake: The power light flashes once per minute once the AP is fully operational. Country Select Management > Country to open the Country page. This page enables you to configure the country in which the AP operates. NOTE: The Country page is not available on APs delivered with a fixed country setting. Set the country in which the AP will operate. This enables the AP to properly customize the list of operating frequencies (channels) that you can configure on the Wireless > Radio(s) page.

Only frequencies that conform to the regulations in your area will be available. LEDs 13 3 Network configuration Working with network profiles The AP uses logical entities called network profiles to manage the configuration of network settings. Network profiles let you define the characteristics of a network and assign a friendly name to it. Once defined, network profiles can then be bound to a port, or VLAN as required. Network profiles make it easy to use the same settings in multiple places on the AP.

For example, if you define a network profile with a VLAN ID of 10, you could use that profile to: • • Map VLAN 10 to an AP port using the Network > VLANs page. Set VLAN 10 as the egress network for a VSC using the VSC > Profiles page. To define a new network profile 1. Select Network > Network profiles. 2. Select Add New Profile. 3. Configure profile settings as follows: • • Under Settings, specify a Name for the profile. Optionally, assign a VLAN ID. Select VLAN ID and then specify an number. You can also define a range of VLANs in the form X-Y, where X and Y can be 1 to 4094. For example: 50-60. An IP address cannot be assigned to a VLAN range. You can define more than one VLAN range by using multiple profiles. Each range must be distinct and contiguous.

4. Select Save. Configuring IP interfaces The IP interfaces page lists all network profiles to which an IPv4 address is assigned.

To open the IP interfaces page, select Network > IP interfaces. The Bridge interface is created by default. It can be edited, but not deleted. It is mapped to the wireless port and all Ethernet port(s) on the AP. (These ports are bridged and share the same IP address.) 14 Network configuration To assign an IP address to a new interface Any network profile that has a VLAN ID and is mapped to a physical port can have an IP address assigned to it. The following steps illustrate how to create a new profile and assign an IP address to it.

1. Select Network > Network profiles. 2. Select Add New Profile. 3.

Specify a name for the profile and assign a VLAN ID to it. This example uses the profile name Network A and a VLAN ID of 25. Select Save. 4. Select Network > VLANs to open the VLANs page.

5. Select the new profile in the table to open the Add/Edit VLAN mapping page. 6. Select the port to which you want to map the profile (in this case Port 1). Configuring IP interfaces 15 7. Select Save. The profile is mapped to Port 1 tagged. 8. Select Network > IP interfaces to open the IPv4 interfaces page. 9.

Select Add New Interface to open the Add/Edit interface page. 10. Under Interface, select the network profile that you defined earlier. 1 Under Assign IP address via, select the addressing method to use. 1. ••DHCP client: Dynamic host configuration protocol. The DHCP server will automatically assign an address to the network profile, which functions as a DHCP client. Static: Specify an IP address, Mask, and Gateway. 12. Select Save.

13. The new interface is added to the IPv4 interfaces table. 16 Network configuration Configuring the Bridge interface All wireless and Ethernet ports on an AP are bridged. As a result, they all share the same configuration settings defined by the Bridge interface. The following configuration options are available if you select the Bridge interface in the table.

By default, the Bridge interface operates as a DHCP client. Select the option you want to use and select Configure. Refer to the following sections for additional configuration information. ••• "Configuring the PPPoE client" (page 17) "Configuring the DHCP client" (page 18) (default setting) "Static addressing" (page 19) Configuring the PPPoE client Configuring IP interfaces 17 1. Under Settings, define the following: •••Username: Specify the username assigned to you by your ISP.

The AP will use this username to log on to your ISP when establishing a PPPoE connection. Password/Confirm password: Specify the password assigned to you by your ISP. The AP will use this password to log on to your ISP when establishing a PPPoE connection. Maximum Receive Unit (MRU): Maximum size (in bytes) of a PPPoE packet when receiving. Changes to this parameter only should be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection. Maximum Transmit Unit (MTU): Maximum size (in bytes) of a PPPoE packet when transmitting. Changes to this parameter should only be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection. Auto-reconnect: The AP will automatically attempt to reconnect if the connection is lost.

Un-numbered mode: This feature is useful when the AP is connected to the Internet and NAT is not being used. Instead of assigning two IP addresses to the AP, one to the Internet port and one to the LAN port, both ports can share a single IP address. •••This is especially useful when a limited number of IP addresses are available to you. 2. Under Assigned by PPPoE server, select Restart Connection. Once you are connected to the server, the following fields will display information about your connection. The Internet connection is not active until this occurs. Refer to the online help for a description of each field. Configuring the DHCP client The DHCP client does not require any configuration, unless you need to set a value for the optional DHCP Client ID parameter for proper operation with your DHCP server. Once you are connected to the server, the fields under Assigned by DHCP server show the settings assigned to the AP by the DHCP server.

The connection is not active until this occurs. Refer to the online help for a description of each field. If you want to force the DHCP client to obtain a new lease, select Release and then Renew. 18 Network configuration Static addressing Under Port settings, define the following: •••IP address: Specify the static IP address you want to assign to the port. Address mask: Specify the appropriate mask for the IP address you specified.

Default gateway: Specify the address of the default gateway on the network. Configuring port settings To configure settings for the physical ports on the AP, select Network > Ports. Status light ••Green: Port is properly configured and ready to send and receive data. Red: Port is not properly configured or is disabled. Jack Indicates the jack (physical interface) to which a port is assigned.

Name Identifies the port. Duplex Indicates if the port is Full or Half duplex. Speed Indicates the speed at which the port is operating. MAC address Indicates the MAC address of the port. Bandwidth control The AP incorporates a bandwidth management feature that provides control of outgoing user traffic on the wireless ports. To configure bandwidth control, select Network > Bandwidth control. Configuring port settings 19 ••If outgoing traffic arrives at the rate defined by the specified bandwidth limit (or less), it is processed without delay. If outgoing traffic arrives at a rate that is greater than the defined bandwidth limit, it causes the AP to throttle the traffic. If the traffic rate is over-limit for just a short burst, the data will be queued and forwarded without loss. If the traffic rate is over-limit for a sustained period, the AP will drop data to bring the rate down to the bandwidth limit that is set.

For example, if you set bandwidth control to 5000 kbps, the maximum rate at which traffic can be sent to wireless client stations is 5000 kbps. Discovery protocols The controller supports two protocols (LLDP and CDP) that provide a mechanism for devices on a network to exchange information with their neighbors. To configure these protocols, select Network > Discovery protocols. CDP configuration The AP can be configured to transmit CDP (Cisco Discovery Protocol) information on all ports. This information is used to advertise AP information to third-party devices, such as CDP-aware switches. When installed with a controller, the controller uses CDP information sent by autonomous APs to collect information about these APs for display in its management tool. LLDP configuration The IEEE 802.1AB Link Layer Discovery Protocol (LLDP) provides a standards-based method for network devices to discover each other and exchange information about their capabilities.

An LLDP device advertises itself to adjacent (neighbor) devices by transmitting LLDP data packets on all ports on which outbound LLDP is enabled, and reading LLDP advertisements from neighbor 20 Network configuration devices on ports that are inbound LLDP-enabled. An LLDP enabled port receiving LLDP packets inbound from neighbor devices stores the packet data in a Neighbor database (MIB).

LLDP information is used by network management tools to create accurate physical network topologies by determining which devices are neighbors and through which ports they connect. LLDP operates at layer 2 and requires an LLDP agent to be active on each network interface that will send and receive LLDP advertisements. LLDP advertisements can contain a variable number of TLV (type, length, value) information elements. Each TLV describes a single attribute of a device. When an LLDP agent receives information from another device, it stores it locally in a special LLDP MIB (management information base).

This information can then be queried by other devices via SNMP. Support is provided for the following MIBs: • • • Physical topology MIB (RFC 2922) Entity MIB version 2 (RFC 2737) Interfaces MIB (RFC 2863) NOTE: LLDP information is only sent/received on Ethernet links. LLDP information is not collected from wireless devices connected to an AP. However, LLDP can function across a local mesh link and will show the AP on the other side of the link as a neighbor. LLDP agent Select this option to enable the LLDP agent on port 1.

Select Configure TLVs to customize TLV support. Transmit Enable this option to have the agent transmit LLDP information to its neighbors. Receive Enable this option to have the agent accept LLDP information from its neighbors. LLDP over local mesh Enables support for LLDP on any active local mesh links. APs on the other side of a local mesh link will be shown as neighbors when this feature is active. LLDP settings Use these options to define global LLDP settings. Transmit interval Sets the interval (in seconds) at which local LLDP information is updated and TLVs are sent to neighboring network devices. Multiplier The value of Multiplier is multiplied by the Transmit interval to define the length of Time to live. Time to live Indicates the length of time that neighbors will consider LLDP information sent by this agent to be valid. Time to live is automatically calculated by multiplying Transmit interval by Multiplier.

Generate dynamic system names When enabled, this feature replaces the system name with a dynamically generated value which you can define. Access point name Specify how the dynamically generated name will be created. You can use regular text in combination with placeholders to create the name. Placeholders are automatically expanded each time the name is regenerated. Discovery protocols 21 If the placeholders cause the generated name to exceed 32 characters, it is truncated. Placeholders • %RN: System name of the neighboring device to which the port is connected, obtained via the System Name TLV. Since this is an optional TLV, if it is not available, the Chassis ID TLV is used instead. %RP: Port description of the port on the neighboring device to which the local port is connected, obtained via the Port Description TLV. Since this is an optional TLV, if it is not available, the Port ID TLV is used instead. %SN: AP name suffix (if specified).

Up to 16 characters can be appended to the name. %IP: AP's IP address. An IP address can require up to 15 characters (nnn.nnn.nnn.nnn). To create the system name, the items are concatenated using a hyphen as separator. For example: systemname-portid-suffix NOTE: Once AP names are dynamically changed by this feature, there is no way to return to the old AP names. • • TLV settings To customize TLV settings, select Configure TLVs on the Network > Discovery protocols page. Basic TLVs The AP supports all mandatory and optional TLVs (type, length, value) information elements that are part of the basic management set.

Mandatory TLVs The AP always sends these TLVs with the values as shown. Chassis ID (Type 1): The MAC address of the AP. Port ID (Type 2): The MAC address of the port on which the TLV will be transmitted. Time to live (Type 3): Defines the length of time that neighbors will consider LLDP information sent by this agent to be valid. Calculated by multiplying Transmit interval by the Multiplier (as defined on the Discovery protocols page). 22 Network configuration Optional TLVs Select the optional TLVs that you want to send with the values as shown. Port description (Type 4): A description of the port. System name (Type 5): Administrative name assigned to the device from which the TLV was transmitted. By default this is the SNMP system name. If the Dynamic system name option is enabled, the system name is replaced by the dynamically generated name.

The controller can only have one system name. If both the LAN and Internet ports have active agents, then the name generated by the LAN port is used. System description (Type 6): Description of the system, comprised of the following information: operational mode, hardware type, hardware revision, and firmware version. System capabilities (Type 7): Indicates the primary function of the device. Set to: WLAN access point for APs Router for controllers. Management IP address (Type 8): Specify the IP address on which the agent will respond to management requests. 802.3 TLVs The IEEE 802.3 organizationally specific TLV set is optional for all LLDP implementations. The AP supports a single optional TLV from the 802.

3 definition. MAC/PHY configuration/status This TLV provides the following information: • • • Bit-rate and duplex capability Current duplex and bit-rating Whether these settings were the result of auto-negotiation during link initiation or manual override. DNS configuration When the Bridge port is configured to obtain an IP address via PPPoE or DHCP: DNS configuration 23 When the Bridge port is configured to use a static IP address: DNS servers Dynamically assigned servers Shows the DNS servers that are dynamically assigned to the controller when PPPoE or DHCP is used to obtain an IP address on the Internet port. Override dynamically assigned DNS servers Enable this checkbox to use the DNS servers that you specify on this page to replace those that are assigned to the controller. Server 1 Specify the IP address of the primary DNS server for the controller to use.

Server 2 Specify the IP address of the secondary DNS server for the controller to use. Server 3 Specify the IP address of the tertiary DNS server for the controller to use. DNS advanced settings DNS cache Enable this checkbox to activate the DNS cache. Once a host name is successfully resolved to an IP address by a remote DNS server, it is stored in the cache. This speeds up network performance, because the remote DNS server does not have to be queried for subsequent requests for this host.

An entry stays in the cache until one of the following is true: • • • An error occurs when connecting to the remote host.

The time to live (TTL) of the DNS request expires. The AP restarts. DNS switch on server failure Controls how the AP switches between servers: • • When enabled, the AP switches servers if the current server replies with a DNS server failure message. When disabled, the AP switches servers if the current server does not reply to a DNS request. 24 Network configuration DNS switch over Controls how the AP switches back to the primary server. • • When enabled, the AP switches back to the primary server once the primary server becomes available again. When disabled, the AP switches back to the primary server only when the secondary server becomes unavailable. Defining IP routes All wireless traffic on the AP is bridged to the egress interface on the VSC with which it is associated. Therefore, IP routes cannot be applied to user traffic.

However, IP routes can be used to ensure that the management traffic generated by the AP is sent to the correct destination. For example, if two VSCs are defined, each with authentication assigned to a different RADIUS server operating on a different subnet and VLAN, routing table entries may be required to ensure proper communication with the RADIUS servers. Configuring IP routes To view and configure IP routes, select Network > IP routes. Active routes This table shows all active routes on the AP. You can add routes by specifying the appropriate parameters and then selecting Add. The routing table is dynamic and is updated as needed. This means that during normal operation the AP adds routes to the table as required. You cannot delete these system routes. The following information is shown for each active route: • • • • Interface: The port through which traffic is routed. When you add a route, the AP automatically determines the interface to be used based on the Gateway address.
Destination: Traffic addressed to this IP address or subnet is routed. Mask: Number of bits in the destination address that are checked for a match. Gateway: IP address of the gateway to which the AP forwards routed traffic (known as the next hop). An asterisk is used by system routes to indicate a directly connected network. • • Metric: Priority of a route.
If two routes exist for a destination address, the AP chooses the one with the lower metric. Delete: Select the garbage can icon to delete a route. If the icon has a red line through it, then the route cannot be deleted. Default routes The Default routes table shows all default routes on the AP. Default routes are used when traffic does not match any route in the Active routes table.
You can add routes by specifying the appropriate parameters and then selecting Add. Defining IP routes 25 The routing table is dynamic and is updated as needed. If more than one default route exists, the first route in the table is used. The following information is shown for each default route: • • Interface: The port through which traffic is routed. When you add a route, the AP automatically determines the interface to be used based on the Gateway address. Gateway: IP address of the gateway to which the AP forwards routed traffic (known as the next hop). An asterisk is used by system routes to indicate a directly connected network. • • Metric: Priority of a route. If two routes exist for a destination address, the AP chooses the one with the lower metric. Delete: Select the garbage can icon to delete a route.

If the icon has a red line through it, then the route cannot be deleted. IP QoS You configure IP quality of service (QoS) by creating IP QoS profiles that you can then associate with a VSC ("Quality of service" (page 67)) or with local mesh profiles ("Quality of service" (page 108)). You can configure up to 32 IP QoS profiles on the AP. You can associate up to 10 IP QoS profiles to a VSC. Configuring IP QoS profiles To view and configure IP QoS profiles, select Network > IP QoS. Initially, no profiles are defined. To create an IP QoS profile, select Add New Profile. Settings • • Profile name: Specify a unique name to identify the profile. Protocol: Specify an IP protocol to use to classify traffic by specifying its Internet Assigned Numbers Authority (IANA) protocol number. Protocol numbers are pre-defined for a number of common protocols.
If the protocol you require does not appear in the list, select Other and specify the appropriate number manually. You can find IANA-assigned protocol numbers on the Internet. 26 Network configuration • Start port/ End port: Optionally specify the first and last port numbers in the range of ports to which this IP QoS profile applies. To specify a single port, specify the same port number for both Start port and End port. Port numbers are pre-defined for a number of common protocols.
If the protocol you require does not appear in the list, select Other and specify the appropriate number manually. NOTE: To accept traffic on all ports for a specified protocol, set Start port to Other and 0. Also set End port to 65535. • Priority: Select the priority level that will be assigned to traffic that meets the criteria specified in this IP QoS profile. NOTE: It is strongly recommended that you reserve Very high priority for voice applications.
Example This example shows how to create two IP QoS profiles and associated them with a VSC. The two profiles are: • • Voice: Provides voice traffic with high priority. Web: Provides HTTP traffic with low priority. Create the profiles 1. 2. 3. 4. 5. Select Network > IP QoS, and then Add New Profile. The IP QoS Profile page opens.

Under Profile name, specify Voice. Under Protocol, from the drop-down list select TCP. Under Start port, from the drop-down list select SIP. Start port and End port are automatically populated with the correct value: 5060. Under Priority, from the drop-down list select Very High. 6. Select Save. NOTE: You could also create another profile using the same parameters but for UDP to cope with any kind of SIP traffic. 7. 8.
9. 10. On the IP QoS Profile page select Add New Profile. Under Profile name, specify Web. Under Protocol, from the drop-down list select TCP. Under Start port, from the drop-down list select http. Start port and End port are automatically populated with the common HTTP port, 80. 1 Under Priority, from the drop-down list select Low. 1. IP QoS 27 12.
Select Save. Assign the profiles to a VSC 1. Select VSC > Profiles, and then select one of the VSC profiles in the Name column. Scroll down to the Quality of service section in the Virtual AP box. 2. 3. 4. Under Quality of service, set Priority mechanism to IP QoS. In IP QoS profiles, Ctrl-click each profile. Select Save.

Customizing DiffServ DSCP mappings (These settings do not apply to IP QoS.) You can create custom DSCP mappings that let you override the standard DSCP mappings that are defined by default when you enable DiffServ as the QoS priority mechanism for a VSC or for local mesh links. This enables you to customize how traffic is assigned to the QoS priority queues.

To view and configure DSCP mappings, select Network > IP QoS. Initially, no mappings are defined. DSCP tag Priority DSCP codepoint value. Indicates the priority level assigned to traffic that matches the DSCP tag. • • • • Background: Assigns the traffic to queue 4 (Lowest priority). Best effort: Assigns the traffic to queue 3. Video: Assigns the traffic to queue 2.

Voice: Assigns the traffic to queue 1 (Highest priority). To create a new mapping Specify a value for DSCP tag, select a Priority, and then select Add. 28 Network configuration 802.1X supplicant The 802.1X supplicant can be used when the AP is connected to a secure switch port that requires 802.

1X authentication. To configure the 802.1X supplicant, select Network > 802.1X supplicant. Important • • If this option is enabled and the AP is connected to a unsecured switch port, 802.

1X is ignored. The AP always performs 802.1X authentication without VLAN tagging. The switch port is expected to be multi-homed, so that once authentication is successful, tagged and untagged traffic for any MAC addresses (including wireless clients) will be accepted by the switch. VLAN attributes received in the RADIUS access accept are not provided to other applications running on the AP. The AP sends the EAPOL start and waits for the Request Identity. On a time-out, the AP will perform a single retry. On a second time-out, the 802.1X supplicant will become idle. The switch is responsible for restarting the IEEE 802.

1X authentication by sending an EAP Request Identity. • • EAP Method Select the extensible authentication protocol method to use: • • • PEAP version 0: Authentication occurs using MS-CHAP V2. PEAP version 1: Authentication occurs using EAP-GTC. TTLS: The Tunneled Transport Layer Security protocol requires that the switch first authenticate itself to the AP by sending a PKI certificate. The AP authenticates itself to the switch by supplying a username and password over the secure tunnel. Username Username that the AP will use inside the TLS tunnel. Password / Confirm password Password assigned to the AP. 802.1X supplicant 29 Anonymous Name used outside the TLS tunnel by all three EAP methods. If this field is blank, then the value specified for Username is used instead.

30 Network configuration 4 Wireless configuration Wireless coverage As a starting point for planning your network, you can assume that when operating at high power, an AP radio provides a wireless networking area (also called a wireless cell) of up to 300 feet (100 meters) in diameter. Before creating a permanent installation however, you should always perform a site survey (see "Wireless neighborhood" (page 49)) to determine the optimal settings and location for the AP. NOTE: Supported wireless modes, operating channels, and power output vary according to the AP model, and are governed by the regulations of the country in which the AP is operating (called the regulatory domain). For a list of all operating modes, see "Radio configuration" (page 36). To set the regulatory domain, see "Country" (page 13).

Factors limiting wireless coverage Wireless coverage is affected by the factors discussed in this section. Radio power More radio power means better signal quality and the ability to create bigger wireless cells. However, cell size should generally not exceed the range of transmission supported by wireless users. If it does, users will be able to receive signals from the AP but will not be able to reply, rendering the connection useless. Further, when more than one AP operates in an area, you must adjust wireless cell size to reduce interference between APs.

An automatic power control feature is available to address this challenge. See "Transmit power control" (page 47). Antenna configuration Antennas play a large role in determining the shape of the wireless cell and transmission distance. See the specifications for the antennas you use to determine how they affect wireless coverage. Interference Interference is caused by other APs or devices that operate in the same frequency band as the AP and can substantially affect throughput. Advanced wireless configuration features are available to automatically eliminate this problem. See "Radio configuration" (page 36). In addition, the several tools are available to diagnose interference problems as they occur. • • • Select Wireless > Overview to view information about each connected wireless client. Select Wireless > Neighborhood to view a list of wireless radios operating nearby.

Enable the Severe interface detection/mitigation feature on the Radio configuration page to automatically switch channels when interference is detected. See "Severe interference detection/mitigation" (page 46). CAUTION: APs that operate in the 2.4 GHz band may experience interference from 2.4 GHz cordless phones and microwave ovens. Physical characteristics of the location To maximize coverage of a wireless cell, wireless APs are best installed in an open area with as few obstructions as possible. Try to choose a location that is central to the area being served. Radio waves cannot penetrate metal; they are reflected instead. A wireless AP can transmit through wood or plaster walls and closed windows; however, the steel reinforcing found in concrete walls and floors may block transmissions or reduce signal quality by creating reflections. This can make Wireless coverage 31 it difficult or impossible for a single AP to serve users on different floors in a concrete building.

Such installations require a separate wireless AP on each floor. Configuring overlapping wireless cells Overlapping wireless cells occur when two or more APs are operating within transmission range of each other. This may be under your control, (for example, when you use several cells to cover a large location), or out of your control (for example, when your neighbors set up their own wireless networks). When APs are operating in the 2.4 GHz band, overlapping wireless cells can cause performance degradation due to insufficient channel separation.

Performance degradation and channel separation When two wireless cells operating on the same frequency overlap, throughput can be reduced in both cells. Reduced throughput occurs because a wireless user that is attempting to transmit data defers (delays) transmission if another station is transmitting. In a network with many users and much traffic, these delayed transmissions can severely affect performance, because wireless users may defer several times before the channel becomes available. If a wireless user is forced to delay transmission too many times, data can be lost. Delays and lost transmissions can severely reduce throughput on a network.

To view this information about your network, select Status > Wireless. For recommendations on using this information to diagnose wireless problems, see the online help for this page.

The following example shows two overlapping wireless cells operating on the same channel (frequency). Since both APs are within range of each other, the number of deferred transmissions can be large. The solution to this problem is to configure the two AP to operate on different channels. Unfortunately, in the 2.4 GHz band, adjacent channels overlap. So even though APs are operating on different channels, interference can still our. This is not an issue in the 5 GHz band, as all channels are non-overlapping. Selecting channels in the 2.

4 GHz band In the 2.4 GHz band, the center frequency of each channel is spaced 5 MHz apart (except for channel 14). Each 802.1 channel uses 20 MHz of bandwidth (10 MHz above and 10 MHz 1 32 Wireless configuration below the center frequency), which means that adjacent channels overlap and interfere with each other as follows: Channel 1 2 3 4 5 6 7 Center frequency 2412 2417 2422 2427 2432 2437 2442 Overlaps channels Channel 2, 3 1, 3, 4 1, 2, 4, 5 2, 3, 5, 6 3, 4, 6, 7 4, 5, 7, 8 5, 6, 8, 9 8 9 10 1 1 12 13 14 Center frequency 2447 2452 2457 2462 2467 2472 2484 Overlaps channels 6, 7, 9, 10 7, 8, 10, 1 1 8, 9, 1 12 1, 9, 10, 12, 13 10, 1 13 1, 1 12 1, To avoid interference, APs in the same area must use channels that are separated by at least 25 MHz (5 channels). For example, if an AP is operating on channel 3, and a second AP is operating on channel 7, interference occurs on channel 5. For optimal performance, the second AP should be moved to channel 8 (or higher). With the proliferation of wireless networks, it is possible that the wireless cells of APs outside your control overlap your intended area of coverage. To choose the best operating frequency, select Wireless > Neighborhood to view a list of all APs that are operating nearby and their operating frequencies. The number of channels available for use in a particular country are determined by the regulations defined by the local governing body and are automatically configured by the AP based on the Country setting you define. (See "Country" (page 13)).
This means that the number of non-overlapping channels available to you varies by geographical location. The following table shows the number of channels that are available in North America, Japan, and Europe. Region North America Japan Europe Available channels 1 to 1 1 1 to 14 1 to 13 Since the minimum recommended separation between overlapping channels is 25 MHz (five channels) the recommended maximum number of overlapping cells you can have in most regions is three. The following table gives examples relevant to North America, Japan, and Europe (applies to 22 MHz channels in the 2.4 GHz band). North America cell 1 on channel 1 cell 2 on channel 6 cell 3 on channel 1 1 Japan cell 1 on channel 1 cell 2 on channel 7 cell 3 on channel 14 Europe cell 1 on channel 1 cell 2 on channel 7 cell 3 on channel 13 In North America you can create an installation as shown in the following figure. Wireless coverage 33 Reducing transmission delays by using different operating frequencies in North America. Alternatively, you can stagger cells to reduce overlap and increase channel separation, as shown in the following figure. Using only three frequencies across multiple cells in North America. This strategy can be expanded to cover an even larger area using three channels, as shown in the following figure.
34 Wireless configuration Using three frequencies to cover a large area in North America. Gray areas indicate overlap between two cells that use the same frequency. Distance between APs In environments where the number of wireless frequencies is limited, it can be beneficial to adjust the receiver sensitivity of the AP. To make the adjustment, select Wireless > Radio and set the Distance between access points option. For most installations, Distance between access points should be set to Large. However, if you are installing several wireless APs and the channels available to you do not provide enough separation, reducing receiver sensitivity can help you to reduce the amount of crosstalk between wireless APs. Another benefit to using reduced settings is that it improves roaming performance. Wireless users switch between APs more frequently. Automatic transmit power control The automatic power control feature enables the AP to dynamically adjust its transmission power to avoid causing interference with neighboring HP APs. For information see "Transmit power control" (page 47).

Supporting 802.1 and legacy wireless clients 1a The 802.1 standard is very similar to the 802.1 standard, in that both provide mechanisms 1n 1g to support older wireless standards. In the case of 802.1 1g, protection mechanisms were created to allow 802.1 and 802.1 wireless devices to co-exist on the same frequencies. The data 1b 1g rates of 802.1 (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) are transmitted using Orthogonal 1g Frequency Division Multiplexing (OFDM) modulation, while the data rates of 802.
1 are 1b transmitted using Direct Sequence Spread Spectrum (DSSS) modulation. Since older 802.1 1b-only clients cannot detect OFDM transmissions, 802.1 clients must "protect" their transmissions by 1g first sending a frame using DSSS modulation. This frame – usually a CTS-to-self or RTS/CTS exchange – alerts 802.
1 clients to not attempt to transmit for a specified period of time. 1b If protection is not used, 802.1 clients may transmit a frame while an 802.1 frame is already 1b 1g being sent. This leads to a collision and both devices need to re-transmit.
If there are enough Supporting 802.1 and legacy wireless clients 1a 35 devices in the network, the collision rate will grow exponentially and prevent any useful throughput from the wireless network. 802.1 clients face the same problem as described above – legacy 802.1 clients cannot 1n 1b detect the High Throughput (HT) rates that 802.1 uses. So to avoid causing excessive collisions, 1n 802.1 clients must use the same protection mechanisms when a legacy client is present. Even 1n the most efficient protection mechanism (CTS-to-self) causes a substantial decline in throughput; performance can decline by as much as 50 percent. For this reason, the protection behavior of the MSM430, MSM460, MSM466, and MSM466-R can be configured (see "Tx protection" (page 46)) to allow network administrators greater flexibility over their deployments.

NOTE: 802.1 clients can only achieve maximum throughput when legacy clients are not 1n present on the same radio. You can use the Allow 802.1 1n clients only setting to segregate 1 802.1 traffic to ensure that 802.1 clients do not experience performance degradation by 1n 1n sharing a wireless network with legacy (slower) client stations. Radio configuration To define configuration settings for a radio, select Wireless > Radio(s). This opens the Radio(s) configuration page. The contents of this page varies depending on the product. The following screen shows the Radio(s) configuration page for the MSM422.

Configuration settings are the same on other products. 36 Wireless configuration Radio configuration parameters This section provides definitions for all configuration parameters that are present on all products. Regulatory domain Indicates the geographical region in which the AP is operating. To set the regulatory domain, see “Country” (page 13). Operating mode Select the operating mode for the radio.

Available options are: • Access point and Local mesh: Standard operating mode provides support for all wireless functions. (Not supported on radio 3 on the MSM335.) The total available bandwidth on the radio is shared between all local mesh links and wireless users. This can result in reduced throughput if lots of traffic is being sent by both wireless users and the local mesh links. You can use the QoS feature to prioritize traffic.

Access point only: Only provides AP functionality, local mesh links cannot be created. (Not supported on radio 3 on the MSM335.) Local mesh only: Only provides local mesh functionality. Wireless client stations cannot connect. Monitor: Disables AP and local mesh functions. Use this option for continuous scanning across all channels in all wireless modes. See the results of the scans by selecting Wireless > Neighborhood. This mode also enables 802.1 traffic to be traced using the Tools > Network 1 trace feature. Sensor: Enables RF sensor functionality on the radio.

HP APs are smart APs, and do not forward broadcast packets when no client stations are connected. Therefore, the RF sensor function will not be able to detect these APs unless they have at least one connected wireless client station. This feature requires that the appropriate license is installed on the AP. See “Managing licenses” (page 119). • • • • The following table shows the operating modes supported for each product. Product MSM310 MSM310-R MSM320 MSM320-R MSM325 MSM335 (Radio 1 + 2) MSM335 (Radio 3) MSM410 MSM422 MSM317 MSM430 MSM460 MSM466   Access point and Local mesh Access point only Local mesh only Monitor Sensor Radio configuration 37 Product MSM466-R Access point and Local mesh Access point only Local mesh only Monitor Sensor The following table shows all radio parameters that are configurable for each operating mode. Parameter “Regulatory domain” (page 37) “Wireless mode” (page 39) “Channel width” (page 40) “Channel extension” (page 41) “Channel” (page 41) “Interval” (page 43) “Time of day” (page 43) “Automatic channel exclusion list” (page 43) “Antenna selection” (page 43) “Antenna gain” (page 44) “Max clients” (page 44) “Allow 802.1 clients 1n only” (page 44) “Collect statistics for wireless clients” (page 45) “Tx beamforming” (page 45) “RTS threshold” (page 45) “Spectralink VIEW” (page 45) “Severe interference detection/mitigation” (page 46) “Tx protection” (page 46) “Guard interval” (page 46) “Maximum range (ack timeout)” (page 47) “Distance between APs” (page 47) “Beacon interval” (page 47) “Multicast Tx rate” (page 47) “Transmit power control” (page 47) Access point and Local mesh   Access point only   Local mesh only   Monitor   Sensor   38 Wireless configuration Certain parameters are not supported on all radios. Refer to the parameter descriptions that follow for details. Wireless mode Supported wireless modes are determined by the regulations of the country in which the AP is operating, and are controlled by the country setting on the AP. To configure the country setting, see “Country” (page 13). 802.1 1n/a (5 GHz) Supported on Frequency band Data rates MSM410, MSM422, MSM430, MSM460, MSM466 5 GHz For 802.1 clients: Up to 450 Mbps on the MSM466, MSM466-R, and 1n MSM460, and up to 300 Mbps on the MSM410, MSM422, and MSM430. For 802.

1 clients: Up to 54 Mbps. 1a When operating in this mode, the AP allows both 802.1 and legacy 802.1 1n 1a clients to associate. The AP advertises protection in the beacon when legacy clients are associated or operating on the same channel.

This alerts associated 802.1 1n clients to use protection when transmitting. The AP also uses protection when necessary when sending 802.1 data. The type of protection is configurable by 1n setting the Tx protection parameter. 802.1 (5 GHz) 1a Supported on Frequency band Data rates MSM310, MSM320, MSM335, MSM410, MSM422, MSM430, MSM460, MSM466 5 GHz Up to 54 Mbps. This is a legacy mode that can be used to support older wireless client stations. 802.1 1n/b/g (2.

4 Ghz) Supported on Frequency band Data rates MSM410, MSM422 Radio 2 on: MSM430, MSM460, MSM466 2.4 GHz For 802.1 clients: Up to 450 Mbps on the MSM466, MSM466-R, and 1n MSM460 and up to 300 Mbps on the MSM430. These values are achievable when using a 40 MHz channel width, which is not recommended in the 2.4 GHz frequency band. For 802.1 clients: Up to 54 Mbps on the MSM430, MSM460, 1g MSM466, and MSM466-R. For 802.1 clients: Up to 1 Mbps on the MSM430, MSM460, 1b 1 MSM466, and MSM466-R. When operating in this mode, the AP allows both 802.

1 and legacy 802.1 1n 1b/g clients to associate. The AP advertises protection in the beacon when legacy clients are associated or operating on the same channel. This alerts associated 802.1 1n clients to use protection when transmitting.

The AP also uses protection when necessary when sending 802.1 data. The type of protection is configurable by 1n setting the Tx protection parameter. Radio configuration 39 802.1 1b/g (2.

4 Ghz) Supported on Frequency band Data rates MSM310, MSM317, MSM320, MSM335, MSM410, MSM422 Radio 2 on: MSM430, MSM460, MSM466 2.4 GHz For 802.1 clients: Up to 54 Mbps. 1g For 802.1 clients: Up to 1 Mbps. 1b 1 This is a legacy mode that can be used to support older wireless client stations. 802.1 (2.4 Ghz) 1g Supported on Frequency band Data rates MSM310, MSM320, MSM335 2.4 GHz Up to 54 Mbps.

This is a legacy mode that can be used to support older wireless client stations. 802.1 (2.4 Ghz) 1b Supported on Frequency band Data rates MSM310, MSM317, MSM320, MSM335 2.4 GHz Up to 1 Mbps. 1 This is a legacy mode that can be used to support older wireless client stations.

802.1 Turbo 1a Supported on Frequency band Data rates MSM310, MSM320, MSM335 5 GHz Up to 108 Mbps. Provides channel bonding in the 5 GHz frequency band for enhanced performance. Useful to provide increased throughput when creating local mesh links between two APs.
Channel width Supported on: MSM410, MSM422 (radio 1), MSM430, MSM460, MSM466, MSM466-R Not available in Monitor or Sensor modes. 802.1 allows for the use of the standard channel width of 20 MHz or a double width of 40 1n MHz. The double width is achieved by using two adjacent channels to send data simultaneously. This results in double the available bandwidth leading to much higher throughput.
Select the Channel width that will be used for 802.1 traffic. Available options are: 1n • •20 MHz: Uses the standard channel width of 20 MHz. Recommended when the AP is operating in the 2.4 GHz band and multiple networks must co-exist in the same location.
Auto 20/40 MHz: The AP will advertise 40 MHz support to clients, but will use 20 MHz for each client that does not support 40 MHz. 40 Wireless configuration NOTE: On the MSM466, MSM466-R, MSM460, and MSM430, when operating in the 2.4 GHz band, the AP will automatically switch to using a 20 MHz channel width if a legacy 802.1 1b/g client or AP is detected on the primary channel. When the legacy device is no longer present, the AP will revert back to using a 40 MHz channel width. The channel selected on the radio page is the primary channel and the secondary (or extension) channel is located adjacent to it. The secondary channel is either above or below depending on which channel was selected as the primary. In the 5 GHz band, the channels are paired: 36 and 40 are always used together, 44 and 48 are always used together, etc. It works slightly differently in the 2.4 GHz band: there you choose whether the extension channel should be above or below the beacon using the Channel extension parameter.

See the Channel parameter for more information. Channel extension Supported on: MSM410, MSM422 (radio 1), MSM430 (radio 2), MSM460 (radio 2), MSM466 (radio 2), MSM466-R (Radio 2) Not available in Sensor mode. This setting only appears when Wireless mode is set to 802.1 (2.4 GHz), 802.1 1n 1n/b/g, or 802.1 n/g and Channel width is set to Auto 20/40 MHz. 1 This setting determines where the second 20 MHz channel is located. • •Above the beacon (+1): The secondary channel is located on a channel above the currently selected channel. Below the beacon (-1): The secondary channel is located on a channel below the currently selected channel.
Channel Select channel (frequency) for wireless services. The channels that are available are determined by the radio installed in the AP and the regulations that apply in your country. Automatic channel selection Use the Automatic option to have the AP select the best available channel. Control how often the channel selection is re-evaluated by setting the Interval parameter. If the Interval parameter is set to any value other than Time of day.
and a wireless client is associated with the radio, automatic channel selection is delayed. The AP will retry at one minute intervals until the radio is unused by wireless clients. • On the MSM430, MSM460, MSM466, MSM466-R: Scanning during the channel selection process can cause interruptions to voice calls. This only occurs each time the Interval expires. Therefore, configuring a short Interval is not recommended.
On the MSM310, MSM320, MSM335, MSM410, MSM422: Scanning is continuously performed on all the channels in the currently selected Operating mode, even though the channel is only re-evaluated each time the Interval expires. (If Interval is set to Disabled, continuous scanning is not performed.) Continuous scanning can cause interruptions to voice calls. On dual-radio APs, you can avoid interruptions by setting one radio to operate in Monitor mode. For example, if radio 1 is set to Automatic and radio 2 is in Monitor mode, scanning occurs on radio 2 and interruptions on radio 1 do not occur. • CAUTION: When using the Automatic option with an external antenna in the 2.4 GHz band, all channels must be set to the lowest acceptable value for your regulatory domain. See "Transmit power control" (page 47). Radio configuration 41 Manual channel selection If setting the channel manually, for optimal performance when operating in 2.4 GHz modes, select a channel that differs from other wireless APs operating in neighboring cells by at least 25 MHz.

For example, if another AP is operating on channel 1, set the AP to channel 6 or higher. See "Wireless neighborhood" (page 49) to view a list of APs currently operating in your area. For detailed information on selecting channels when operating at 2.4 GHz, see "Configuring overlapping wireless cells" (page 32). When operating in 802.1 or 802.1 (5 GHz) modes, channels do not interfere with each 1a 1n other, enabling APs to operate on two adjacent channels without interference. HP APs support Dynamic Frequency Selection (802.1 and Transmit Power Control (802.1 1h) 1d) for 802.
1 operation in European countries. These options are automatically enabled as required. 1a Channels used by dynamic frequency selection (DFS) for radar avoidance, are identified with an asterisk "". • On the MSM410, MSM422 (radio 1), MSM430, MSM460, MSM466, MSM466-R: When Wireless mode is 802.1 (5 GHz) or 802.*
1 1n 1n/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 36(1) 40(-1) 44(1) 48(-1) Channels used 36+40 40+36 44+48 48+44 NOTE: The channel selected is the primary channel and the channel above or below it becomes the secondary channel. The AP beacon is transmitted only on the primary channel and all legacy client traffic is carried on the primary channel.
• On the MSM410, MSM422 (radio 1): When Wireless mode is 802.1 (2.4 GHz) or 802.1 1n 1n/g or 802.1 1n/b/g, and Channel width is Auto 20/40 MHz, the Channel extension parameter value affects which channels are shown in the Channel list. Although it is recommended that you use the 5 GHz band for all 802.1 activity, if you insist upon using 802.1 and a 40 1n 1n MHz Channel width in the crowded 2.4 GHz band, it is best to select channels as follows, according to the number of 2.4 GHz channels available in your region.

Available 2.4 GHz channels 1 to 13 1 to 13 1 to 1 1 1 to 1 1 Channel width 20 MHz 40 MHz 20 MHz 40 MHz Recommended non-overlapping channels 1, 7, 13 1, 13 (If both are used, there will be some performance degradation.) 1, 6, 1 1 1, 1 (If both are used, there will be some performance 1 degradation.