Part No. NN47250-400 Rev.02
(320659-D Rev.02)
February 2007

4655 Great America Parkway
Santa Clara, CA 95054

Nortel WLAN—Security Switch 2300 Series Release Notes

Release 5.0

NORTEL

Contents

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel solutions center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

http://www.nortel.com/callus

Getting help from a specialist by using an express routing code

To access some Nortel Enterprise Technical Support Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Nortel WLAN Security Switch 2300 Series Release Notes

Nortel recommends that you familiarize yourself with the "Best practices and common issues" section in this document before installing WLAN Security Switch 2300 Series (WSS Software) Version 5.0.9. For additional product information, refer to the following manuals in addition to these release notes:

- Nortel WLAN Security Switch 2300 Series Quick Start Guide.
- Nortel WLAN Security Switch 2300 Series Installation and Basic Configuration Guide.
- Nortel WLAN Access Point 2330/2330A Installation Guide.
- Nortel WLAN Security Switch 2300 Series Configuration Guide.
- Nortel WLAN Security Switch 2300 Series Command Line Reference.
- Nortel WLAN Management System 2300 Series User Guide.
- Nortel WLAN Management System 2300 Series Reference Guide.

What's new in WSS Software version 5.0.9.4

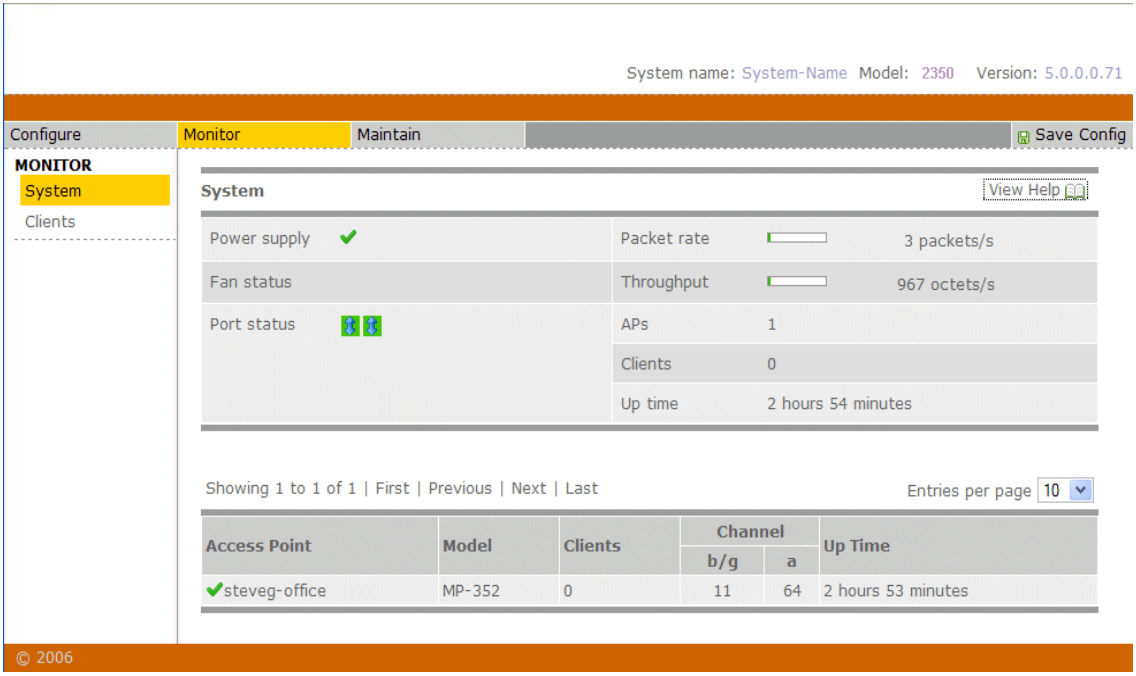
WSS Software Version 5.0 contains the following enhancements:

- New Web View interface
- WSS-WSS security
- AirDefense software support on APs

- AeroScout RFID tag support
- Persistent VLAN assignment for roaming clients
- Simplified Web-Portal and last-resort configuration
- Auto-RF enhancements
- Unscheduled Automatic Powersave Delivery (U-APSD) support
- Local software images on APs
- DHCP server enhancements
- RADIUS accounting enhancements
- Support for special characters in SNMP community names
- Increased life span of new self-signed certificates
- CLI commands to specify location and contact information for APs

New Web View interface

WSS Software Version 5.0 includes a major renovation of Web View, the switch's web-based management interface. Web View now provides more configuration and management features, including numerous configuration wizards and a monitor dashboard. Here is an example of the dashboard for a 2350:

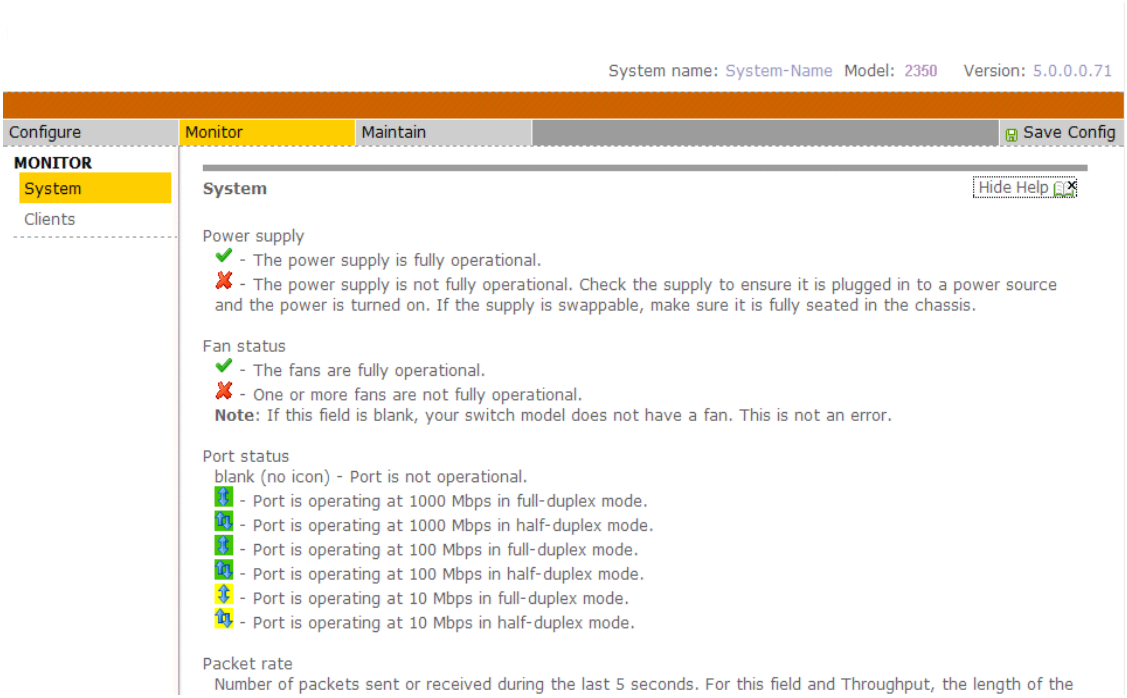


The switch's system name, model, and running software version are listed at the top of the display. The interface provides three major categories:

- Configure
- Monitor
- Manage

To display the options within a category, click on the category. Its options are listed on the left. Click on an option to display the page for that option.

To access help for the displayed page, click View Help. Here is an example of the help for the monitor dashboard.



System requirements

Browser requirements

Web View is supported on the following browsers:

- Mozilla Firefox Version 1.0 or later
- Microsoft Internet Explorer Version 6.0 or later

TLS 1.0, SSL 2.0, or SSL 3.0 must be enabled in the browser. To enable TLS 1.0, SSL 2.0, or SSL 3.0 in Microsoft Internet Explorer:

1 Select **Tools > Internet Options** to display the Internet Options dialog box.

2 Select the **Advanced** tab.

3 Scroll to the bottom of the list of options and select the TLS 1.0, SSL 2.0, or SSL 3.0 option to enable it.

4 Click **OK**.

WSS requirements

- The WSS's HTTPS server must be enabled. (This option is enabled by default.) If HTTPS is disabled, you can enable it using the following command:

  set ip https server enable

- The switch must have an IP interface that can be reached by the PC where the browser is installed.

Logging into Web View

1 Type **https://***ip-addr* in the Web browser's Address or Location field and press Enter.

For *ip-addr*, type an IP address you configured on the switch.

2 If your browser displays a certificate warning, select an option to accept the certificate.

The certificate is presented to your browser by the WSS to authenticate the switch's identify. You can select to accept the certificate for the current web management session or for all web management sessions.

After you accept the certificate, the browser might display another dialog asking whether you want to view the certificate. You can view the certificate or continue without viewing it.

3 In the User Name field, type **admin**.

4 In the Password field, type the enable password configured on the switch.

5 Click **OK**.

Accessing the Quick Start

If you are configuring a new 2360/2361, or 2350, you can access Web View without any preconfiguration. Attach your PC directly to any 10/100 Ethernet port on a 2360/2361 or 2350. Then enter **http://192.168.100.1** in the web browser's Location or Address field.

If the switch is already configured, you still can access the Quick Start wizard from within Web View. Select Configure, then select Quick Start.

Secure WSS to WSS communications

WSS Software Version 5.0 extends WSS Software security by adding secure WSS to WSS communications. secure WSS to WSS communications encrypts management traffic exchanged by WSSs in a Mobility Domain. When secure WSS to WSS communications is enabled, management traffic among WSSs in the Mobility Domain is encrypted using AES. The keying material is dynamically generated for each session and passed among switches using public keys that you configure.

(For more information, see the "Configuring secure WSS to WSS communications" section in the "Configuring and Managing Mobility Domain Roaming" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

AirDefense software support on APs

WSS Software Version 5.0 enables you to convert APs into AirDefense sensors. The AirDefense system is an enterprise-class security solution that allows you to protect against threats and intrusions into your wireless network. The AirDefense solution can be integrated with the Nortel WLAN 2300 Series System, complementing Nortel network security features by providing a centralized server dedicated to security analysis and record keeping.

(For configuration information, see the "AirDefense Integration with the Nortel WLAN 2300 Series System" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

AeroScout RFID tag support

WSS Software Version 5.0 enables APs to detect AeroScout RFID tags, and respond to commands from an AeroScout Engine.

AeroScout RFID tags are wireless transmitters that you can place on assets such as office equipment to track the equipment's location. Each tag regularly transmits its unique ID. AeroScout listeners detect the transmissions from the RFID tags and relay this information to an AeroScout Engine or WSS. You can use an AeroScout Engine or WMS to locate the asset.

AP access points can be configured as AeroScout listeners. An AP configured to be an AeroScout listener detects RFID tag IDs and sends the tag information to the AeroScout Engine.

(For more information, see the "Configuring APs To Be AeroScout Listeners" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Persistent VLAN assignment for roaming clients

WSS Software Version 5.0 provides a new service profile option, **keep-initial-vlan**, that allows you to keep users who roam on the same VLAN after roaming, even after they roam to another WSS.

In some cases, a user can be assigned to a different VLAN after roaming to another WSS. Table 1 lists the ways a VLAN can be assigned to a user after roaming from one WSS to another.

Table 1. VLAN Assignment After Roaming from One WSS to Another

Location Policy	AAA	keep-initial-vlan	SSID	VLAN Assigned By...
Yes	Yes or No	Yes or No	Yes or No	location policy
No	Yes	Yes or No	Yes or No	AAA
No	No	Yes	Yes or No	**keep-initial-vlan**
No	No	No	Yes	SSID
No	No	No	No	Not set—authentication error

Yes in the table means the VLAN is set on the roamed-to WSS, by the mechanism indicated by the column header. *No* means the VLAN is not set. *Yes or No* means the mechanism does not affect the outcome, due to another mechanism that is set.

The *VLAN Assigned By* column indicates the mechanism that is used by the roamed-to switch to assign the VLAN, based on the various ways the VLAN is set on that switch.

Note. The **keep-initial-vlan** option does not apply to Web-Portal clients. Instead, VLAN assignment for roaming Web-Portal clients automatically works the same way as when **keep-initial-vlan** is enabled. The VLAN initially assigned to a Web-Portal user is not changed except by a location policy, AAA, or SSID default setting on the roamed-to switch.

(For more information, see the "Keeping Users on the Same VLAN Even After Roaming" section of the "Configuring AAA for Network Users" chapter in the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Simplified Web-Portal and Last-Resort configuration

WSS Software Version 5.0 simplifies configuration of the following authentication types:

- Web Portal
- Last resort

In previous WSS Software Versions, each of these authentication types required configuration of special users in the local database for wireless access: **web-portal-*ssid*** for Web Portal and **last-resort-*ssid***. In WSS Software Version 5.0, these special users are not supported. In fact, they cannot even be configured in the local database. However, special users **web-portal-wired** and **last-resort-wired** are still required for Web-Portal or last-resort access on a wired authentication port.

The default authorization attributes set on the SSID are applied to last-resort users and also to Web-Portal users while they are being authenticated (that is, while they are in the *portal*). For example, if the **vlan-name** attribute on the service profile is set to *guest-vlan*, users are placed in *guest-vlan*.

The Web-Portal ACL (*portalacl* by default), which used to be associated with the **web-portal-*ssid*** or **last-resort-*ssid*** user, is now associated with the SSID's service profile instead. The ACL is still automatically generated by WSS Software the first time you set the fallthru authentication type on any service profile or wired authentication port to **web-portal**. If you use a different ACL, you can change the ACL name used by the service profile, with the **set service-profile** *name* **web-portal-acl** *aclname* command.

To further simplify last-resort configuration, last-resort AAA rules (configured by **set authentication last-resort** commands) are no longer required or supported. Instead, if the fallthru authentication type for an SSID or wired authentication port is set to **last-resort**, and no 802.1X or MAC access rules are configured for a service profile's SSID, users are automatically granted access.

Note. Authentication and authorization support for non-802.1X users of third-party APs still uses the **web-portal-*ssid*** and **last-resort-*ssid*** usernames. However, for third-party AP support, these names must be on a RADIUS server, not in the switch's local database.

If you are upgrading from WSS Software Version 4.2 or earlier, WSS Software 5.0 automatically changes the Web-based AAA and last-resort portions of the configuration file. (See "Migrating your Web-based AAA and Last-Resort configurations from WSS Software version 4.x to WSS Software version 5.0" (page 40).)

(For more information, see the "Configuring Web Portal Web-based AAA" section in the "Configuring AAA for Network Users" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Auto-RF enhancements

WSS Software Version 5.0 contains new commands that provide the following Auto-RF options:

- Lockdown options for dynamically assigned channels and power levels. You can convert dynamically assigned channel or power settings into statically configured settings. Previous WSS Software Versions allowed this capability only through WLAN Management System.
- Configurable time interval for ramped power changes. When Auto-RF determines that power should be increased or decreased, WSS Software gradually ramps the power up or down, in 1 dBm increments. By default, power is ramped up or down by 1 dBm every 60 seconds. every 60 seconds until the power setting is reached. You can use the following command to change this interval to anywhere from 1 to 65535 seconds.

In addition to these changes, for added stability, Auto-RF no longer changes a radio's transmit power based on client proximity. Accordingly, the following Auto-RF commands are deprecated in WSS Software Version 5.0:

- **set {ap | dap} radio auto-tune max-retransmissions**
- **set {ap | dap} radio auto-tune min-client-rate**
- **set radio-profile auto-tune power-backoff-timer**

Likewise, the **min-client-rate** and **max-retransmissions** options of the **clear {ap | dap} radio** and **set dap auto** commands are deprecated. The **min-client-rate** and **max-retransmissions** fields no longer appear in **show {ap | dap} config** output.

(For more information, see the "Configuring Auto-RF" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Unscheduled Automatic Powersave Delivery (U-APSD) support

WSS Software Version 5.0 enables WMM clients that use powersave mode to more efficiently request buffered unicast packets from AP radios by using U-APSD.

When U-APSD support is enabled in WSS Software, a client can retrieve buffered unicast packets for a traffic priority enabled for U-APSD by sending a QoS data or QoS-Null frame for that priority. U-APSD can be enabled for individual traffic priorities, for individual clients, based on the client's request. A client enables U-APSD for a traffic priority by indicating this preference when (re)associating with the AP radio.

A client can retrieve buffered unicast packets for a traffic priority enabled for U-APSD by sending a QoS data or QoS-Null frame for that priority.

A client can but is not required to request U-APSD for all four traffic priorities. The AP radio still buffers packets for all traffic priorities even if the client does not request U-APSD for them. However, to retrieve buffered packets for priorities that are not using U-APSD, a client must send a separate PSpoll for each buffered packet.

U-APSD is supported only for QoS mode WMM.

(For more information, see the "Configuring Quality of Service" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Clear option for show {ap | dap} qos-stats commands

The following commands now have a **clear** option:

- **show dap qos-stats** [*dap-num*] [**clear**]
- **show ap qos-stats** [*port-list*] [**clear**]

Repeating either of these commands with the **clear** option at regular intervals allows you to monitor transmission and drop rates.

Local software images on APs

WSS Software Version 5.0 supports local storage of AP software images on the APs themselves. When an AP boots, it can load its local image and does not need to download its image from a WSS unless the image on the WSS is newer. This enhancement allows APs to become operational faster.

(For more information, see "Boot Process for Distributed APs" in the "Configuring AP Access Points" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

DHCP server enhancements

WSS Software Version 5.0 allows configuration of the following new options on the WSS Software DHCP server:

- DNS domain name
- Primary and secondary DNS servers
- Default router (gateway)

In previous WSS Software Versions, the WSS Software DHCP server obtained values for these options from other parts of the switch's configuration. (This is still the default, if the options are not set on the server.)

(For more information, see the "DHCP Server" appendix of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

RADIUS accounting enhancements

WSS Software Version 5.0 includes support for the **acct-interim-interval** user attribute. You can use this attribute to configure WSS Software to send accounting update records at periodic intervals. WSS Software Version 5.0 also supports *system accounting*. When system accounting is enabled, WSS Software generates an Accounting-On message when the WSS starts, and an Accounting-Off message when the WSS is administratively shut down. This new accounting functionality can be used in conjunction with billing systems that require periodic accounting messages.

(For more information, see "Configuring Accounting for Wireless Network Users" in the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Support for special characters in SNMP community names

WSS Software Version 5.0 allows any printable ASCII characters except white space to be used in SNMP community names. Previous WSS Software versions allowed letters and numbers only.

Note. In WSS Software Version 5.0 and previous versions, SNMP community names cannot begin with numerals.

Increased life span of new self-signed certificates

Self-signed certificates created using WSS Software Version 5.0 have a longer life span than self-signed certificates generated using previous WSS Software versions. Self-signed certificates generated in WSS Software Version 5.0 are valid for three years. Self-signed certificates generated in previous WSS Software versions are valid for one year.

Specifying location and contact information for APs

WSS Software 5.0 includes the following CLI commands that allow you to specify information about the physical location of an AP, as well as contact information for the AP:

- **set** {**ap** *port-list* | **dap** *dap-num*} **location** *string*
- **set** {**ap** *port-list* | **dap** *dap-num*} **contact** *string*

For example, the following commands specify the location of AP 7 as *The conference room*, and the contact person as *Bob the IT guy.*

WSS# **set ap 7 location 'The conference room'**
success: change accepted.

WSS# **set ap 7 contact 'Bob the IT guy'**
success: change accepted.

To display the AP's location and contact information, use the **show ap config** command. For example:

WSS# **show ap config**
Port 7: AP model: AP-2330A, POE: enable, bias: high, name: MP07
boot-download-enable: YES
force-image-download: NO
load balancing group: none
location: The conference room
contact: Bob the IT guy
Radio 1: type: 802.11g, mode: disabled, channel: dynamic
tx pwr: 1, profile: default
auto-tune max-power: default,
Radio 2: type: 802.11a, mode: disabled, channel: dynamic
tx pwr: 1, profile: default

auto-tune max-power: default,

Version compatibility

WLAN Management System

This version of WLAN Security Switch 2300 Series (WSS Software) is intended for use with WLAN Management System Version 5.0 or higher only.

Minimum WSS Software requirements for upgrade

Table 2 lists the minimum WSS Software version a WSS must be running when you upgrade the switch to WSS Software Version 5.0.9. If your switch is running an older WSS Software version, you can use the upgrade path to upgrade the switch to 5.0.9.

Table 2. Software Requirements for Upgrade to WSS Software Version 5.0.9

Product	Minimum WSS Software Version Required	Upgrade Path
2350	4.0.10	4.0.x -> *5.0.x* 4.1.x -> *5.0.x*
2360/2361	4.0.*20*	4.0.*x* -> *5.0.x* 4.1.x -> *5.0.x*
2380	4.0.10	4.0.*x* -> *5.0.x* 4.1.x -> *5.0.x*

Caution! If you need to downgrade from WSS Software Version 5.0, you must downgrade to WSS Software Version 4.0 or later. If you downgrade to a WSS Software version that is earlier than 4.0, the switch's flash memory might be reformatted, which will cause all files, including configuration files and image files, to be lost. (To downgrade a 2360/2361, downgrade to 4.0 first.)

Best practices and common issues

Follow these best-practice recommendations during configuration and implementation to avoid or solve issues you might experience.

Best practice when powering down a switch

If a 2350 or 2360/2361 is connected to Power Sourcing Equipment (PSE), it is possible for the switch to remain powered on even when the power cord is unplugged. PSE can be a dedicated PoE injector or even another networking switch such as the WSS that is capable of supplying PoE. To ensure that the switch is powered off, unplug the power cord, then unplug all Ethernet cables that are connected to other PoE devices.

System configuration best practices

Nortel strongly recommends that you use WMS for archiving and version control of network-wide WSS configurations. Nortel also recommends that you archive the CLI-based configuration files of individual WSSs by copying the configurations to a server.

Client and AAA best practices

Follow these best-practice recommendations during configuration and implementation to avoid or solve issues you might experience.

Get clients and AAA working first

The greatest majority of installation issues are related to clients and AAA server (authentication, authorization, and accounting) operation, due to their diverse nature. Nortel recommends first establishing a baseline of proper operation with a sampling of wireless clients and the AAA server you plan to use. Working out client and AAA configuration methods first provides valuable information as you scale the deployment.

The selection of client and AAA server software will depend heavily on the requirements of your deployment. First, decide which EAP Protocol you will be using as that will restrict the available clients and servers. Each protocol has different advantages and disadvantages, which you will need to consider in your deployment. For most enterprise deployments, Nortel recommends using PEAP-MS-CHAP-V2 as the 802.1X protocol. Table 3 compares the EAP protocols.

Table 3. EAP Protocol Comparison

Protocol	Advantages	Disadvantages
PEAP-MS-CHAP-V2	• Does not require client certificates • Compatible with Nortel 802.1X Acceleration • Native support in Microsoft Windows XP and 2000 • Broad support in 802.1X clients	Username/password-based access might not be as strong as certificate-based access

Table 3. EAP Protocol Comparison (continued)

Protocol	Advantages	Disadvantages
EAP-TTLS	• Does not require client certificates • Broadest compatibility with user directories	• Requires third-party 802.1X client software • Username/password-based access might not be as strong as certificate-based access
EAP-TLS	• Strongest authentication using X.509 certificates. • Native support in Windows XP and 2000 • Broad support in all 802.1X clients	Client-side certificates require full PKI infrastructure and management overhead
PEAP-TLS	• Strongest authentication using X.509 certificates. • Native support in Windows XP and 2000 • Broad support in all 802.1X clients	• Client-side certificates require full PKI infrastructure and management overhead • Minimal advantage over EAP-TLS

Although LEAP uses the same ethertype as 802.1X (0x888e), the LEAP protocol is proprietary and does not conform to the IEEE 802.1X standard. Additionally, the LEAP protocol has serious security flaws. For example, LEAP-authenticated networks can be breached using a simple dictionary attack.

When testing and evaluating the Nortel WLAN 2300 Series System, enterprises using primarily Microsoft platforms are recommended to use Windows XP clients running PEAP-MS-CHAP-V2 with a Windows 2000 or 2003 server running Internet Authentication Service (IAS) as the RADIUS back end. This provides a test environment that is quick to set up and does not require additional third-party software.

Driver dependant behavior

- Some clients prefer a beaconed clear SSID to their configured SSIDs. If you configure WSS Software to beacon a clear SSID, some client adapters prefer this beaconed SSID over the SSIDs they are configured to use. Conversely, some adapters can associate only with a beaconed SSID. Determine whether to beacon the clear SSID based on the types of clients in the network.
- Standby mode can prevent some clients from reassociating. If a laptop PC whose wireless adapter is associated with an AP access point goes into standby (hibernate) mode, the operating system can either freeze or experience a Blue Screen of Death (BSOD) when the laptop comes out of standby mode and attempts to reassociate with the access point. To work around this behavior, disable standby mode. Alternatively, disable and reenable the wireless adapter after the client emerges from standby mode.
- If a client passes authentication but fails authorization, the client might indicate that authentication has succeeded but the AP access point nonetheless disassociates from the client. In this case, the client might indicate that the network is unavailable. For example, this situation can occur if the certificate exchange is valid but the requested VLAN or ACL filter is not available, or a Mobility Profile™ denies service to the client. Once the AP disassociates from the client, the network continues to be unavailable to the client through the AP for the duration of the 802.1X quiet-period timer, which defaults to 60 seconds. An error message indicating that a client has failed authorization appears in the WSS's system log.

802.1X clients

Properly preparing your clients for wireless connectivity is one of the most important things you can do to ensure an easy rollout. Here are some guidelines for preparing common 802.1X clients and platforms.

Windows XP

Windows XP is a popular platform for wireless clients because of its native support of 802.1X authentication and simplified configuration of wireless networks. If you choose to use the 802.1X client built-in to Windows XP, please note the following:

- Microsoft has extensive documentation on how to configure and use wireless 802.1X authentication in an Active Directory environment, published on their website. You can start with Microsoft's Wi-Fi center at:

  www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx

- Installing Windows XP Service Pack 2 is recommended for all wireless clients as it includes several important hotfixes.
- If you are not prepared to install Service Pack 2, Nortel strongly recommends that all wireless clients use Service Pack 1a with the following hotfixes installed:
  - KB826942—This is the WPA Hotfix Rollup and is available through Microsoft Update
  - KB834669—This corrects an 802.1X client issue which can cause system instability problems in Windows XP. You will need to contact Microsoft or Nortel Support directly for this hotfix.
- If your network uses logon scripts, Active Directory group policies, or your users regularly share their laptops, you should enable computer authentication (also known as machine authentication) to achieve full functionality over your wireless connection.
- Download current drivers for your NICs from the NIC vendor(s).
- If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, Nortel recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. Nortel strongly recommends that you update the driver manually using the driver properties in the Network control panel instead of installing the client manager.
- If you use computer authentication with different VLANs for the Computer and User accounts and do not have the WPA hotfix rollup (KB826942) or Service Pack 2, you need to install Microsoft hotfix KB822596. Otherwise, DHCP will not operate correctly after the user authenticates. You must contact Microsoft technical support for this hotfix. It is not available from their website. For more information on computer authentication, see "Computer authentication" (page 21).
- If MD5 challenge is configured on a Windows XP client for wired authentication, Nortel recommends that you set the quiet period to 5 to allow successful authentication. In addition, if the authentication is carried out manually, the timeout value must be set to no less than 30 seconds in order to allow the user ample time to enter their username and password. For example, to configure 802.1X on a WSS to allow these users time to log in, type the following commands:

  2380# **set dot1x quiet-period 5**
  2380# **set dot1x tx-period 30**

  The same recommendations for the quiet period and transmit period also apply to PEAP with manual entry of credentials.

Windows 2000

Many enterprises have a large installed base of Windows 2000 laptops, making this a common choice of platform. Windows 2000 Service Pack 4 includes a native 802.1X client. If you choose to use the 802.1X client built-in to Windows 2000, please note the following:

- Microsoft has extensive documentation on how to configure and use wireless 802.1X authentication in an Active Directory environment, published on their website. Most of this documentation is geared towards Windows XP, but both operating systems have many similarities in the client. You can start with Microsoft's Wi-Fi center at:

  www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx

- Installing Windows 2000 Service Pack 4 is required for all wireless clients.
- Some clients might experience system instability when using PEAP-MS-CHAP-V2 in an Active Directory environment. The primary symptom of this is a message displayed after login informing the user that the service svchost.exe has stopped unexpectedly. If you experience this problem, please contact Microsoft technical support and request hotfix KB833865.
- If your network uses logon scripts, Active Directory group policies, or your users regularly share their laptops, Nortel recommends that you enable computer authentication to achieve full functionality over your wireless connection.
- Download current drivers for your NICs from the NIC vendor(s).
- Windows 2000 does not include a full implementation of the Wireless Zero-Config service from Windows XP, so you will need to use the client manager software provided with your NIC to configure your SSID and enable WEP encryption. When using dynamic WEP in Windows 2000, select *static WEP 128bit* and enter any static WEP key as a placeholder. This temporary key configures the driver to use WEP to encrypt packets, and the Microsoft 802.1X client then overrides the static WEP key you entered with a dynamic key after you authenticate successfully.
- If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, Nortel recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. If you are unable to install the client manager without the AEGIS component, contact the driver manufacturer or download an earlier version that does not contain the AEGIS component.
- 16-bit PCMCIA and built-in NICs (some 802.11b cards in Dell, Toshiba, and other manufacturers' laptop PCs) might require a registry setting to be changed before they will be able to associate with any SSID. Microsoft Knowledge Base article 327947 documents the changes necessary to resolve the problem. Multi-band cards (A/B or A/B/G) are generally 32-bit and do not experience this problem.
- If you use computer authentication with different VLANs for the Computer and User accounts, you need to install Microsoft hotfix KB822596. Otherwise, DHCP will not operate correctly after the user authenticates. You must contact Microsoft technical support for this hotfix. It is not available from their website. For more information on computer authentication, see "Computer authentication" (page 21).
- If you experience a delay in receiving your DHCP IP address wirelessly while using 802.1X authentication, you might need to install Microsoft hotfix KB829116. You must contact Microsoft technical support for this hotfix. It is not available from their website.

Funk Odyssey

The Funk Odyssey client is required when you require WPA support on Windows 2000, or when you need to authenticate to an LDAP backend database that does not support MS-CHAP-V2 over LDAP. If you choose to use this client, please note the following:

- Download the latest version from Funk's website at: www.funk.com
- Be sure to turn off Wireless Zero Config in Windows 2000 by disabling the service.
- If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, Nortel recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. Nortel recommends that you update the driver manually using the driver properties in the Network control panel instead of installing the client manager.

Macintosh OS/X

OS/X Version 10.3, also known as Panther, includes an 802.1X client that supports Dynamic WEP and WPA/TKIP. If you choose to use this client, please note the following:

- The Panther client will only connect successfully to an SSID which is only dynamic WEP, or only WPA/TKIP. Any other configuration involving WEP with WPA enabled or AES is not supported by the current Panther client. If you need to run both WPA/TKIP and Dynamic WEP at the same time you must configured separate service profiles for each encryption type in order to maintain compatibility with Macintosh clients.
- The Panther client requires you to specify the inner and outer PEAP-MS-CHAP-V2 usernames in separate areas. Depending on your AAA backend, both usernames might require a domain prefix in the form of *DOMAIN\username*.

Computer authentication

Windows clients support 802.1X authentication of the computer itself. This is called *computer authentication* (also known as *machine authentication*). Computer authentication is useful when you want your computer to be active on the domain even when no users are logged in to the computer. Some features of Windows XP Professional and Windows 2000 Professional work correctly only with an active network connection to the domain controller enabled before a user is logged on to the PC. Using computer authentication ensures that this network connection is established during the boot sequence, providing a wire-like infrastructure that allows you to use the following features on a wireless network. Table 4 lists Microsoft networking features that require computer authentication.

Table 4. Microsoft networking features that require computer authentication

Feature	Scenario Requiring Computer Authentication
Active Directory computer Group Policy	Computer–based Group Policy is applied during computer start up and at timed intervals—even when no on is logged in to windows.
Network logon scripts	Network logon scripts are run during initial user login.
Systems management agents	Systems management application agents such as those that come with Microsoft Systems Management Server (SMS) frequently need network access without user intervention.
Remote Desktop Connection	Computers are accessible from Windows Remote Desktop Connection when no one is logged in to windows.
Shared folders	Files and folders shared from a computer are still available, even when no user is logged in.

Configuring computer authentication on the client is simple, though it requires the use of the Microsoft 802.1X client built-in to Windows XP and Windows 2000. Keep the following information in mind when configuring computer authentication on Microsoft clients:

- To enable computer authentication, go to the **Authentication** tab where you normally select your 802.1X authentication method and enable the checkbox labeled **Authenticate as computer when computer information is available**.

- The authentication protocol that is configured for your user accounts will also be used for the computer account.
- If the EAP protocol you are using requires client certificates, you must use the Microsoft Enterprise Certificate Authority built-in to Windows 2000 Server and Windows Server 2003 to generate *Computer* certificates for PCs on your active directory domain. Microsoft Knowledgebase Article KB313407 explains how to enable the automatic distribution of computer certificates through Active Directory.
- If the user and machine accounts use different VLANs, you must install hotfixes on the client PCs to enable them to DHCP for a new IP address when the user authentications. Windows XP requires either the WPA Rollup Hotfix (KB826942) or Hotfix KB822596. Windows 2000 requires hotfix KB822596.
- Using PEAP-MS-CHAP-V2 with computer authentication will allow users who have never logged on to a PC authenticate wirelessly without having to login to the PC over a wired connection the first time. EAP-TLS still requires the user to connect to the network over a wired connection to generate a profile on the PC and a user certificate.

Enabling computer authentication also requires minor reconfiguration of Active Directory and IAS. Please note the following when configuring computer authentication on an active directory domain:

- You must grant dial-in access for the computer accounts in Active Directory that you wish to enable computer authentication on. If the tab to configure dial-in access does not appear, follow the directions in Microsoft Knowledgebase article KB306260.
- Review your remote access policies in IAS to insure that the computer accounts have appropriate group membership to allow them to match the proper policy.

Computer authentication also requires specific configuration considerations on the WSS:

- The username of a computer authentication connection will be in the form of host/*fully-qualified-domain-name*, for example host/bob-laptop.nrtl.com or host/tac1-laptop.support.nrtl.com. This username is the same regardless of the configured protocol (PEAP-MS-CHAP-V2 or EAP-TLS). An appropriate userglob would be *host/*.domain.com* where domain.com is the Active Directory domain name. Alternatively, in a smaller deployment you could use a userglob of ** and have both user and computer authentication go to the same RADIUS server.
- PEAP-MS-CHAP-V2 offload mode is not supported with computer authentication. You must use pass-through 802.1X authentication policies with computer authentication.

AAA

Table 5 lists the AAA servers and configurations that have been tested with WSS Software. Tests were performed to a local user database in most cases, and additionally to Microsoft Active Directory and LDAP with specific protocols as noted in the table. The tests were initially performed using Dynamic WEP, though subsequent testing has revealed no noticeable differences in RADIUS compatibility when using WPA.

A result of *Pass* indicates that the combination is supported by the Nortel WSS Software. A result of *Not Applicable* indicates that the RADIUS server tested does not support the feature. A result of *Fail* indicates that the RADIUS server does not interoperate with WSS Software for that feature. A result of *Not Tested* indicates that the feature was not tested.

Table 5. AAA servers tested with Nortel WSS Software

Configuration	RADIUS Servers Tested				
	Windows 2000 IAS	**Windows 2003 IAS**	**Funk Steel Belted Radius**	**Cisco ACS**	**FreeRadius (Linux)**
PEAP-MS-CHAP-V2	Pass	Pass	Pass	Pass	Pass
PEAP-MS-CHAP-V2 Offload	Pass	Pass	Pass	Pass	Pass
EAP-TLS	Pass	Pass	Pass	Not Tested	Pass
EAP-TTLS	Not Applicable	Not Applicable	Pass	Not Applicable	Not Tested
Single-Sign-On Active Directory & PEAP-MS-CHAP-V2	Pass	Pass	Pass	Pass	Not Applicable
Single-Sign-On LDAP & EAP-TTLS	Not Applicable	Not Applicable	Pass	Not Tested	Not Tested
Nortel VSAs	Pass	Pass	Pass	Pass	Pass
MAC-based authentication	Pass	Pass	Pass	Pass	Pass
Microsoft Active Directory computer authentication	Pass	Pass	Not Applicable	Pass	Not Applicable

Testing notes

- Single-Sign-On is defined as clients being able to use the same username and password for 802.1X authentication that they use to authenticate with network services and logon to their local PC.
- A *Pass* result for Nortel VSAs indicates that the VSAs were able to be added to the RADIUS server manually. Future versions of Steel Belted RADIUS and FreeRadius are planned to include standard definitions of the Nortel VSAs.
- Funk Steel Belted Radius version used for testing is 4.53
- Windows 2000 with Service Pack 4
- Cisco ACS 3.2 or later is required to support PEAP-MS-CHAP-V2

WPA

If you choose to use WPA to secure your wireless network, please note the following:

- CCMP (AES 802.11i draft support) is supported only when it is the only encryption type enabled on that SSID. Enabling TKIP or Dynamic WEP on the same SSID with CCMP can cause serious connectivity issues as most clients do not properly support this configuration. Nortel recommends that you create a separate service profile and SSID for WPA/CCMP.
- Enabling TKIP and Dynamic WEP on the same SSID is not recommended. This configuration forces the group key (multicast/broadcast key) to use the lowest common encryption type, in this case Dynamic WEP. Additionally, compatibility with wireless NICs is reduced.

- Downloading the latest drivers for your wireless NIC is strongly recommended. See "802.1X clients" (page 18) for specific information on installing drivers for your operating system.
- When a session key is changed, Microsoft WPA clients can sometimes incorrectly start using the new key before the end of the four-way handshake that is used to establish the key information. This issue can occur when the session timeout for the client session expires. As a result, the AP access point rejects the client's re-association attempt because the key information presented by the client is invalid. If you experience this issue, clear the Session-Timeout attribute on the affected users. The WSS will not force a reauthentication of WPA/TKIP and WPA/CCMP users periodically like it does with dynamic WEP users.
- Do not use the **set service-profile shared-key-auth** command in a WPA configuration. This command does not enable PSK authentication for WPA. To enable PSK for WPA, use the **set service-profile auth-psk** command.
- Use one WPA authentication method per SSID, either 802.1X authentication or preshared key (PSK) authentication, but not both.

Security—best practice when mixing encrypted access and clear access

It is possible to configure a RADIUS server or an WSS's local authentication database so that a user with encrypted access and a user with unencrypted access are authorized to join the same VLAN from different SSIDs. This configuration might allow a hacker to more quickly discover keys by listening to both the encrypted traffic and unencrypted traffic for comparisons. You can either use the Nortel SSID VSA or the encryption assignment VSA to prevent this problem.

If you only have one VLAN that each MAC-auth client should connect to, add the SSID VSA to the account for the MAC-address (either local or RADIUS). This will force the WSS to only allow that MAC address to connect to the specified SSID.

If you require the same MAC user to be able to connect to more than one SSID, you can use encryption assignment to enforce the type of encryption a user or group must have to access the network. When you assign the Encryption-Type attribute to a user or group, the encryption type or types are entered as an authorization attribute into the user or group record in the local WSS database or on the RADIUS server. Encryption-Type is a Nortel VSA. Clients who attempt to use an unauthorized encryption method are rejected. In this way, a client could connect to any WEP encrypted SSID, but not a clear SSID. (See the *Nortel WLAN 2300 Series System Software Configuration Guide* for more information.)

Security best practices

WSS Software and WLAN Management System provide robust options for securing management access, to WSSs and to the WLAN Management System client and WLAN Management System monitoring service. To optimize security for management access, use the following best practices.

Certificates

When anyone attempts to access a WSS, the switch authenticates itself by presenting a signed certificate to the management application that is requesting access. The switch's certificate can come from a certificate authority (CA) or it can be generated and signed by the switch itself. Nortel recommends that you use certificates assigned by a CA. Certificates from a trusted CA are more secure than self-signed certificates. Here are some trusted CAs:

- www.verisign.com
- www.entrust.com
- www.microsoft.com

If you use a self-signed certificate, configure the clients to not validate server certificates. If a client is configured to validate server certificates, the client will not be able to validate a self-signed certificate from the WSS.

Usernames

Nortel recommends that you do not create usernames that have the same spelling but use different case. For example, do not create both username *dang* and username *DANG*.

Passwords

The CLI, as well as WLAN Management System, can be secured using passwords. By default, the following access types do not have passwords configured. Each uses a separate password.

- Console access to the CLI. To secure console access, configure a username and password in the WSS's local database, using the **set user** command. After you configure at least one username and password, access to the CLI through the console requires a password. (Access through Telnet or SSH is not possible without a password, even on an unconfigured switch.)
- Access to the enable (configuration) level of the CLI, through the console, or through Telnet or SSH. To secure enable access, configure the enable password using the **set enablepass** command.
- Access to WLAN Management System client. To secure access, configure user accounts within WLAN Management System, on each machine on which the client is installed.
- Access to the WLAN Management System monitoring service. To secure access, configure user accounts within the monitoring service.

Do not use passwords that are easy to guess, such vehicle registration plates, family birthdays and names, or common words. Use combinations of uppercase and lowercase letters as well as numbers in all passwords.

SNMP

SNMP is disabled by default. Leave SNMP disabled unless you need it. If you do need to use SNMP, do not use the well-known community strings *public* (commonly used for read-only access) or *private* (commonly used for read-write access.) Likewise, if you are using SNMPv3, do not use a well-known or easy to guess string for the User Security Model (USM) username. By default, no SNMP community strings or USM users are configured. If you are using SNMPv1 or SNMPv2c, use it on an isolated management VLAN so that the clear text community strings are not visible on the public network. If you are using SNMPv3, set the security to a setting that is stronger than **unsecured**.

To disable SNMP (if not already disabled), use the **set ip snmp server disable** command.

CLI access

WSS Software allows CLI access through the console, through Telnet, and through SSH. Console and SSH access are enabled by default. Telnet is disabled by default.

Configure a username and password, so that WSS Software requires login even for console access. Usernames and their passwords are not specific to the type of management access. You can use the same username and password for access through the console, Telnet, or SSH.

Leave Telnet disabled unless you need it. Use SSH instead.

Web access

Web View uses HTTPS for encrypted communications and certificate-based server authentication, and requires use of the enable password.

Beginning in WSS Software Version 4.0, Web View access through HTTPS is disabled by default. Unless you need to use Web View, leave the HTTPS server on the WSS disabled. (Even though WLAN Management System also uses HTTPS, disabling the HTTPS server does not disable access by WLAN Management System.)

If you do need to use Web View, you can enable it using the **set ip https server enable** command. Use the following best practices to preserve or increase the security level related to Web access:

- Use an enable password that follows the password recommendations given above.
- Use a CA-signed certificate instead of a self-signed certificate on the WSS.

Note. If a user's wireless client does not trust the certificate, the user might experience an additional delay during login. To avoid the additional delay, use a certificate signed by your CA or an Internet CA.

WLAN Management System

By default, access to the WLAN Management System client and the WLAN Management System monitoring service do not require passwords. To secure access, configure user accounts within each instance of WLAN Management System client and within the monitoring service.

The monitoring service uses a signed certificate for authentication. The monitoring service has a self-signed certificate by default. For added security, used a certificate signed by a CA instead. To use a CA-signed certificate, install the certificate in a key store file on the machine where the monitoring service is installed, and change the name of the key store file used by the monitoring service from its default to the one where you installed the certificate signed by the CA.

Guest access (unencrypted SSIDs)

If you need to prevent all guest access (access to unencrypted SSIDs):

- Do not create any service profiles for SSID type clear.
- Delete any existing service profiles for a clear SSID.

VLANs

VLANs used for Web Portal must be separate from VLANs used for WSS System IP addresses. When configuring Web Portal users, ensure that users are assigned to VLANs different from those containing the System IP address of any WSS in the mobility domain."

Web-based AAA best practices

If you plan to use Web-based AAA, see the "Configuring Web-based AAA" section in the "Configuring AAA for Network Users" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*. The section has configuration requirements and recommendations, in addition to an overview of the Web-based AAA process.

Mobility Domain™ (Multiple WSSs) best practices

Run the same WSS Software version on all WSSs in the Mobility Domain.

Nortel recommends that you run the same WSS Software version on all the WSSs in a Mobility Domain.

Note. Switches running WSS Software Version 5.0 will operate in the same Mobility Domain with switches running WSS Software Versions 4.0 or higher.

Helpful commands

Description Use the following commands to verify the proper operation of a Mobility Domain in support of features such as subnet roaming:

- **show mobility-domain status**—In a functioning Mobility Domain, the output on every WSS displays every WSS in the Mobility Domain.
- **show roaming vlan**—In a functioning Mobility Domain, the output on every WSS displays the network-attached VLAN of every other WSS in the Mobility Domain.

Other useful commands, documented in the *Nortel WLAN Security Switch 2300 Series Command Reference*, include **show tunnel** and **show roaming station**.

Distributed AP best practice when using STP

A Distributed AP is a leaf device. You do not need to enable STP on the port that is directly connected to the AP.

If Spanning Tree Protocol (STP) is enabled on the port that is directly connected to a Distributed AP, you might need to change the STP configuration on the port, to allow the AP to boot.

Note. STP on a port directly connected to a Distributed AP can prevent the AP from booting.

Use IGMP snooping effectively

Using IGMP (11909, 12863, 12866)

Description WSS Software supports the Internet Engineering Task Force (IETF) draft *draft-ietf-magma-snoop* for controlling the forwarding of IP multicast traffic by a Layer 2 switch. The draft mandates the use of a 0.0.0.0 source IP address if no IP address is available on the switch for the subnet. However, some multicast routers and even other Layer 2 switches report errors in the presence of the 0.0.0.0 source IP address.

Workaround Apply the following methods to use IGMP snooping effectively:

- **Set IP addresses on all VLAN interfaces.** This straightforward workaround prevents most known issues. If querier functionality might be needed, ensure that the IP address of the WSS VLAN is higher than the address of any multicast router servicing the same subnet.
- **Consider disabling IGMP proxy reporting.** The IGMP proxy reporting function is enabled by default, but some multicast routers do not accept reports using a 0.0.0.0 source IP address. In this case, either assign an IP address to the VLAN interface on the WSS switch or disable IGMP proxy reporting. To disable proxy reporting, use the command **set igmp proxy-report disable**.

Note. Disabling proxy reporting can increase IGMP overhead traffic to the multicast router.

- **Enable the IGMP querier only if needed.** The IGMP pseudo-querier function is disabled by default. Enable it only if the source of a multicast stream is on a subnet the WSS switch is also connected to. If this is the case, you must assign an IP address to the VLAN interface. The IP address must be higher than the IP address of the querier multicast router on the same subnet. To enable the IGMP pseudo-querier, use the command **set igmp querier enable**.
- **Disable multicast router discovery.** This multicast router solicitation protocol (part of *draft-ietf-magma-snoop*) is known to cause error messages with other IGMP snooping switches and multicast routers. To disable the protocol, use the command **set igmp mrsol disable**. (The protocol is disabled by default in the current software version.)

User ACLs require explicit source and destination addresses

A user ACL is an ACL that is applied to a specific username. You can apply ACLs to a user's inbound or outbound wireless traffic. For a user ACL to take effect, you must explicitly set both the source and destination addresses in the ACL.

Rogue detection active scan interval is longer during a SpectraLink SVP call. (23317)

The active scan feature can be used during SVP calls. However, when a call is active, the interval at which active scan goes off-channel to look for rogues is increased from once a second to once every 60 seconds.

Due to the longer interval between active scans, it can take longer for WSS Software to detect a rogue AP when an SVP call is active. Generally, detection of a rogue while a call is active can take from 3.5 to around 7.5 minutes. To reduce the detection time, add more APs to the coverage area.

IPv6 support

WSS Software 5.0 can forward IPv6 traffic transparently, at Layer 2. IPv6 clients in the same subnet can communicate with one another through a WSS.

VoIP devices vendor support

These are the Nortel supported options:

- SpectraLink—Non-WMM SVP devices
- Vocera—Non-WMM Vocera devices

System parameter support

Table 6, Table 7, Table 8, and Table 9 list the recommended or maximum supported values for major system parameters.

Table 6. Mobility system parameters

Parameter	Supported Value
WSSs in a single Network Domain	500
WSSs in a single Mobility Domain	32
Roaming VLANs per WSS	300 Does not include local statically configured VLANs
VLANs per Mobility Domain	400 This number consists of 300 roaming VLANs plus 100 local statically configured VLANs.
APs per WSS	• 2380: 300 configured, 120 active • 2360/2361: 30 configured, 12 active • 2350: 8 configured, 3 active Includes directly attached APs and Distributed APs. Inactive configurations are backups.
Minimum link speed within a Mobility Domain	128 Kbps

Table 7. Network parameters

Parameter	Supported Value
Forwarding database entries	• 2380: 16383 • 2360/2361: 8192 • 2350: 8192
Statically configured VLANs	128
Virtual ports (sum of all statically configured VLAN physical port memberships)	256
Spanning trees (STP/PVST+ instances)	64

Table 7. Network parameters (continued)

Parameter	Supported Value

ACLs and Location Policies	• ACEs per switch
	  • 2380: 2308
	  • 2360/2361: 700
	  • 2350: 700
	• ACEs per ACL:
	  • 2380: 267
	  • 2360/2361: 267
	  • 2350: 25
	• Location Policies per switch:
	  • All models: 1
	  The Location Policy can have up to 150 rules.

IGMP streams	500 **Note:** Replication of a stream on multiple VLANs counts as a separate stream on each VLAN.

Table 8. Management parameters

Parameter	Supported Value
Maximum instances of WLAN Management System simultaneously managing a network	3
Telnet management sessions	• 2380: 8 • 2360/2361: 4 • 2350: 4 **Note:** The maximum combined number of management sessions for Telnet and SSH together is 8 for the 2380, or 4 for the 2360/2361 and 2350, in any combination.
SSHv2 management sessions	• 2380: 8 • 2360/2361: 4 • 2350: 4
Telnet client sessions (client for remote login)	• 2380: 8 • 2360/2361: 4 • 2350: 4
NTP servers	3
SNMP trap receivers	8
Syslog servers	4
RADIUS servers	100 configured on the switch 10 in a server group 4 server groups in a AAA rule

Table 9. Client and session parameters

Parameter	Supported Value
Authenticated and associated clients per radio	100 Clients who are authenticated but not yet associated are included in the total.
Active clients per radio	50 Total number of active clients simultaneously sending or receiving data.
Active AAA sessions (clients trying to establish active connections) per WSS	• 2380: 2500 • 2360/2361: 300 • 2350: 75 **Note:** These are the suggested maximums. The switch might be able to support even more sessions, but performance or system stability might be affected.
AAA users configured in local database	• 2380: 999 • 2360/2361: 250 • 2350: 250

Known behaviors and issues

In addition to the more common items indicated in "Best practices and common issues" (page 17), the current software version contains the following known behaviors and issues.

System configuration issues

Unexpected local changes are available after upgrade from version 4.1.11 software release to version 5.0.9 software release. (Q01468246)

Workaround Undo the local changes.

"Upgrade of bootstrap failed" and "not allowing upgrade" messages are displayed when downgrading a 2350 from 5.0.9 to 4.1(Q01468252)

Workaround It is safe to ignore the error messages, but you will see it during a downgrade of the 2350.

Adding a static VLAN with the same name as a VLAN whose traffic is being tunneled through the switch can cause the switch to restart. (18367)

Description WSS Software can tunnel traffic for a VLAN through a WSS that does not have that VLAN statically configured. If you attempt to add a static VLAN to a switch that is already tunneling traffic for a VLAN with the same name, this can cause the switch to restart.

Workaround To create the VLAN, clear the Mobility Domain configuration from the switch, create the VLAN, then configure the Mobility Domain again.

Time and date do not synchronize with an NTP server, if the switch's NTP client is enabled before the NTP service is started on the server. (20382)

Web portal service profile issue when using the Administrator level user access. (Q01505923)

Description **The user receives the Web View screen and a second window showing Certificate Acceptance which once accepted shows the Web View screen that sometimes allows changes to the switch and other times causes the window to lock.**

Workaround Web Portal with Web View enabled. Changes to the Certificate were made which has made significant improvements. The common name was the IP address of the vlan interface. This was changed to web.local.

- 1.) Using Web Portal with the switches within the Mobility Domain - DNS needs to be disabled
- 2.) Using Web Portal the certificate common name should be left as default or web.local should be tried.

When downgrading from 5.0.9.4 to 4.1 software it is necessary to re-enter the Radius keys. (Q01570753)

Description When downgrading from 5.0.9.4 to 4.1, the shared secret for Radius servers become corrupted.

Workaround Re-enter the Radius keys

Switching and port issues

Router redundancy protocol on intermediary devices between WSSs in a Mobility Domain can interfere with communication among the switches. (16910)

Description If the Mobility Domain contains intermediary switches or routers that use a router redundancy protocol, WSSs that communicate through those intermediary devices might lose communication with one other due to the way some router redundancy protocols handle MAC addresses. If this issue occurs, log messages appear periodically on the seed WSS indicating that member WSSs are entering or leaving the Mobility Domain.

Workaround Set the FDB timer (default 300 seconds) and the ARP timer (default 1200 seconds) to the same values on the WSSs. Nortel recommends using 300 seconds as the value for both timers. To set the FDB timer, use the **set fdb agingtime** command. To set the ARP timer, use the **set arp agingtime** command.

Mixing autonegotiation with full-duplex mode on a link causes slow throughput and can cause a WSS port to stop forwarding. (26276)

Description Nortel recommends that you do not configure the mode of a WSS port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although WSS Software allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to a WSS port in such a configuration can cause forwarding on the link to stop.

On model 2360/2361, errors were being reported for ports that were not in use on the switch. (30111)

Continuous SNMP MIB walk can cause the WSS to restart. (33683)

Description Cycling through the entire SNMP V2C MIB using the MibBrowser of SNMPc v7.0.12 caused the WSS to restart

On the 2360, direct connected APs reset with ports 1 to 3 resetting every few minutes during stress testing. (33919)

Access Point (AP) issues

Distributed APs and Link Autonegotiation (16726)

Description The Ethernet interfaces on an AP are configured to autonegotiate the link speed (10 Mbps or 100 Mbps) and mode (half duplex or full duplex). The setting cannot be changed. A common setting on third-party switches is 100 Mbps, with full duplex. If you connect a Distributed AP to a port that is set for 100 Mbps with full duplex, the AP operates at 100 Mbps with half duplex. This results in an unusable link.

Workaround Configure the port on the other device to autonegotiate.

AP Reset: “Image download failed” message appears after downgrading from 5.0.9.4 to 4.1.14 (37284)

Description The ”Image download failed” message appears after downgrading from release 5.0.9.4 to release 4.1.14 software. This spurious message does not prevent the normal operation of the AP. This issue does not occur when upgrading from 4.1.14 to 5.0.9.4.

Distributed AP can change IP addresses during boot sequence in environments with multiple DHCP servers. (16499)

Description To become fully active, a Distributed AP does a full restart after downloading its software image. The first time the AP is powered up, it sends a DHCP discover for an IP address, uses DNS to find its configured WSS, then downloads its software image from that WSS. After downloading the image, the AP restarts itself with the downloaded image and sends a second DHCP discover to again obtain its IP address. In a network containing more than one DHCP server, it is possible for the AP to use one IP address when downloading the image, but end up with a second IP address after rebooting the second time. This can occur if the DHCP server that responds to the DHCP request after the second reboot is not the same server that responded to the first request.

Workaround This issue does not prevent the AP from operating normally but can make managing the AP more difficult if the address the AP receives the second time is not predictable. To prevent the AP from using more than one address, use static address assignment in your DHCP server.

Session load balancing is supported only for directly connected APs, not for Distributed APs. (25315)

Description If you plan to use the session load balancing feature, you must use directly connected APs. The feature does not work on Distributed APs.

DAPs configured with different DAP security values between the high/low bias switches do not load image after reboot. (28157)

Description In a configuration where a redundantly configured DAP has DAP security configured differently on each of the redundant WSSs (one switch had DAP security set to Optional while the other switch had DAP security set to None) the boot image does not load on the DAP after reboot.

Workaround Set DAP security setting to None on both WSSs or delete the low bias configuration.

During WSS stress testing the error message : "Resetting radio 2 because unable to send 6 beacons" occurred every 1 to 2 minutes in the the syslog. (33883)

The command "set dap auto model (null) radiotype 11g" appears after staged WSS remote configuration. (33767)

Active scan operates in the wrong period when the "priority" or "traffic bandwidth" settings are changed. (33484)

DAPS rebooting every 30 minutes (Q01537459 Q01561861)

Description A DHCP NAK can cause the AP to reboot. This issue only exists on a network with 2 DHCP servers, where one server is unconfigured or disabled.

Workaround

AP does not successfully upgrade the Air Defense sensor image. (Q01569641)

Description 2330A AP's OUI MAC addresses were not registered with SM3, the server rejects MAC addresses it does not recognize as a server.

Workaround Perform an OUI update – go to ADDadmin > dbase > OUI update.

WMS issues

Deleting PEAP-MS-CHAP-V2 AAA methods in an 802.1X policy with WMS might not be reflected on the WSS**. (14157)**

Description If you specify multiple AAA methods (for example, multiple server groups) for a PEAP-MS-CHAP-V2 802.1X policy, and you remove the last method with WMS, the WSS might still use the removed method. For example, if the 802.1X policy contains the following methods, and you use WMS to remove method *sg3*, the WSS continues to use *sg3:*

set authentication dot1x ssid any EXAMPLE* peap-mschapv2 sg1 sg2 sg3

Workaround To restore the intended configuration, restart the switch.

Changing rate configuration using WMS (Q01576410)

Description When radio transmission rates for both b and g radios are changed at the same time and deployed to the switch through WMS the transmission rates can be corrupted through CLI output seed switch and some users will lose connection. If both radio transmission rates are set to default, the g radio will only transmit rates of 1.0 and 2.0.

Workaround Deploy only one radio at a time.

IP services issues

VLANs used for Web Portal should be separate from VLANs used for WSS System IP addresses. (Q01468251)

Workaround When configuring Web Portal users, ensure that users are assigned to VLANs different from those containing the System IP address of any WSS in the mobility domain

Traceroute on 2360/2361 can contain an extra line. (18123)

Description If the route from a 2360/2361 to a traceroute destination contains more than one hop, the CLI output contains an extra line, for a non-existent hop. The extra line is easy to identify because it does not list an IP address. Here is an example:

2360/2361# **traceroute 192.168.2.1**
traceroute to 192.168.2.1 (192.168.2.1), 30 hops max, 38 byte packets
1 192.168.1.111 (192.168.1.111) 9.229 ms 4.186 ms 2.251 ms
2 * 4.365 ms *
3 192.168.2.1 (192.168.2.1) 5.657 ms * 4.356 ms

In this example, the second hop does not exist, and line 3 is the second hop.

Workaround This issue is cosmetic only and does not invalidate the information in the other lines of the display.

Mac client needs to renew IP address when using DHCP restrict option (Q01559320)

Description Release 5.0.9.4 includes a feature that allows the administrator to restrict access to clients that do not have a DHCP address. When the DHCP-restrict feature is enabled, it does not allow proper connectivity of Mac clients.

Workaround Renew the IP address for the Mac client.

AAA and RADIUS issues

Radius server disappears after downgrading from version 5.0.9 software release to version 4.1.11 software release (Q01468244)

Multiple RADIUS servers with the same IP address are not supported. (13895)

Description You cannot configure multiple instances of RADIUS on the same machine, with the same IP address. This method is sometimes used as a scaling technique if RADIUS transactions on the default UDP port become congested and another instance of the RADIUS server on the same machine is configured to use a different UDP port number. WSS Software does not allow you to specify the UDP port number of a RADIUS server and therefore cannot distinguish among multiple server entries with the same IP address.

Workaround Use a unique IP address for each RADIUS server.

CLI accepts a subnet mask with a RADIUS server IP address. (16594)

Description When you configure a RADIUS server on the WSS, the server's IP address does not require a subnet mask. If you do specify a subnet mask, the CLI changes the server IP address and the incorrect address is placed into the switch's configuration.

Workaround Do not specify a subnet mask with a RADIUS server address.

Default 802.1X retransmit interval is too short for manual login. (18032)

Description The default 802.1X retransmit interval is 5 seconds. Although this interval is adequate for clients that are configured to automatically use the user's Windows login information as the network login information, the interval is too short for users who must manually enter their network login information.

Workaround If the network has clients that do not automatically use the Windows username and password as the network username and password, use the **set dot1x tx-period** command to increase the retransmit time.

Caution! Changes to 802.1X parameters affect all SSIDs managed by the WSS.

Deleting a user group or MAC user group does not delete membership from its members. (14833)

Description If you type the **clear usergroup** or **clear mac-usergroup** command to delete a user group or MAC user group, the **show aaa** command shows that the user group is gone. However, the user profiles for the users still show them to be members of the deleted groups.

Workaround Use the **clear user group** and **clear mac-user group** commands in addition to the **clear usergroup** and **clear mac-usergroup** commands to explicitly remove individual users or MAC users from a group.

WSS Software allows ** to be specified as a MAC address wildcard, but this is invalid for MAC wildcards. (20060)

Description The ** value is valid for userwildcards, and matches on all usernames. However, ** is not a valid MAC address wildcard.

Workaround To match on all MAC addresses, specify * instead.

Radius server disappears from client access after downgrading from software release 5.0.9.3 to software release 4.1.x.

Description Using Radius passthru configuration a client running software release 5.0.9.3 is connected to a dot1x WLAN. If the client is downgraded to 4.1.x then the client is rejected for authentication failure.

Web-based AAA issues

IPv6 clients cannot authenticate using Web Portal. (26291)

Description The web-portal ACL does not work on IPv6 traffic. IPv6 clients will not be able to authenticate using Web Portal unless the clients also run IPv4.

Workaround This issue affects Web-Portal authentication only. The other authentication types (802.1X, MAC, and Last Resort) can be used with IPv6 clients.

Fast roaming non-aaa authorization should do additional checks. (27698)

Description The start-date, end-date, time-of-day, and session-timeout attributes, if configured for a user, are checked by the WSS where a client connects initially. For fast roaming (for example, VOIP phones, RSN PMK caching), these attributes are not checked on the roamed-to WSSs. The configured **dot1x reauth-period** is used to reauthorize all clients periodically at every WSS, roaming or not.

Location policy, if any, is checked by the WSS where a client connects initially. For fast roaming, location policy is not checked on the roamed-to WSSs. If the location policy of the first WSS configured ACLs or a VLAN for the user, those ACLs and VLAN will be applied in the roamed-to WSSs.

Encryption issues

Default 802.11i cipher suite is TKIP, not CCMP. (19342)

Description The 802.11i standard, in section 7.3.2.25.1, states that CCMP shall be the default cipher suite. However, the default cipher suite in WSS Software is TKIP.

Workaround If you need CCMP, select it when configuring encryption settings in a service profile.

ACL issues

ACE names that begin with CLI keywords are not supported. (17521)

Description When configuring an access control entry (ACE), if the name you specify for the ACE begins with a word that is also a keyword used by the CLI, the CLI rejects the ACE name. In the following examples, the ACE names that begin with *port* and *vlan* are rejected, but the ACE name that starts with *abc*, which is not a CLI keyword, is accepted:

2380# **set security acl ip port_abc deny 0.0.0.0 255.255.255.255**
error: Wrong ACL name input = port_abc
2380# **set security acl ip vlan_abc deny 0.0.0.0 255.255.255.255**
error: Wrong ACL name input = vlan_abc
2380# **set security acl ip abc_port deny 0.0.0.0 255.255.255.255**

Workaround Do not use a CLI keyword in the beginning of an ACE name.

SODA issues

While virtual desktop is active, reauthenticating Web Portal user cannot log in. (25754)

Description It is possible that even though the SODA agent has been downloaded and the virtual desktop started, the browser is redirected to the login page. This could happen if the session was re-established after the SODA agent was downloaded.

Workaround If this happens, exit out of the virtual desktop, open the browser, and authenticate again.

Remediation ACL is not applied to a client after roaming back to its native WSS. (26547)

Description In a configuration where two WSSs have the same SODA configuration and remediation ACL, the remediation ACL is applied to a client whose agent fails the host integrity check when the client logs on, and is applied by the other WSS when the client roams to it. However, the remediation ACL is not applied to the client when the client roams back to the first WSS. As a result, the client is able to access the network despite the host integrity check failure.

Session issues

The show session network wired command does not list wired authentication sessions. (17829)

Description If you use the **wired** option with the **show sessions network** command, no sessions are listed.

Workaround Use the **show sessions network** command, without the **wired** option. In this case, the wired authentication sessions are included in the output.

The Unicast bytes fields in show sessions network sessions-id output can show a negative number. (18174)

Attributes not present in "show sessions network verbose" command. (27698)

Description For fast-roaming stations, the output of the **show sessions network verbose** command displays the roaming history, but attributes such as VLAN name, mobility profile, and filter-id, although they are processed by the WSS when the station is authenticated, are not displayed.

Documentation errata

Preventing 802.11b clients from connecting to your network. (30741)

Description To prevent 802.11b clients from connecting to your network, enter the following command:

 # set service-profile *profile_name* **transmit-rates 11g mandatory 12**

Changes to syntax for "set dap boot" commands. (33021)

Description In the WSS Software manuals, the syntax for the **set dap boot-ip**, **set dap boot-switch**, and **set dap boot-vlan** commands is incorrect. The actual commands in WSS Software 5.0 are **set dap boot-configuration ip**, **set dap boot-configuration switch**, and **set dap boot-configuration vlan**.

Upgrading to WSS Software version 5.0

Before you upgrade, see "Version compatibility" (page 16). After you verify that the switch is running the minimum WSS Software version required to upgrade to WSS Software Version 5.0, return to this section.

Preparing the WSS for the upgrade

Caution! Create a backup of your WSS files before you upgrade the switch. Nortel recommends that you make a backup of the switch, before you install the upgrade. If an error occurs during the upgrade, you can restore your switch to its previous state.

If the switch is running WSS Software Version 4.0 or later, you can use the following command to back up the switch's files:

backup system [**tftp:/**/*ip-addr*/]*filename* [**all** | **critical**]

To restore a switch that has been backed up, use the following command:

restore system [**tftp:/**/*ip-addr*/]*filename* [**all** | **critical**] [**force**]

"Upgrade scenario" (page 39) shows an example use of the **backup** command. For more information about these commands, see the "Backing Up and Restoring the System" section in the "Managing System Files" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.

Note. If you have made configuration changes but have not saved the changes, use the **save config** command to save the changes, before you backup the switch.

If the switch is running an earlier version of WSS Software, use the **copy tftp** command to copy files from the switch onto a TFTP server.

Upgrading an individual switch using the CLI

1. Back up the switch, using the **backup system** command. (See "Preparing the WSS for the upgrade".)
2. Copy the new system image onto a TFTP server.

   For example, log in to http://www.nortel.com/support/ using a web browser on your TFTP server and download the image onto the server.
3. Copy the new system image file from the TFTP server into a boot partition in the switch's nonvolatile storage.

   You can copy the image file only into the boot partition that was *not* used for the most recent restart. For example, if the currently running image was booted from partition 0, you can copy the new image only into partition 1.
4. Set the boot partition to the one with the upgrade image for the next restart.

   To verify that the new image file is installed, type **show boot**.
5. Reboot the software.

   To restart a WSS and reboot the software, type the following command:

   reset system [**force**]

When you restart the WSS, the switch boots using the new WSS Software image. The switch also sends the AP version of the new boot image to APs and restarts the APs. After an AP restarts, it checks the version of the new AP boot image to make sure the boot image is newer than the boot image currently installed on the AP. If the boot image is newer, the AP completes installation of its new boot image by copying the boot image into the AP's flash memory, which takes about 30 seconds, then restarts again. The upgrade of the AP is complete after the second restart.

Upgrade scenario

To upgrade a 2360/2361 switch, type commands such as the following.

Note. This example copies the image file into boot partition 1. On your switch, copy the image file into the boot partition that *was not* used the last time the switch was restarted. For example, if the switch booted from boot partition 1, copy the new image into boot partition 0. To see boot partition information, type the **show boot** command.

2360/2361# **save config**
success: configuration saved.

2360/2361# **backup system tftp:/10.1.1.107/sysa_bak**
success: sent 28263 bytes in 0.324 seconds [87231 bytes/sec]

2360/2361# **copy tftp://10.1.1.107/NT504103.001 boot1:NT504103.001**
.....
.....
.....success: received 10266629 bytes in 92.427 seconds [111078 bytes/sec]

2360/2361# **set boot partition boot1**
success: Boot partition set to boot1:NT504103.001 (5.0.0.1).

2360/2361# **show boot**
Configured boot version: 5.0.0.1
Configured boot image: boot1:NT504104.001
Configured boot configuration: file:configuration
Backup boot configuration: file:backup.cfg
Booted version: 4.1.4.9
Booted image: boot1:NT504103.001
Booted configuration: file:configuration
Product model: WSS

2360/2361# **reset system force**
..... rebooting .....

Migrating your Web-based AAA and Last-Resort configurations from WSS Software version 4.*x* to WSS Software version 5.0

When you upgrade from 4.*x*, the Web-Portal and last-resort configuration is upgraded automatically. WSS Software makes the following configuration changes during upgrade.

The changes affect **web-portal-*ssid*** and **last-resort-*ssid*** users but they do not affect **web-portal-wired** or **last-resort-wired** users.

Web-Portal changes during upgrade

During upgrade, WSS Software automatically makes the following changes for each service profile whose fallthru type is set to **web-portal**.

- Copy the **vlan-name** attribute the **web-portal-*ssid*** user to the **vlan-name** attribute of the same SSID's service profile.
- Copy the **filter-id** *aclname*.**in** attribute from the **web-portal-*ssid*** user to the **web-portal-acl** option of the SSID's service profile.
- Delete the **web-portal-*ssid*** user from the configuration.

Last-Resort changes during upgrade

During upgrade, WSS Software automatically makes the following changes for each service profile whose fallthru type is set to **last-resort**.

- Copy the **vlan-name** attribute and all other user attributes set on the **last-resort-*ssid*** user to the **vlan-name** attribute and other attributes of the same SSID's service profile. If an attribute is already configured on the service profile, the value is changed to the last-resort value for the same attribute, if set.
- Delete the **last-resort-*ssid*** user from the configuration.
- Delete the **set authentication last-resort** command from the configuration.

Considerations when using Third-Party APs (30061)

If you are using a third-party AP for Web-Portal and last-resort authentication, a service profile must exist on the WSS that provides authentication attributes for clients. The name of the service profile must match the name of the SSID configured for the third-party AP.

If your 4.*x* configuration already had a service profile with the same name as the SSID of the third-party AP, then the upgrade does not require any additional action. If your 4.*x* configuration did not have a service profile with the same name as the SSID of the third-party AP, then you must create one and set the authentication attributes. In release 5.0, last-resort authentication is always *local*.

Although it is possible to create multiple service profiles for a given SSID, Nortel recommends that you have only one service profile with the SSID of the third party AP.

If you need to downgrade from 5.0.9 to a 4.x release, the configuration will work properly if it had worked properly in 5.0.9

WSS 2380 supported AP license activation key upgrade

A License Activation Key upgrade supports an additional 40 or 80 AP's up to the maximum of 120 AP's per WSS 2380. A License Certificate is used to provide a single software license and its associated License Activation Key. The number of supported Access Points beyond 40 for your Nortel WLAN WSS 2380 will depend on the upgrade License Activation Key that is installed and activated. To enable the additional support of Access Points, you must obtain a License Activation Key from Nortel.

To obtain the License Activation Key, follow the instructions on the License Certificate provided with the WSS 2380 supported AP License Upgrade Kit.

When the proper License Activation Key has been obtained, follow the instructions below to enable the WLAN WSS 2380 features:

1. Use the following command at the enable (configuration) level of the CLI to install the activation key:

   set license *activation-key*

2. Type in the entire activation key and press *enter*

   In the following example, an activation key for additional AP's is installed:

   2380# set license 3B02-D821-6C19-CE8B-F20E

   success: license accepted

3. Verify installation of the new license by typing the following command: **show license**

Support for the additional AP's begins immediately. The switch does **not** need to be restarted for the upgrade to be effective.

Note: Contact NETS (Nortel Enterprise Technical Support) for Replacement of License Activation Keys

Issues resolved in version 5.0.9.4

CPU on the WSS spiked to 100% usage at a certain time of the day. (33320)

Description The SSH CLI response became sluggish, and new sessions were difficult to establish causing the DAPs to reboot.

A core dump file caused by unknown reasons was located on a WSS. (32526)

Description Unspecified network events created a core dump file.

The auto blacklist counter in show rfdetect counters seems incorrect. (32510)

Description A configured blacklist client should not be counted for the automatic blacklist counter.

If a DNS query name is too long, it caused the WSS to stop functioning. (32418)

Description Two WSSs stopped functioning and user traffic ceased to flow when a DNS query name was used that had too many characters.

A WSS stopped functioning when the session was terminated due to a corrupted data structure. (32340)

Description The RADIUS server did not responding to access requests within the configured timeout period which triggers re-transmissions of requests. Or, the response (or responses) were received at the WSS after stations have moved to another AP or to another WSS.

The WSS sometimes reports that the CPU is idle more than 100% of the time. (32331)

Problems getting DAPs to boot in an L3 environment using option 43. (32231)

Description It appears that the comma character that designated the option 44 portion of the DHCP lease (ASCII character associated with 44 is the comma) caused the AP to interpret the option 44 data as continuing option 43 data. Since the format of the option 43 data now appeared to be invalid, the AP rejects the lease.

After configuring a DAP with a static IP number and then configuring it as a directly attached port, moving it back to a DAP port causes the DAP to become unresponsive. (31965)

Remediation ACL does not work if client's browser has proxy enabled. (26478)

Description A client whose browser has web proxy enabled was able to access the network despite failing the host integrity check.

The WSS produced a core file and restarted when a Web Portal session was cleared after the SODA agent was downloaded by the client. (28356)

When multiple ACLs were exercised at once, messages indicating an illegal memory access error appeared in the system log. (30943, 30560)

Invalid port or channel numbers reported from an AP resulted in a crash of the WSS. (31007)

Clearing an AP caused WSS Software to access an invalid memory location, resulting in a crash of the WSS. (31008)

Creating a policy in WMS caused AAA-related settings for a WSS to be overwritten. (31402)

An invalid access to a location in the EAP module caused the WSS to restart. (31808)

Enabling a DAP to use a WSS as its boot device caused the WSS to crash. (31993)

Corrupt packets generated by an AP caused the APs management software to crash. (32152)

An error message was displayed when attempting to read a value in the Nortel-AP-STATUS-MIB::nrtlApStatNumAps object. (32159)

APs deassociated from a WSS, at which time the WSS restarted and produced a core file. After the WSS restarted, it registered high CPU usage, and the APs could not associate with the WSS. (29110)

WSS crashed as a result of EAPOL deleting information cached by the RADIUS client to handle outstanding authentication requests. (29518)

The ID of the final EAP success message was incorrectly being incremented by 1 over the last EAP conversation. (29556)

2350 stays in boot loop following software upgrade. (29677)

Description After a new software image was loaded on an 2350, and the new image was set as the active boot partition, when the 2350 was restarted, it entered a loop in which it constantly rebooted. The boot prompt was not accessible while the 2350 was in this loop.

Authentication packets sent from the WSS's IP interface were being fragmented into segments larger than was allowable by remote routers. (29843)

When summertime was set to Eur-S, GMT was displayed as time zone. (30126)

Description Specifying a non-alphanumeric character (for example, a hyphen) as part of the time zone in the **set summertime** command was accepted by the CLI, but the time zone for the WSS was then set to GMT.

SNMP traps generated as a result of errors from a wireless client were reported as coming from "Radio 0", which is an invalid radio number for an AP. (30419)

The WSS crashed when accessing an invalid port number in the virtual port table. (30446)

WSSs created unicast "loop" when upgraded to 4.2. (30880)

Description A WSS that had been upgraded to a 4.2 release encountered a DHCP packet whose destination was not defined in its FDB. As a result, the WSS flooded the DHCP packet out all interfaces. When the DHCP packet reached another WSS also running a 4.2 release, it was similarly flooded out all interfaces. This caused a forwarding loop between the two WSSs.

Retrieving an invalid model name from an AP in a mobility domain was causing a WSS to crash and not reboot. (30928)

The WSS crashed when it encountered a packet with an invalid TAPA File Transfer packet type. (31154)

Description The WSS now logs an error message when this event occurs instead of restarting and producing a core file.

The WSS core dumps when an 802.1x client attempts to authenticate to a third-party AP. (33470)

Description The client associates and attempts to authenticate to a third-party AP. The WSS proxies the request to the RADIUS server. The RADIUS server sends an "Accept" message. The WSS core dumps and resets.

The following messages are displayed on the console. IP communication is completely lost (telnet, syslog) and you are unable to extract any debugs or traces from the WSS:

Example 1:

supervisor: 7526.894063 ERROR: process_sigchld: process netsys exited pid=823322 status=0x8b (0/139)

TELNET Oct 19 14:24:43.838097 ERROR TELNET_ERROR: can't accept the session, errno -3
supervisor: 7527.150328 ERROR: process_sigchld: process netsys. 823322 **core dumped**

Example 2:

No more recordssupervisor: 7899.107253 ERROR: process_sigchld: process netsys exited pid=913434 status=0x8b (0/139)

TELNET Oct 19 14:30:56.048672 ERROR TELNET_ERROR: can't accept the session, errno -3
supervisor: 7899.196630 ERROR: process_sigchld: process netsys. 913434 **core dumped**

WSS fails to recognize a broadcast deauthentication attack. Attached clients are deauthenticated by the attack. (28537)

AP will not reboot if it is changed from Directly Connected AP to DAP after booting. (32247)

Description If an AP was connected previously as Directly Connected and then reconnected as DAP it will not boot.

When "last-resort accounting" is configured using WMS it cannot be deleted using CLI. (33438)

Using CLI on the 2360 and executing the "show port mirror" command on port 8 of the switch does not show the settings. (33536)

DAPs could be disconnected from a WSS 2360, if the switch had been running at a very high bit rate >180Mbps for an extended period of time. (33643)

Workaround Reset the 2360

The command "set dap auto model (null) radiotype 11g" appears when executing the "set auto-dap" command using WMS. (33680)

Customized Web-based AAA pages from 4.0 and 4.1 configuration do not work properly in 5.0.9. (33708)

Description Customized Web-based AAA pages that worked in Release 4.0 and 4.1 no longer function in release 5.0.9. When enabled in 5.0.9 the client session is not captured and the client recieves an HTTP 404 error message in the browser.

Quality of Service (QoS) Tx/Rx counters do not work properly. Using the CLI command *show ap qos-stat* shows incorrect information. (33971)

WSS logs show excessive "Recv Seq Cntr Failures" log entries. (33977)

The end user is able to see more CLI test commands than are supported for use on the switch. (34022)

Description Executing the "test simulate" command can cause the WSS to crash.

Workaround Do not use the "test simulate <device> operations" command.

Issues resolved since version 4.1.13

Web View did not require a username. (16799)

Web View did not display more than 32 service profiles. (18374)

Web View allowed configuration of duplicate SSID names in the same service profile. (18375)

Layer 2 traffic restrictions did not affect client-to-client traffic on the remote switch of a tunneled VLAN. (21700, 27117)

WSS Software could serve a login unsuccessful page to a Web-Portal client who had successfully logged on. (22881)

A successfully authenticated Web-Portal client could be redirected to a seemingly random web page. (22886)

The WSS crashed periodically in configurations where AAA Accounting was enabled. (24325)

Putty versions older than 0.58 and Tera Term Pro version 3.1 each reported fatal errors when SSH connection to a WSS was attempted. (24833)

In a service profile with WEP enabled, if a client was encrypting packets with key index 1, and the WSS had the same value configured for key index 2 (not key index 1), then the WSS was decrypting packets from the client using key index 2 and passing them on to the wired network. (24913)

WSS Software upgrades that included an upgrade to the AP boot loader could take a long time. (25229)

On a 2360/2361, internal buffers were occasionally not being freed, causing sporadic packet loss. (25394)

AP error message appeared too frequently in system log. (26007)

Description Error messages such as the following could occur too frequently in the log for similar but distinct errors:

AP Jan 09 09:33:52.577041 ERROR SYSLOG_DUP: last message repeated 1 time.
AP Jan 09 09:33:52.559474 ERROR DAP 80 ap_network: ip_fragment: fail, do clean up

Description In the current version, different messages are displayed depending on the error.

Distributed APs could restart around every two hours after running normally for 3 to 7 days. (26027)

VLAN ports on port group between WSS and Cisco device could be marked down on Cisco device even though the ports were up. (26047)

The Auto Tune function was setting the channel and power settings for an AP radio to values that were not permissible for the US country code (26146)

Invalid OID BER encoding packet sent to switch caused SNMP process to lockup, requiring a switch restart to restart SNMP. (26173)

RADIUS accounting could not be used for billing Web-Portal sessions. (26175)

Receiving an EAP packet 1750 bytes long or longer cause aWSS to restart. (26597)

CLI did not clearly indicate that STP was disabled on a port. (26668)

Corrupted EAP packet from a client could cause a WSS to restart. (26744)

Reconfiguring a wired authentication port as a network port in a tagged VLAN causes the switch to restart if the port is enabled. (27164)

> **Description** If you reconfigured a port from a wired authentication port to a network port in a tagged VLAN, without disabling the port before adding it the VLAN, the switch restarted.

Latency of 1 to 2 seconds occurred when a Vocera badge roamed, if the filter-id attribute was set for the badge (last-resort user). (27330)

An AP directly connected to a WSS on both the AP's Ethernet ports restarted if it received an ARP request on both ports. (27531)

Some PDA devices did not work with WPA using the Windows Mobile 5.0 supplicant. (27570)

Static WEP decryption errors were encountered on a WSS, apparently leading to loss of connectivity for some clients. (27593)

On a 2380, an ACL applied to the outbound direction of a virtual port (port plus tag value) did not take effect. (27656)

Distributed APs converted from Auto-DAPs into statically configured APs were always assigned to the default radio profile, even if another profile had been selected for them. (27692)

Empty identity response from a client could case a WSS to restart. (27999)

Transmission PM value was incorrectly set following CCMP keying. (28018)

Starting a Zebra wireless 802.11 printer could cause a WSS to restart. (28080)

SpectraLink handsets configured with static IP addresses took a long time to connect to a WPA2 SSID. (28268)

Intel 3945ABG wireless NICs could not connect to Nortel radios, or could not use the network once connected. (28863)