Part No. 320659-A
September 2005

4655 Great America Parkway
Santa Clara, CA 95054

Nortel WLAN Security Switch 2300 Series Release Notes

Release 4.0.10

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

This chapter contains the following sections:

Getting Started

Nortel recommends that you familiarize yourself with "Best Practices and Common Issues" on page 35 in this document before installing WLAN Security Switch 2300 Series (Software) Version 4.0.(or variation)

For additional product information, refer to the following manuals in addition to these release notes:

- Nortel WLAN Security Switch 2300 Series Quick Installation Guide
- Nortel WLAN Security Switch 2300 Series Installation and Basic Configuration Guide
- Nortel WLAN Access Point 2330 Installation Guide
- Nortel WLAN 2300 Series Regulatory Information
- Nortel WLAN Security Switch 2300 Series Configuration Guide
- Nortel WLAN Security Switch 2300 Series Command Line Reference
- Nortel WLAN Management Software 2300 Series User Guide
- Nortel WLAN Management Software 2300 Series Reference Guide

What's New in WSS Software Version 4.0

WSS Software Version 4.0 contains the following enhancements:

Web Quick Start Wizard (2350 and 2360 Only)

WSS Software Version 4.0 simplifies configuration of new, unconfigured 2350 and 2360 switches with a web-based quick start wizard application. You can use the Web Quick Start Wizard to configure the switch to provide wireless access to up to ten network users.

To access the Web Quick Start Wizard, attach a PC directly to port 1 or port 2 on the switch and use a web browser on the PC to access IP address 192.168.100.1. (For more detailed instructions, see the Nortel *WLAN Security Switch 2300 Series Quick Installation Guide*.)

Note: The Web Quick Start Wizard application is different from Web View. Web View is a web-based management application that is available at any time on a switch that already has IP connectivity. (Web View access also requires the switch's HTTPS server to be enabled.) The Web Quick Start Wizard application is accessible only on unconfigured switches.

Note: The Web Quick Start Wizard application is supported only on switch models 2350 and 2360. After you finish the Web Quick Start Wizard, it will not be available again unless you clear (erase) the switch's configuration.

WSS 2350 Remote Auto Configuration

WSS Software Version 4.0 enables WSSs to be configured remotely by a WLAN Management Software server. The following remote configuration scenarios are supported:

- Drop ship—A WLAN Management Software server in the corporate network can configure a 2350 switch shipped directly to a remote office. This option does not require any preconfiguration of the switch.
- Staged—You can stage any model of switch by preconfiguring IP connectivity and enabling "auto-config", then sending the switch to the remote office. The switch uses the WLAN Management Software server in the corporate network to complete its configuration.

The drop ship option is supported only for the 2350. The staged option is supported for all switch models. Both options require a WLAN Management Software server. If you know a switch's serial number, you can create a complete configuration for the switch in WLAN Management Software. When the switch requests its configuration from WLAN Management Software, WLAN Management Software sends the configuration for that serial number. If you do not know the switch's serial number, you can upload the partially configured switch into WLAN Management Software, finish its configuration, then deploy the completed configuration back to the switch.

(For more information, see the *Nortel WLAN Security Switch 2300 Series Installation and Basic Configuration Guide*.)

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

Upgrading from WSS Software Version 4.0

Preparing the WSS for the Upgrade

Caution! Save the configuration, then 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. Also, if you later decide to downgrade the switch, commands that have new syntax in WSS Software Version 4.x.x might not be converted correctly.

Use the following command to save the configuration. Unsaved changes will be lost during the upgrade procedure.

save config [*filename***]**

If the switch is running WSS Software Version 4.0 or later, you can use the following command to backup the system 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" on page 13 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.

Upgrading an Individual Switch Using the CLI

1. Save the configuration, using the **save config** command.
2. Back up the switch, using the **backup system** command.
3. 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.
4. 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.

5. 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**.

6. 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 2380 switch from WSS Software Version 4.0 or later, type commands such as the following.

2380# **save config**

success: configuration saved.

2380# **backup system tftp:/10.1.1.107/sysa_bak**

success: sent 28263 bytes in 0.324 seconds [87231 bytes/sec]

2380# **copy tftp://10.1.1.107/WSS040007.020 boot1:WSS040007.020**

success: received 8586 bytes in 4.06 seconds [2112 bytes/sec]

2380# **set boot partition boot1**

success: Boot partition set to boot1.

2380# **show boot**

Configured boot image: boot1:WSS040007.020
Configured boot configuration: file:configuration
Booted version: 4.0
Booted image: boot0:WSS040202.020
Booted configuration: file:configuration
Product model: 2380

2380# **reset system**

..... rebooting .....

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.

2350 WSS support for RFC 2131 and RFC 2132

The WSS Software DHCP client enables a WSS to obtain its IP configuration from a DHCP server. A switch can use the DHCP client to obtain the following configuration information:

- IP address
- Default gateway
- DNS domain name
- DNS server IP address

The DHCP client is implemented according to "RFC 2131: Dynamic Host Configuration Protocol" and "RFC 2132: DHCP Options and BOOTP Vendor Extensions".

The DHCP client is enabled by default on an unconfigured 2350 when the factory reset switch is pressed and held during power on. The DHCP client is disabled by default on all other switch models, and is disabled on a 2350 if the switch is already configured or the factory reset switch is not pressed and held during power on. You can enable the DHCP client on one VLAN only.

(For more information, see the "Adding an IP Interface" section in the "Configuring and Managing IP Interfaces and Services" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Automatic Configuration of Distributed APs

WSS Software Version 4.0 simplifies deployment of Distributed APs by allowing you to use a configuration template to configure them. A Distributed AP that does not have a configuration on a WSS can receive its configuration from the template instead.

The template assigns a Distributed AP number and name to the AP, from among the unused valid AP numbers available on the switch. The template also configures the AP with the AP and radio parameter settings in the template. The AP and radio parameter settings in the template are configurable. A WSS can have one template.

(For more information, see the “Configuring a Template for Automatic AP Configuration” section in the “Configuring AP Access Points” chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Third-Party Access Point (AP) Support with User Authentication

WSS Software Version 4.0 enables a WSS to provide network access for users associated with a third-party AP that has authenticated the users with RADIUS. You can connect a third-party AP to a WSS and configure the WSS to provide authorization for clients who authenticate and access the network through the AP.

(For more information, see the “Configuring AAA for Users of Third-Party APs” section in the “Configuring AAA for Network Users” chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Support for a third party APs requires certain features and capabilities to be present in the AP. With many APs on the market having varying feature sets ranging from basic capabilities to advanced capabilities, support for third party APs is broken into two main categories. See Table 1

Level 1 support requires a minimal feature set from a third party AP. The goal is to pull WLAN clients into the Web Based-AAA architecture of the WSS 2300 by authenticating them through fallback methods (last resort, MAC authentication, and web portal), and allowing them to roam freely between 2330 APs and third party APs. If multiple SSIDs are implemented, the WSS 2300 needs the AP to segregate those SSIDs into separate tagged VLANs so that a mapping from VLAN back to SSID can be established on the WSS 2300. So the main feature requirement for Level 1 support is that the AP must be able to map SSIDs to VLANs. Note that some of the APs in the chart only support one SSID in which case the requirement is relaxed to allow the AP to not tag at all on the link between AP and WSS 2300. In theory, most APs would probably qualify for Level 1 support, including most legacy APs, but the list below represents what Nortel has tested and certified as "compatible".

Level 2 support includes all the requirements of Level 1 but further integrates advanced authentication options, such as 802.1x, between third party AP and WSS 2300. As with Level 1 the goal is to tie everything back into the Web Based-AAA structure of the WSS 2300, thus the WSS 2300 inserts itself into the RADIUS communication by acting as a RADIUS proxy to the third party AP. Because of this, Level 2 support requires compliance to RFC 3580 for formatting the called station ID (SSID is included in the field). Since few APs on the market implement this properly, the list of compatible Level 2 APs is short.

The APs listed in the Level 1 column have passed testing for roaming, for the "un-authenticated" authentication types, such as last resort, MAC authentication, and web portal, and other basic capabilities in conjunction with the WSS 2300. The APs listed in the Level 2 column have passed more rigorous testing which includes all Level 1 tests plus use of 802.1x authentication methods.

Table 1: 3rd Party AP Support Matrix

	Level 1	Level 2	PoE Compatibility
*Nortel 2220	Yes	No	ERS5520, ERS460, WSS2300
**Nortel 2270/2230	Not Supported	Not Supported	ERS5520, ERS460, WSS 2300
Symbol 4131	Yes	No	No
°Symbol 4121	Yes	No	No
Cisco 1200	Yes	Yes	ERS5520 only
Cisco 1100/ 350	Yes	Yes	Not Tested
Proxim 2000/ 4000	Yes	Yes	Not Tested

°Symbol 4121 only supports a single SSID and no VLAN tagging.

*Nortel 2220 supports up to two SSIDs and limited VLAN tagging capabilities. For support as a third party AP, only one SSID should be implemented with VLAN tagging as an optional feature.

**Nortel 2270/2230 passed both Level 1 and Level 2 testing but due to some restrictions and a number of additional implementation caveats, it is not officially supported as a third party AP.

Control Traffic Security

WSS Software Version 4.0 provides security for management traffic between WSSs and Distributed APs. For Distributed APs that support this feature, all management traffic between the AP and the WSS is encrypted.

The encryption uses RSA as the public key cryptosystem, with AES-CCM for data encryption and integrity checking and HMAC-MD5 for keyed hashing and message authentication during the key exchange. Bulk data protection is provided by AES in CCM mode (AES CTR for encryption and AES-CBC-MAC for data integrity). A 64-bit Message Authentication Code is used for data integrity.

(For more information, see the “Configuring AP-WSS Security” section in the “Configuring AP Access Points” chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Terse Option for show ap status and show dap status Commands

The **show ap status** and **show dap status** commands are enhanced in WSS Software Version 4.0. The commands now have a **terse** option. You can use the **terse** option to display a brief line of essential status information for each directly connected AP or Distributed AP.

The **show dap status** command also has another new option. You can specify **all** to display information for all APs (directly connected APs and Distributed APs). The **all** option is already supported with the **show ap status** command in previous WSS Software releases.

Here is the new syntax for these commands:

show ap status [**terse**] | [*port-list* | **all** [**radio** {**1** | **2**}]]

show dap status [**terse**] | [*dap-num* | **all** [**radio** {**1** | **2**}]]

Support for More than Eight Service Profiles that Use Static WEP

In WSS Software Version 3.x, a radio profile could not be mapped to more than eight service profiles that use static WEP. In WSS Software Version 4.0, this restriction is removed.

Rogue Detection Enhancements

WSS Software Version 4.0 contains many rogue detection enhancements, as well as changes to rogue detection features available in 3.*x*. Table 2 lists the rogue detection features in WSS Software Version 4.0.

Table 2: Rogue Detection Features in WSS Software Version 4.0

Rogue Detection Feature	Description	Applies To	
		Third-Party APs	Clients
Classification	WSS Software can classify third-party APs as rogues or interfering devices. A rogue is a third-party AP whose MAC address WSS Software knows. An interfering device does not have a MAC address known to WSS Software. WSS Software can detect rogue clients, locate their APs, and issue countermeasures against the APs.	Yes	Yes
Permitted vendor list	List of Organizationally Unique Identifiers (OUIs) to allow on the network. An OUI is the first three octets of a MAC address and uniquely identifies an AP's or client's vendor.	Yes	No
Permitted SSID list	List of SSIDs allowed on the network. WSS Software can issue countermeasures against third-party APs sending traffic for an SSID that is not on the list.	Yes	No
Client black list	List of client MAC addresses that are not allowed on the wireless network. WSS Software drops all packets from these clients.	No	Yes

Table 2: Rogue Detection Features in WSS Software Version 4.0 (continued)

Rogue Detection Feature	Description	Applies To	
		Third-Party APs	Clients
Attack list	List of AP MAC addresses to attack. WSS Software can issue countermeasures against these APs whenever they are detected on the network.	Yes	No
Ignore list	List of MAC addresses to ignore during RF detection. WSS Software does not classify devices on this list as rogues or interfering devices, and does not issue countermeasures against them. Note: In WSS Software Version 4.0, an ignore list can be configured on any switch in the Mobility Domain and applies only to that switch.	Yes	Yes
Countermeasures	Packets sent by Nortel APs to interfere with the operation of a rogue. In WSS Software Version 4.0, they are configurable on a radio profile basis instead.	Yes	Yes
Active scan	Active scan sends probe any requests (probes with a null SSID name) to look for rogue APs. The feature is configurable on a radio profile basis instead.	Yes	No
Nortel AP signature	Value in an AP's management frames that identifies the AP to WSS Software. AP signatures help prevent spoofing of the AP MAC address.	No	No
Show commands	WSS Software Version 4.0 has new **show rfdetect** commands and enhancements to the **show rfdetect** commands	Where applicable	Where applicable

Table 2: Rogue Detection Features in WSS Software Version 4.0 (continued)

Rogue Detection Feature	Description	Applies To	
		Third-Party APs	Clients
Log messages and traps	Messages and traps for rogue activity	Yes	Yes

Wireless Intrusion Detection System (IDS) and Denial of Service (DoS) Alerts

WSS Software Version 4.0 also can detect illegitimate network access attempts and attempts to disrupt network service. In response, WSS Software generates messages and SNMP traps (also called notifications).

Automatic Channel Retuning in the Presence of Dynamic Frequency Selection (DFS) or Radar

If an AP radio detects radar on a channel, WSS Software switches to another channel and does not attempt to use the channel where the radar was detected for 30 minutes. WSS Software also generates a message.

Note: The RF Auto-tuning feature must be enabled. Otherwise WSS Software cannot change the channel.

(For more information about all these features, see the "Rogue Detection and Countermeasures" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Portal Web-based AAA

Portal Web-based AAA is an enhanced version of Web-based AAA that provides accelerated login for users. Portal Web-based AAA provides faster login by immediately placing the user in their VLAN, instead of placing the user in a temporary VLAN during authentication and authorization.

In WSS Software Version 3.*x*, Web-based AAA placed the user in a temporary VLAN and issued a temporary IP address, while authenticating and authorizing the user. After authorization, WSS Software moved the user to the VLAN specified by the authorization attributes associated with the user. After moving to the new VLAN, the user obtained a new IP address from a DCHP server in the user's VLAN.

Portal Web-based AAA simplifies Web-based AAA operation and enhances its usability by immediately placing the user in their VLAN. This enables the user to obtain an IP address from their subnet and keep that address after authentication and authorization are complete.

Wi-Fi Multimedia (WMM) Support

WSS Software Version 4.0 supports Wi-Fi Multimedia (WMM). WMM provides wireless Quality of Service for time-sensitive applications such as voice and video. WMM is a pre-standard version of IEEE 802.11e, provided by the Wi-Fi Alliance to enable vendors to provide interoperable multimedia support before ratification of the standard.

WMM maps priority information between wired and wireless packets, so that high priority traffic receives end-to-end high priority treatment through the network.

WMM is enabled by default and does not require any configuration. You can disable the feature on individual radio profiles.

Compatibility with Legacy VoIP

WSS Software can support non-WMM VoIP devices and WMM VoIP devices at the same time. However, to provide priority service to non-WMM VoIP traffic, you must configure an ACL to set the CoS for the traffic. The AP maps this CoS value to a forwarding queue.

- If you plan to leave WMM enabled, use an ACL to set the CoS for any type of non-WMM VoIP wireless traffic to 6 or 7.
- If you plan to disable WMM, set the CoS for SVP traffic to 6 or 7, but set the CoS for other types of non-WMM VoIP traffic to 4 or 5. When WMM is disabled, the AP forwarding queue that maps to CoS values 6 and 7 is optimized for SVP.

Note: If you are upgrading a switch that uses ACLs to map VoIP traffic to CoS 4 or 5, and you plan to leave WMM enabled, Nortel recommends that you change the ACLs to map the traffic to CoS 6 or 7.

You must map the ACL to the outbound traffic direction on an AP port, Distributed AP, or user VLAN. An ACL can set a packet's CoS only in these cases.

(For more information about WMM, see the "Wi-Fi Multimedia" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

SNMPv2c and SNMPv3 Support

WSS Software Version 4.0 adds support for SNMP version 2c (SNMPv2c) and SNMP version 3 (SNMPv3). The WSS Software SNMP engine (also called the SNMP *server* or *agent*) can run any combination of the following SNMP versions:

- SNMPv1—SNMPv1 is the simplest and least secure SNMP version. Community strings are used for authentication. Communications are in the clear (not encrypted). Notifications are traps, which are not acknowledged by the notification target (also called a *trap receiver*).
- SNMPv2c—SNMPv2 is similar to SNMPv1, but supports informs. An inform is a notification that is acknowledged by the notification target.

- SNMPv3—SNMPv3 adds authentication and encryption options. Instead of community strings, SNMPv3 supports user security model (USM) users, with individually configurable access levels, authentication options, and encryption options.

All SNMP versions are disabled by default.

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

Nortel Management Information Base (MIB) Enhancements

The Nortel MIB contains new SNMP notifications (also called *traps*) to support the new rogue detection, IDS, and DoS protection features:

- RFDetectClientViaRogueWiredAPTraps—Generated when WSS Software detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP.
- RFDetectDoSPortTraps—Generated when WSS Software detects an associate request flood, reassociate request flood, or disassociate request flood.
- RFDetectDoSTraps—Generated when WSS Software detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood.
- RFDetectInterferingRogueAPTraps—Generated when an interfering device is detected.
- RFDetectInterferingRogueDisappearTraps—Generated when an interfering device is no longer detected.
- RFDetectSpoofedMacAPTraps—Generated when WSS Software detects a wireless packet with the source MAC address of a Nortel AP, but without the spoofed AP's signature (fingerprint).
- RFDetectSpoofedSsidAPTraps—Generated when WSS Software detects beacon frames for a valid SSID, but sent by a rogue AP.
- RFDetectUnAuthorizedAPTraps—Generated when WSS Software detects the MAC address of an AP that is on the attack list.
- RFDetectUnAuthorizedOuiTraps—Generated when a wireless device that is not on the list of permitted vendors is detected.
- RFDetectUnAuthorizedSsidTraps—Generated when an SSID that is not on the permitted SSID list is detected.

WSS Software Version 4.0 also has a new trap to indicate when a Distributed AP whose fingerprint has not been configured in WSS Software establishes a management session with the switch. This trap's name is DAPConnectWarningTraps.

(For more information about the IDS/DoS notifications, see the "IDS and DoS Alerts" section in the "Rogue Detection and Countermeasures" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*. For information about the AP fingerprint notification, see the "Configuring AP-WSS Security" section in the "Configuring AP Access Points" chapter of the same guide.)

All notifications are disabled by default. To enable notifications, edit the *default* notification profile or create a new one, and change the action from drop to send for individual notifications, or for all notifications. (See the "Configuring SNMP" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

Remote Traffic Monitoring

Remote traffic monitoring enables you to snoop wireless traffic, by using a Distributed AP as a sniffing device. The AP copies the sniffed 802.11 packets and sends the copies to an observer, which is typically a protocol analyzer such as Ethereal or Tethereal.

(For more information, see the "Remotely Monitoring Traffic" section in the "Troubleshooting a WSS" appendix of the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.)

DHCP Server

WSS Software Version 4.0 has a DHCP server that the switch uses to allocate IP addresses to the following:

- Directly connected APs
- Host connected to a new (unconfigured) 2350 or 2360, to configure the switch using the Web Quick Start

DHCP service for these items is enabled by default.

Optionally, you can configure the DHCP server to also provide IP addresses to Distributed APs and to clients.

Note: Use of the WSS Software DHCP server to allocate client addresses is intended for temporary, demonstration deployments and not for production networks. Nortel recommends that you do not use the WSS Software DHCP server to allocate client addresses in a production network.

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

Version Compatibility

This version of WLAN Security Switch 2300 Series (WSS Software) is intended for use with WLAN Management Software (WMS)Version 4.0 only.

Nortel WLAN 2300 Series Configuration and Deployment Guide for using Nortel Spectralink Handsets

SpectraLink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between WLAN Handsets 221x and WLAN infrastructure products. The products listed below have been thoroughly tested in SpectraLink's lab and have passed VIEW Certification. This document details how to configure the Nortel WLAN Security Switch and 2330 AP access point with WLAN Handsets 221x.

Certified Product Summary

Manufacturer	Nortel: www.nortel.com	
Approved products	WLAN Security Switches	Access Points
	2350 2360† 2380	2330†
RF technology	802.11b/g	
Radio	2.4 – 2.484 GHz	
Security	WPA-PSK and WPA2-PSK	
Security Switch/AP software version tested	Release_4_0_3	
WLAN Handsets 221x software version tested	Version 97.060 This is the Nortel version of “NetLink 2.0”	
Maximum telephone calls per AP	10	
Recommended network topology	Switched Ethernet (required)	

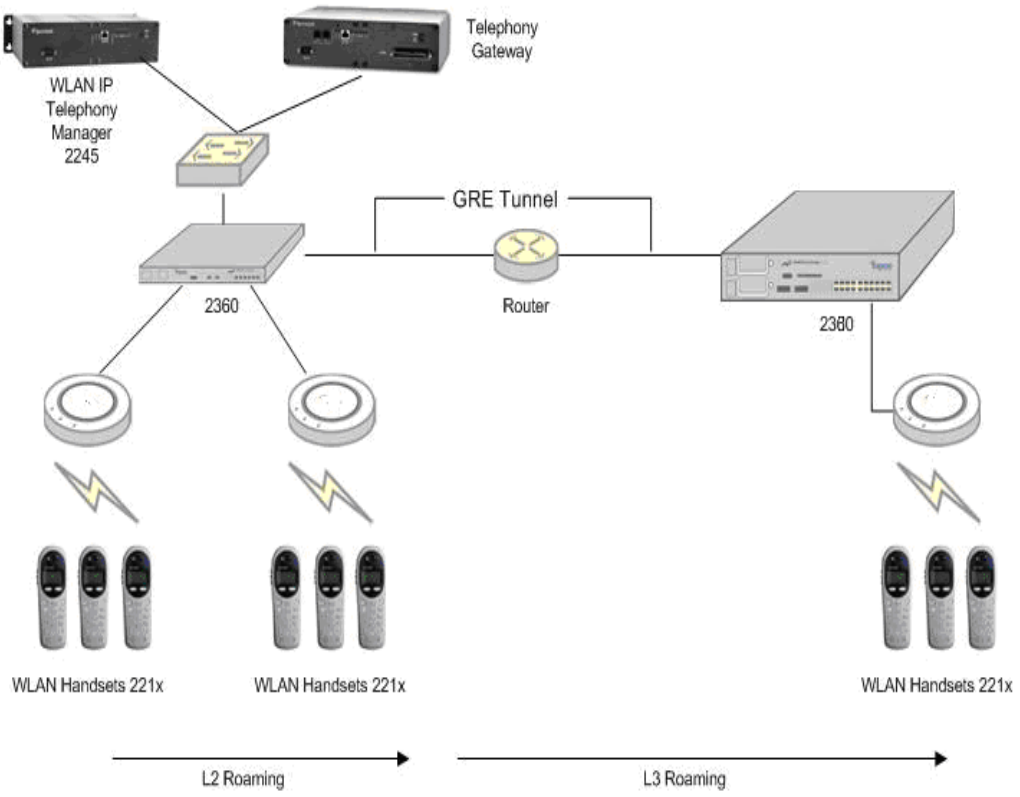
† Denotes products directly used in Certification Testing

Network Topology

The following topology was tested during VIEW Certification. It is important to note that these do not necessarily represent all "certified" configurations.

Both layer 2 and layer 3 roaming were tested. Layer 3 roaming of WLAN Handsets 221x requires the use of a tunnel. See Figure 1 on page 26

Figure 1: Network Topology



Known Limitations

During VIEW Certification testing, the following limitations were discovered.

1. You cannot have WPA and WPA2 configured on handsets simultaneously within the same ESSID. The phones will not check-in.
2. RF Active Scan must be disabled on AP radios that are providing voice services, including WLAN Handsets 221x.

Access Point Setup and Configuration

Installing Software

Nortel WLAN Security Switch firmware cannot be downloaded from the SpectraLink website, therefore, you must use the software that was shipped with your product, or contact Nortel for the latest software release.

Configuring the WLAN Security Switch

1. Using a standard RS-232 cable, connect the WLAN Security Switch to the serial port of a terminal or PC.
2. Run a terminal emulation program (such as HyperTerminal™) or use a VT-100 terminal with the following configuration:
   Bits per second: 9600
   Data bits: 8
   Parity: None
   Stop bits: 1
   Flow control: None.
3. Press Enter three times to display the WLAN Security Switch login screen, and to get past the "User-name:" prompt and the "Password:" prompt. There are no default usernames and passwords.
4. Enter "enable" to enter privileged mode. There is no default password.

Service Profile Commands (SSID and Security Policy Setup)

WPA2-PSK

Assume you are creating service profile "vowlan-wpa2" to define the ESSID "phones", as well as a WPA2-PSK security policy. The following commands are needed to setup the service for 2330 access points:

```
set service-profile vowlan-wpa2 ssid-name phones
set service-profile vowlan-wpa2 wpa-ie disable
set service-profile vowlan-wpa2 rsn-ie enable
set service-profile vowlan-wpa2 cipher-tkip disable
set service-profile vowlan-wpa2 cipher-ccmp enable
set service-profile vowlan-wpa2 auth-dot1x disable
set service-profile vowlan-wpa2 auth-psk enable
```

set service-profile vowlan-wpa2 psk-raw <256-bit passkey>

WPA-PSK

Assume you are creating service profile "vowlan-wpa" to define the ESSID "phones", as well as a WPA-PSK security policy. The following commands are needed to setup the service for 2330 access points:

```
set service-profile vowlan-wpa ssid-name phones
set service-profile vowlan-wpa wpa-ie enable
set service-profile vowlan-wpa rsn-ie disable
set service-profile vowlan-wpa cipher-tkip enable
set service-profile vowlan-wpa cipher-ccmp disable
set service-profile vowlan-wpa auth-dot1x disable
set service-profile vowlan-wpa auth-psk enable
set service-profile vowlan-wpa psk-raw <256-bit passkey>
```

Radio Profile Commands

Assume you are creating radio profile "voice" for all radios that will be providing voice services. The following commands are needed to setup the radio profile for the access points:

```
set radio-profile voice service-profile vowlan-wpa2   # maps the service profile to the radio profile
set radio-profile voice dtim-interval 3
set radio-profile voice active-scan disable     # prevents the AP from going off-channel to scan
set radio-profile voice wmm disable      # wmm must be disabled for SVP to be supported
```

Network Topology and 2330 Access Point Hardware Configuration

The network topology and access point hardware configuration can be configured using the WLAN 2300 Series Management Software. Please refer to the Nortel WLAN 2300 Series documentation for more information. Some useful commands are:

To create VLAN "v1" and add port 3 as a member of "v1":

```
set vlan 2 name v1 port 3    # 2 is the VLAN ID (must be unique for every VLAN on the switch)
```

To create a configuration for a model 2330 access point that is directly attached to port 1 of an WLAN Security Switch:

```
set port type ap 1 model mp-2330 poe enable
```

Radio Configuration

During VIEW Certification, 2330 access points were tested directly connected to a port on the WLAN Security Switch (e.g. port 1), then the following commands will configure a specific access point's radio to support the voice service:

```
set ap 1 radio 1 mode disable    #if the radio is currently enabled. Radio 1 is the 802.11b/g radio
set ap 1 radio 1 radio-profile voice mode enable  #maps radio to the radio-profile and enables it
```

2330 access points that are not directly connected to a port on the WLAN Security Switch, which Nortel calls a distributed access point (DAP), were not tested. If they are desired, the radio is configured with this command:
set dap 1 radio 1 mode disable #if the radio is currently enabled. Radio 1 is the 802.11b/g radio
set dap 1 radio 1 radio-profile voice mode enable #maps radio to the radio-profile and enables it

Authentication, VLAN and SVP Configuration

Assume you want the voice traffic to run on VLAN "v1". To specify that the "phones" SSID be trivially authenticated and placed on VLAN "v1", type the following commands:

set authentication last-resort ssid phones local
set user last-resort-phones attr vlan-name v1

The following commands are needed to enable SpectraLink Voice Priority via access control list (ACL) "SVP":

This rule places all IP protocol 119 (SVP) traffic on CoS queue 7 (SVP support):
set security acl ip SVP permit cos 7 119 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255

(Optional) This rule permits all other data traffic. Do not use if the VLAN "v1" is dedicated to voice services. Note: There is an implicit "deny all" rule at the end of the ACL.

set security acl ip SVP permit 0.0.0.0 255.255.255.255
set security acl map SVP vlan v1 out #Maps the ACL to VLAN v1 for outbound traffic
commit security acl SVP #activates the ACL
Be sure to disable IGMP snooping on VLAN "v1" by using the command:
set igmp disable vlan v1

Subnet Roaming Configuration between multiple WLAN Security Switches

To set up subnet roaming between two switches, a mobility domain must be configured on both switches. Choose one of the switches to be the "seed" switch. Note: The IP addresses used in mobility domain configuration must use the System IP address of each switch).

The following commands are performed on the seed WLAN Security Switch:
set system ip-address 1.1.1.1
set mobility-domain mode seed domain-name <domain name>
set mobility-domain member 1.1.3.1#configures the domain member
The following commands are performed on the other (member) WLAN Security Switch:
set system ip-address 1.1.3.1
set mobility-domain mode member seed-ip 1.1.1.1

If you have a previous mobility-domain configuration that is no longer valid, you must clear the existing mobility-domain before a new one can be defined.
clear mobility-domain # system will respond success: change accepted.
show mobility-domain config# system will respond "There is no mobility domain configuration"
To check the mobility domain, use the following command:
show mobility-domain
The system will respond:
Mobility Domain name: default
Member State
1.1.13.1 STATE_UP SEED
1.1.3.1 STATE_UP MEMBER

Checking the Configuration

Once the switch is configured, issue the following command at the command prompt to check the SVP settings:

sh ap qos-stats

The following information should be displayed (repeat the command to see changes):

CoSQueueTx

==========

```
   port: 1  radio:1
1,2   Background    0
0,3   BestEffort    604
4,5   Video         0
6,7   Voice         79106    #voice should have the most traffic
port: 1  radio: 2
1,2   Background    0
0,3   BestEffort    0
4,5   Video         0
6,7   Voice         0
```

The switch and AP are now ready for use with the WLAN Handsets 221x.

The network topology and other functions can also be configured using the WLAN 2300 Series Management Software. Please refer to the Nortel WLAN 2300 Series documentation for more information.

If you encounter difficulties or have questions regarding the configuration process of the Nortel WLAN 2300 Series, please contact Nortel by calling Nortel Technical Support.

Access Point Capacity and Positioning

Each site is unique in its AP requirements. Therefore, please take the following points into account when determining how many APs are needed and where they should be placed in the facility:

- Handset range: There must be wireless LAN coverage wherever the WLAN Handsets 221x will be used. Adequate coverage for a WLAN Handsets 221x can be determined by using the Site Survey mode on the Handset that displays dB levels and channel when the phones are in range of an access point (within approximately a -60dBM signal strength radius). Alternatively, you can make use of the planning capabilities built into WLAN Management Software 2300 Series to perform a virtual site survey for voice services.
- Number of Wireless Telephone calls per AP: The number of WLAN Handsets that can be in call simultaneously was determined based on call quality within a lab environment. Since call quality is impacted by packet retry rate and missed packets, test criteria was established for the maximum data rate (11Mb/s) for phones in range of the AP.
- As the WLAN Handsets move near the limits of optimal RF coverage from the AP, they will automatically drop to lower Mb/s operation. WLAN Handsets 221x require approximately 15% of the available bandwidth per call for 1 Mb/s operation, approximately 10% of the available bandwidth per call for 2 Mb/s operation, approximately 7% of the available bandwidth for 5.5 Mb/s operation, and 5% of available bandwidth for 11 Mb/s operations.

- LAN Bandwidth: Estimate anticipated peak call volume to ensure that the LAN has enough bandwidth to handle the network traffic generated by all of the wireless devices.
- WLAN Bandwidth: The WLAN Handsets 221x share bandwidth with other wireless devices. To ensure adequate RF bandwidth availability, consider the number of wireless data devices in use per AP when estimating the necessary number of devices.

Configuration File (For Reference Only)

The following configuration file was used during VIEW Certification testing. The configuration below includes all configuration attributes, including defaults. Use the command "show configuration all" for this detailed version. To only see non-default configuration values, use the command "show configuration".

#General Configuration

```
set ip dns domain (my network).com
set ip dns enable
set log console enable severity error
set log session disable severity info
set log buffer enable severity error
set log trace enable severity debug mbytes 1
set web-aaa enable
set dot1x timeout supplicant 30
set dot1x timeout auth-server 30
set dot1x quiet-period 0
set dot1x reauth-max 2
set dot1x tx-period 5
set dot1x reauth-period 3600
set dot1x max-req 2
set dot1x key-tx enable
set dot1x reauth enable
set dot1x authcontrol enable
set dot1x wep-key-period 1800
set dot1x wep-rekey enable
set dot1x bonded-period 0
set prompt
set system ip-address x.x.x.x
set system countrycode US
set auto-config disable
```

#Security Profile

```
set service-profile VoWLAN-WPA ssid-name <SSID name>
set service-profile VoWLAN-WPA shared-key-auth disable
set service-profile VoWLAN-WPA wep active-unicast-index 1
set service-profile VoWLAN-WPA wep active-multicast-index 1
set service-profile VoWLAN-WPA wpa-ie disable
set service-profile VoWLAN-WPA rsn-ie enable
set service-profile VoWLAN-WPA cipher-tkip enable#for WPA this should be disabled
set service-profile VoWLAN-WPA cipher-ccmp enable     #for WPA this should be enabled
set service-profile VoWLAN-WPA cipher-wep104 disable
set service-profile VoWLAN-WPA cipher-wep40 disable
set service-profile VoWLAN-WPA auth-dot1x disable
set service-profile VoWLAN-WPA auth-psk enable
set service-profile VoWLAN-WPA beacon enable
```

```
set service-profile VoWLAN-WPA ssid-type crypto
set service-profile VoWLAN-WPA auth-fallthru last-resort
set service-profile VoWLAN-WPA psk-raw <256-bit passkey>
set service-profile VoWLAN-WPA tkip-mc-time 60000
set radius deadtime 0
set radius timeout 5
set radius retransmit 3
set enablepass password <password>
set authentication last-resort ssid <SSID name> local
set authentication admin * local
set user last-resort-<ssid_name> attr vlan-name v1
```

#AP Radio Profile

```
set radio-profile RealRadio service-profile VoWLAN-WPA
set radio-profile RealRadio 11g-only disable
set radio-profile RealRadio beacon-interval 100
set radio-profile RealRadio dtim-interval 3
set radio-profile RealRadio max-tx-lifetime 2000
set radio-profile RealRadio max-rx-lifetime 2000
set radio-profile RealRadio rts-threshold 2346
set radio-profile RealRadio short-retry 5
set radio-profile RealRadio long-retry 5
set radio-profile RealRadio frag-threshold 2346
set radio-profile RealRadio preamble-length short
set radio-profile RealRadio auto-tune channel-config disable
set radio-profile RealRadio auto-tune power-config disable
set radio-profile RealRadio auto-tune channel-interval 3600
set radio-profile RealRadio auto-tune power-interval 600
set radio-profile RealRadio auto-tune channel-holddown 300
set radio-profile RealRadio auto-tune power-backoff-timer 10
set radio-profile RealRadio active-scan disable
set radio-profile RealRadio wmm disable
set radio-profile default 11g-only disable
set radio-profile default beacon-interval 100
set radio-profile default dtim-interval 1
set radio-profile default max-tx-lifetime 2000
set radio-profile default max-rx-lifetime 2000
set radio-profile default rts-threshold 2346
set radio-profile default short-retry 5
set radio-profile default long-retry 5
set radio-profile default frag-threshold 2346
set radio-profile default preamble-length short
set radio-profile default auto-tune channel-config enable
set radio-profile default auto-tune power-config disable
set radio-profile default auto-tune channel-interval 3600
set radio-profile default auto-tune power-interval 600
set radio-profile default auto-tune channel-holddown 300
set radio-profile default auto-tune power-backoff-timer 10
set radio-profile default active-scan enable
set radio-profile default wmm enable
set dap security optional
set port type ap 1 model ap-2330 PoE enable
```

#AP Basic Configuration

set port type ap 1 model ap-2330 PoE enable
set ap 1 name <name>
set ap 1 bias high
set ap 1 blink disable
set ap 1 upgrade-firmware enable
set ap 1 group none
set ap 1 radio 1 channel 6 tx-power2 radio-profile RealRadio mode enable
set ap 1 radio 1 auto-tune max-power default min-client-rate 5.5 max-retransmissions 10
set ap 1 radio 2 channel 36 tx-power 17 radio-profile default mode disable
set ap 1 radio 2 auto-tune max-power default min-client-rate 24 max-retransmissions 10
set port type ap 2 model ap-2330 PoE enable
set ap 2 name AP02
set ap 2 bias high
set ap 2 blink disable
set ap 2 upgrade-firmware enable
set ap 2 group none
set ap 2 radio 1 channel 6 tx-power 2 radio-profile default mode disable
set ap 2 radio 1 auto-tune max-power default min-client-rate 5.5 max-retransmissions 10
set ap 2 radio 2 channel 36 tx-power 17 radio-profile default mode disable
set ap 2 radio 2 auto-tune max-power default min-client-rate 24 max-retransmissions 10
set arp agingtime 1200
set ip https server disable
set ip snmp server disable
set ip ssh server enable
set ip ssh 22
set ip telnet server enable
set ip telnet 23
set port enable 1
set port speed 1 AUTO
set port poe 1 enable
set port trap 1 NO
#set additional ports as appropriate

#SNMP Configuration

set snmp notify profile default drop all
set snmp protocol v1 enable
set snmp protocol v2c disable
set snmp protocol usm disable
set snmp security unsecured

#VLAN Configuration

set vlan tagtype dot1q
set vlan 1 name v1
set vlan 1 port 3
set vlan 1 port 4
set vlan 1 port 5
set vlan 1 port 6
set vlan 1 port 7
set vlan 1 port 8
set spantree backbonefast disable
set spantree uplinkfast disable
set spantree fwddelay 15 vlan 1

```
set spantree hello 2 vlan 1
set spantree maxage 20 vlan 1
set spantree priority  32768 vlan 1
set spantree disable vlan 1
set igmp disable vlan 1
set igmp proxy-report enable vlan 1
set igmp querier disable vlan 1
set igmp mrsol disable vlan 1
set igmp version 2 vlan 1
set igmp mrsol mrsi 30 vlan 1
set igmp qi 125 vlan 1
set igmp oqi 255 vlan 1
set igmp qri 100 vlan 1
set igmp lmqi 10 vlan 1
set igmp rv 2 vlan 1
set igmp mrouter port 3 disable
set igmp receiver port 3 disable
#disable router and receivers on other ports as appropriate

set fdb agingtime 1 age 300
set interface 1 ip 10.30.1.1 255.0.0.0
set mobility-domain mode seed domain-name mobdom
set mobility-domain member 10.30.1.2
set security acl ip SVP permit cos 7 119 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
set security acl ip SVP permit 0.0.0.0 255.255.255.255
set security acl map SVP vlan v1 out
commit security acl SVP
set ntp disable
set ntp update-interval 64

#  If you are performing cross-subnet roaming, this command must be issued on the "remote" WLAN Security
Switch (the one that doesn't have the VLAN statically configured. This command must be re-issued whenever
the tunnel  is re-established, since IGMP snooping is(re)enabled each time. A future Nortel release will resolve
this limitation.

set igmp disable vlan v1
```

Best Practices and Common Issues

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

System Configuration Best Practices

Nortel strongly recommends that you use WLAN Management Software 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.

"store error for EAP" on console at the end of web quickstart (20320)

Description: Harmless EAP_STORE_ERR message can appear after using a quick start. After you use the Web Quick Start or the CLI quickstart command, a message such as the following might appear on the CLI console:
EAP May 25 16:45:46.996611 ERROR EAP_STORE_ERR: store error for EAP: read error for get certificate request.

This message is harmless and can safely be ignored.

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. 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 EAP offload • 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
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

When testing and evaluating the Nortel Mobility 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.

Wireless NICs

Most wireless NICs available now support 802.1X authentication. Table 4 on page 37 lists the NICs that have been used successfully with the Nortel Mobility System. The majority were tested using recently available drivers using the Microsoft native 802.1X client and a Microsoft IAS RADIUS server. Nortel has not experienced any compatibility problems with NICs being unable to support specific EAP protocols or specific RADIUS servers, so only the differences in encryption type are documented. Entries that have both Windows 2000 and Windows XP listed together have the same results for both operating systems. A result of *Pass* indicates successful authentication and roaming with the listed model and operating system. A result of *Fail* indicates an inability to successfully complete authentication. A result of *NA* indicates that the NIC does not support the listed encryption type. A result of *Not Tested* indicates that the combination has not been tested yet.

Currently, WPA/CCMP (AES) encryption is supported only when configured as the only cryptographic type in service profile. Enabling dynamic WEP or WPA/TKIP with AES on the same SSID can cause severe connectivity issues as some manufacturers' drivers do not work properly when both encryption types are enabled. Nortel recommends that you set up a separate service profile for WPA/CCMP with a different SSID for compatibility. If you are migrating from Dynamic WEP to WPA/TKIP, Nortel recommends creating separate service profiles for each encryption type and migrating users from one SSID to the other when they are configured to use TKIP.

As new drivers are released by the manufacturers, Nortel expects general compatibility to improve.

Table 4: Wireless NICs Tested With Nortel WSS Software

Manufacturer	Model, Driver, and Driver Date	Windows Operating System	Dynamic WEP	Mixed WPA/TKIP & WEP	WPA/TKIP	WPA/ CCMP (AES)	Web-based AAA
3Com	3CRPAG175	XP	Pass	Pass	Pass	Pass	Not Tested
Belkin	F5D8010 1000 1.2.0.80, 9/ 21/2004	XP	Pass	Pass[1]	Pass	Pass	Pass
Buffalo	WLI-CP-G5 4	XP	Pass	Not Tested	Pass	Pass	Not Tested
Cisco	Aironet MPI350 3.8.26.0, 5/4/ 2004	XP	Pass	Pass	NA	Pass	Pass
Cisco	Aironet AIR-CB20A 3.9.16.0, 9/ 20/2004	XP	Pass	Not Tested	Not Tested	Not Tested	Not Tested
Cisco	Aironet 350	XP, 2000	Pass	Pass	Not Tested	Not Tested	Not Tested
Dell	TrueMobile 1150[2] A00 7.43.0.9	XP	Fail	Fail	NA	NA	Pass
Dell	TrueMobile 1150[3]	2000	Pass	Fail	Not Tested	NA	Not Tested
Dell	TrueMobile 1300	XP	Pass	Not Tested	Not Tested	Not Tested	Not Tested
Dell	TrueMobile 1400	XP	Pass	Pass	Pass	Pass	Not Tested
Dell	TrueMobile 1450 3.100.35.0, 11/27/2004	XP	Pass	Pass	Pass	Pass	Pass
D-link	DWLAG650	XP	Pass	Fail	Pass	Pass	Not Tested

Table 4: Wireless NICs Tested With Nortel WSS Software (continued)

Manufacturer	Model, Driver, and Driver Date	Windows Operating System	Dynamic WEP	Mixed WPA/TKIP & WEP	WPA/TKIP	WPA/ CCMP (AES)	Web-based AAA
D-link	DWL-AG660 A1,A2 3.0.0.44, 10/22/2003	XP	Pass	Pass	Pass	Pass	Pass
Intel	Pro/Wireless WCB5000 1.0.1.33, 6/4/2003	XP, 2000	Pass	Pass	NA	NA	Pass
Intel	Pro2100(Centrino)[4]	XP	Pass	Pass[5]	Not Tested	Not Tested	Not Tested
Linksys	WUSB54GS 1.0.0.1, 6/18/2004	XP	Pass	Pass	Pass	Pass	Pass
Linksys	WPC54G 1.0 3.60.7.0, 3/22/2004	XP	Pass	Pass	Pass	Pass	Pass
Linksys	WPC54GS 3.50.21.10, 1/23/2004	XP	Pass	Pass	Pass	Pass	Pass
Linksys	WPC54G version 2	XP	Fail	Fail	Fail	Fail	Not Tested
Netgear	WG-511 1.0 2.1.25.0, 9/6/2004	XP	Pass	Pass	Pass	Pass	Fail[6]
Netgear	WAG-511 0.1 3.1.1.754, 11/2/2004	XP	Pass	Pass	Pass	Pass	Fail[6]
Nortel	2202	XP, 2000	Pass	Pass	Pass	Pass	Pass
Proxim	Orinoco Gold 8410	XP, 2000	Pass	Pass	NA	NA	Not Tested
Proxim	Orinoco Gold 8460[7] 3.1.2.19, 8/5/2004	XP, 2000	Pass	Pass	Pass	Pass	Pass
Proxim	Orinoco Gold 8470-WD 3.1.2.19, 8/5/2004	XP	Pass	Pass	Pass	Pass	Pass

Table 4: Wireless NICs Tested With Nortel WSS Software (continued)

Manufacturer	Model, Driver, and Driver Date	Windows Operating System	Dynamic WEP	Mixed WPA/TKIP & WEP	WPA/TKIP	WPA/ CCMP (AES)	Web-based AAA
Proxim	Orinoco Gold 8480	XP	Pass	Pass	Pass	NA	Not Tested
Proxim	Harmony 8450 1.4.1.1, 8/1/ 2002	XP	Fail	Fail	NA	NA	Fail[8]
SMC	SMC2336A-AG 2.0 (99-012084-221) 2.4.1.32, 9/ 29/2003	XP	Pass	Pass	Pass	Pass	Pass
SMC	SMC2835W 1.0 (99-012084-163) 1.0.17.0, 6/ 16/2003	XP	Pass	Pass	Pass	NA	Pass
Symbol	LA-4121-1020-US 3.9.71.178, 3/25/2004	XP	Pass	Pass	Pass	NA	Pass

1. Belkin Wireless Pre-N requires WPA/TKIP on a TKIP/WEP mixed SSID.
2. Dell TrueMobile 1150 drivers v7.86 and newer might not work with Dynamic WEP when you have WPA/TKIP enabled. If you experience problems such as an inability to associate with the AP, install the previous revision of the driver, which is available from Dell's support site.
3. Requires a registry change to work properly; for more information, see "Windows 2000" on page 41.
4. Intel Centrino based chipsets might not associate with the SSID when power-save mode is enabled. Future drivers or laptop firmware might resolve this issue, but until then Nortel recommends disabling power-save mode completely in the driver properties for the NIC.
5. The Intel Centrino based chipset has not been tested with WPA yet, though Dynamic WEP does operate properly in a mixed TKIP and WEP configuration.
6. NetGear WG511/WAG511 doesn't associate properly to a Web-based AAA SSID. The NIC does not support DHCP.
7. Use the 848x driver, not the 846x driver.
8. Proxim Harmony 802.11a (8450) cannot associate properly.

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 web site. You can start with Microsoft's Wi-Fi center at:

  http://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 vendors.
- If your wireless NIC 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" on page 42.
- If MD5 challenge is configured on a Windows XP client for wired authentication, the quiet period must be set to 0 to guarantee 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:

```
2370# set dot1x quiet-period 0
2370# set dot1x tx-period 30
```

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:

  http://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" on page 42.

- 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 web site.
- 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 5 on page 43 lists Microsoft networking features that require computer authentication.

Table 5: 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 logon.
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.trpz.com or host/tac1-laptop.support.trpz.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 6: 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

Table 6: AAA Servers Tested With Nortel WSS Software (continued)

Configuration	RADIUS Servers Tested				
	Windows 2000 IAS	Windows 2003 IAS	Funk Steel Belted Radius	Cisco ACS	FreeRadius (Linux)
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

Nortel conducted WPA compatibility testing with a variety of NICs. See "Wireless NICs" on page 36 for complete details of the results. 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" on page 40 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.
- The Web-based AAA fallthru authentication type is not supported in conjunction with WPA encryption using preshared keys (PSK) for the same SSID. These options are configurable together but are not compatible. Web-based AAA traffic is not encrypted, whereas the PSK four-way handshake requires a client to already be authenticated and for encryption to be in place.

Security—best practice when mixing encrypted access and clear access

It is possible to configure a RADIUS server or a 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 Security Switch 2300 Series Configuration Guide* for more information.)

Security Best Practices

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

SNMP Security holes (21283)

Description: SNMP was found to have high vulnerability to hackers viewing community strings. There are many open TCP/UDP ports

For improved SNMP security, Nortel recomments use of SNMP v3, which supports authentication and encryption. If the TCP/UDP ports are not used, it's highly recommended to close them to minimize hackers/ virus/warms attacks

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

Passwords

The CLI, as well as WLAN Management Software, 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 Software client. To secure access, configure user accounts within WLAN Management Software, on each machine on which the client is installed.
- Access to the WLAN Management Software 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.

Note: Even though the SSH service is enabled by default, you need to generate a key pair before you can use SSH. Use the **crypto generate key ssh** command.

WLAN Management Software

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

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.

Note: Nortel recommends that you read the manual even if you are upgrading a switch that already uses Web-based AAA. The 4.0 implementation of Web-based AAA has changed.

Communication between the WSS and WLAN Management Software

Administration certificate requirement (11974)

Description: Before the WSS switch can communicate successfully with WLAN Management Software, you must create an administrative encryption certificate on the WSS switch. For details, see the *Nortel WLAN Security Switch Installation and Basic Configuration Guide.*

Mobility Domain™ (Multiple WSS) 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.

Caution! If any switch in a Mobility Domain is running WSS Software Version 4.0.X, all switches in the Mobility Domain must run 4.0.X If the Mobility Domain contains switches that are running an older WSS Software Version, a software issue might cause these switches to continuously restart. To avoid this issue, upgrade all the switches in the Mobility Domain to WSS Software Version 4.0.X You can use WLAN Management Software to upgrade them all at the same time. (19219)

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 Access Point 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.

As part of the boot process, an AP disables and reenables the link on the port over which the AP is attempting to boot. If STP is enabled on the device that is directly connected to the port, the link state change can cause the port on the other device to leave the forwarding state and stop forwarding traffic. The port remains unable to forward traffic for the duration of the STP forwarding delay.

An AP waits 30 seconds to receive a reply to its DHCP Discover message, then tries to boot using the other AP port. If the boot attempt fails on the other port also, the AP then reattempts to boot on the first port. The process continues until a boot attempt is successful. If STP prevents the other device's port from forwarding traffic during each boot attempt, the AP repeatedly disables and reenables the link, causing STP to repeatedly stop the other device's port from forwarding traffic. As a result, the boot attempt is never successful.

To allow an AP to boot over a link that has STP enabled, do one of the following on the other device:

- Disable STP on the other device's port.
- Enable the port Fast-Start feature, if supported, on the other device's port. (On some vendors' devices, this feature is called *PortFast*.)

DAP QoS Configuration on AP 2330

All transit ports on switches between DAP and WSS should be configured to trust ToS/CoS bits set by AP and WSS for example:
In a 2330 DAP configuration where the PoE device is an ERS460, it is important to ensure that the ERS460 Interface QoS setting is set to "trusted". The default ERS460 setting is "untrusted" and results in the QoS bit being set to "0" (zero) by either the WLAN 23xx switch and/or the AP. By setting the ERS460 QoS interface to "trusted" the QoS values will be kept as set by either the WLAN 2300 switches and/or AP .

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.)

ICMP dropping when roaming from AP 2330 to AP 2330.(Q01176441)

Description: When roaming, any transfer from an AP 2330 to a different AP 2330 requires a Wireless Interface (WI) card disable/enable for connectivity. ICMP drops after roaming to a different AP.

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.

Set 802.11b/g radios to 802.11b only for Siemens SpectraLink VoIP phones. (19124)

If you plan to use Siemens SpectraLink Voice over IP (VoIP) phones, you must change the AP radios that will support the phones to operate in 802.11b mode only. This type of phone expects the AP to operate at 802.11b rates only, not at 802.11g rates. To change a radio to support 802.11b mode only, use the **radiotype 11b** option with the **set port type ap** or **set dap** command.

Disable WSS Software Spanning Tree Protocol if the switch is connected to a switch running Nortel Passport 8600 code earlier than 3.7. (20043)

If you plan to connect a 2380, 2360, or 2350 switch to a switch running a Nortel Passport version earlier than 3.7, you must disable STP on both devices. WSS Software STP used PVST+, which is supported only in Passport version 3.7 and higher

DAP reports an invalid system IP address when using a DHCP client IP address. (21013)

Description: Errors about an "Invalid system ip-address found/seen in cluser" when trying to set a system-ip address equal to an IP address that was obtained from dhcp-client

Workaround: Nortel recommends that you use the DHCP client only for 2350 switches that you plan to configure using the drop-ship method

System Parameter Support

Table 7, Table 8, Table 9 on page 53, and Table 10 on page 54 list the recommended or maximum supported values for major system parameters.

Table 7: Mobility System Parameters

Parameter	Supported Value
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: 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 8: Network Parameters

Parameter	Supported Value
Forwarding database entries	• 2380: 16383 • 2360: 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 8: Network Parameters (continued)

Parameter	Supported Value

Access Control Lists (ACLs) and Location Policies	• Access Control Entries (ACEs) per switch
	  • 2380: 2308
	  • 2360: 700
	  • 2350: 700
	• ACEs per ACL:
	  • 2380: 267
	  • 2360: 267
	  • 2350: 25
	• Location Policies per switch:
	  • All models: 1
	• ACEs per Location Policy:
	  • 2380: 1024
	  • 2360: 256

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

Table 9: Management Parameters

Parameter	Supported Value
Maximum instances of WLAN Management Software simultaneously managing a network	3
Telnet management sessions	• 2380: 8 • 2360: 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, in any combination.
SSHv2 management sessions	• 2380: 8 • 2360: 4 • 2350: 4
Telnet client sessions (client for remote login)	• 2380: 8 • 2360: 4 • 2350: 4
NTP servers	3
SNMP trap receivers	8
Syslog servers	4

Table 10: 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: 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	999

Known Behaviors and Issues

In addition to the more common items indicated in "Best Practices and Common Issues" on page 35, the current software version contains the following known behaviors and issues.

Software Upgrade and Downgrade Issues

Upgrading only some WSS in a Mobility Domain can cause switches to continuously restart. (19219)

Description: If the Mobility Domain contains switches that are running an older WSS Software Version, a software issue might cause these switches to continuously restart.

Workaround: To avoid this issue, upgrade all the switches in the Mobility Domain to WSS Software Version 4.0.X You can use WMS to upgrade them all at the same time. (19219)

On rare occasions, a switch might not boot properly during upgrade or downgrade, and stop at the boot prompt. (19022)

Description: A software issue can cause a switch to stop at the boot prompt instead of completing the boot process, following a software upgrade or downgrade. When this occurs, the boot process is aborted and the console displays the boot prompt: boot>

Workaround: If this issue occurs, use boot prompt commands to edit the image filename in the boot profile from *default* to the actual image filename, then reboot.

Here is an example:

boot> **dir**

Internal Compact Flash Directory (Primary):
WSS020104.008 5523634 bytes
BLOAD 696176 bytes
BSTRAP 38056 bytes

Internal Compact Flash Directory (Secondary):
WSS030105.008 5524593 bytes

boot> **change**
Changing the default configuration is not recommended.
Are you sure that you want to proceed? (y/n)**y**

BOOT TYPE: [c] <CR>
DEVICE: [boot0:] <CR>
FILENAME: [default]WSS**020104.008**
FLAGS: [0x00000000] <CR>
OPTIONS: [run=nos;root=md0a] <CR>

boot> **boot**

When changing the boot profile, press Enter at the end of each boot parameter except Filename to retain the current values.

System Configuration Issues

Note: After using Quickstart or Web Quickstart, you must reboot the WSS.

The radiotype option of the set port type ap and set dap commands is applicable to two-radio models

The “Configuring a Template for Automatic AP Configuration” section of the “Configuring AP Access Points” chapter states that the radiotype option, which specifies the IEEE radio technology for the radio to use, does not apply to AP models with two radios. This is incorrect. On two-radio AP models, the option applies to the 802.11b/g radio, and configures the radio for 802.11b only or 802.11g only.

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)

Description: 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.

Workaround: Enable ntp server first, and then enable WSS ntp client to sync properly.

Configuration loss on partial load with errors. (19574)

Description: When NOS doesn't understand part of a configuration file, it will stop processing and not use any of the file. As part of an upgrade or downgrade, it is common to lose the entire configuration because some minor part of the config file is not understood.

Workaround: Go back in on the console to restore IP addressing, process the parts of the file that can be understood so that WMS or ssh/telnet can be used to push down new configuration remotely.

RF Auto channel tuning feature never selects a channel in 149-161 range. (21220)

Description: RF Auto-Tuning of channels on 802.11a radios uses only the bottom eight channels in the band (36, 40, 44, 48, 52, 56, 60, and 64).

Workaround: To use a higher channel number, you must disable RF Auto-Tuning of channels on the radio profile the radio is in, and statically configure the channel.

Clear dap" command will fail with a "range too big" error if the range contains more than 201 DAPs. The rlist does not support a range greater than 200. (21343)

Description: CLI supports a maximum range of 201 in commands that accept ranges.

Workaround: To delete more than 201 instances of a configuration item, type the appropriate clear command multiple times, with ranges of 201 or smaller.

Need to reset WSS for location policy to take affect (20698)

Description: WSS must be reset in order for location policy to take affect.

Workaround: Reset WSS for location policy to take affect

WSS rejects ** as mac wildcard (20060)

Description: The WSS allows ** as a MAC wildcard, but this is invalid for MAC wildcards

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

CLI auto-tune min-client-rate unrecognized when dap is given as a list (20471)

Description: Cannot enter a valid min-client-rate when the dap is provided as a list

Workaround: Set min-client rate individually on each dap

Invalid MAC address is not rejected in set authentication MAC wired. (20559)

Description: The set authentication MAC wired command does not check for validity of MAC addresses.

Workaround: Use correct format for MAC address.

Service profile creation does not accept a numeric character as the first character but SSID does. (20711)

Description: Service profile name cannot start with numeric characters.

Workaround: Use an alpha character as lead character.

The ACL MAP to port group cannot be cleared on the console. (21533)

Description: Can not clear ACL MAP to port group

Workaround: Use WMS to clear acl maps to port groups.

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.

Port group in a VLAN running STP can cause Layer 2 loop when the WSS is not the root bridge. (18171)

Description: If you configure a port group containing ports that are already in a VLAN that is running STP, and you then add the port group to the VLAN, a Layer 2 loop can occur in the VLAN. This can occur when the WSS is not the root bridge.

Workaround: Instead of adding the port group's ports to the VLAN individually, configure the port group before you add the groups ports to the VLAN, then add the port group to the VLAN.

Workaround:

ESL: Link do not come up between WS 2350 and ES 5520 - auto off

Description: When auto negotiation is disabled and the speed and duplex are set, the link does not come up between the switches. It only comes up when auto negotiation is enabled.

Workaround: Enable auto negotiation

ESL: sm_handle_boot_expiry error was seen while doing link tests (20217)

IPTV multicast video stream does not roam to a tunneled VLAN. (20900)

Description: IPTV multicast video stream does not roam to a tunneled vlan. Clients using video streams from Cisco IPTV can experience delays when roaming from one subnet to another

Workaround: None

Inter operability issue — The WSS PVST is incompatible with Ethernet Routing Switch. (20134)

Description: BayStacks do not support PVST.

Workaround: Disable spanning tree protocol on both sides.

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.

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.

2380: Corrupted AP report (20752)

Description: 2380 reports: Corrupted AP report on console — for example: trpz# APM Jun 02 20:20:49 ERROR AP_NOTICE: Handle_tapa_event_ap_report: Corrupted AP report, ignoring. channel 105 lowch 111 highch 110 rssi -67 crypto 5020.

Workaround: These messages can be safely ignored

APs log message about boot code when dap blink command is used (20470)

Description: APs log message about boot code when dap blink command is used. This happens because the WSS sends the BOOT_DOWNLOAD_ENABLE TLV when sending the LED_TEST_STATE TLV. The WSS should send the LED_TEST_STATE TLV by itself

Workaround: These messages can be safely ignored.

Rogue AP Detection and Containment

An interfering AP became a rogue AP after a rogue client previously associated with another Rogue AP associated with the interfering AP. (20880)

Description: Client that connects to a Mobility Domain AP and then to a neighboring network's AP might result in the neighboring AP being classified as a rogue.

Workaround: If the neighboring AP is legitimate, you can avoid this issue by adding the AP to the ignore list. In multi-tenant environments, it might be easier to disable countermeasures.

IDS client on wired network messages not surpressed by ignore list (20461)

Description: WSS generates log messages for a client seen on the wired network even when both the client and its AP are in the ignore list

Workaround: None

Rogue AP with same BSSID (MAC) on both radios (2.4GHz & 5GHz) may not be correctly attacked (21212)

Description: Due to a limitation in the rf-detection design. The periodic AP reports that are sent to the WSS are keyed on the BSSID of the device, as are the records stored on the WSSs. This leads to problems when the bssid value is same for 11a radio as well as 11b radio as used by several dual-radio APs. There is no way of distinguishing between these two radios at this point in time and countermeasures might run against the incorrect radio.

Workaround: None

After the AP is classified as rogue, a reboot of the WSS is required to clear the rogue status. (20651)

Description: If you add a device that WSS has classified as a rogue to the permitted OUI or permitted SSID list but not to the ignore list, WSS can still classify the device as a rogue. Adding an entry to the OUI or SID list merely indicates that the device is from an allowed manufacturer or is using an allowed SSID. However, to cause WSS to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

Workaround: After you add a device that has been classified as a rogue to the ignore list, the device remains classified as a rogue for at least 10 minutes. After 10 minutes, WSS reclassifies the device as an interfering device. (WSS can still attack the device with countermeasures, unless countermeasures are enabled to attack rogues only.)

AutoRF: AP (MP372) not selecting optimum channel on b-radio (20819)

Description: When a radio is actively sending countermeasures, the radio is tuned to the channel on which the rogue was detected, and stays on that channel while sending countermeasures, even if RF Auto-Tuning of the radio's channel is enabled.

Workaround: None

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 WLAN Management Software, 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 switch 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 a WSS's system name or system IP address from WLAN Management Software causes the switch to be unmanageable from WLAN Management Software. (18414)

Description: If you use WLAN Management Software to change a managed switch's system name or system IP address, other changes to the switch are not received from WLAN Management Software by the switch.

Workaround: Use the CLI to change the system name or system IP address. You can then use WLAN Management Software to make other changes.

WLAN Management Software can deploy a configuration that contains a user with no password, user group, or attributes. (18431)

Description: If you use WLAN Management Software to deploy a set of configuration changes to a WSS, the changes can contain a user with no password, user group, or attributes (such as VLAN name). Without a password or VLAN assignment, the user cannot access the network.

Workaround: Make sure each user has a password (if applicable) and is assigned to a VLAN, or is assigned to a user group that has a VLAN assigned.

"ERROR HTTPD: SSL accept error " after connecting to WMS server (20311)

Description: Log into WMS server and accept the certificate check (127.0.0.1:443) and you will see the following message on the 2380 console. "ERROR HTTPD: SSL accept error = error:14094"

Workaround: None. This error can be safely ignored.

Web View Issues

Unless otherwise noted, the workaround for Web View issues is to use the CLI or WMS. WebView is not supported in WSS rel 4.0.

IP Services Issues

Logging in to SSH requires hitting Enter twice. (15613)

Description: When you start an SSH session with a WSS, the switch does not display the login prompt the first time you press Enter.

Workaround: Press Enter a second time to display the login prompt.

Clearing Telnet management sessions also clears SSH sessions. (16100)

Description: If you type the **clear session telnet** command to clear all Telnet sessions with the switch, the command also clears all SSH sessions.

Workaround: None.

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

Description: If the route from a 2360 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# **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.

AAA and RADIUS Issues

If a RADIUS server and server group have the same name, the WSS restarts when an administrative user attempts to log in. (18434)

Description: If you use the same name for a RADIUS server and a RADIUS server group, and use the server group as the authentication method for a AAA rule for administrative access, the WSS switch restarts when the administrative user attempts to log in.

Workaround: Do not use the same name for a RADIUS server and a RADIUS server group.

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.

CLI allows set authentication dot1x command with invalid combination of pass-through and local options. (15562)

Description: The CLI allows you to enter a command such as the following:

set authentication dot1x ssid any * pass-through local

The pass-through and local AAA methods are mutually exclusive. Even if a server group named *local* exists, WSS Software does not use the group. In either case, the EAP session fails and the 802.11 session is deauthenticated when the client responds to the first identity request.

Workaround: Do not name a server group *local* and do not attempt to mix mutually exclusive authentication methods in the same command.

A set authentication mac *mac-addr-wildcard* rule does not restrict input. (13907)

Description: The **set authentication mac** *mac-addr-wildcard* command should accept only a properly formatted MAC address or a MAC address glob, which can use an asterisk (*) as a prefix or suffix to the MAC address. However, the command actually accepts any string.

Workaround: Provide only properly formatted MAC addresses or MAC address wildcards. For more information, see the *Nortel WLAN Security Switch 2300 Series Command Reference*.

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.

Incorrect zero value for Acct-Authentic appears in accounting statistics. (14851)

Description: In the output of the **show accounting statistics** command, the Acct-Authentic field in accounting records always displays 0 (zero) to indicate the location where a user was authenticated for the session. The correct value is 1 (one) if RADIUS performed authentication or 2 if authentication took place in the local WSS database.

Workaround: None. Ignore the Acct-Authentic value in **show accounting statistics** output.

Acct-Session-Id not sent for Admin sessions (20742)

Description: When enabling accounting for admins sessions (through Telnet or CLI), neither the Acct-Session-Id nor the Acct-Unique-Session-Id are sent to the Radius server. WSS does not send Acct-Session-Id or Acct-Unique-Session-Id values to RADIUS servers for administrative sessions.

Workaround: None

Web-based AAA Issues

Web-based AAA using a Windows client and a WSS that has a self-signed certificate can intermittently fail if Windows is configured to update root certificates. (18597)

Description: If the WSS uses a self-signed certificate (as opposed to a CA-issued certificate), and the Microsoft OS on the Web-based AAA client is configured to update root certificates (the default setting), Windows tries to contact microsoft.com to get updated certificates. This causes a 15-second delay, after which IE displays a popup dialog asking whether the user wants to accept the untrusted certificate from the WSS. Even when the user selects Yes, IE sometimes does not display the Web-based AAA login page served by the WSS.

Workaround: This issue occurs intermittently. If the issue occurs, reattempt the login.

Web-portal or last-resort username can change to MAC address in show sessions output. (20250)

Description: A change to a web-portal or last-resort user's session can cause the **web-portal** or **last-resort** username in the **show sessions** output to change to the MAC address of the user's NIC. Some circumstances under which this can occur are if the user roams or the user's NIC is disabled and reenabled.

Workaround: This issue is cosmetic only and does not affect the user's actual connection.

Web-portal login page refers to "WebAAA" (20058)

Description: Web-portal login page refers to "WebAAA"

Workaround: Web-portal, Web-based AAA and WebAAA are interchangeable terms within the system.

WebPortal login page cannot be accessed when web browser is configured for proxy server. (21550)

Description: WebPortal login is not supported when the client web browser is configured to use a web proxy. Login fails.

Workaround: Do not use a web browser configured to use a proxy to receive the WebPortal login page.

WebPortal and WPA-PSK compatibility. The web portal and WPA-PSK are described as incompatible in the documentation. (20824)

Description: Currently the documentation states that the WebAAA fallthru authentication type is not supported in conjunction with WPA encryption using preshared keys (PSK) for the same SSID. These options are configurable together but are not compatible. WebAAA traffic is not encrypted, whereas the PSK four-way handshake requires a client to already be authenticated and for encryption to be in place. WebPortal and WPA-PSK authentication can co-exist

Workaround: This is no longer the case with the new Web Portal. With the new Web Portal, WPA-PSK is possible since there is the web-portal-ssid user account that pre-authenticates in AAA.

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:

2370# **set security acl ip port_abc deny 0.0.0.0 255.255.255.255**
error: Wrong ACL name input = port_abc
2370# **set security acl ip vlan_abc deny 0.0.0.0 255.255.255.255**
error: Wrong ACL name input = vlan_abc
2370# **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.

ACL hits are not displayed for ACLs mapped only to users. (15686)

Description: If an ACL with the hit-sample-rate option enabled is mapped only to a user (and not to a port or VLAN, and so on), WSS Software does not display hit information for the ACL. This issues does not affect ACLs that are mapped to anything besides users. This issue also does not affect the operation of the ACL. WSS Software correctly applies the ACL even if the hit data is not displayed.

Workaround: None.

ACLs: VLAN-in mapping filters packets in both directions. (21428)

Description: ACLs have the same effect whether they are mapped to a VLAN's inbound traffic direction or outbound traffic direction

Workaround: Always map the ACL to the outbound traffic direction of the VLAN.

IPSec user ACL does not take affect until after reboot. (21458)

Description: IPSec user ACL does not take effect until after reboot

Workaround: IPSec user-based ACL could require a WSS reboot to take effect.

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)

Workaround: None

Snoop not capturing bi-directional traffic from client (20450)

Description: At this time snoop does not capture un-associated traffic

Workaround: None

Console session never times out (20823)

Description: If you physically remove the console cable and reconnect the next day, you are still logged in when you reconnect.

Workaround: Always logout at the end of the session.

Station not found error. (21495)

Description: Error DAP ## ap_network:tqs_enqueue:Station not found: [mac-address]. The message occurs when a station has neither sent no received traffic for over two minutes, and the WSS begins sending null data probe packets. The most common cause for this error is that the client has moved out of range or has disconnected from the system without sending a disassociate frame.

Workaround: It is safe to ignore this message.

WSS rejects ** as a MAC wildcard. (20060)

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

Workaround: Specify * instead of ** to match on all MAC addresses.

Web quickstart wizard appends an hour if daylight savings time is enabled. (20491)

Description: During the time configuration phase of the web quickstart wizard, if the user checks the daylight savings time box, at the end of the wizard an hour will be added to the time entered

Workaround: Set the time to one hour earlier than the actual time. Alternatively, use the CLI to reset the date after finishing with the Web Quick Start.

Algorithm for selecting AP to do countermeasures does not take into account proximity to rogue. (20761)

Description: The AP that heard the rogue at the strongest signal level is not picked. WSS does not take proximity to a rogue AP into account when selecting an AP to issue countermeasures against the rogue. It is possible for WSS to select an AP to issue countermeasures against a rogue that is too far from the AP. This can occur if the rogue and the AP incorrectly selected by WSS are on the same channel and the incorrect AP can hear the rogue's traffic.

Workaround: None

Clients in the same VLAN cannot ping each other if they are on the same port with different tagging. (20908)

Description: Clients that come in on the same 3rd party AP, but each on a different SSID, and the clients both authorize to the same VLAN cannot ping each other.

Workaround: Make sure that each SSID authorizes to a different VLAN

The Web quickstart wizard should not be presented to web portal users(21182)

Description: When configuring a system that supports web quickstart (currently 2350 and 2360), web quickstart will take precedence over web portal. The result is that, if a user configures web portal from the CLI, and attempts to access web portal from a browser, the web quickstart wizard will be returned to the user instead of the web portal login page. This is an unexpected behavior. Web portal users should never see the web quickstart page.

Workaround: Save the configuration and reset the switch as soon as configuration is finished.

Client authentication traps are not being sent (21321)

Description: When a web portal login session fails (either due to a non-existent user or a wrong password), no trap is sent to SNMPC or syslog server. A ClientAuthorizationSucessTrap is sent when the login is successful

Workaround: None

Error message when using "crypto generate self-signed" command is unclear. (21334)

Description: When generating a self-signed certificate through the crypto generate self-signed command an error message, **error: no such file**, means that the corresponding key pair is not generated.

Workaround: First use the crypto generate key command to generate the key pair, then use the crypto generate self-signed command.

Harmless error message displayed when a client connects to a Distributed AP configured by a Distributed AP template. (21375)

Description: If a Distributed AP is configured by a template, rather than explicitly by a set dap command that identifies its serial number, WSS generates a message such as the following when a client connects to the AP: 2370-1# APM Jul 29 19:50:22.137817 ERROR AP_CONFIG_ERR: type(CIPHER), reason: Variable not implemented.

Workaround: You can safely ignore these messages. To stop the messages, add a permanent configuration for the Distributed AP.

Inconsistent rogue ignore list on different WSS in mobility domain. (21556)

Description: If the Rogue Ignore list is not identical across all switches in the same area, the seed WSS receives inconsistent data from each non-seed member and displays the wrong type in the show rfdetect mobility-domain.

Workaround: Ensure that the Rogue Ignore list is identical across all switches in the same area.

Disabling power on WSS 2360 switch remains powered by POE links. (20386)

Description: Best Practice When Powering Down a Switch: If a 2350 or 2360 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.

Workaround: To ensure that the switch is powered off, unplug the power cord, then unplug all Ethernet cables that are connected to other PoE devices