Part No. 320659-C Rev.03
November 2006

4655 Great America Parkway
Santa Clara, CA 95054

Nortel WLAN Security Switch 2300 Series Release Notes

Release 4.1.14

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 for release 4.1.14

Nortel recommends that you familiarize yourself with the "Best Practices and Common Issues" section in this document before installing WLAN 2300 System Software (WSS Software) Version 4.1.14. For additional product information, refer to the following manuals in addition to these release notes:

- Nortel WLAN Security Switch 2300 Series Quick Start Guide.
- Nortel WLAN Security Switch 2300 Series Installation and Basic Configuration Guide.
- Nortel WLAN Access Point 2330A Installation Guide.
- 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 4.1.14

Nortel has enhanced the WLAN 2300 series software to meet regulatory requirements in specific EU, CALA and APAC countries. A mandatory upgrade is required for: Australia, Brazil, Chile, France, Korea, Malaysia, Mexico, Panama, Peru, Venezuela. It is recommended all other customers in EU, APAC and CALA upgrade to WSS Release 4.1.14 and their WMS software to Release 4.1.15.

Please refer to the "Approved Countries for the WLAN 2300 Series Components"at http://www.nortel.com/support for a complete listing of approved counties for using WLAN 2300 series software and their associated two-letter country codes.

Description of regulatory compliance modifications to WSS and WMS software

The following software updates have been made to the WSS and WMS software to ensure global regulatory compliance:

- Modified the antenna gain specifications to coincide with the measured results.
  - The accurate peak and average gain values are now used to calculate the correct power settings for the radios.
  - Adjusted band edge power settings for all 802.11g entries to match measured regulatory data and ensure compliance to local regulatory limits.
- Additional regulatory information and operating parameters were implemented for newly homologated countries.
- Corrected operating parameters for DFS performance in selected “Affected Countries”.
- Disabled operation in the 5.25GHz to 5.35GHz and 5.47GHz to 5.725GHz for France to meet the DFS requirements for EN301-893v1.3.1

Issues resolved since software release 4.1.13 are as stated beginning on page 44

WSS Software Version 4.1 contains the following enhancements:

- Default AAA attributes for SSIDs
- On-demand countermeasures
- Layer 2 traffic restriction among clients in a VLAN
- Network domains (Mobility Domain clustering)
- Configurable idle timeout for CLI management sessions
- Configurable Class-of-Service (CoS) mapping
- Support for periodic mark messages in the system log, to provide date and time information for troubleshooting
- MIB additions
- Support for 150 rules in a location policy
- New boot failover mechanism

This release also enables you to use a Sygate LAN Enforcer Server for authentication. (See“Using a Sygate LAN Enforcer Server for Authentication” on page 25.)

Default AAA Attributes for SSIDs

WSS Software Version 4.1 enables you to configure a service profile with a set of default AAA authorization attributes that are used when the normal AAA process or a location policy does not provide them. These authorization attributes are applied by default to users accessing the SSID managed by the service profile. You can configure any of the following attributes in a service profile:

- **encryption-type**
- **end-date**
- **filter-id**
- **idle-timeout**
- **mobility-profile**
- **service-type**
- **session-timeout**
- **start-date**
- **time-of-day**
- **url**
- **vlan-name**

The **ssid** attribute cannot be configured because the user is already associated with the SSID.

By default, a service profile contains no SSID default authorization attributes. When specified, attributes in a service profile are applied *in addition* to any attributes supplied for the user by the RADIUS server or the local database. When the same attribute is specified both as an SSID default attribute and through AAA, then the attribute supplied by the RADIUS server or the local database takes precedence over the SSID default attribute. If a location policy is configured, the location policy takes precedence over both AAA and SSID default attributes. The SSID default attributes serve as a fallback when neither the AAA process, nor a location policy, provides them.

(For more information, see the "Assigning SSID Default Attributes to a Service Profile" section in the "Configuring AAA for Network Users" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide.*)

On-Demand Countermeasures

WSS Software Version 4.1 provides greater rogue control by enabling you to configure WSS Software to issue on-demand countermeasures. On-demand countermeasures are those launched against devices that you have manually specified in the WSS's attack list. When you enable on-demand countermeasures, WSS Software issues them only against the devices that have been manually specified in the attack list, not to other devices determined to be rogues for other reasons, such as policy violations.

When WSS Software directs an **AP** radio to issue countermeasures against a rogue, WSS Software changes the channel on the radio to the channel on which the rogue traffic is detected. The radio remains on that channel as long as the radio is issuing countermeasures against the rogue, even if RF Auto-Tuning is enabled. On-demand countermeasures are disabled by default.

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

Layer 2 Traffic Restriction Among Clients in a VLAN

WSS Software Version 4.1 enables you to enhance network security by restricting Layer 2 forwarding among clients in the same VLAN. By default, clients within a VLAN are able to communicate with one another directly at Layer 2. When you restrict Layer 2 forwarding in a VLAN, WSS Software allows Layer 2 forwarding only between a client and a set of MAC addresses, generally the VLAN's gateway routers. Clients within the VLAN are not permitted to communicate among themselves directly. To communicate with another client, the client must use one of the specified gateway routers.

(For more information, see the "Restricting Layer 2 Forwarding Among Clients" section in the "Configuring and Managing Ports and VLANs" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide.*)

Network Domains

WSS Software Version 4.1 allows functionality found in Mobility Domains to be extended over a multiple-site installation, in a Network Domain. A Network Domain is a group of geographically dispersed Mobility Domains that share information over a WAN link. This shared information allows a user configured in one Mobility Domain to establish connectivity on a WSS in a remote Mobility Domain. The WSS forwards the user traffic by creating a VLAN tunnel to a WSS in the remote Mobility Domain.

In a Network Domain, one or more WSS switches acts as a seed device. A Network Domain seed stores information about all of the VLANs on the Network Domain members. The Network Domain seeds share this information among themselves, so that every seed has an identical database.

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

Configurable Idle Timeout for CLI Management Sessions

By default, WSS Software automatically terminates a console or Telnet session that is idle for more than one hour. WSS Software Version 4.1 enables you to change the idle timeout for CLI management sessions to a value from 1 to 86400 seconds (one day). You can disable the idle timeout by setting the value to 0. The idle timeout applies to all types of CLI management sessions: console, Telnet, and SSH. A change to the idle timeout applies to new sessions only, not to existing sessions.

The timeout interval is in 30-second increments. For example, the interval can be 0, or 30 seconds, or 60 seconds, or 90 seconds, and so on. If you enter an interval that is not divisible by 30, the CLI rounds up to the next 30-second increment. For example, if you enter 31, the CLI rounds up to 60.

(For more information, see the "Changing the Idle Timeout for CLI Management Sessions" section in the "Configuring and Managing IP Interfaces and Services" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide.*)

Configurable Class-of-Service (CoS) Mapping

WSS Software Version 4.1 enhances Quality of Service (QoS) support with configurable CoS mapping. CoS mapping helps ensure consistent markings for all packets in a network. QoS configuration is simplified with consistent packet classification and marking across an enterprise. High priority traffic received by a WSS or AP retains high priority when forwarded.

- WSSs classify and mark traffic based on 802.1p tag value (for tagged traffic) or Differentiated Services Code Point (DSCP) value.

- AP access points classify ingress traffic from wireless clients based on the service type value in the 802.11 header, and mark the DSCP value in the IP tunnel on which the AP forwards the user traffic to the WSS.

  APs place traffic from a WSS to a wireless client in a forwarding queue based on the DSCP value in the tunnel carrying the traffic, then forward the traffic based on the queue's priority.

The **show qos default** command shows the default CoS mappings.

WSS Software# **show qos default**

Ingress QoS Classification Map (dscp-to-cos)

```
Ingress DSCP      CoS Level
================================================================================
=========
    00-09     0   0   0   0   0    0   0   0   1   1
    10-19     1   1   1   1   1    1   2   2   2   2
    20-29     2   2   2   2   3    3   3   3   3   3
    30-39     3   3   4   4   4    4   4   4   4   4
    40-49     5   5   5   5   5    5   5   5   6   6
    50-59     6   6   6   6   6    6   7   7   7   7
    60-63     7   7   7   7
```

Egress QoS Marking Map (cos-to-dscp)

```
CoS Level          0    1    2    3    4    5    6    7
================================================================================
=========
Egress DSCP        0    8    16   24   32   40   48   56
Egress ToS byte    0x00 0x20 0x40 0x60 0x80 0xA0 0xC0 0xE0
```

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

Date and Time Mark Messages in the System Log

WSS Software Version 4.1 simplifies troubleshooting by allowing WSS to generate mark messages at regular intervals in the system log. The mark messages indicate the current system time and date. Nortel can use the mark messages to determine the approximate time when a system restart or other event causing a system outage occurred.

(For more information, see the "Enabling Mark Messages" section in the "Troubleshooting a WSS" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide.*)

SNMP Additions

WSS Version 4.1 includes the following SNMP enhancements.

New MIBs

- New AP and radio MIBs (nrtl-ap-status-mib.my and nrtl-ap-tc.my). These MIBs list configuration and status information for APs and their radios.
- New client MIB (nrtl-client-session-mib.my). This MIB provides information about all wired and wireless clients, including their roaming histories and statistics.

New Traps

The nrtl-trap.my MIB contains the following new traps (notification types):

- **ApNonOperStatusTraps**—Generated to indicate an AP radio is nonoperational.
- **ApOperRadioStatusTraps**—Generated when the status of a AP radio changes.

You can enable them in notification profiles, along with other notification types.

WLAN Management Software 4.1 uses these new traps to provide up-to-date information in monitoring, while minimizing the system load by polling just for individual AP or client data when needed.

(For information, see the "Configuring a Notification Profile" section in the "Configuring SNMP" chapter of the *Nortel WLAN Security Switch 2300 Series Configuration Guide.*)

Support for 150 Rules in a Location Policy

WSS Software Version 4.1 increases the number of rules you can configure in a location policy. In previous WSS Software versions, the maximum number of rules supported was 50. In WSS Software Version 4.1, the maximum number of rules supported is 150.

New Boot Failover Mechanism

When a WSS is booted, if it cannot load the WSS Software software image it is configured to load, the switch attempts to load the last image it was able to load successfully. In previous releases, if the configured image could not be loaded, the boot process would stop at the boot prompt.

Each time the WSS successfully loads a WSS Software software image, a reference to this image is saved as the "safe boot" image. If the WSS Software software cannot be loaded the next time the WSS is booted, then the WSS automatically attempts to load the safe boot image.

Boot failover might occur when an image update is attempted, and the update process fails. For example, with image A loaded on the WSS, you can configure the WSS to load image B the next time the switch is booted. When the switch is reset, if image B fails to load, the switch then attempts to load image A (the last image successfully loaded on the WSS).

Version Compatibility

WLAN Management Software

This version of WLAN 2300 System Software (WSS Software) is intended for use with WLAN Management Software Version 4.1.15 or higher only.

Minimum WSS Software Requirements for Upgrade

Table 1 lists the minimum WSS Software version a WSS must be running when you upgrade the switch to WSS Software Version 4.1. If your switch is running an older WSS Software version, you can use the upgrade path to upgrade the switch to 4.1.

Table 1. Software Requirements for Upgrade to WSS Software Version 4.1

Product	Minimum WSS Software Version Required	Upgrade Path
2350	4.0.*x*	4.0.*x* -> 4.1.*x*
2360		
2380		

Best Practices and Common Issues

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

Best Practice When Powering Down a Switch

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

System Configuration Best Practices

Nortel strongly recommends that you use 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.

Client and AAA Best Practices

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

Get Clients and AAA Working First

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

The selection of client and AAA server software will depend heavily on the requirements of your deployment. First, decide which EAP Protocol you will be using as that will restrict the available clients and servers. Each protocol has different advantages and disadvantages, which you will need to consider in your deployment. For most enterprise deployments, Nortel recommends using PEAP-MS-CHAP-V2 as the 802.1X protocol. Table 2 compares the EAP protocols.

Table 2. 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

LEAP is not supported. LEAP is a proprietary protocol and LEAP-authenticated networks can be breached using a simple dictionary attack.

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. The 2300 series switches should work with any vendor's NIC that is 802.1X compliant. Nortel has not experienced any compatibility problems with NICs being unable to support specific EAP protocols or specific RADIUS servers.

Currently, WPA/CCMP (AES) encryption is supported only when configured as the only cryptographic type in a 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. With that said, Nortel recommends that you make sure that the latest NIC drivers are being used.

Driver Dependant Behavior

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

802.1X Clients

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

Windows XP

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

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

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

- Installing Windows XP Service Pack 2 is recommended for all wireless clients as it includes several important hotfixes.
- If you are not prepared to install Service Pack 2, Nortel strongly recommends that all wireless clients use Service Pack 1a with the following hotfixes installed:
  - KB826942—This is the WPA Hotfix Rollup and is available through Microsoft Update
  - KB834669—This corrects an 802.1X client issue which can cause system instability problems in Windows XP. You will need to contact Microsoft or Nortel Support directly for this hotfix.
- If your network uses logon scripts, Active Directory group policies, or your users regularly share their laptops, you should enable computer authentication (also known as machine authentication) to achieve full functionality over your wireless connection.
- Download current drivers for your NICs from the NIC vendor(s).
- If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, Nortel recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. Nortel strongly recommends that you update the driver manually using the driver properties in the Network control panel instead of installing the client manager.
- If you use computer authentication with different VLANs for the Computer and User accounts and do not have the WPA hotfix rollup (KB826942) or Service Pack 2, you need to install Microsoft hotfix KB822596. Otherwise, DHCP will not operate correctly after the user authenticates. You must contact Microsoft technical support for this hotfix. It is not available from their website. For more information on computer authentication, see "Computer Authentication" on page 17.
- If MD5 challenge is configured on a Windows XP client for wired authentication, Nortel recommends that you set the quiet period to 5 to allow successful authentication. In addition, if the authentication is carried out manually, the timeout value must be set to no less than 30 seconds in order to allow the user ample time to enter their username and password. For example, to configure 802.1X on a WSS to allow these users time to log in, type the following commands:

  2370# **set dot1x quiet-period 5**
  2370# **set dot1x tx-period 30**

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

Windows 2000

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

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

  www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx
- Installing Windows 2000 Service Pack 4 is required for all wireless clients.
- Some clients might experience system instability when using PEAP-MS-CHAP-V2 in an Active Directory environment. The primary symptom of this is a message displayed after login informing the user that the service svchost.exe has stopped unexpectedly. If you experience this problem, please contact Microsoft technical support and request hotfix KB833865.

- If your network uses logon scripts, Active Directory group policies, or your users regularly share their laptops, Nortel recommends that you enable computer authentication to achieve full functionality over your wireless connection.
- Download current drivers for your NICs from the NIC vendor(s).
- Windows 2000 does not include a full implementation of the Wireless Zero-Config service from Windows XP, so you will need to use the client manager software provided with your NIC to configure your SSID and enable WEP encryption. When using dynamic WEP in Windows 2000, select *static WEP 128bit* and enter any static WEP key as a placeholder. This temporary key configures the driver to use WEP to encrypt packets, and the Microsoft 802.1X client then overrides the static WEP key you entered with a dynamic key after you authenticate successfully.
- If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, Nortel recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. If you are unable to install the client manager without the AEGIS component, contact the driver manufacturer or download an earlier version that does not contain the AEGIS component.
- 16-bit PCMCIA and built-in NICs (some 802.11b cards in Dell, Toshiba, and other manufacturers' laptop PCs) might require a registry setting to be changed before they will be able to associate with any SSID. Microsoft Knowledge Base article 327947 documents the changes necessary to resolve the problem. Multi-band cards (A/B or A/B/G) are generally 32-bit and do not experience this problem.
- If you use computer authentication with different VLANs for the Computer and User accounts, you need to install Microsoft hotfix KB822596. Otherwise, DHCP will not operate correctly after the user authenticates. You must contact Microsoft technical support for this hotfix. It is not available from their website. For more information on computer authentication, see "Computer Authentication" on page 17.
- If you experience a delay in receiving your DHCP IP address wirelessly while using 802.1X authentication, you might need to install Microsoft hotfix KB829116. You must contact Microsoft technical support for this hotfix. It is not available from their website.

Funk Odyssey

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

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

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 3 lists Microsoft networking features that require computer authentication.

Table 3. Microsoft Networking Features That Require Computer Authentication

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

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

- To enable computer authentication, go to the **Authentication** tab where you normally select your 802.1X authentication method and enable the checkbox labeled **Authenticate as computer when computer information is available**.
- The authentication protocol that is configured for your user accounts will also be used for the computer account.
- If the EAP protocol you are using requires client certificates, you must use the Microsoft Enterprise Certificate Authority built-in to Windows 2000 Server and Windows Server 2003 to generate *Computer* certificates for PCs on your active directory domain. Microsoft Knowledgebase Article KB313407 explains how to enable the automatic distribution of computer certificates through Active Directory.
- If the user and machine accounts use different VLANs, you must install hotfixes on the client PCs to enable them to DHCP for a new IP address when the user authentications. Windows XP requires either the WPA Rollup Hotfix (KB826942) or Hotfix KB822596. Windows 2000 requires hotfix KB822596.
- Using PEAP-MS-CHAP-V2 with computer authentication will allow users who have never logged on to a PC authenticate wirelessly without having to login to the PC over a wired connection the first time. EAP-TLS still requires the user to connect to the network over a wired connection to generate a profile on the PC and a user certificate.

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

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

Computer authentication also requires specific configuration considerations on the WSS:

- The username of a computer authentication connection will be in the form of host/*fully-qualified-domain-name*, for example host/bob-laptop.wlan-switch.com or host/tac1-laptop.support.nrtl.com. This username is the same regardless of the configured protocol (PEAP-MS-CHAP-V2 or EAP-TLS). An appropriate userwildcard would be *host/*.domain.com* where domain.com is the Active Directory domain name. Alternatively, in a smaller deployment you could use a userwildcard 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 4 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 4. AAA Servers Tested With Nortel WSS Software

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

Testing notes

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

WPA

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

- CCMP (AES 802.11i draft support) is supported only when it is the only encryption type enabled on that SSID. Enabling TKIP or Dynamic WEP on the same SSID with CCMP can cause serious connectivity issues as most clients do not properly support this configuration. Nortel recommends that you create a separate service profile and SSID for WPA/CCMP.
- Enabling TKIP and Dynamic WEP on the same SSID is not recommended. This configuration forces the group key (multicast/broadcast key) to use the lowest common encryption type, in this case Dynamic WEP. Additionally, compatibility with wireless NICs is reduced.
- Downloading the latest drivers for your wireless NIC is strongly recommended. See “802.1X Clients” on page 15 for specific information on installing drivers for your operating system.
- When a session key is changed, Microsoft WPA clients can sometimes incorrectly start using the new key before the end of the four-way handshake that is used to establish the key information. This issue can occur when the session timeout for the client session expires. As a result, the AP access point rejects the client’s re-association attempt because the key information presented by the client is invalid. If you experience this issue, clear the Session-Timeout attribute on the affected users. The WSS will not force a reauthentication of WPA/TKIP and WPA/CCMP users periodically like it does with dynamic WEP users.
- Do not use the **set service-profile shared-key-auth** command in a WPA configuration. This command does not enable PSK authentication for WPA. To enable PSK for WPA, use the **set service-profile auth-psk** command.
- Use one WPA authentication method per SSID, either 802.1X authentication or preshared key (PSK) authentication, but not both.

Security—best practice when mixing encrypted access and clear access

It is possible to configure a RADIUS server or 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 2300 System Software 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.

Certificates

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

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

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

Usernames

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

Passwords

The CLI, as well as WLAN Management 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 and an access rule that permits them, 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.

Web Access

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

Unless you need to use Web View, leave the HTTPS server on the WSS disabled. (Even though WLAN Management Software also uses HTTPS, disabling the HTTPS server does not disable access by WLAN Management Software.)

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

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

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

WLAN Management 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, use 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 2300 System Software Configuration Guide*. The section has configuration requirements and recommendations, in addition to an overview of the Web-based AAA process.

Communication between the WSS and WLAN Management Software or Web View

Administration certificate requirement (11974)

Description Before the WSS can communicate successfully with WLAN Management Software, you must create an administrative encryption certificate on the WSS. 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.

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 2300 System Software 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.

(For more information, see the *Release Notes for Nortel AP Access Points*.)

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 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**.

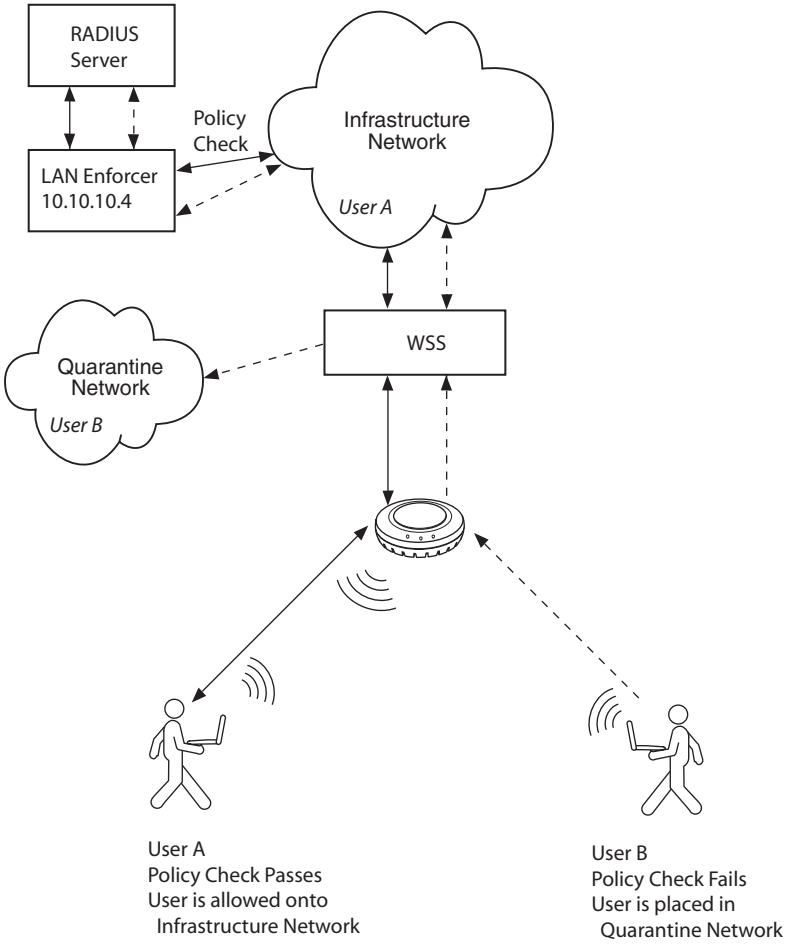
- **Disable multicast router discovery.** This multicast router solicitation protocol (part of *draft-ietf-magma-snoop*) is known to cause error messages with other IGMP snooping switches and multicast routers. To disable the protocol, use the command **set igmp mrsol disable**. (The protocol is disabled by default in the current software version.)

Using a Sygate LAN Enforcer Server for Authentication

WSS Software Version 4.1 supports using a Sygate LAN Enforcer server for authenticating users. WSS Software supports standalone operation of the Enforcer, in non-transparent mode. In this mode, the user is authenticated against a RADIUS server, but the Sygate server is a front-end to the RADIUS server and uses host integrity information to rewrite RADIUS attributes.

To configure WSS Software for this option, add the Enforcer to a server group and use the server group as the authentication method in an 802.1X authentication rule. If the user passes the policy check on the Enforcer, the Enforcer allows the user onto the network. If the user fails the policy check, the Enforcer places the user into a quarantine network instead. Figure 1 shows an example.

Figure 1. Authentication Using Sygate LAN Enforcer



To configure a WSS to use a Sygate LAN Enforcer for authentication of 802.1X clients, use commands such as the following:

WSS# **set radius server lan-enforcer address 10.10.10.4 key MyEnforcerSharedSecret**
success: change accepted.

WSS# **set server group sygate-group members lan-enforcer**
success: change accepted.

WSS# **set authentication dot1x ssid EndpointSecurityNetwork ** pass-through sygate-group**
success: change accepted.

The first two commands create an authentication server named *lan-enforcer* and a server group named *sygate-group* and adds the *lan-enforcer* server to the group. The last command creates an 802.1X authentication rule for SSID *EndpointSecurityNetwork*, matches on all usernames (**), and passes through authentication of the users to *sygate-group*.

You also must configure the policies on the LAN Enforcer. For information, see the documentation for the server.

User ACLs Require Explicit Source and Destination Addresses

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

Rogue Detection Active Scan Interval Is Longer During a SpectraLink SVP Call. (23317)

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

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

System Parameter Support

Table 5, Table 6, Table 7, and Table 8 list the recommended or maximum supported values for major system parameters.

Table 5. Mobility System Parameters

Parameter	Supported Value
WSSs in a single Network Domain	500
WSSs in a single Mobility Domain	32
Roaming VLANs per WSS	300 Does not include local statically configured VLANs
VLANs per Mobility Domain	400 This number consists of 300 roaming VLANs plus 100 local statically configured VLANs.

Table 5. Mobility System Parameters (continued)

Parameter	Supported Value
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 6. 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

ACLs and Location Policies	• 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
	  The Location Policy can have up to 150 rules.

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

Table 7. 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 and 2350, 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
RADIUS servers	100 configured on the switch 10 in a server group 4 server groups in a AAA rule

Table 8. 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.

Table 8. Client and Session Parameters (continued)

Parameter	Supported Value
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	• 2380: 999 • 2360: 250 • 2350: 250

Known Behaviors and Issues

In addition to the more common items indicated in "Best Practices and Common Issues" on page 13, the current software version contains the following known behaviors and issues.

Software Upgrade and Downgrade Issues

DAPs will not boot up when upgrading from WSS version 4.0.20 to WSS 4.1.x if DNS is used instead of Option 43.

Description In 4.0.20.0, the DAPs perform a DNS query for both trpz.com and wlan-switch.com. In 4.1.x, the DAPs only perform a DNS query for wlan-switch.com. Issue observed by customers that use DNS instead of Option 43 and have DNS configured with trpz.com. Issue not observed if customer uses Option 43, as that fallback option occurs before DNS within the DAP bootup sequence.

Workaround Change DNS server configuration to wlan-switch.com instead of trpz.com.

System Configuration Issues

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)

Client connection to an open SSID on an Auto-DAP can cause "Variable not implemented" message. (22467)

Description If a service profile is configured with SSID type clear, a message such as the following can appear on the WSS console when a client connects to the service profile's SSID on an Auto-DAP:

APM Oct 10 12:25:37.880782 ERROR AP_CONFIG_ERR: type(CIPHER), reason: Variable not implemented

Description This issue is cosmetic only and occurs only if the AP the user connects to received its configuration from a WSS's Auto-DAP profile, the service profile type is clear, and the fallthru authentication type is web-portal or a static WEP key is configured on the service profile.

DAP or VLAN creation commands fail when entered at the CLI, but are reported as successful. (25409)

Description If a large number of DAP or VLAN creation commands are entered at the CLI in a short amount of time, as with a script, WSS Software may return messages for some of the commands that indicate the operation was successful, when actually it was not. This problem occurs very rarely.

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 another due to the way some router redundancy protocols handle MAC addresses. If this issue occurs, log messages appear periodically on the seed WSS indicating that member WSSs are entering or leaving the Mobility Domain.

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

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

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

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

Description If an IP tunnel exists between clients in a VLAN that is configured for Layer 2 traffic restrictions, traffic between the clients on the remote switch will not be blocked. This is because the Layer 2 traffic restrictions are not present on the remote switch.

Workaround Ensure the VLAN is configured with Layer 2 traffic restrictions on all switches that require connectivity to that VLAN. Additionally, use location policy rules to block roaming of these clients to any switches that should not tunnel this traffic.

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

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.

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

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

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

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

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

WLAN Management Software Issues

Deleting PEAP-MS-CHAP-V2 AAA methods in an 802.1X policy with WLAN Management Software 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 switch might still use the removed method. For example, if the 802.1X policy contains the following methods, and you use WLAN Management Software to remove method *sg3*, the WSS continues to use *sg3:*

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

Workaround To restore the intended configuration, restart the switch.

CLI Issues

Port group names containing dashes prevent port groups from being listed by the show port-group command. (23874)

Description WSS Software allows you to use a dash or hyphen (-) in a port group name. However, if you configure a port group name that contains a dash or hyphen, no port groups are listed by the **show port-group** command.

Workaround Do not use dashes or hyphens in port group names.

Web View Issues

Unless otherwise noted, the workaround for Web View issues is to use the CLI or WLAN Management Software.

Web View does not require a username. (16799)

Description To log into Web View on a WSS, you must enter the switch's enable password as the password, but no username is required or supported.

Workaround To increase security, disable Web View and require administrators to log in to the CLI or use WLAN Management Software. To disable Web View access, use the **set ip https server disable** command. If WLAN Management Software is used, make sure access to the WLAN Management Software client and WLAN Management Software Services is secured by configuring account names and passwords on each.

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

Cannot add or configure AP-262 using Web View. (17749)

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

In Web View, self-signed certificate for network user is not accepted with only a Common Name value. (15651)

Description If you use Web View to configure a self-signed certificate for network users, the switch does not generate the certificate if you enter information only in the Common Name field and not in other fields. This issue does not affect the CLI. In the CLI, you can generate a self-signed certificate with only the common name specified.

Workaround Use the CLI to generate the certificate or use the additional fields in Web View.

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.

KVM over IP product caused 2360 to crash. (31106)

Description A KVM over IP product, the Raritan Dominion KX-216, was found to be sending malformed packets to the broadcast address of the network. When a 2360 encountered such packets, it stopped responding.

AAA and RADIUS Issues

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 wildcard, 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 2300 System Software 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.

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

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

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

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.

Encryption Issues

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

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

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

ACL Issues

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

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

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

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

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)

IGMP Snooping and IP Multicast Issues

IP multicast streams can stop for all receivers on an AP if IGMP snooping is disabled. (15971)

Description If you disable IGMP snooping, all clients that are receiving a multicast group stream through an AP stop receiving the stream if one of the clients leaves the group.

Workaround Do not disable IGMP snooping. (The feature is enabled by default.)

Invalid IP multicast forwarded. (12784)

Description IGMP multicast streams with an invalid source IP address (for example, 0.0.0.0) are forwarded by the WSS.

Workaround None.

Documentation Errata

New boot failover mechanism is not described. (20479)

Description The new boot failover mechanism added in WSS Software Version 4.1 is not described in the 4.1 manuals. However, it is described in these release notes. (See "New Boot Failover Mechanism" on page 12.)

Clarifications on CLI quickstart command. (21217)

Description If you select the CLI **quickstart** option to generate an EAP key, the key does not take effect until you restart the switch.

Clarification on Valid Length of State Name in Certificate Requests. (22548)

Description The 4.1 manuals state that the string length for specifying the State Name in certificate requests is 2 characters. This is incorrect. In WSS Software Version 4.1, the maximum string length for State Name is increased from two to 64 alphanumeric characters. Spaces are allowed in the string.

Clarification on enabling shared-key authentication. (23882, 24484, 24661)

Description Shared-key authentication is supported only for encrypted SSIDs. In addition, if you enable shared-key authentication, RSN, WPA, TKIP, and CCMP must be disabled. By default, RSN, WPA, and CCMP are already disabled, but TKIP is enabled; you must manually disable TKIP. (TKIP is not automatically disabled when WPA is disabled.) To disable TKIP, use the **set service-profile cipher-tkip disable** command.

Clarification on display of the login page in Web-based AAA (Web-Portal). (24125)

Description When a Web-based AAA client first tries to access a web page, the client's browser sends a DNS request to obtain the IP address mapped to the domain name requested by the client's browser. The WSS proxies this DNS request to the network's DNS server, then proxies the reply back to the client. If the DNS server has a record for the requested URL, the request is successful and the WSS serves a web login page to the client. However, if the DNS request is unsuccessful, the WSS displays a message informing the user of this and does not serve the login page.

If the WSS does not receive a reply to a client's DNS request, the WSS spoofs a reply to the browser by sending the WSS's own IP address as the resolution to the browser's DNS query. The WSS also serves the web login page. This behavior simplifies use of the Web-based AAA feature in networks that do not have a DNS server. However, if the requested URL is invalid, the behavior gives the appearance that the requested URL is valid, since the browser receives a login page. Moreover, the browser might cache a mapping of the invalid URL to the WSS IP address.

If the user enters an IP address, most browsers attempt to contact the IP address directly without using DNS. Some browsers even interpret numeric strings as IP addresses (in decimal notation) if a valid address could be formed by adding dots (dotted decimal notation). For example, 208194225132 would be interpreted as a valid IP address, when converted to 208.194.225.132.

Clarification on the CLI idle timeout. (25365, 25366, 25770)

Description The 4.1 manuals state that a change to the CLI session idle timeout (**set system idle-timeout** command) affects existing sessions as well as new sessions started after the command is entered. This is incorrect. The command applies only to new sessions started after the command is entered.

The timeout interval is in 30-second increments. For example, the interval can be 0, or 30 seconds, or 60 seconds, or 90 seconds, and so on. If you enter an interval that is not divisible by 30, the CLI rounds up to the next 30-second increment. For example, if you enter 31, the CLI rounds up to 60.

Default setting for AP-WSS security is optional. (25696)

Description In the *Nortel WLAN 2300 System Software Configuration Guide*, the introductory paragraph of the "Configuring AP-WSS Security" section in the "Configuring AP Access Points" chapter states that "AP-WSS security is disabled by default.". This should say "AP-WSS security is set to **optional** by default.". The description of the default is correct in other manuals.

Clarification on configuring VoIP for SVP. (26269)

Description ACLs can be used to give voice packets high priority on a radio interface by setting CoS. The *Nortel WLAN 2300 System Software Configuration Guide* states that the ACL used to set CoS for SVP traffic must be applied to the outbound traffic direction of the voice VLAN. This is correct. However, CoS will not be marked in the traffic if the path to the SVP handset is over a tunnel. WSS Software does not support mapping an ACL to a tunneled VLAN. (When configured in a Mobility Domain, WSSs dynamically create tunnels to bridge clients to non-local VLANs. A non-local VLAN is a VLAN that is not configured on the WSS that is forwarding the client's traffic. WSS Software does not support mapping an ACL to a non-local VLAN. The CLI accepts the configuration command but the command is not saved in the configuration.)

Consider switch-1 with VLAN_A and switch-2 with VLAN_B. If a handset connected to switch-2 is placed in VLAN_A, a tunnel is created between switch-1 and switch-2. If an ACL is mapped to VLAN_A-out on switch-1, it will affect local clients but not clients using the same VLAN on switch-2. Also, if an ACL is mapped to VLAN_A-in on switch-1, it will affect remote clients on switch-2, but not local clients. Nortel recommends mapping ACLs both vlan-in and vlan-out to ensure proper CoS marking in both directions.

Clarification on show security acl commands. (26819)

Description The manuals do not correctly describe the **show security acl** and **show security acl info** commands. Instead, they incorrectly state that the **show security acl** command lists the committed ACLs.

To display ACLs, use the following commands:

show security acl editbuffer

show security acl info all editbuffer

show security acl info

show security acl

Use the first two commands to display the ACLs that you have not yet committed to nonvolatile storage. The first command lists the ACLs by name. The second command shows the ACLs in detail.

Use the **show security acl info** command to display ACLs that are already committed. ACLs are not available for mapping until you commit them. (To commit an ACL, use the **commit security acl** command.)

ACLs do not take effect until you map them to something (a user, Distributed AP, VLAN, port, or virtual port). To display the mapped ACLs, use the **show security acl** command, without the **editbuffer** or **info** option.

Correction to descriptions of set radio-profile frag-threshold, set radio-profile long-retry, and set radio-profile short-retry commands. (26863)

Description The descriptions of these commands in the manuals is incorrect.

- **set radio-profile frag-threshold**—The manuals state that this command specifies the maximum length a frame is allowed to be without being broken into multiple frames before transmission. This is incorrect. Nortel APs do not support fragmentation upon transmission, only upon reception. The **set radio-profile frag-threshold** command actually sets the threshold at which the long-retry-count is applicable instead of the short-retry-count.
- **set radio-profile long-retry**—The manuals state that this command specifies the number of times a radio can send a long unicast frame without receiving an acknowledgment. This is correct. However, the manuals also define a long unicast frame as a frame that is equal to or longer than the Request-to-Send (RTS) threshold. This is incorrect. A long unicast frame in this case is actually a frame that is equal to or longer than the frag-threshold.
- **set radio-profile short-retry**—The manuals state that this command specifies the number of times a radio can send a short unicast frame without receiving an acknowledgment. This is correct. However, the manuals also define a short unicast frame as a frame that is shorter than the Request-to-Send (RTS) threshold. This is incorrect. A short unicast frame in this case is actually a frame that is shorter than the frag-threshold.

Note. The frag-threshold does not change the RTS threshold, which specifies the maximum length a frame can be before the radio uses the RTS/CTS method to send the frame. To change the RTS threshold, use the **set radio-profile rts-threshold** command instead. (The description of this command in the manuals is correct.)

Clarification on RF detection operation when a Mobility Domain is not fully operational. (27250)

Description RF Detection requires the Mobility Domain to be completely up. If a Mobility Domain is not fully operational (not all members are up), no new RF Detection data is processed. Existing RF Detection information ages out normally. Processing of RF Detection data is resumed only when all members of the Mobility Domain are up. If a seed switch in the Mobility Domain cannot resume full operation, you can restore the Mobility Domain to full operation, and therefore resume RF Detection data processing, by removing the inoperative switch from the member list on the seed.

Setting speed of gigabit port to “auto” is not applicable. (27758)

Workaround WSS Software allows the port speed of a gigabit port to be set to **auto** (for autonegotiation). However, this setting is invalid. If you set the port speed of a gigabit port to **auto**, the link will stop working.

The show network-domain command's output does not contain a Mobility-Domain field. (28015)

Description The output examples of the **show network-domain** command in the WSS Software manuals include a Mobility-Domain field. This field is not part of the output.

Remote pass-through authentication with local backup is not supported.

Description In the *Nortel WLAN 2300 System Software Configuration Guide*, the "Remote Authentication with Local Backup" section shows a sample configuration using remote pass-through authentication with local authentication as a backup. This is not a valid configuration. As an alternative, you can configure the WSS to use PEAP offload with local authentication as a backup.

Correction to key sequence for entering the boot prompt.

Description The "Troubleshooting a WSS" appendix in the *Nortel WLAN 2300 System Software Configuration Guide* states that you can press any key while the countdown is occurring during system boot to enter the boot prompt. This is incorrect. You must press **q**, then Enter. However, the manual is correct that you can enter the boot prompt only during the countdown that occurs while the switch is booting.

Correction to show spantree syntax.

Description The *Nortel WLAN 2300 System Software Configuration Guide* and *Nortel WLAN 2300 System Software Command Reference* each show incorrect syntax for the following command:

show spantree [**port** *port-list* | **vlan** *vlan-id*] [**active**]

The syntax shown here is correct. The manuals do not show the **port** keyword.

Corrections to instructions for obtaining and starting Netcat

Description The instructions in the *Nortel WLAN 2300 System Software Configuration Guide* for setting up a snoop observer for traffic snooping have two small errors. The URL for obtaining Netcat should be http://www.vulnwatch.org/netcat/. And in Step 3, the command for starting Netcat on Windows should be as follows: **netcat -l -u -p 37008 -v -v**

The instructions appear in the "Troubleshooting a WSS" chapter, in the "Preparing an Observer and Capturing Traffic" section.

Clarification on configuring Network Domains. (25881)

Description If the seed in a Network Domain is also intended to be a *member* of the Network Domain, you must enter the **set network-domain mode member seed-ip** *ip-addr* command on the seed, with *ip-addr* pointing to the seed itself.

Upgrading from WSS Software Version 4.1 or 4.0

To upgrade a 2350, 2360, or 2380 the switch must be running WSS Software Version 4.0 or later.

Preparing the WSS for the Upgrade

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

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

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

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

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

"Upgrade Scenario" on page 42 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 2300 System Software Configuration Guide*.

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

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

Upgrading an Individual Switch Using the CLI

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

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

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

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

When you restart the WSS switch, 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.

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

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/NT504111.020 boot1:NT504111.020**
.....
.....
.....success: received 74418349 bytes in 106.899
seconds [69615 bytes/sec]

2380# **set boot partition boot1**
success: Boot partition set to boot1:nt504111.020 (4.1.11).

2380# **show boot**
Configured boot version: 4.1.11
Configured boot image: boot1:nt504111.020
Configured boot configuration: file:configuration
Backup boot configuration: file:backup.cfg
Booted version: 4.1.11
Booted image: boot1:nt504105.020
Booted configuration: file:configuration
Product model: 2380

2380# **reset system force**
..... rebooting .....

Migrating your Web-based AAA configuration from WSS software release 4.0 to release 4.1 (23546)

If you upgrade directly from WSS Software Version 4.0 to WSS Software Release 4.1, the Web-based AAA configuration will not work until you manually change some settings. The Web-based AAA implementation was changed in WSS Software Version 4.0. In some cases, a WSS Software Version 4.0 Web-based AAA configuration works without manual changes when you upgrade to WSS Software Version 4.0. However, if you upgrade directly from WSS Software Version 4.0 to 4.1, you will need to perform some changes manually.

For each service profile or wired authentication port that supports Web-based AAA, you must do the following:

- In case the SSID name is not already set in the service profile used for a Web-based AAA SSID, set it now. (The name needs to be set before you change the fallthru authentication type.)
- Change the fallthru authentication type to **web-portal**.

  In WSS Software Version 4.0, the default fallthru authentication type for service profiles is **none**. The default was changed to **none** in WSS Software Version 4.0. In addition, the option name **web-auth** was changed to **web-portal** in WSS Software Version 4.0. During upgrade from WSS Software Version 4.0 to 4.0, **web-auth** is automatically changed to **web-portal**. However, during an upgrade directly from WSS Software Version 4.0 to 4.1, the deprecated **web-auth** option is not recognized, so any instances of this fallthru value are set to the default, **none**.
- In the Web-Portal implementation of Web-based AAA, users are placed in a *portal* while they are being authenticated, under the username **web-portal-***ssid* or **web-portal-wired**, where *ssid* is the SSID or **wired** indicates the user is on a wired authentication port. If they are not created automatically when you change the fallthru authentication type to **web-portal**, create a **web-portal-***ssid* or **web-portal-wired** user.
- The **web-portal-***ssid* or **web-portal-wired** user has two required attributes: VLAN-Name and Filter-ID. VLAN-Name must be set to the VLAN you want to place the user on after authentication and authorization, and is the same VLAN the user is on while in the portal. If WSS Software creates the user automatically, the VLAN-Name is set to *default*. To use a different VLAN, you must edit the user entry.

  The Filter-ID must be set to *portalacl.in*. The *portalacl* ACL is automatically created by WSS Software when you set the fallthru authentication type of any SSID or wired authentication port to **web-portal**. The *portalacl* ACL controls user traffic while a user is in the portal, and must be applied to the inbound traffic direction for the user. The ACL ensures that while in the portal, users can send and receive DHCP traffic but other traffic is captured by the WSS.
- The user's VLAN must be statically configured on the switch where the user will first access the network (where the other configuration items described above are located). An IP interface must also be configured on this VLAN.

For more information, including configuration examples, see the "Configuring Web Portal Web-based AAA" section in the "Configuring AAA for Network Users" chapter of the *Nortel WLAN 2300 System Software 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

Issues Resolved Since Version 4.1.13

Session information updated with an IP address based on requests coming from httpd. (32948)

ARP cache is populated by incoming DNS queries (32947)

100 byte memory leak occurred when logging in through web portal. (32946)

Fortress client would not function with WMM enabled. (32819)

Description With WMM enabled, the client could not key exchange with the Fortress gateway controller due to an issue with header information.

Version checking is incorporated to prevent non-supported WSS upgrade/downgrade. (32630)

Phase 2 diagnostics correctly indicate fan operation and Xicor EEPROM memory error messages. (32328)

Corrupt packets from APs can cause the AP manage code in netsys to crash. (32152)

AP channel for 802.11a is disabled for use in France. (31710)

WSS 2360/2361 failed to reboot after upgrading to 4.1.13. (31537)

Web-portal redirected browser requests to non-browsable pages resulting in partial SSL negotiation. (31147)

Loading the web portal login page in the browser kept SSL sockets open for up to 90 seconds limiting the number of authentications available in a given amount of time. (31145)

WSS reset with core memory dump when configuring Direct Connect AP with no PoE port available in WMS. (30829)

Reduced traffic throughput on channel 1 when using 802.11g setting. (29896)

Changed DFS global sheet for Buglaria, Hong Kong, Mexico, New Zealand, Peru, and Saudi Arabia. (33363)

Some country codes missing from WSS. (33978)

CLI command to set ap-download-values is not hidden. (33423)

DFS is enabled in Hong Kong for non-DFS channels. (33926)

Issues Resolved Since Version 4.1.11

The WSS was sending duplicate RF detect traps over brief intervals. (26209)

In a mobility domain where all the WSSs but one were upgraded to the latest software release, spurious packets from the WSS that was not upgraded may have caused other WSSs in the mobility domain to restart and produce a core file. (27826)

During a WPA or WPA2 4-way handshake, the AP was incorrectly setting the transmission packet number (PN) value to 0, instead of the PN value of 1 specified in the 802.11i standard. This caused the first packet sent following the handshake to be either lost or retransmitted. (28018)

WSS crashed when encountering corrupt TAPA packets or AP port mismatch. (28194)

Description The WSS restarted and produced a core file when one of the following events occurred:

- Invalid or corrupt TAPA packets were received from an AP
- An AP port mismatch was encountered when the WSS retrieved statistics from the AP's second radio.

Instead of restarting and producing a core file, the WSS now logs an error message when either of these events occur.

In a network where a number of third-party APs were installed, a corrupt packet entering the system may have caused the WSS to restart. (28616)

Clients using the Intel 3945ABG wireless NIC were unable to connect reliably to the network. (28863)

Description Some client laptops using the Intel 3945ABG adapter card were not able to connect reliably to the network. This was due to the client ignoring the initial GKHS message sent by the WSS, timing out, and deassociating before the WSS could retransmit the GKHS message.

Workaround Set the 802.1X supplicant timeout to 1 second. To do this, use the **set dot1x timeout supplicant** command.

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

APs were booting and immediately crashing, or were booting and then crashing shortly afterwards. (28915)

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

WSS crashed as a result of EAPOL deleting information cached by the RADIUS client to handle outstanding authentication requests. (29518, 28546)

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

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

Deploying changes from WLAN Management Software to a WSS caused the WSS to produce a core file. (29773)

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

Packets of invalid data length caused the WSS to crash. (30243)

Invalid 802.11 association request packets encountered by a WSS prevented wireless clients from authenticating. (30504)

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

Issues Resolved Since Version 4.0.22

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

Description The switch supports packets of up to 1500 bytes. In the current release, the WSS no longer

restarts if it receives an EAP packet that is longer. Instead, the WSS silently drops the packet.

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

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

WSS did not renew IP address of a Distributed AP with the same address. (27484, 27667)

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

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

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

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

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

A WSS could restart when a Proxim a/b/g client NIC configured for dynamic WEP attempted to connect to an AP radio. (24625)

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

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

In WLAN Management Software, the incorrect AP boot loader version was displayed in the Bootloader field of the Access Points tab. (25622)

Incorrect fingerprint propagation from a Mobility Domain seed WSS to member WSSs generated alert messages identifying non-existent rogues in the network. (25672)

The output of the "show rfdetect data" CLI command displayed devices that were legitimately on the network as interfering devices. (25721)

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

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

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

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

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

Invalid SNMP packets could cause SNMP to stop working on the switch, requiring a switch restart to restart SNMP. (26173)

Entering the show tech-support command from multiple Telnet sessions could cause the switch to restart. (26481)

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

Description In previous WSS Software versions, the **show spantree** and **show spantree port** commands showed *Disabled* in the STP-State or Port-State column to indicate any of the following conditions:

- The port is inactive.
- The port is disabled.
- STP is enabled on the port but the port is not forwarding traffic. (The port is active and enabled but STP has just started to come up.)
- STP is disabled on the port.

In WSS Software Version 4.0.22, *Disabled* can still mean any of the first three conditions listed above. However, if STP is disabled on the port, *STP Off* is shown instead. The **show config area spantree** output also is enhanced. It now lists **set spantree disable port** *port-list vlan-id* commands for ports on which STP is disabled, and **set spantree enable port** *port-list vlan-id* commands for ports on which STP is enabled.

A WSS managing around 100 Distributed APs or more could restart when receiving service profile changes from WLAN Management Software. (26852)

Entering the following CLI command caused the WSS to restart and produce a core file: set port type ap *num* model *model* poe enable radiotype. (27214)

In WLAN Management Software, after using the drop-ship method to configure a WSS, the switch's WSS Software version number was not being displayed in the Version field of the Managed Devices tab. (27234)

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

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

Intel PRO/Wireless 2915ABG cards could not see or associate with 802.11a channels in countries where DFS is required. (20114)

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

Description This issue could occur if authentication using a RADIUS server took more than about 5 seconds. WSS Software would wait for 5 seconds, then serve the unsuccessful login page. If authentication was successful but took longer than 5 seconds, the client actually did get a session on the network despite receiving the login unsuccessful page. In the current WSS Software version, the timer has been increased to 10 seconds.

Roaming from a third-party AP back to a Nortel AP did not work. (24865)

Rogue detection report failed after a short interval. (25053)

Description A symptom of this issue was log messages such as the following:

AUTORF_ERROR: Cannot update rssi for uninitialized neighbor

Login attempt for Web Portal user took longer than usual when the user was attempting to log on outside of the start-date and end-date specified for the user. (25487)

Queues on the WSS for AP management packets could become overrun during configuration for multiple APs with large numbers of clients (around 255), causing the WSS to restart and produce a core file. (25841, 25845)

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

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

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

Description WSS Software started accounting when a web-portal-*ssid* user associated with an AP, but then sent an update message rather than a start message when the authenticated user's session began. Also, WSS Software sent a stop message when the user roamed. In the current WSS Software version, WSS Software starts accounting when a Web-Portal user is authenticated (when the session for the username starts) and sends a stop message only when the user's session ends. WSS Software continues sending accounting updates for sessions that roam. Accounting messages will not be sent while the session is in the unauthenticated Web-Portal state (while the session for the web-portal-*ssid* username is still active).

A Web-based AAA client with proxy enabled in the browser could not access the login page. (21550, 21812)

An internal error could occur during processing of egress ACLs. (23429, 24399)

Description A symptom of this issue was log messages such as the following:

ASO Jan 11 08:43:25.124116 ERROR nos_npms_cb: NP_NPMS_EXCEPTION_NOTIFICATION

ASO Jan 11 08:43:25.124249 ERROR wr_npms_exception: Exception: Msg="Stack overflow error", cnt=1,value=0x80000000

Web Portal redirection of user to requested URL sometimes did not work, and an incorrect redirect URL ending in .crl was listed on the redirect message page. (24667)

Distributed APs were not responding correctly to redundant bias settings. (25281)

During an IP ping, WSS Software reflected an 802.1p-tagged BPDU back to the sender, which could appear to the sender to indicate a network loop. (25467)

RF Auto-Tuning could change a radio's channel even if clients had active sessions on the radio. (24250)

Description In WSS Software Version 4.1.11, WSS Software does not change the channel if the radio has active sessions. If the radio does not have any active sessions, WSS Software uses the parameters described in the *Nortel WLAN 2300 System Software Configuration Guide* to determine whether to change the channel. (See the "Channel Tuning" section in the "Configuring RF Auto-Tuning" chapter.)

If a RADIUS server and server group had the same name, the WSS restarted when an administrative user attempted to log in. (18434)

Radar detection (DFS) holddown could go into effect when radar was not present. (23104)

2380 could stop working if traffic from a Distributed AP was corrupted but had a valid checksum. (23422)

Description This issue also caused "IP Checksum Error" messages to appear in the system log.

WSS Software rejected authentication if the RADIUS server returned Service-Type value Callback Framed. (23764)

Description In the current version, WSS Software will quietly accept Callback Framed instead of rejecting authentication. However, you cannot select this access type in WSS Software.

Certificates larger than 4096 bytes could not be imported into the switch. (24232)

Description Attempting to import a certificate larger than 4096 bytes did not work and resulted in the following error message: Maximum certificate size exceeded. In WSS Software Version 4.0.22, the maximum certificate size the switch can import has been increased to 5120 bytes.

SSIDs with 32-character long names could be configured but could not be accessed by clients. (24345)

Failed DNS lookup on WSS where DNS was not configured could cause a WSS to restart. (24373)

802.1X clients stopped when trying to associate with a 32-character SSID name. (24575)

Authentication failed for Web-Portal users whose passwords contained = (equal sign) or @ (at sign). (24628)

Issues Resolved Since Version 4.0.20

ACL hits were not displayed for ACLS mapped only to users. (15686)

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

Note. This issue does not occur in a Mobility Domain with switches running WSS Software 4.0 and WSS Software 4.1.

The web login page could take up to 60 seconds to be displayed for Web-based AAA users on wired authentication ports. (20323)

Setting AP-WSS security to required or optional limited the number of Distributed APs the WSS could boot and manage. (20425)

Web Quick Start added an hour to system time if Daylight Savings Time was selected. (20491)

AP management traffic from a 2380 to an AP was not remarked for priority. (20704)

Online help listed unimplemented command: test mobility-domain show. (20748)

Mobility Domain names could not be longer than 16 characters. (23690)

Description In WSS Software Version 4.1, Mobility Domain names can be up to 32 characters long.