Part No. NN47250-400 (320659-G)
December 2007

4655 Great America Parkway
Santa Clara, CA 95054

Nortel WLAN - Security Switch 2300 Series Release Notes – Software Release 6.0

* 3 2 0 6 5 9 - G *

NORTEL

Copyright © 2007 Nortel Networks. All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks reserves the right to make changes to the products described in this document without notice.

Nortel Networks does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

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.

Regulatory information

Global changes in Release 6.0

WSS/ WMS Global	The following countries are not supported by Nortel: • Belize (BZ) • Macedonia (MK) • Bosnia & Herzegovina (BA)
Outdoor 2330A	Created new outdoor antennas for the 2330A: 2.4 GHz band (24113-OUT, 24123-OUT, 24143-OUT, 24883-OUT, 24993-OUT) 5 GHz bands (5643-OUT, 5133-OUT).
Outdoor 2330A	Created new antennas for the 2.4 GHz & 5.0 GHz bands for the NEMA enclosure (-NEMA, -NEMA-10 & -NEMA-25).
2330A	Enabled operation for Greece, Italy, Latvia, Spain & France for the 24113 & 24123 antennas.
2330A	Disabled operation in the US for the 5250 - 5350 MHz band for the 5643 -OUT, -OUT-10, & -OUT-25 and 5133 -OUT, -OUT-10, & -OUT-25 antennas.
Series 2332	Added the (16) new regional locked APs: 2332-A1, 2332-A2, 2332-A3, 2332-A4, 2332-A5, 2332-A6, 2332-E1, 2332-E2, 2332-E3, 2332-E4, 2332-E5, 2332-E6, 2332-E7, 2332-E8, 2332-E9, and 2332-J1.
COUNTRY	**ASIA PACIFIC**
Hong Kong	Disabled DFS in the 5.25 - 5.35 GHz band. It is NOT required. Restricted operation in the 5.15 - 5.35 GHz band to indoors only per HK rules.
India	Enabled operation on the 5725 - 5850 MHz band per recent approval. Outdoor operation is limited to the 2.4 GHz band. All 5 GHz bands are indoor only operation.
Malaysia	Enabled operation on CH 165 for 2330/2330A.
Thailand	Limited operation in the 2.4 GHz band to indoors only per the rules.
Taiwan	Updated 24113 & 24123 operation for 802.11b & 802.11g to operate up through CH 11. It only used to work up to CH 7. Updated 5.25 GHz band to be indoors only per SRD rules.
Vietnam	Updated outdoor operation as follows: • Enabled operation for "indoors only" for the 5.15 to 5.25 GHz band. • Enabled operation in the 5.25 to 5.35 GHz and 5.725 to 5.85 GHz (5 CH) bands.
COUNTRY	**CALA**
Guam	Added Guam to 2332-A1. Follows FCC rules.
US Virgin Islands	Added US Virgin Islands to 2332-A1. Follows FCC rules.

COUNTRY	**EU & EUROPE**
EU & EFTA	Disabled 5250 - 5350 & 5470 - 5725 GHz bands on 2332-E1 to be compliant to EN 301-893 v1.3.1 by March 31, 2008.
Greece	Modified 802.11b/g settings for Outdoor Operation.
Spain	Modified 802.11b/g settings for Outdoor Operation.
Ukraine	Updated outdoor operation for 2.4 GHz and 5.0 GHz bands.
COUNTRY	**MIDDLE EAST & AFRICA**
Bahrain	Updated Outdoor parameters per country requirements. Enabled DFS for Bahrain in the 5.25 - 5.35 GHz band.
Egypt	Restricted operation in the 802.11b/g 2.4 GHz band to indoor only. Outdoor operation requires NTRA approval. Restricted use in 5725 -5850 MHz to "indoor only". Outdoor operation requires NTRA approval/license.
Jordan	Modified operation in the 2.4 GHz and 5.15 - 5.25 GHz bands for indoor operation only.
Kuwait	Enabled operation for 2.4 GHz based on EU. Operation is limited to indoor use only. Enabled 5 GHz operation in the 5150 - 5250 & 5250 -5350 MHz band for indoors only.
Lebanon	Enabled outdoor operation for 802.11b/g in the 2.4 GHz band. Enabled operation in the 5.725 - 5.85 GHz band for both indoor and outdoor. Added technical operating parameters for the 5.0 GHz band on all antenna tabs.
Mauritius	Added all 2.4 GHz and 5.0 GHz operating parameters on all antenna tabs. Follows the EN 300-328 & 301-893 ETSI standards. DFS is required in the 5.25 - 5.35 GHz & 5.470 - 5.725 GHz bands. Updated Outdoor operation per local rules.
Morocco	Enabled outdoor operation for 802.11b/g in the 2.4 GHz band for Channels 8 - 13. Operation on Channels 1 - 7 is allowed indoors only. Enabled operation in the 5.15 - 5.25 GHz band for indoor only.
Nigeria	Updated operation in the 2.4 GHz band to follow the EU rules. Operation is allowed in the 5725 - 5850 MHz band, but requires DFS so it is currently disabled.
Oman	Changed 2.4 GHz operation to allow for outdoor use. Restricted use on 5150 - 5350 MHz to "indoor only". DFS is required in the 5250 - 5350 & 5470 -5725 MHz bands. Disabled operation in the 5725 - 5850 MHz band because it is restricted to outdoor only operation and requires DFS.
Qatar	Changed 2.4 GHz operation from 13 to 11 channels and allowed outdoor use. DFS required for this country in the 5752 - 5850 MHz band (4 CHs). 5.0 GHz operation is currently disabled.

Series 2332 Access Points Region Lock Mechanism

A regional regulatory lock function has been implemented in the Series 2332 access points to manage the various worldwide operating channels and country approval requirements. The regional lock function contains sixteen (16) regions that are grouped by their operating frequency channels for both the 2.4 GHz and 5.0 GHz 802.11a/b/g bands for indoor operation. The following is a current list of the proposed regions:

Region Name	Regions	Operating Bands
[Models]		
US Based	**US Based**	**US Based**
2332-A4	11 : 1, 2, 4, 7	2.4 : 5.1, 5.2, 5.4, 5.7
2332-A3	11 : 1, 2, 7	2.4 : 5.1, 5.2, 5.7
2332-A1	11 : 1, 7	2.4 : 5.1, 5.7
2332-A2	11 : 2, 7	2.4 : 5.2, 5.7
2332-A5	11 : 7	2.4 : 5.7
2332-A6	11 : NO 5	2.4 : NO 5.0 GHz
EU Based	**EU Based**	**EU Based**
2332-E4	13 : 1, 2, 4, 7	2.4 : 5.1, 5.2, 5.4, 5.7
2332-E1	13 : 1, 2, 4	2.4 : 5.1, 5.2, 5.4
2332-E3	13 : 1, 2, 7	2.4 : 5.1, 5.2, 5.7
2332-E2	13 : 1, 2	2.4 : 5.1, 5.2
2332-E5	13 : 1, 7	2.4 : 5.1, 5.7
2332-E6	13 : 2, 7	2.4 : 5.2, 5.7
2332-E7	13 : 1	2.4 : 5.1
2332-E8	13 : 7	2.4 : 5.7
2332-E9	13 : NO 5	2.4 : NO 5.0 GHz
Specials	**Specials**	**Specials**
2332-J1	14 : 1, 2	2.4 : 5.1, 5.2

IEEE 802.11a/b/g Channel Designations:

2400 - 2483.5 MHz band

IEEE Mode	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**
Channel Number	1	2	3	4	5	6	7	8	9	10	11
Frequency [GHz]	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462
IEEE Mode	11b/g	11b/g	11b/g								
Channel Number	12	13	14								
Frequency [GHz]	2.467	2.472	2.484								

Legend:

- 11: Channels 1 through 11, inclusive (US Based)
- 13: Channels 1 through 13, inclusive (EU Based)
- 14: Channels 1 through 14, inclusive (Japan Based)

5.15 - 5.35 GHz bands

IEEE Mode	11a	11a	11a	11a	11a	11a	11a	11a
Channel Number	36	40	44	48	52	56	60	64
Frequency [GHz]	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320

5.470 - 5.725 GHz bands

IEEE Mode	11a	11a	11a	11a	11a	11a	11a	11a	11a	11a	11a
Channel Number	100	104	108	112	116	120	124	128	132	136	140
Frequency [GHz]	5.500	5.520	5.540	5.60	5.580	5.600	5.620	5.640	5.660	5.680	5.700

5.725 - 5.85 GHz bands

IEEE Mode	11a	11a	11a	11a	11a
Channel Number	149	153	157	161	165
Frequency [GHz]	5.745	5.765	5.785	5.805	5.825

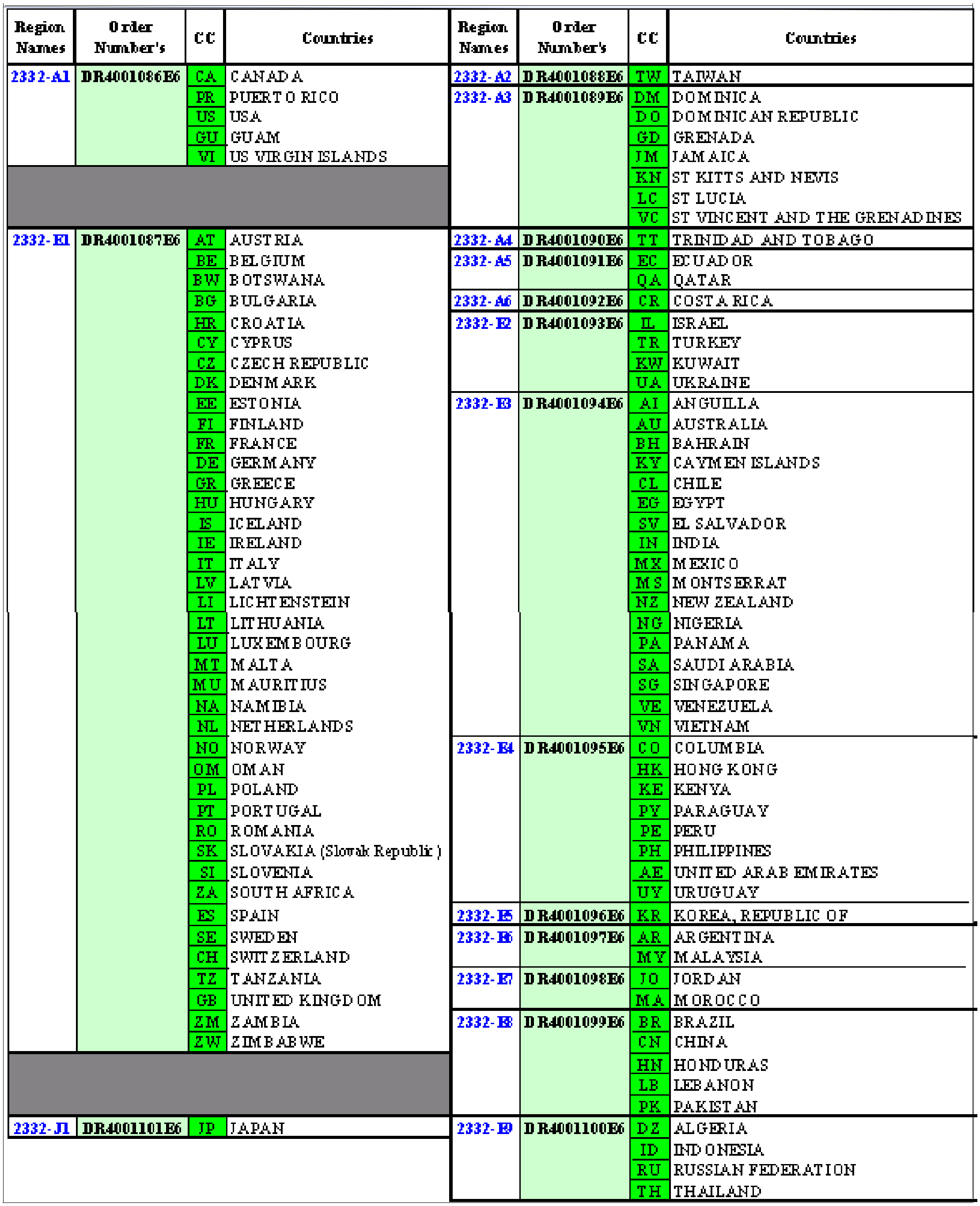
Legend:

- 1: Channels 36, 40, 44 & 48
- 2: Channels 52, 56, 60 & 64
- 4: Channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
- 7: Channels 149, 153, 157, 161, 165
- All combinations, such as 1, 2, 7 represent all of the channels listed in the separate sections of 1, 2 and 7: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165

The two base Series 2332 Access Points are the 2332-A1 and the 2332-E1. Their operating channels are listed below for reference:

2332-A1:	2.4 GHz band (802.11b/g):	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
	5.0 GHz bands (802.11a):	36, 40, 44, 48, 149, 153, 157, 161, 165
2332-E1:	2.4 GHz band (802.11b/g):	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
	5.0 GHz bands (802.11a):	36, 40, 44, 48

Series 2332 Access Points Country to Region Map



Region Names	Order Number's	CC	Countries
2332-A1	DR4001086E6	CA	CANADA
		PR	PUERTO RICO
		US	USA
		GU	GUAM
		VI	US VIRGIN ISLANDS
2332-E1	DR4001087E6	AT	AUSTRIA
		BE	BELGIUM
		BW	BOTSWANA
		BG	BULGARIA
		HR	CROATIA
		CY	CYPRUS
		CZ	CZECH REPUBLIC
		DK	DENMARK
		EE	ESTONIA
		FI	FINLAND
		FR	FRANCE
		DE	GERMANY
		GR	GREECE
		HU	HUNGARY
		IS	ICELAND
		IE	IRELAND
		IT	ITALY
		LV	LATVIA
		LI	LICHTENSTEIN
		LT	LITHUANIA
		LU	LUXEMBOURG
		MT	MALTA
		MU	MAURITIUS
		NA	NAMIBIA
		NL	NETHERLANDS
		NO	NORWAY
		OM	OMAN
		PL	POLAND
		PT	PORTUGAL
		RO	ROMANIA
		SK	SLOVAKIA (Slovak Republic)
		SI	SLOVENIA
		ZA	SOUTH AFRICA
		ES	SPAIN
		SE	SWEDEN
		CH	SWITZERLAND
		TZ	TANZANIA
		GB	UNITED KINGDOM
		ZM	ZAMBIA
		ZW	ZIMBABWE
2332-J1	DR4001101E6	JP	JAPAN
2332-A2	DR4001088E6	TW	TAIWAN
2332-A3	DR4001089E6	DM	DOMINICA
		DO	DOMINICAN REPUBLIC
		GD	GRENADA
		JM	JAMAICA
		KN	ST KITTS AND NEVIS
		LC	ST LUCIA
		VC	ST VINCENT AND THE GRENADINES
2332-A4	DR4001090E6	TT	TRINIDAD AND TOBAGO
2332-A5	DR4001091E6	EC	ECUADOR
		QA	QATAR
2332-A6	DR4001092E6	CR	COSTA RICA
2332-E2	DR4001093E6	IL	ISRAEL
		TR	TURKEY
		KW	KUWAIT
		UA	UKRAINE
2332-E3	DR4001094E6	AI	ANGUILLA
		AU	AUSTRALIA
		BH	BAHRAIN
		KY	CAYMEN ISLANDS
		CL	CHILE
		EG	EGYPT
		SV	EL SALVADOR
		IN	INDIA
		MX	MEXICO
		MS	MONTSERRAT
		NZ	NEW ZEALAND
		NG	NIGERIA
		PA	PANAMA
		SA	SAUDI ARABIA
		SG	SINGAPORE
		VE	VENEZUELA
		VN	VIETNAM
2332-E4	DR4001095E6	CO	COLUMBIA
		HK	HONG KONG
		KE	KENYA
		PY	PARAGUAY
		PE	PERU
		PH	PHILIPPINES
		AE	UNITED ARAB EMIRATES
		UY	URUGUAY
2332-E5	DR4001096E6	KR	KOREA, REPUBLIC OF
2332-E6	DR4001097E6	AR	ARGENTINA
		MY	MALAYSIA
2332-E7	DR4001098E6	JO	JORDAN
		MA	MOROCCO
2332-E8	DR4001099E6	BR	BRAZIL
		CN	CHINA
		HN	HONDURAS
		LB	LEBANON
		PK	PAKISTAN
2332-E9	DR4001100E6	DZ	ALGERIA
		ID	INDONESIA
		RU	RUSSIAN FEDERATION
		TH	THAILAND

For more information on the ‘Regulatory Information”, go to nortel website: http://www.nortel.com/support.

See the following:

- Approved Countries for the WLAN Security Switches 2300 Series and 2330-2330A-2330B Access Points.
- Approved Countries for the WLAN Security Switches 2300 Series and Series 2332 Access Points.
- Approved 5.0 GHz Antennas for the WLAN 2330/2330A/2330B Access Points.
- Approved 2.4 GHz Antennas for the WLAN 2330/2330A/2330B Access Points.
- Approved 5.0 GHz Antennas for the WLAN Series 2332 Access Points.
- Approved 2.4 GHz Antennas for the WLAN Series 2332 Access Points.

Nortel WLAN - Security Switch 2300 Series Release Notes – Software Release 6.0

Nortel recommends that you familiarize yourself with the "Best practices and common issues" section in this document before installing WLAN Security Switch Software (WSS Software) Version 6.0. For additional product information, refer to the following manuals in addition to these release notes:

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

What's new in WSS Software version 6.0

Nortel WSS 2382 switch is introduced.

WSS 6.0 version contains the following enhancements:

- RF Load Balancing
- Mesh Services

- Local Switching
- Wireless Bridging
- Licensing by Feature
- Enforceable Beacon Data Rate Control
- Logout for Web Authentication
- WSS Seed Redundancy
- Password Management

RF Load Balancing

RF load balancing is the ability to reduce network congestion over an area by distributing client sessions across the AP (access points) with overlapping coverage in the area.

Mesh Services

WLAN mesh services allows an AP to provide wireless services to clients, without a wired interface on the AP. Instead of a wired interface, there is a radio link to another AP with a wired interface.

Local Switching

It allows packets to be switched directly from the AP to the wired network.

Wireless Bridging

It allows you to use WLAN mesh services in a wireless bridge configuration, implementing APs as bridge endpoints in a transparent Layer 2 bridge.

Licensing by Feature

Installing license keys allows you to unlock WSS Software features on an as-needed basis.

Enforceable Beacon Data Rate Control

It helps you to completely prevent clients from transmitting at disabled data rates.

Logout for Web Authentication

Configure the Web Portal web-based AAA to allow a user to manually terminate the session. When this feature is enabled, the Web Portal web-based AAA user is successfully authenticated and redirected to the requested page, a window appears behind the user browser. The window has a button labeled “Logout”. When you click Logout, a URL appears and terminates the user session on the Mobility Domain.

WSS Seed Redundancy

on specifying a secondary seed in a Mobility Domain, it provides redundancy for the primary seed switch in the Mobility Domain. If the primary seed becomes unavailable, then the secondary seed assumes the role of the seed switch. This allows the Mobility Domain to continue functioning, if the primary seed becomes unavailable.

Password Management

It has control over handling passwords when users are authenticated on WSS.

For more information on the above features, see “Nortel WLAN - Security Switch Configuration Guide” and “Nortel WLAN - Management Software Reference Guide”.

Nortel WSS 2382 Switch

The 2382 switch provides high-bandwidth centralized control of many indirectly connected access points. It contains two gigabit Ethernet ports and has two 100-240V VAC autosensing AC power supplies.

Version compatibility

WLAN Management System

This version of WLAN Security Switch Software (WSS Software) is intended for use with WLAN Management System Version 6.0 or higher.

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 6.0. If your switch is running an older WSS Software version, you can use the upgrade path to upgrade the switch to 6.0.

Table 1. Software Requirements for Upgrade to WSS Software Version 6.0

Product	Minimum WSS Software Version Required	Upgrade Path
2350	4.0.10	4.0.x -> 5.0.x -> 6.0.x *4.1.x -> 5.0.x -> 6.0.x*
2360/2361	4.0.*20*	4.0.x -> 5.0.x -> 6.0.x 4.1.x -> 5.0.x -> 6.0.x
2380	4.0.10	4.0.x -> 5.0.x -> 6.0.x *4.1.x -> 5.0.x -> 6.0.x*

Table 1. Software Requirements for Upgrade to WSS Software Version 6.0 (continued)

Product	Minimum WSS Software Version Required	Upgrade Path
2382	6.0.4.6	N/A

➡ **Note.** You must upgrade to WSS Release 5.0 or later before upgrading to WSS Release 6.0.

Best practices and common issues

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

Best practice when powering down a switch

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

System configuration best practices

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

Client and Web-based AAA best practices

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

Get clients and Web-based AAA working first

The greatest majority of installation issues are related to clients and web-based 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 web-based AAA server you plan to use. Working out client and web-based AAA configuration methods first provides valuable information as you scale the deployment.

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

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

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

Driver dependant behavior

- Some clients prefer a beaconed clear SSID to their configured SSIDs. If you configure WSS Software to beacon a clear SSID, some client adapters prefer this beaconed SSID over the SSIDs they are configured to use. Conversely, some adapters can associate only with a beaconed SSID. Determine whether to beacon the clear SSID based on the types of clients in the network.

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

802.1X clients

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

Windows XP

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

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

  www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx
- Installing Windows XP Service Pack 2 is recommended for all wireless clients as it includes several important hotfixes.
- If you are not prepared to install Service Pack 2, Nortel strongly recommends that all wireless clients use Service Pack 1a with the following hotfixes installed:
  - KB826942—This is the WPA Hotfix Rollup and is available through Microsoft Update
  - KB834669—This corrects an 802.1X client issue which can cause system instability problems in Windows XP. You will need to contact Microsoft directly for this hotfix.
- If your network uses logon scripts, Active Directory group policies, or your users regularly share their laptops, you should enable computer authentication (also known as machine authentication) to achieve full functionality over your wireless connection.
- Download current drivers for your NICs from the NIC vendor(s).
- If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, Nortel recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. Nortel strongly recommends that you update the driver manually using the driver properties in the Network control panel instead of installing the client manager.
- If you use computer authentication with different VLANs for the Computer and User accounts and do not have the WPA hotfix rollup (KB826942) or Service Pack 2, you need to install Microsoft hotfix KB822596. Otherwise, DHCP will not operate correctly after the user authenticates. You must contact Microsoft technical support for this hotfix. It is not available from their website. For more information on computer authentication, see "Computer authentication" (page 22).

- If MD5 challenge is configured on a Windows XP client for wired authentication, Nortel recommends that you set the quiet period to 5 to allow successful authentication. In addition, if the authentication is carried out manually, the timeout value must be set to no less than 30 seconds in order to allow the user ample time to enter their username and password. For example, to configure 802.1X on a WSS to allow these users time to log in, type the following commands:

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

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

Windows 2000

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

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

  www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx
- Installing Windows 2000 Service Pack 4 is required for all wireless clients.
- Some clients might experience system instability when using PEAP-MS-CHAP-V2 in an Active Directory environment. The primary symptom of this is a message displayed after login informing the user that the service svchost.exe has stopped unexpectedly. If you experience this problem, please contact Microsoft technical support and request hotfix KB833865.
- If your network uses logon scripts, Active Directory group policies, or your users regularly share their laptops, Nortel recommends that you enable computer authentication to achieve full functionality over your wireless connection.
- Download current drivers for your NICs from the NIC vendor(s).
- Windows 2000 does not include a full implementation of the Wireless Zero-Config service from Windows XP, so you will need to use the client manager software provided with your NIC to configure your SSID and enable WEP encryption. When using dynamic WEP in Windows 2000, select *static WEP 128bit* and enter any static WEP key as a placeholder. This temporary key configures the driver to use WEP to encrypt packets, and the Microsoft 802.1X client then overrides the static WEP key you entered with a dynamic key after you authenticate successfully.
- If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, Nortel recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. If you are unable to install the client manager without the AEGIS component, contact the driver manufacturer or download an earlier version that does not contain the AEGIS component.
- 16-bit PCMCIA and built-in NICs (some 802.11b cards in Dell, Toshiba, and other manufacturers' laptop PCs) might require a registry setting to be changed before they will be able to associate with any SSID. Microsoft Knowledge Base article 327947 documents the changes necessary to resolve the problem. Multi-band cards (A/B or A/B/G) are generally 32-bit and do not experience this problem.
- If you use computer authentication with different VLANs for the Computer and User accounts, you need to install Microsoft hotfix KB822596. Otherwise, DHCP will not operate correctly after the user authenticates. You must contact Microsoft technical support for this hotfix. It is not available from their website. For more information on computer authentication, see "Computer authentication" (page 22).

- If you experience a delay in receiving your DHCP IP address wirelessly while using 802.1X authentication, you might need to install Microsoft hotfix KB829116. You must contact Microsoft technical support for this hotfix. It is not available from their website.

Funk Odyssey

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

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

Macintosh OS/X

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

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

Computer authentication

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

Table 3. Microsoft networking features that require computer authentication

Feature	Scenario Requiring Computer Authentication
Systems management agents	Systems management application agents such as those that come with Microsoft Systems Management Server (SMS) frequently need network access without user intervention.
Remote Desktop Connection	Computers are accessible from Windows Remote Desktop Connection when no one is logged in to windows.
Shared folders	Files and folders shared from a computer are still available, even when no user is logged in.

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

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

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

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

Computer authentication also requires specific configuration considerations on the WSS:

- The username of a computer authentication connection will be in the form of host/*fully-qualified-domain-name*, for example host/bob-laptop.nrtl.com or host/tac1-laptop.support.nrtl.com. This username is the same regardless of the configured protocol (PEAP-MS-CHAP-V2 or EAP-TLS). An appropriate userglob would be *host/*.domain.com* where domain.com is the Active Directory domain name. Alternatively, in a smaller deployment you could use a userglob of ** and have both user and computer authentication go to the same RADIUS server.

- PEAP-MS-CHAP-V2 offload mode is not supported with computer authentication. You must use pass-through 802.1X authentication policies with computer authentication.

Web-based AAA

Table 4 lists the Web-based 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. Web-based AAA servers tested with Nortel WSS Software

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

Testing notes

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

- Cisco ACS 3.2 or later is required to support PEAP-MS-CHAP-V2

WPA

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

- CCMP (AES 802.11i draft support) is supported only when it is the only encryption type enabled on that SSID. Enabling TKIP or Dynamic WEP on the same SSID with CCMP can cause serious connectivity issues as most clients do not properly support this configuration. Nortel recommends that you create a separate service profile and SSID for WPA/CCMP.
- Enabling TKIP and Dynamic WEP on the same SSID is not recommended. This configuration forces the group key (multicast/broadcast key) to use the lowest common encryption type, in this case Dynamic WEP. Additionally, compatibility with wireless NICs is reduced.
- Downloading the latest drivers for your wireless NIC is strongly recommended. See “802.1X clients” (page 20) for specific information on installing drivers for your operating system.
- When a session key is changed, Microsoft WPA clients can sometimes incorrectly start using the new key before the end of the four-way handshake that is used to establish the key information. This issue can occur when the session timeout for the client session expires. As a result, the AP access point rejects the client’s re-association attempt because the key information presented by the client is invalid. If you experience this issue, clear the Session-Timeout attribute on the affected users. The WSS will not force a reauthentication of WPA/TKIP and WPA/CCMP users periodically like it does with dynamic WEP users.
- Do not use the **set service-profile shared-key-auth** command in a WPA configuration. This command does not enable PSK authentication for WPA. To enable PSK for WPA, use the **set service-profile auth-psk** command.
- Use one WPA authentication method per SSID, either 802.1X authentication or preshared key (PSK) authentication, but not both.

Security—best practice when mixing encrypted access and clear access

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

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

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

Security best practices

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

Certificates

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

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

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

Usernames

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

Passwords

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

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

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

SNMP

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

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

CLI access

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

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

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

Web access

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

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

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

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

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

WLAN Management System

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

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

Guest access (unencrypted SSIDs)

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

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

VLANs

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

Web-based AAA best practices

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

Mobility Domain™ (Multiple WSSs) best practices

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

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

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

Helpful commands

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

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

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

Distributed AP best practice when using STP

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

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

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

Use IGMP snooping effectively

Using IGMP (11909, 12863, 12866)

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

Workaround Apply the following methods to use IGMP snooping effectively:

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

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

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

User ACLs require explicit source and destination addresses

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

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

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

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

IPv6 support

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

VoIP devices vendor support

These are the Nortel supported options:

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

System parameter support

Table 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.
APs per WSS	• 2382: 320 configured, 128 active • 2380: 300 configured, 120 active • 2360/2361: 30 configured, 12 active • 2350: 8 configured, 3 active Includes directly attached APs and Distributed APs. Inactive configurations are backups.
Minimum link speed within a Mobility Domain	128 Kbps

Table 6. Network parameters

Parameter	Supported Value
Forwarding database entries	• 2382: 8192 • 2380: 16383 • 2360/2361: 8192 • 2350: 8192
Statically configured VLANs	128
Virtual ports (sum of all statically configured VLAN physical port memberships)	256
Spanning trees (STP/PVST+ instances)	64
ACLs and Location Policies	• ACEs per switch • 2382: 2308 • 2380: 2308 • 2360/2361: 700 • 2350: 700 • ACEs per ACL: • 2382: 267 • 2380: 267 • 2360/2361: 267 • 2350: 25 • Location Policies per switch: • All models: 1 The Location Policy can have up to 150 rules.
IGMP streams	500 **Note:** Replication of a stream on multiple VLANs counts as a separate stream on each VLAN.

Table 7. Management parameters

Parameter	Supported Value
Maximum instances of WLAN Management System simultaneously managing a network	3
Telnet management sessions	• 2382: 8 • 2380: 8 • 2360/2361: 4 • 2350: 4 **Note:** The maximum combined number of management sessions for Telnet and SSH together is 8 for the 2382, 2380, or 4 for the 2360/2361 and 2350, in any combination.

Table 7. Management parameters (continued)

Parameter	Supported Value
SSHv2 management sessions	• 2382: 8 • 2380: 8 • 2360/2361: 4 • 2350: 4
Telnet client sessions (client for remote login)	• 2382: 8 • 2380: 8 • 2360/2361: 4 • 2350: 4
NTP servers	3
SNMP trap receivers	8
Syslog servers	4
RADIUS servers	100 configured on the switch 10 in a server group 4 server groups in a Web-based 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.
Active Web-based AAA sessions (clients trying to establish active connections) per WSS	• 2382: 3200 • 2380: 2500 • 2360/2361: 300 • 2350: 75 **Note:** These are the suggested maximums. The switch might be able to support even more sessions, but performance or system stability might be affected.
Web-based AAA users configured in local database	• 2382: 999 • 2380: 999 • 2360/2361: 250 • 2350: 250

Interoperability

Wireless NICs tested with Nortel WSS Software

Manufacturer Model	Driver version	Dynamic WEP	Mixed WPA/TKIP with Dynamic WEP	WPA with TKIP	WPA with AES CCMP	WPA2 with TKIP	WPA2 with AES CCMP	Web AAA
3COM 3CRPAG175B	4.1.2.56	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Cisco Air CB21AG-A-K9	2.6	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Cisco Air CB21AG-E-K9	2.6	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Dell 1470	3.100.35.0	Pass	Pass	Pass	Pass	Pass	Pass	Pass
D-Link DWL-AG530	3.00.51031	Pass	Pass	Pass	Pass	-	-	Pass
Intel 2200	9.0.4.17	Pass	Pass	Pass	Pass	-	-	Pass
Intel 2915	9.0.4.17	Pass	Pass	Pass	Pass	-	-	Pass
NetGear WAG511U	3.3.0.1156	Pass	Pass	Pass	Pass	-	-	Pass
NetGear WG311T	3.3.0.1156	Pass	Pass	Pass	Pass	-	-	Pass
Orinoco PC24E-11-FCR	7.64.1.316	Pass	-	-	-	-	-	Pass
Planet WDL-U357	3.1.3.115	Pass				-	-	Pass
Proxim Orinoco 8480-FC	4.1.0.161	Pass						
SMC 2802W	3.0.11.1	-	-	-	-	-	-	Pass
SMC 2532W-AG2	4.1.2.133	Pass	Pass	Pass	Pass	Pass	Pass	Pass

Note. SMC 2532W-AG2 model is available in Q1 2008.

Note. Nortel does not guarantee interoperability with cards and configurations that are not tested.

Known behaviors and issues

In addition to the more common items indicated in "Best practices and common issues" (page 18), the current software version contains the following known behaviors and issues.

If you experience issues with Certificates or Private keys installed on WSS switches after upgrading to newer 5.0 and 6.0 releases. (32833)

Description Affected services may include SSH, Web-portal, PEAP-offload, WebView, and WMS administrative access and/or Domain Security. Error messages relating to this issue include the following:

- HTTPD Aug 14 16:32:13.648823 ERROR HTTPD: SSL connection failure (bad cert?).
- Admin client 145.36.245.51 EAP Aug 14 16:32:14.110502 ERROR EAP_STORE_ERR: No EAP key pair. Cannot do PEAP.

Workaround You can prevent this issue by generating new private keys and any related Certificates prior to upgrading to a newer version of WSS. Third party Certificates must be exempt from this issue provided a new private key was explicitly generated previous to the CSR request generation. If you are unsure whether a new private key was generated before the initial CSR the best course of action may be to request a replacement certificate from your provider using a new private key.

Auto AP command has no effect on Directly connected AP. It is meant for Distributed AP only. (39474)

If local changes are not deployed and WSS software is upgraded, local changes will be lost. (41914)

Uploading one WSS overwrites local switching configuration on other WSS. (38317)

Converting a mobility-domain member to a secondary-switch, the seed switch will see the secondary switch as a member. (39424)

Workaround Reboot the seed switch.

'show rfdetect measures' command may display wrong channel for AP while countermeasuring. (41235)

'show session output' is not updated when roaming between a 3rd party AP and a Nortel AP. (41124)

Mesh Services

The mesh AP attempts to connect to the AP with the lowest radio channel number.(40473)

System configuration issues

The default value for RADIUS "deadtime" shown in the CLI help is incorrect.

Workaround The correct default value is 0.

When upgrading systems with very large configurations, for example, hundreds of APs or hundreds of users, do the following. (41689)

Workaround It may be necessary to save the configuration to a backup file, generate a minimal configuration, perform the update, load the backup configuration from the command line, and then save the configuration.

The set ap <apnum> boot-configuration switch switch-ip cannot be set at the same time. set ap <apnum> boot-configuration switch name <switch-name> dns <ip addr>. The commands overwrite each other when used. (41330)

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)

Switching and port issues

Antenna sensing has been deprecated from system software. The antenna configuration is the authoritative source to enabling external antenna operation on the MP, even if the external antenna isn't actually connected.

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

Description Nortel recommends that you do not configure the mode of an WSS port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although WSS 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 an WSS port in a certain configuration can cause forwarding on the link to stop.Router redundancy protocol on intermediary devices between WSS 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, WSS switches communicating through those intermediary devices might lose communication with each other due to the way some router redundancy protocols handle MAC addresses. If this issue occurs, log messages appear periodically on the seed WSS indicating that member WSS switches 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 WSS switches. 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.

Access Point (AP) issues

Wireless clients connected to directly attached APs may not display as connected in the show system output information. (41792)

If a Series 2332 access point is configured with a transmission power less than 10, wireless clients cannot connect to the AP. (41018)

When connected to the network using an Intel 2100 wireless network card, large file transfers may cause the wireless client to disconnect. (40721)

A distributed AP may not successfully boot if Port 1 of the AP has an operational Ethernet link, but an WSS is unreachable via this data link. All other combinations of power and data connectivity are fully supported. (38807)

Web-based AAA issues

IPv6 clients cannot authenticate using Web Portal. (26291)

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

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

Web View Issues

If you are running Linux Redhat 9 and use Firefox 2.0 to open WebView, the browser may become unresponsive. This behavior is noted on the 2382 and 2380 (40676)

Upgrading to WSS Software version 6.0

Before you upgrade, see “Version compatibility” (page 17). After you verify that the switch is running the minimum WSS Software version required to upgrade to WSS Software Version 6.0, return to this section.

Preparing the WSS for the upgrade

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

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

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

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

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

"Upgrade scenario" (page 40) shows an example use of the **backup** command. For more information about these commands, see the "Backing Up and Restoring the System" section in the "Managing System Files" chapter of the *Nortel WLAN Security Switch 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.

DAP to AP conversion during Upgrade from Release 5.0 to 6.0

The "DAP" configuration is changed to an "AP" configuration when you upgrade from Release 5.0 to 6.0.

For example:

Release 5.0 DAP configuration:

```
set dap 1 serial-id stp1111111 model 2330A
set dap 1 name AP-North
set dap 1 bias low
set dap 1 radio 1 radio-profile RadioProfile-1
set dap 1 radio 2 radio-profile RadioProfile-1 mode enable
```

Release 5.0 DAP configuration converted to Release 6.0 AP Configuration:

```
set ap 1 serial-id stp1111111 model 2330A
set ap 1 name AP-North
set ap 1 bias low
set ap 1 radio 1 radio-profile RadioProfile-1
set ap 1 radio 2 radio-profile RadioProfile-1 mode enable
```

To upgrade a mobility network with “dap” configurations, do the following:

When upgrading from Release 5.0 to 6.0, the “dap” configuration is updated to an “ap” configuration. When using the WMS to install the Release 6.0 image on the WSS, a backup configuration file is created on the WSS as “configuration-bak.5.0”. This backup file is the only way to go back to a “dap” configuration if the WSS software needs to be downgraded to Release 5.0 in future. It is highly recommended that another copy of the configuration is created on the WSS under a different file name. The administrator must store a copy on an external server. There is no method to convert an AP configuration to a DAP configuration when downgrading from Release 6.0 to 5.0 without a backup 5.0 configuration file. All associated AP configurations needs to be reconfigured if backup file is not available to use.

For more information on “Upgrading from WMS Version 5.0.8.1 or 5.0.11.3”, refer “*Nortel WLAN – Management Software 2300 Series Release Notes – Software Release 6.0*”.

Note. After the WSS reboots and is operational, go to WMS and "refresh devices". The WMS server indicates that there are network changes available. These changes are due to the “dap” configurations being converted to “ap” configurations. Accept the network change (**WMS, Devices, Networks Changes**).

Upgrading an individual switch using the CLI

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

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

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

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

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

   reset system [**force**]

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

Upgrade scenario

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

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

```
2360# save configuration
success: configuration saved.

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

2360# copy tftp://10.1.1.107/N6060500.005 boot1: N6060500.005
.........................................................................
.........................................................................
success: received 10266629 bytes in 92.427
seconds [ 111078 bytes/sec]2360# set boot partition boot1
success: Boot partition set to boot1:N6060500.005(6.0.5.0.5).
2360# show boot
Configured boot version: 6.0.5.0.5
Configured boot image: boot1:N6060500.005
Configured boot configuration: file:configuration
Backup boot configuration: file:backup.cfg
Booted version: 6.0.5.0.5
Booted image: boot1: N6060500.005
Booted configuration: file:configuration
Product model: 2360
2360# reset system force
```

To copy the saved running configuration to a backup file:

2382#**copy <running-filename><backup-file>**

Example: copy configuration configuration.bak

To tftp a copy of the configuation.bak file:

2382#**copy <backup-filename>tftp:<tftp server IP>/<backup-filename>**

Example: copy configuration.bak tftp:192.160.160.1/configuration.bak

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.

Downgrade scenario

The WMS can be used to downgrade the WSS switches. After downgrading the WSS to Release 5.0, and that WSS comes back up and is operational, go to WMS and execute the refresh devices (**WMS, Devices, Refresh**). The WMS server will indicate that there are network changes. Undo these network changes and deploy the local changes. The local changes are related to the file “configuration-bak.5.0”. The “ap” configurations in Release 6.0 will not be changed to “dap” configurations when WMS is used to deploy the local changes if the “configuration-bak.5.0” file does not exist upon downgrading. Another Release 5.0 backup configuration can be loaded after the WSS boots back up if there is no backup Release 5.0 configuration available on the WSS.

Migrating your Web-based AAA and Last-Resort configurations from WSS Software version 5.*x* to WSS Software version 6.0

When you upgrade from 5.*x*, the Web-Portal and last-resort configuration is upgraded automatically. WSS Software makes the following configuration changes during upgrade.

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

Web-Portal changes during upgrade

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

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

Last-Resort changes during upgrade

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

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

Considerations when using Third-Party APs (30061)

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

If your 5.*x* configuration already had a service profile with the same name as the SSID of the third-party AP, then the upgrade does not require any additional action. If your 4.*x* configuration did not have a service profile with the same name as the SSID of the third-party AP, then you must create one and set the authentication attributes. In release 6.0, last-resort authentication is always *local*.

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

If you need to downgrade from 6.0 to a 5.x release, the configuration will work properly if it had worked properly in 6.0

Considerations for configuring Mesh Services

WSS Version 6.0 supports five Mesh APs per Mesh Portal and a single Mesh Services link between the Mesh AP and the Mesh Portal. It is also recommended to configure local switching for the Mesh AP.

WSS 2380 and 2382 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 Activation Key upgrade for an WSS 2382 supports an additional 32, 64 or 96 AP's up to the maximum of 128 AP's per WSS 2382

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 and beyond 32 for your Nortel WLAN WSS 2382 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 either the WSS 2380 or 2382 supported AP License Upgrade Kits.

For 2382, to get maximum APs you will have to obtain multiple coupons. Each coupon needs to be activated against their 2382 Serial number. Only the last key is activated from the key activation Website and it will activate the max number of APs on the switch.

When the proper License Activation Key has been obtained, follow the instructions below to enable the WLAN WSS 2380 or 2382 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.

To upgrade an WSS license:

1. Obtain a license coupon for the upgrade from Nortel or your reseller.
2. Establish a management session with the WSS to display the serial number. To use the CLI to display the serial number, type the following command:

```
show version
```

In the following example, the switch serial number is 1234567890:

```
WSS> show version
Wireless Security Switch, Version: 6.0.3.0 QA 98
Copyright (c) 2005 - 2007 Nortel, Inc. All rights reserved.
Build Information: <build#98> REL_6_0_branch 2007-05-15 14:21:00
Model: 2360
Hardware
Mainboard: version 1 ; revision 01 ; FPGA version 8
Serial number STP1W5002M
Flash: 1.0.0 - 0
Kernel: QNX-630
BootLoader: 4.3 / 6.0.7
```

3. Use a Web browser to access the Nortel Networks license server at the following URL:

http://www.globalwaresolutions.com/

4 Type your e-mail address in the E-mail and Confirm E-mail fields.

5 Select your WSS model from the Product Selection list.

6 Type or copy and paste the WSS serial number into the Product Serial Number field, and click OK. The Product Licensing page appears.

7 Type the coupon activation code(s) into the Coupon Code(s) fields and click OK. The Licensing Confirmation page appears, and displays the activation key (also called the license key).

8 Highlight and copy the entire activation key.

9 On the WSS, use the following command at the enable (configuration) level of the CLI to install the activation key:

```
set license activation-key
```

In the following example, an activation key for an additional 96 APs is installed:

```
WSS-2382# set license 3B02-D821-6C19-CE8B-F20E
success: license accepted
```

10 Verify installation of the new license by typing the following command:

```
WSS-2382# show licenses
Feature : 96 additional APs
```

11 Support for the additional APs begins immediately. You do not need to restart the WSS to place the upgrade into effect.

Issues resolved since version 5.0.11.4

Downgrade WSS from V6 to V5 looses AP/DAP configuration. Deploy of local change failed because WSS response contains errors. "Verification" field does not contain error message. The only option left now is Undo local change, thus WSS looses all the dap configuration (43799).

FTP based ACLs which deny traffic will deny all the traffic when mapped to user or SSID (44179).

Workaround Use VLAN or port based ACLs.

DAP-Static-IP: When configuring the IP address on the DAP you cannot leave the gateway field empty. (32583)

Wireless clients connected to WLAN were unable to communicate with other wireless clients, but they could communicate with wired hosts. (41801)

Certain URLs that contain escape characters (of the form %HexHex) are not handled by Web Portal and may result in the client unable to fetch the login page or loss of Web connectivity. Such URLs are known to be generated by applications like Windows Live Messenger. It is recommended that clients do not run such applications before performing Web Authentication. (41477)

When configuring a mesh service profile, Nortel recommended increasing the service-profile retry limit. (40939)

In some instances, when traffic is roaming between WSS, the WSS may not send an accounting "interim" packet. (40743)

PoE compatibility with certain APs was improved.(40150)

In the show dhcp output, VLAN 0 is the subnet used for all APs configured as directly attached ports. (39775)

Static CoS configuration causes the following behavior: (39210)

Static CoS sets a fixed priority for client packets. When static-cos is not enabled, packets are classified and marked based on rules for flow-through CoS. In overlay mode, the WSS marks downstream packets in 802.1p and tunnel DSCP.In local-switching mode, the WSS is passive, and flow-through CoS rules affect downstream 802.1p.

Workaround Static CoS works in both modes on the AP to give wireless priority downstream and to mark packets upstream. In local-switching mode, packets are only marked in 802.1p.

A Mesh AP failed during a WPA 4-way handshake. (39216)

An AP was taking too long to reboot on the network. (38346)

After a power interruption, APs configured for Mesh Services could not reconnect to the network. (39241, 39216)

The WSS requires the CERTIFICATE header for PKCS7 PEM formatted certificates. (39207, 36658)

If the sensor image has been downloaded at least once to a distributed AP since the WSS booted, a new version is not used by the WSS until after reboot. (35084)

An AP would remain in the unconfigured state unless the ap <apnum> time-out setting was configured manually. (38346)

Loading a large configuration on an 2350 caused the WSS to become unresponsive. (37975)

On APs with the country code US, it is recommend to avoid configuring radio 2 for channels 52, 56, pr

60, and 64. Using these channels may cause periodic outages on the wireless network. This will be resolved in the next release of WSS Software. (37134)

A mobile client cannot associate with WSS Software configured for WEBAAA WPA/TKIP encryption and PSK authentication SSID if the PSK is provisioned by WMS 6.0.2.1.0. (37096)

An IP address of 0.0.0.0 was incorrectly processed by arp-request and arp-reply in WSS Software. (36438)

Configuring too many ACLs and ACEs caused the WSS to become unresponsive. (36261)

Rebooting the WSS via CLI command 'reset system' does not generate a 'warm start' trap on system reboot. Instead a 'cold start' trap is sent. (35357)

In WMS, the Disable Auto-Tune task at the Network plan level has confusing wording. (34058)

The views from a previously created floor plan appear in a new floor plan. (33041)

Load Balancing does not work well when a Load Balancing group has a mix of directly attached APs and DAPs. (32931)

On an untethered AP, the force-image-download flag should NOT be set. If it is set, clear it with the set ap <apnum> force-image-download disable command. (32341)

WSS Software sometimes reports that the CPU is idle more than 100% of the time. (32331). When accessing the Web Portal Login page, the SSL socket stays open until you submit the page or the browser closes. (31145)

A 'ping' initiated from a WMM client associated with an AP gets corrupted when the ping packet size is equal to or greater than 561 bytes. (30945)

The source-ip option of the ping command accepts an inappropriate IP address. (30289)

The clear trace command does not work when multiple tracing is enabled. You must use the command clear trace all to stop the process. (29473)

There are upgrade and downgrade issues with 3rd party APs for AAA. (29400)

Directly attached AP-352 stays in reboot loop when WSS Software is upgraded (29320)

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

Attributes not present in “show sessions network verbose” command. (27886)

Login page is not served to Web-Portal client authenticated on tunneled VLAN. (27226)

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

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

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

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

If SODA is enabled but the enforce-check option is disabled, WSS Software does not download the agent to clients with browsers that have proxy enabled. (26213)

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

Occasionally a DAP/VLAN configuration is returned as a successful operation when it did not succeed. (25409)

Converting a Distributed AP with a static IP address into a directly connected AP results in harmless error message. (25563)

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

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

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

In WSS 5.0.10.3, when a DAP updates the IP address, it takes longer to come up due to TAPA Announce timeout. (38693)

The AP crashed after receiving a UDP packet to port 1325. (38676)

When using WebView to monitor the network, the system page and the clients page did not match. (38414)

When using WebView to monitor the network and viewing more than 50 users, you could not click Next or Last. (38303)

The 802.1p QoS bits were not being properly set by the AP for traffic sent to the WSS. (37917)

The 'radio' value was missing from the 'ap/radio' field in the show sessions command. (37758, 37495)

Traces show MAC addresses with all 0's because the encapsulation buffer was not replicated when a packet was replicated, so tunnel encapsulated packets with no tunnel header were flooding the network.(38381)

With port-groups enabled or disabled, network traffic was looping on the network. (38247)

No broadcast flags were advertised on the network and certain clients could not communicate to each other on the same AP. (38114)

When configuring the Web portal and saving the default login page, remove everything between the quotes in the Action value.(38010)

To use PKCS#7 certificates on an WSS, you must enter the CERTIFICATE header for PKCS7 PEM formatted certificates.(37995)

ERROR AP 2 network: IP Checksum Error was occuring on the network when mesh services was enabled. (36650)

An invalid configuration file caused the WSS to become unresponsive and lose the core configuration. (36621)

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

CPU utilization spikes on RBT systems were observed when 'rogue detection' polling is enabled. (32985)

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

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

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

It is possible that, even though the SODA agent has been downloaded and the virtual desktop started,

the browser is redirected to the login page. This could happen if the session was re-established after the SODA agent download. If this happens, exit out of the Virtual Desktop, open the browser and authenticate again. (25754)

An exception occurred when a DAP configured for 802.11a attempted to tune to a 802.11b radio channel. (37896)

Phantom DAP 0 entries showed up in the show dap connection and global commands.(37561)

On an WSS, static IP addresses had higher priority than IP addresses obtained through DHCP. (37326)

An invalid read operation caused the AP to cease responding. (37017)

Users are placed on the wrong VLAN after roaming to a different SSID.(36910)

The new D-Link DWA-642 pre-N adapter was not able to connect to the wireless network. (36694)

Client MAC address was not flushed from the forwarding database (FDB) after the DAP was disconnected. (36460)

DHCP renewal time of DAP was incorrect. (36336)

Multicast traffic was received from a source client, forwarded from an AP to an WSS but never forwarded back to the same AP. Other wireless clients associated to that AP cannot see the traffic.(36286)

An invalid configuration caused the WSS to cease responding. (36261)

STP was not working correctly when an WSS was connected to another WSS via tagged ports. (36072)

After upgrading to WSS 4.1.x, the user cannot enable 802.11a on a AP-252. (35973)

WebAAA tunneling a user to a VLAN on another WSS caused the WSS to cease responding. (35682)

The AP is broadcasting a DHCP REQUEST with every IP address renewal, thus, enabling another DHCP server to send a DHCP NAK which reboots the AP. (35632)

Unexpected errors occurred when a too long or too short packet is transmitted. (35614)

If an AP is powered using DC power, it will not re-establish an Ethernet link after the device it is plugged into is rebooted. (35472)

A DAP with clients on a low bias switch should not automatically move back to the high bias switch when available. (35143)

Rebooting the WSS via CLI command 'reset system' does not generate a 'warm start' trap on system reboot. Instead a 'cold start' trap is sent. (35357)

After executing the show session command, the WSS ceased to function. (35356)

A basic wireless frame header was not updating after decryption. (35321)

After a certain threshold of sessions on a very active VLAN, some users could not obtain IP addresses using DHCP.(35290)

If the sensor image has been downloaded at least once to a DAP since switch boot, a new version is not used by the switch until after reboot. (35084)

Cannot configure and enable a AP-620 in EMEA countries other than Netherlands. (34961)

A very high rate of error messages caused the WSS to become unresponsive. (34077)

A gno-broadcasth flag was applied to broadcasts sent on the wired network. (34470)

WSS was sending IGMP Membership Queries to the wired network when IGMP was disabled. (34429)

The config cores and WPA2 is configured on 2211 handset and does not work when the auto dap feature is enabled. (34436)

When attempting to boot 120 distributed APs, the WSS becomes unstable and causes an error message to be displayed. (34337)

Too many TCP connections caused the packet memory to degrade over time. (34231)

A MAC client needs to manually renew IP address when using DHCP restrict option. (34183)

Fast roaming between APs was not working. The key cache was not referenced by clients and, therefore the pmkid generated was incorrect and never matched any of the pmkids sent by the clients.(34077)

An WSS is unresponsive to telnet/http connections, and a ping command initiated from the WSS CLI fails with an "unable to allocate socket" error. (33881)

You have to reset the WSS to change the System IP Address and generate new Trap PDUs from this address. (33713)

A corrupt EAP instance causes an WSS to become unresponsive and must be rebooted. (33515)

Flooding of unknown destination unicasts to DAPs on the same VLAN seemed cause network problems. There was an issue where TAPA packets from one WSS to one of its DAPs were flooded to another WSS which then encapsulated the packet in another packet TAPA header and flooded it out to the rest of the DAPs. (33228)

Custom Web-AAA pages that worked in Release 4.0 and 4.1 no longer function in release 5.0. (34181)

When booting 120 DAPs, most APs are timing out when ~80Mbps of aggregate traffic is injected.

(34171, 34168)

Issues resolved in version 5.0.9.4

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

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

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

Description Unspecified network events created a core dump file.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Example 1:

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

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

Example 2:

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

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

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

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

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

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

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

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

Workaround Reset the 2360

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

Customized Web-based AAA pages from 4.0 and 4.1 configuration do not work properly in 6.0. (33708)

Description Customized Web-based AAA pages that worked in Release 4.0 and 4.1 no longer function in release 6.0. When enabled in 6.0 the client session is not captured and the client receives an HTTP 404 error message in the browser.

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

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

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

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

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

Issues resolved since version 4.1.13

Web View did not require a username. (16799)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Nortel WLAN - Security Switch 2300 Series Release Notes – Software Release 6.0

WLAN 2300 Series

Release 6.0

Document Number: **NN47250-400**
Document Status: **Standard**
Document Version: **02.02**
Part Code: **320659-G**
Release Date: **December 2007**

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

To provide feedback or to report a problem in this document go to www.nortel.com/documentfeedback.