

Nortel Secure Network Access 2.0 Engineering

# > Nortel Secure Network Access 2.0 802.1X Authentication Technical Configuration Guide

Enterprise Business Solutions Document Date: August 5, 2008 Document Number: NN48500-566 Document Version: 2.0 Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at <u>www.nortel.com</u>.

#### Copyright © 2008 Nortel Networks. All Rights Reserved.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice. Nortel Networks, the Nortel Networks logo and the Globemark are trademarks of Nortel Networks.

# Abstract

This document provides an overview on how to configure the Nortel Secure Network Access Switch to authenticate Wired and Wireless LAN Microsoft Windows workstations using PEAP against the Local Database or Active Directory.

# **Revision Control**

No	Date	Version	Revised by	Remarks
1	07/08/2008	1.0	EBS	Initial draft and first release internally. Approved by PLM
2	08/05/2008	2/0	EBS	PLM approved for external release.

# Table of Contents:

FIGURES:	4
TABLES:	4
DOCUMENT UPDATES:	5
CONVENTIONS:	5
1. OVERVIEW:	6
1.1     TOPOLOGY:       1.2     PRE-REQUISITES:	6 7
2. CONFIGURATION:	9
2.1Nortel Secure Network Access Switch:2.2Ethernet Routing Switch:2.3Nortel Wireless LAN 2300 Controller:2.4Microsoft Windows Server 2003:2.5Microsoft Windows XP Professional:2.6Microsoft Windows Vista:	9 7 1 5 5
3. VERIFICATION:	9
3.1Nortel Secure Network Access Switch:63.2Nortel Ethernet Switch:73.3Nortel Wireless LAN Controller:7	9 0 2
4. APPENDIX:	4
<ul> <li>4.1 Stackable Ethernet Switch Return Attributes:</li></ul>	4 5 6 7
5. SOFTWARE BASELINE:	8
6. REFERENCE DOCUMENTATION:7	9

# Figures:

Figure 2.1.2 – Server Certificate	.11
Figure 2.1.3 – Local User Database	.14
Figure 2.1.4.1 – LDAP and NTLM Servers	21
Figure 2.4 – Active Directory Tree	.46

# Tables:

Table 2.1.6.1 – WlanEAPUsers Return Attributes	. 33
Table 2.1.6.2 – WlanEAPUsers Return Attributes	. 33
Table 4.1 – Stackable Ethernet Switch RADIUS Attributes	.74
Table 4.2 – Modular Ethernet Switch RADIUS Attributes	. 75
Table 4.3 – WLAN 2300 RADIUS Attributes	. 76
Table 4.1 – Example Realms	. 77
Table 5.0 – Software Baseline	. 78
Table 6.0 – Reference Documentation	. 79

# **Document Updates:**

Not Applicable

# **Conventions:**

This section describes the text, image, and command conventions used in this document.

### Symbols:



Tip – Highlights a configuration or technical tip.



Note - Highlights important information to the reader.



Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

### Text:

Bold text indicates emphasis.

*Italic* text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

```
ERS5520-48T# show running-config
```

Output examples from Nortel devices are displayed in a Lucinda Console font:

```
ERS5520-48T# show running-config
```

! Embedded ASCII Configuration Generator Script ! Model = Ethernet Routing Switch 5520-24T-PWR ! Software version = v5.0.0.011 enable configure terminal

# 1. Overview:

This document provides an overview on how to configure the Nortel Secure Network Access Switch to authenticate Wired and Wireless Microsoft Windows XP and Vista workstations using PEAP against the Local User Database or Active Directory.

# 1.1 Topology:

Figure 1.1 shows the topology that will be used in this configuration guide using the following Nortel and Microsoft platforms:



Windows XP SP3 / Vista Workstations

Figure 1.1 – Topology

• The Nortel Secure Network Access Switch will be configured to support PEAP Authentication from the Windows XP and Vista workstations and authenticate the users against the Local User Database or Active Directory using NTLM. Additionally the Nortel Secure Network Access Switch will be configured to assign authenticated Wired and Wireless users to a user VLAN id 40.

- The Nortel Ethernet Routing Switch will be configured to support EAPOL clients and forward RADIUS authentication requests to the Nortel Secure Network Access Switch. Additionally the user VLAN id 40 will be created on the switch which will be dynamically assigned to authenticated wired users using standard IETF RADIUS return attributes from the Nortel Secure Network Access Switch.
- The Nortel WLAN 2300 Controller will be configured to support EAPOL clients and forward RADIUS authentication requests to the Nortel Secure Network Access Switch. Additionally the user VLAN id 40 named USERS1 will be created on the controller which will be dynamically assigned to authenticated users using standard IETF RADIUS return attributes from the Nortel Secure Network Access Switch.
- The Microsoft Windows 2003 Server will be configured with the appropriate Active Directory User and Group objects to support user authentication and group associations. During authentication the Nortel Secure Network Access Switch will perform NTLM user authentication against Active Directory and using LDAP lookup will determine the user's group membership which will determine the VLAN outcome based on compliance state.
- The Microsoft Windows Workstations will be configured to perform Single Sign-On PEAP authentication to the Nortel Ethernet Switch and Nortel WLAN 2300 Controller. Upon successful PEAP authentication the wired and wireless users will be placed into a user VLAN id 40.

This document provides configuration details for Nortel and Microsoft components shown in figure 1.0 but does not address installation of the core Windows operating systems or services such as Active Directory, DHCP, DNS or Certificate Services. These topics are out of the scope of this document and the reader should reference the appropriate vendor documentation.

# **1.2 Pre-Requisites:**

This document makes the following assumptions in regards to the Network Infrastructure, Windows 2003 server, Windows XP workstation and Windows Vista workstations:

- 1. A Windows 2003 Advanced or Enterprise Server is installed with the following:
  - a. Latest service pack and updates installed
  - b. The following services have been installed:
    - i. Active Directory (Domain Controller).
    - ii. Certificate Services (Enterprise Root CA).
    - iii. Domain Name Services (DNS).
    - iv. Dynamic Host Configuration Protocol (DHCP).
    - v. Internet Information Services (IIS).
  - c. A server certificate with public key has been issued from the Enterprise Root CA and has been exported as a PKCS#12 file.
  - d. A CA root certificate has been issued from the Enterprise Root CA and has been exported to a file.
  - e. The server can ping the Nortel Secure Network Access Switch.
- 2. Windows XP / Vista Workstations with the following:
  - a. Latest service pack and updates installed.

- b. The workstation is a member of the Domain.
- c. A CA Root certificate issued from the Enterprise Root CA is installed.
- 3. A core routing switch is in place and has been configured to provide inter-VLAN routing and DHCP forwarding services.

# 2. Configuration:

# 2.1 Nortel Secure Network Access Switch:

This section provides configuration steps required to configure a Nortel Secure Network Access Switch to authenticate clients EAP on a Nortel Ethernet Switch or Nortel WLAN 2300 controller using Protection EAP. For this section the following configuration steps will be performed:

- 1. Base Configuration (<u>Section 2.1.1</u>)
- 2. Certificates (Section 2.1.2)
- 3. Local Authentication (<u>Section 2.1.3</u>)
- 4. Active Directory Authentication (Section 2.1.4)
- 5. RADIUS Server (Section 2.1.5)
- 6. RADIUS Attributes (Section 2.1.6)

### 2.1.1 Base Configuration:

The following baseline configuration will performed on the Secure Network Access Switch:

- IP Addressing The Real, Management and Virtual IP Addresses will be defined.
- DNS DNS Server IP Address and Domain Name will be defined.
- Time The Timezone and NTP Server IP Address will be defined.
- Management The administrator password will be defined and the Browser Based Interface (BBI) enabled.

A baseline configuration may be established on the Secure Network Access Switch with a console connection using the following procedure:

Define the NSNAS base host configuration by issuing the following command on the NSNAS Setup Menu:

-----

[Setup Menu]				
j oi n	- Join an existing cluster			
new	- Initialize host as a new installation			
boot	- Boot menu			
i nfo	- Information menu			
exi t	- Exit [global command, alw	ays available]		
>> Setup# <i>new</i>				
2 Define the f	ollowing parameters:			
Interface IP:	192.168.20.10	The real IP address (RIP) assigned to the NSNAS.		
Network Mask:	255.255.255.0	The network mask assigned to the NSNAS. In this example the NSNAS is deployed in an isolated VI AN but a smaller subpat with fewer		

NSNA 2.0 802.1X Authentication TCG	v2.0 NN48500-566
	address space.
VLAN Tag: 0	Defines the 802.1Q tag used for the physical Ethernet interface. A value of 0 disables 802.1Q tagging.
Two Armed Configuration: no	This example utilizes a one-armed configuration.
Default Gateway: 192.168.20.1	The default gateway on the core used by the NSNAS.
Management IP: 192.168.20.11	Defines the management IP address for the NSNAS.
DNS Server: 192.168.10.5	The IP address of the Windows 2003 Enterprise Server providing DNS services.
Generate SSH Host Keys: <i>yes</i>	Generates a new SSH host keys used for SSH management and communication with SREM.
Enter a password for the "admin" user: <i>admin-password</i>	Enter and confirm the password assigned to the admin user account. The admin user has full access to the NSNAS.
Run NSNAS quick configuration wizard?: <i>yes</i>	Invokes a wizard which creates basic parameters that we will use to provide 802.1X authentication.
NSNAS Portal Virtual IP address: 192.168.20.12	The virtual IP address on the NSNAS used to provide DHCP, DNS and HTTP/HTTPS services to guest users.
NSNAS Domain name: <i>eselab.com</i>	The DNS domain name for the system. For this example the domain name is eselab.com.
Create http to https redirect server: <i>yes</i>	Allows the NSNAS to capture users HTTP sessions and re-direct the browser to the HTTPS portal login page for authentication.
Create default tunnel guard user: no	Local user accounts will not be used in this example.
Create default system account: <i>no</i>	Local host authentication will not be used in this example.
Would you like to enable the Nortel TunnelGuard Desktop Agent? <b>Yes</b>	The TunnelGuard desktop agent will not be required for this example but will be enabled.
Enable secure web based configuration management: <b>yes</b>	The browser based interface (BBI) will be enabled to perform the remaining configuration on the NSNAS.

Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.

# 2.1.2 Certificates:

A Server and CA Root Certificate issued from Windows 2003 Certificate Services will be installed on the Secure Network Access Switch to support PEAP authentication:

- Server Certificate Issued from an Enterprise or Public Certification Authority and is used to secure client credentials during PEAP authentication.
- CA Root Certificate Issued from an Enterprise or Public Certification Authority and is installed on the SNAS and Windows Workstations to verify the validity of all certificates issued from the Certification Authority.

In this example the server and CA root certificates were issued from Microsoft Certificate Services using the Web Enrolment tool and exported to a PKCS#12 file. The Server Certificate was issued with the Common Name (CN) nsnas-vip.eselab.com which resolves to the Virtual IP Address on the Secure Network Access Switch.



Figure 2.1.2 – Server Certificate

Certificates may be defined and installed on the Secure Network Access Switch using the Browser Based Interface with the following procedure:

1 Using the Browser Based Interface (BBI) navigation tree click *Certificates* and then *Add*.

NØRTEL	Nortel S	ecure Netwo	rk Access Sv	vitch		Apply   Diff   Revert	Logout   Help
Monitor Config	Managing: 2.0.0.8 Certific	53 cates				in an	Logged as admin 🔓
- Wizards - Portal Launch + Network + Secure Access Domain	Certificat	es					
+ Cluster - Certificates	Add Ed	it Delete Show	)				
+ Import	D ID	Name	Cert	CA Cert	Key	Key Size	Key Match
+ Export	<b>1</b>	test cert	Yes	Yes	Yes	1024	Yes

NN48500-566

2 Specify a unique name for the server certificate and then click (	Update.
Managing: 2.0.0.53 Certificates	Logged as admin 🖉 🔒
Certificates	
Add New Certificate	
Identifier: 2	
Name: ESELAB-Server	
Warning: New certificates are directly applied to the database.	Update Back
3 Click <i>Add</i> and specify unique a name for the CA root certificate <i>Updat</i> e.	and then click
Managing: 2.0.0.53 Certificates	Logged as admin 🔒
Certificates	
Add New Certificate	
Identifier: 3	
Name: ESELAB-CA	
Warning: New certificates are directly applied to the database.	Update Back
Using the navigation tree click <i>Certificates</i> , <i>Import</i> and then <i>File</i>	e. In the <i>Certificate</i>

Using the navigation tree click *Certificates*, *Import* and then *File*. In the *Certificate* pull-down menu select the server certificate name created in step 2. Click Browse and locate the PKCS#12 server certificate issued from the Certificate Authority. Enter and verify the *Private Key Password* then click *Import*.

NSNA 2.0 802.1X Authentication TCG v2.0	NN48500-566	
Managing: 2.0.0.53 Certificates » Import » File	Logged as admin 🚺	
File		
Certificate: 2 ESELAB-Server Refresh		
The current certificate is Not set, and the current key is Not set.		
Certificate and/or Key File		
File System: O Protocol O Loca	al	
Certificate and/or Key File: C:\Images\ESELAB_Ro	Browse	
Private Key Password (if required)		
Private Key Password:		
Confirm Private Key Password:		
Certificates with multiple keys/certs are not currently supported. The first certificate and key will be	e chosen	
Note that the CA root certificate does not require a <i>Priva</i>	ate Key Password.	
Certificates » Import » File		
File		
Certificate: 3 ESELAB-CA		
The current certificate is Set, and the current key is Not set.		
Certificate and/or Key File		
File System: O Protocol 💿 Lo	ical	
Certificate and/or Key File: C:\Images\ESELAB_	Ro Browse]	
Private Key Password (if required)		
Private Key Password:		
Confirm Private Key Password:		
Certificates with multiple keys/certs are not currently supported. The first certificate and key will	be chosen.	
6 The server and CA root certificates will now be installed Access Switch.	on the Secure Network	

NSNA 2.0 802.1X Authentication TCG			v2.0			NN48500-566	
(	Add Edi	t Delete Show					
	ID	Name	Cert	CA Cert	Key	Key Size	Key Match
	1	test cert	Yes	Yes	Yes	1024	Yes
	2	ESELAB-Server	Yes	No	Yes	1024	Yes
	3	ESELAB-CA	Yes	Yes	No		
Ν	lortel S	ecure Network	ges by clicki Access Sv	ing <i>Apply</i> an vitch	a then Ap	Apply Diff   Revert	Logout   Help
N	Iortel S anaging: 2.0.0.4		ges by clicki Access Sv	ing <i>Apply</i> an vitch		oly Changes.	Logout   Help ged as admin 🖉 🔒
M	Iortel S anaging: 2.0.0.1	ecure Network	des by clicki Access Sv on Changes	ng <i>Apply</i> an vitch	a then Ap	Apply Diff   Revert	Logout   Help ged as admin 🖉 🔒
M A	Iortel S anaging: 2.0.0.4 Apply Pe	ecure Network	ges by clicking of the second	ing <i>Apply</i> an vitch	a then Ap	Apply Diff   Revert Log	Logout   Help ged as admin 🖉 🔒
	Apply Char	ecure Network moing Configurati Applying changes will save	ges by clicki Access Sv on Changes them to the configu	ing <i>Apply</i> an vitch	a then Ap	אַסָּרָשָּׁרָע Changes. אַסָרָשָׁרָ Diff   Revert Log	Logout   Help ged as admin 🖉 🔒

# 2.1.3 Local Authentication:

This section provides details on how to configure the Secure Network Access Switch to authenticate RADIUS access requests against the local database.



Figure 2.1.3 – Local User Database

# 2.1.3.1 Authentication Servers:

A local authentication server will need to be created on the Secure Network Access Switch to authenticate RADIUS access requests from the Nortel Ethernet Switch or Nortel WLAN 2300 Controller against the local user database:

- A local authentication server will be created
- The local authentication server will be added to the authentication order

Local authentication can be enabled and authentication order defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:

# <sup>1</sup> Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA*, *Authentication* and then *Add*.

v2.0

NN48500-566

Logged as admin 🔒

Logged as admin 🔒

#### Managing: 2.0.0.53

Secure Access Domain » AAA » Authentication

#### Authentication

			Secu	re Access Domain: 1 e	selab.com 💌 <u>Refresh</u>		
Add							
	ID	Name	Display Name	Mechanism	Servers Created		
	No authentication servers configured.						

# <sup>2</sup> Specify a Local Server *Name*, *Display Name* and set the Mechanism to *local*. Click *Update*.

#### Managing: 2.0.0.53

Secure Access Domain » AAA » Authentication

### Authentication

#### Add New Authentication Server

Domain:	1
Auth Id:	1 💌
Name:	local
Display Name:	local
Mechanism:	local 💌
Group Authentication Servers:	Available Selected
	Update Back

In the navigation tree click Secure Access Domain, AAA, Authentication and *AuthOrder.* In the Available list highlight the name of the local authentication server and click move. Click Update.

Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.

NA 2.0 802.1X Authentication TCG	v2.0	NN48500-566
Managing: 2.0.0.53 Secure Access Domain » AAA » Authentication »	AuthOrder	Logged as admin 🌌 🕯
AuthOrder		
Secure Access Domain: 1 eselab.com 💌 Refi	resh	
Fallback Order		
A	zailable Selected	

K

# 4 Apply and save the changes by clicking *Apply* and then *Apply Changes*.

Nortel Secure Network Access Switch	Apply   Diff   Revert   Logout   Help		
Managing: <b>2.0.0.53</b>	Logged as admin 🖉 🔒		
Apply Pending Configuration Changes			
Warning: Applying changes will save them to the configuration.			
Apply Changes			
Back			

# 2.1.3.2 AAA Groups:

Two groups will be defined on the Secure Network Access Switch which will be used to separate Wired and Wireless LAN users and determine VLAN membership upon successful authentication. Separate groups are required as the Nortel Ethernet Switch and Nortel WLAN 2300 Controllers require different RADIUS Return Attributes to determine VLAN membership:

• WiredEAPUsers – Authenticated Wired users will be placed into VLAN Id 40.

WlanEAPUsers – Authenticated Wireless users will be placed into VLAN Named USERS1.

Groups can be defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:

1	Using AAA,	g the Bi <i>Group</i>	rowser Based Inter s and then <i>Add</i> .	rface (BBI) na	avigation tree click S	Secure Access Domain
N	lanaging: <b>2.0.</b> Sec	0.53 sure Access	Domain » AAA » Groups			Logged as admin 🔒
C	Groups					
					Secure Access Domain:	1 eselab.com 💌 <u>Refresh</u>
l	Add					
	ID	Name		M	aximum Login Sessions	
				No Groups co	nfigured.	

2 In the *Group Name* field enter the name *WiredEAPUsers* and then click *Update*.

NSNA 2.0 802.1X Authentication TCG	v2.0	NN48500-566

Logged as admin 🔒

Logged as admin 🔒

#### Managing: 2.0.0.53

Secure Access Domain » AAA » Groups

### Groups

Add	New	Group	
-----	-----	-------	--

Group Id:	1		Available Selected
Group Name:	WiredEAPUsers		À .
Maximum Login Sessions:	0	Locations	>>
Maximum Session Length:	31 d 0 h 0 m 0 s	s	
SRS Rule:	<no selection=""> 💌</no>		
MAC Trust Level:	none 💌		Ý
Nortel Health Agent running mode:	continuous 💌		
Enable MAC Registration:	disabled 💌		
Enable User Registration:	disabled 💌		
Enforcement Type:	vlan_filter 💌		
Cache Password Locally:	disabled 💌		
Comments:			
The "runonce" option for Nortel Heal and is not applicable for the Nortel H	th Agent running mode is for browser based aut ealth Desktop Agent	hentication only	Update Back

# 3 In the Group Name field enter the name WlanEAPUsers and then click Update.

### Managing: 2.0.0.53

ps	Groups	AAA	»	Secure Access Domain
----	--------	-----	---	----------------------

# Groups

### Add New Group

Group Id:	2 💌		Available Selected
Group Name:	WlanEAPUsers		A .
Maximum Login Sessions:	0	Locations	>>
Maximum Session Length:	31 d 0 h 0 m 0 s	Locations.	
SRS Rule:	<no selection=""></no>		
MAC Trust Level:	none 💌		Ý
Nortel Health Agent running mode:	continuous 💌		
Enable MAC Registration:	disabled 💌		
Enable User Registration:	disabled 💌		
Enforcement Type:	vlan_filter 💌		
Cache Password Locally:	disabled 💌		
Comments:			
The "runonce" option for Nortel Heal and is not applicable for the Nortel He	th Agent running mode is for browser based auth ealth Desktop Agent	entication only	Update Back
Apply and save the char	nges by clicking Apply and the	n Apply C	hanges.

Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.

NSNA 2.0 802.1X Authentication TCG	v2.0	NN48500-566	-
Nortel Secure Network Access	Switch	Apply   Diff   Revert   Logout   Help	
Managing: 2.0.0.53		Logged as admin 🖉 😭	
Apply Pending Configuration Chan	ges		
Warning: Applying changes will save them to the co	onfiguration.		
Apply Changes			

# 2.1.3.3 Local Users:

Two local users will be created Secure Network Access Switch and assigned to the groups created in <u>Section 2.1.3.2</u>:

Username	Group
wireduser	WiredEAPUsers
wlanuser	WlanEAPUsers

Local users can be created on the Secure Network Access Switch using the Browser Based Interface with the following steps:

Using the Browser Based Interface (BBI) navigation tree click Secure Access Domai AAA, Groups, Authentication, Local, Users then Add.
---

Managing: 2.0.0.53	Logged as admin 🖉 🚦
Secure Access Domain » AAA » An	entication » Local » Users
Users	
	Secure Access Domain: 1 eselab.com 💌 <u>Refresh</u> Auth ID: 1 💌 <u>Refresh</u>
	Prefix: Max: 50 •
	List
Users	
Add Import/Export	
ID Name	Groups
	No matching users

2 In the Name field enter the name wireduser and specify a password. In the Available

Nortel Confidential Information Copyright  ${\ensuremath{\mathbb C}}$  2008 Nortel Networks. All Rights Reserved.

Logged as admin 🔒

### Groups list highlight the group *WiredEAPUsers* and then click *Move*. Click Save User.

#### Managing: 2.0.0.53

Secure Access Domain » AAA » Authentication » Local » Users

#### Users

Nam	e: wireduser	
Passwore	l: *******	
Confirm Passwore	l: *******	
	Available	Selected
Group	WianEAPUsers	WiredEAPUsers

In the *Name* field enter the name *wlanuser* and specify a password. In the Available Groups list highlight the group *WlanEAPUsers* and then click *Move*. Click *Save User*.

#### Managing: 2.0.0.53

Secure Access Domain » AAA » Authentication » Local » Users

Logged as admin 🔒

#### Users

Add Single User   Add Bulk Users Add Single User		
Name: Password: Confirm Password:	wlanuser	
Groups:	Available WiredEAPUsers	Selected
Warning: Users are added immediately to the database. No	apply is required.	Save User Back

### 2.1.4 Active Directory Authentication:

This section provides details on how to configure the Secure Network Access Switch to authenticate RADIUS access requests against Active Directory using NTLM for user authentication and LDAP for group association.

### 2.1.4.1 Authentication Servers:

LDAP and NTLM authentication servers will be created on the Secure Network Access Switch to authenticate RADIUS access requests against Microsoft Active Directory:

- A LDAP authentication server entry will be created which will be used for Active Directory • group association.
- A NTLM authentication server entry will be created which will be used for Active Directory user authentication.
- The NTLM authentication server will be added to the authentication order.



Figure 2.1.4.1 – LDAP and NTLM Servers

-

This section assumes that NTLMv1 is enabled on the Domain Controller. Details for enabling NTLMv1 authentication are provided by the following Microsoft Knowledge Base Article: http://support.microsoft.com/kb/942564.

LDAP and NTLM authentication servers can be created and the authentication order defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:

1	Using the Browser Based Interface (BBI) navigation tree click Sec AAA, Authentication, LDAP and then Add.	ure Access Domain,
М	anaging: 2.0.0.53 Secure Access Domain » AAA » Authentication » LDAP	Logged as admin 🔒

LDAP				
		Secure /	Access Domain: 1 ese	elab.com 💌 <u>Refresh</u>
Add				
ID	Name	Display Name	Mechanism	Servers Created
		No LDAP Authentication servers configu	red.	

v2.0

NN48500-566

Logged as admin 🔒

#### Managing: 2.0.0.53

3

Secure Access Domain » AAA » Authentication

#### Authentication

#### Add New Authentication Server

Domain:	1
Auth Id:	2 •
Name:	w3kserver1-ldap
Display Name:	w3kserver1-ldap
Mechanism:	Idap 💌
Group Authentication Servers:	Available Selected
	Update Back

Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain, AAA, Authentication, LDAP and then LDAP Settings. Enter the following required information then click Update.

Search Base Entry	Assigns the DN (Distinguished Name) of the Active Directory container where the user entries are found. In this example the following DN was used: <i>CN=Users,DC=eselab,DC=com</i> .
	Note: To support both computer and user authentication for the eselab.com domain the searchbase <i>DC=eselab,DC=com</i> should be used.
Group Attribute	Defines the LDAP attribute that contains the name(s) of the group(s) of which a particular user is a member. For Active Directory this value needs to be set to: <i>memberOf</i> .
User Attribute	Defines the LDAP attribute that contains the user names used for authentication of a user in the domain. For Active Directory this value needs to be set to: <i>sAMAccountName</i> .
iSD Bind DN	Points to an entry in the Active Directory server used for authenticating the Nortel Secure Network Access Switch. In this example a user named 'nsnas' was created in Active Directory which requires the following DN to be used: <i>CN=nsnas,CN=Users,DC=eselab,DC=com</i> .
iSD Bind Password	Defines the password assigned to the Active Directory user defined by the iSD Bind DN.
Short Group Format	Specify if the short group format should be enabled or not. This value needs to be set to: <i>Enabled</i> .

NSNA 2.0 802.1X Authentication TCG v2.0 NN48500-566	
Managing: 2.0.0.53 Logged as admin 🖉 🔒 Secure Access Domain » AAA » Authentication » LDAP » LDAP Settings	
LDAP Settings	
Secure Access Domain: 1 eselab.com 💌 Refresh Auth ID: 2 💌 Refresh	
Search Base Entry: ers,DC=eselab,DC=com (example: ou=People,dc=bluetail,dc=com)	
Group Attribute: memberOf	
User Attribute: sAMAccountName	
iSD Bind DN: ers,DC=eselab,DC=com	
iSD Bind Password:	
iSD Bind Password (again):	
Enable LDAPS:	
Server Timeout: 5 (seconds)	
User Preferences: disabled	
Short Group Format:	
Cut Domain from User Name: disabled	
Update	
Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain, 4 AAA, Authentication, LDAP and then Servers. Specify the Active Directory Servers IP — Address and click Update.	
Managing: 2.0.0.53 Secure Access Domain » AAA » Authentication » LDAP » Servers	
Servers	
Add New LDAP Server	
Domain: 1	
Auth Id: 2	
Port: 389	

v2.0

NN48500-566

Ма	anaging: <b>2.0.0.53</b> Secure A	ccess Domain » AAA »	Authentication » NTLM		Logged as admin 🖉 📴
A	uthentica	tion			
			Se	cure Access Domain: 1	eselab.com 💌 <u>Refresh</u>
	Add				
	ID	Name	Display Name	Mechanism	Servers Created
			No NTLM Authentication servers c	onfigured.	
6	Specify a Available Update.	a NTLM Serve e list highlight	r <i>Nam</i> e, <i>Display Name</i> and the LDAP server name cro	set the Mechanis eated in step 2 and	m to <i>NTLM</i> . In the d click <i>Move</i> . Click

Managing: 2.0.0.53	Logged as admin 🔒
Secure Access Domain » AAA » Authentication	

### Authentication

#### Add New Authentication Server

Domain:	1
Auth Id:	3 💌
Name:	w3kserver-ntlm
Display Name:	w3kserver-ntlm
Mechanism:	ntim
Group Authentication Servers:	Available Selected
	Update Back

NN48500-566

Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain,
 AAA, Authentication, NTLM, NTLM Settings. Specify the hostname of the Windows
 Domain Controller then click Update.

Managing: 2.0.0.53	Logged as admin 🖉 💼
Secure Access Domain » AAA » Authentication » NTLM » NTLM Settings	_
Authentication	
Secure Access Domain: 1 eselab.com 💌 Refresh Auth ID: 3 💌 Refresh	
Windows domain controller name: w3kserver1	
	Update

<sup>8</sup> Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *AAA*, *Authentication*, *NTLM*, *Servers* and click *Add*.

Managing: 2.0.0.53	Authoritation - NTLM - Servers	Logged as admin 🌌 🔒
	Authentication » NTLM » Servers	
, a diona o di o d		
	Secure Access Domain: 1 eselab.com	Refresh Auth ID: 3 💌 Refresh
Add		
ID IP Address		Reorder
	No Servers Configured.	
Managing: <b>2.0.0.53</b> Secure Access Domain » AAA »	Authentication » NTLM » Servers	Logged as admin 🖉 🔒
Managing: 2.0.0.53 Secure Access Domain » AAA » Authentication	Authentication » NTLM » Servers	Logged as admin 🖉 🔒
Managing: 2.0.0.53 Secure Access Domain » AAA » Authentication Add New NTLM Server	Authentication » NTLM » Servers	Logged as admin 🖉 🔒
Managing: 2.0.0.53 Secure Access Domain » AAA » Authentication Add New NTLM Server	• Authentication » NTLM » Servers Domain: 1	Logged as admin 🖉 🔒
Managing: 2.0.0.53 Secure Access Domain » AAA » Authentication Add New NTLM Server	Domain: 1 Auth Id: 3	Logged as admin 🖉 🔒
Managing: 2.0.0.53 Secure Access Domain » AAA x Authentication Add New NTLM Server	Domain: 1 Auth Id: 3 IP Address: 192.168.10.5 (for	Logged as admin 2 🔒

Update

# Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain, AAA, Authentication, NTLM and then Join. Specify the Domain Administrator username and password and click Join.

	Managing: <b>2.0.0.5</b> 3 Secure	; Access Domain » AAA » Auther	Logged as admin 🔒			
	Authentication					
	Secure Acces	s Domain: 1 eselab.com	<u>Refresh</u>			
	Domain administrator account: administrator					
	Domain administrator password:					
		Domain administrator	password (again):	*****		
					Join	
1'	The LD Switch.	AP and NTLM serve	ers will now be insta	alled on the Secur	e Network Access	
	Add Edit	Delete				
	D ID	Name	Display Name	Mechanism	Servers Created	
	1	local	local	LOCAL	Not applicable	
	2	w3kserver1-ldap	w3kserver1-Idap	LDAP	Yes	
	3	w3kserver-ntlm	w3kserver-ntlm	NTLM	Yes	
12	In the n 2 <i>AuthOr</i> click <i>m</i>	avigation tree click <i>der.</i> In the <i>Available</i> ove and then <i>Upda</i> t	Secure Access Do e list highlight the r te.	<i>main, AAA, Authe</i> name of the NLTM	<i>ntication</i> and authentication server	
Ma	anaging: <b>2.0.0.53</b> Secure A	ccess Domain » AAA » Authen	tication » AuthOrder		Logged as admin 🔒	
A	uthOrder					
5	Secure Access Domain: 1 eselab.com 💌 Refresh					
F	allback Orde	er				
	Available Selected       2 w3kserver1-ldap     1 local       3 w3kserver-ntlm					

NN48500-566

# 13 Apply and save the changes by clicking *Apply* and then *Apply Changes*.

Nortel Secure Network Access Switch	Apply   Diff   Revert   Logout   Help
Managing: 2.0.0.53	Logged as admin 🖉 🔒
Apply Pending Configuration Changes	
Warning: Applying changes will save them to the configuration.	
Apply Changes	
Back	

# 2.1.4.2 AAA Groups:

Two groups will be defined on the Secure Network Access Switch which will be used to separate Wired and Wireless LAN users and determine VLAN membership upon successful authentication. Separate groups are required as the Nortel Ethernet Switch and Nortel WLAN 2300 Controllers require different RADIUS Return Attributes to determine VLAN membership:

- WiredEAPUsers Authenticated Wired users will be placed into VLAN Id 40.
- WlanEAPUsers Authenticated Wireless users will be placed into VLAN Named USERS1.

Groups can be defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:

1	Using the Browser Based Interface (BBI) navigate <i>AAA</i> , <i>Groups</i> and then <i>Add</i> .	tion tree click Secure Access Domain,
м	Innaning: 2 0 0 52	Logned as admin

Secu	ure Access [	Domain » AAA » Groups		
Groups				
		Secure Acc	cess Domain:	1 eselab.com 💌 Refresh
Add				
ID	Name	Maximum Login	Sessions	
		No Groups configured		

v2.0

Managing: 2.0.0.53

#### Logged as admin 🔒

NN48500-566

Secure Access Domain » AAA » Groups

### Groups

### Add New Group

Group Id:	1		Available Selected
Group Name:	WiredEAPUsers		<b>A</b>
Maximum Login Sessions:	0	Locations	>>
Maximum Session Length:	31 d 0 h 0 m 0 s	Locations.	
SRS Rule:	<no selection=""> 💌</no>		
MAC Trust Level:	none 💌		Y
Nortel Health Agent running mode:	continuous 💌		
Enable MAC Registration:	disabled 💌		
Enable User Registration:	disabled 💌		
Enforcement Type:	vlan_filter 💌		
Cache Password Locally:	disabled 💌		
Comments:			
The "runonce" option for Nortel Heal and is not applicable for the Nortel H	h Agent running mode is for browser base ealth Desktop Agent	ed authentication only	Update Back
In the Group Name field	enter the name WlanEAP	Jsers and then	click <i>Update</i> .

NSNA 2.0 802.1X Authentication TCG	v2.0	NN48500-566	
			C
Managing: 2.0.0.53		Logged as admin 🔒	

Secure Access Domain » AAA » Groups

### Groups

Group Id:	2 💌		Available Selecte
Group Name:	WIanEAPUsers		<b>A</b>
Maximum Login Sessions:	0	Locationa	
Maximum Session Length:	31 d 0 h 0 m 0 s	Locations:	
SRS Rule:	<no selection=""> 💌</no>		
MAC Trust Level:	none 💌		Y
ortel Health Agent running mode:	continuous 💌		
Enable MAC Registration:	disabled 💌		
Enable User Registration:	disabled 💌		
Enforcement Type:	vlan_filter 💌		
Cache Password Locally:	disabled 💌		
Comments: The "runonce" option for Nortel Heal and is not applicable for the Nortel H	th Agent running mode is for browser based aut ealth Desktop Agent	hentication only	Update Back
Comments: The "runonce" option for Nortel Heal and is not applicable for the Nortel H Apply and save the chai	th Agent running mode is for browser based aut ealth Desktop Agent nges by clicking <i>Apply</i> and the	hentication only en <i>Apply C</i>	Update Back
Comments: The "runonce" option for Nortel Heal and is not applicable for the Nortel H Apply and save the char ortel Secure Network	th Agent running mode is for browser based aut ealth Desktop Agent nges by clicking <i>Apply</i> and the Access Switch	hentication only en <i>Apply C</i> Apply (	Update Back Changes.
Comments: The "runonce" option for Nortel Heal and is not applicable for the Nortel H Apply and save the chair ortel Secure Network aging: 2.0.0.53	th Agent running mode is for browser based aut ealth Desktop Agent nges by clicking <i>Apply</i> and the Access Switch	hentication only en <i>Apply C</i> Apply 1	Update Back Changes. Diff   Revert   Logout   Help Logged as admin 🖉
Comments: The "runonce" option for Nortel Heal and is not applicable for the Nortel H Apply and save the char ortel Secure Network aging: 2.0.0.53	th Agent running mode is for browser based aut ealth Desktop Agent nges by clicking <i>Apply</i> and the Access Switch	hentication only en <i>Apply C</i> Apply (	Update Back Changes. Diff   Revert   Logout   Help Logged as admin 👔
Comments: The "runonce" option for Nortel Heal and is not applicable for the Nortel H Apply and save the chai ortel Secure Network aging: 2.0.0.53 oply Pending Configurat	th Agent running mode is for browser based aut ealth Desktop Agent anges by clicking <i>Apply</i> and the Access Switch	hentication only en <i>Apply C</i> Apply 1	Update Back Changes. Diff   Revert   Logout   Help Logged as admin 🏹
Comments: The "runonce" option for Nortel Heal and is not applicable for the Nortel H Apply and save the char ortel Secure Network haging: 2.0.0.53 oply Pending Configurat	th Agent running mode is for browser based aut ealth Desktop Agent nges by clicking <i>Apply</i> and the Access Switch	hentication only en <i>Apply C</i> (Appiy )	Update Back Changes. Diff   Revert   Logout   Help Logged as admin 2
Comments: The "runonce" option for Nortel Heal Apply and save the chain ortel Secure Network haging: 2.0.0.53 Oply Pending Configuration Warning: Applying changes will sav	th Agent running mode is for browser based aut ealth Desktop Agent anges by clicking <i>Apply</i> and the Access Switch tion Changes e them to the configuration.	hentication only en <i>Apply C</i> (Apply 1	Update Back Changes. Diff   Revert   Logout   Help Logged as admin 2

### 2.1.5 RADIUS Server:

Back

The RADIUS server needs to be configured to allow the Secure Network Access Switch to support RADIUS access requests from the Nortel Ethernet Switch and Nortel WLAN 2300 Controller:

- 1. Certificates The Server and Root CA Certificates created in <u>Section 2.1.2</u> will be selected for use with EAP-TLS and PEAP authentication.
- Clients The Ethernet Routing Switch 5500 and WLAN 2300 Controller will be defined as RADIUS clients.

• Realms – A realm will be defined to direct authentication requests to the Secure Network Access Switch local authentication server.

RADIUS Server configuration can be defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:

Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain
 then RADIUS Server. In the Server Certificate and Server CA Certificate pull-down menus select the certificate added in section 2.1.2. Click Update.

Managing: 2.0.0.53 Secure Access Domain » RADIUS Server	Logged as admin 🔒
RADIUS Server	
	Secure Access Domain: 1 eselab.com 💽 <u>Refresh</u>
Authentication Port:	1812
Accounting Port:	1813
Server Certificate:	2 ESELAB-Server
Server CA Certificate:	3 ESELAB-CA
	Update

### <sup>2</sup> Using the Browser Based Interface (BBI) navigation tree click *Secure Access Domain*, *RADIUS Server* then *Client*. Click *Add*.

Client		
		Secure Access Domain: 1 eselab.com 💌 Refrest
Add		
ID	IP Address	Shared Secret
		No Radius Clients Configured.

NSNA 2.0 802.1X Authentication TCG	v2.0	NN48500-566	
Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Client		Logged as admin 🔒	
Client			
Add Radius Client			
Domai	n: 1		
Client IP Addres	ss: 192.168.10.10		
Shared Secre			
		Update	
5 Enter the IP Address and Shared Secre	et of the WLAN 230	00 Controller. Click <i>Update</i> .	
Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Client		Logged as admin 🔒	
Client			
Add Radius Client			
Domai Client IP Addres	n: 1		
Shared Secret	et: sharedsecret		
		Update Back	
6 RADIUS client entries for the Ethernet created.	Switch and WLAN	2300 Controllers will now be	•
Add Insert Delete			
D ID IP Address	Shared S	ecret	
<ul> <li>1 192.168.10.10</li> <li>2 192.168.10.22</li> </ul>	eselab eselab		
The Shared Secret defined on the Se Client must match the Shared Secret the client or authentication will fail.	cure Network Acce defined on the RAI	ss Switch for the RADIUS DIUS Server configuration on	
7 Using the Browser Based Interface (BE RADIUS Server then Realms. Click Ad	3I) navigation tree Id.	click Secure Access Domair	Ι,
Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Realms		Logged as admin 🖉 🔒	
Realms			
	Secure Access	Domain: 1 eselab.com 💌 Refresh	
Add			
ID Name	lms configured	Authentication server ID	
NO Rea	inna coningureu.		

Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.

NN48500-566

Local Authentication – In the Name field 8 down menu select the name of the local 2.1.3.1 then click <i>Update</i> .	type <i>local</i> . In the <i>Authentication Server</i> pull- authentication server created in section
Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Realms Realms	Logged as admin 🖉 🔒
Add RADIUS Proxy Realm	
Domain: Name: Authentication Server:	1 local 1 local 💌
Active Directory Authentication – In the 9 Directory Domain <i>ESELAB</i> . In the <i>Authe</i> name of the NTLM authentication server	Name field type enter the name of the Active <i>ntication Server</i> pull-down menu select the created in section 2.1.4.1 then click <i>Update</i> .
Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Realms	Logged as admin 🔒
Realms	
Add RADIUS Proxy Realm	
Domain:	1
Name:	ESELAB
Autonucation Server.	Update



Additional details on Realms may be located in the Appendix in Section 5.

# 10 Apply and save the changes by clicking *Apply* and then *Apply Changes*.



# 2.1.6 RADIUS Attributes:

RADIUS return attributes will be assigned to the Wired and WLAN User groups to determine VLAN membership upon successful client authentication:

Attribute Name	Vendor-ID	Attribute-ID	Attribute-Value
Tunnel-Type	0	64	13
Tunnel-Medium-Type	0	65	6
Tunnel-Private-Group-ID	0	81	40

### Table 2.1.6.1 – WlanEAPUsers Return Attributes

Attribute Name	Vendor-ID	Attribute-ID	Attribute-Value
VLAN-Name	562	231	USERS1

Table 2.1.6.2 – WlanEAPUsers Return Attributes

A full list of supported	d attributes for the Nortel Et	thernet Switch ar	nd Nortel WL	AN 2300
Controllers is provide	d in the Appendix.			

RADIUS Attributes can be defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:

1 Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain, AAA, Groups then RADIUS Attributes. In the Group pull-down menu select the group

Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.

SNA 2.0 802.1X Authentication TCG	v2.0	NN48500-566	
WiredEAPUsers and click Add.			
Managing: <b>2.0.0.53</b> Secure Access Domain » AAA » Groups » RAI	DIUS Attributes	Logged as admin 🔒	
RADIUS Attributes			
Secure Access Domain: 1 eselab.com 💌 <u>R</u>	efresh Group: 1 WiredEAPUse	rs Refresh	
Add Id Vendor Id	Attribute Id	Attribute Value	
In the Vendor Id list select $0 - L$	Default. In the Attribute lo	d field enter 64. In the Attribute	е
Value field enter 13. Click Creat	e RADIUS Attribute.		
Managing: 2.0.0.53 Secure Access Domain » AAA » Groups » RAI	DIUS Attributes	Logged as admin 🌌 🔒	
RADIUS Attributes			
Add RADIUS Attribute			
	0 - Default 4 - Unix Vendor Id: 5 - Acc		
	9 - Cisco 11 - HP	-	
	9 - Cisco 11 - HP Attribute Id: 64	×	

Create RADIUS Attribute

2	In the Vendor Id list select 0 – Default. In the Attribute Id field enter 65. In the Attribute
3	Value field enter 6. Click Create RADIUS Attribute.

v2.0

NN48500-566

Logged as admin Ma

Logged as admin 🖉 🔒

Managing: 2.0.0.53

Secure Access Domain » AAA » Groups » RADIUS Attributes

#### **RADIUS Attributes**

#### Add RADIUS Attribute

Vendor Id:	0 - Default 4 - Unix 5 - Acc 9 - Cisco 11 - HP
Attribute Id:	65
Attribute Value:	6
	Create RADIUS Attribute Back

<sup>4</sup> In the Vendor Id list select 0 – Default. In the Attribute Id field enter 81 In the Attribute Value field enter the VLAN ID 40. Click Create RADIUS Attribute.

#### Managing: 2.0.0.53

Secure Access Domain » AAA » Groups » RADIUS Attributes

#### **RADIUS Attributes**

#### Add RADIUS Attribute

Vendor Id:	0 - Default 4 - Unix 5 - Acc 9 - Cisco 11 - HP
Attribute Id:	81
Attribute Value:	40
	Create RADIUS Attribute Back

# <sup>5</sup> RADIUS attributes will now be assigned to the WiredEAPUsers group which will assign authenticated users to VLAN 40.

Add Insert Delete			
🗌 Id	Vendor Id	Attribute Id	Attribute Value
1	0	64	13
2	0	65	6
3	0	81	40

### 6 Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain, AAA, Groups then RADIUS Attributes. In the Group pull-down menu select the group

Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.
			0
NSNA 2.0 802.1X Authentication TCG	v2.0	NN48500-566	
WlanEAPUsers and click Add			
Managing: <b>2.0.0.53</b> Secure Access Domain » AAA » Groups » R	ADIUS Attributes	Logged as admin 🔒	
RADIUS Attributes			
Secure Access Domain: 1 eselab.com	Refresh Group: 2 WlanEAPU	Jsers Refresh	
Add			
Id Vendor Id	Attribute Id	Attribute Value	
	No RADIUS Attributes configured.		
7 In the Vendor Id list select 562 <i>Attribute Value</i> field enter the	2 – Nortel. In the Attribu VLAN name Users1. C	<i>ute Id</i> field select 231. In the lick <i>Create RADIUS Attribute</i> .	
Managing: 2.0.0.53 Secure Access Domain » AAA » Groups » R	ADIUS Attributes	Logged as admin 🔒	
RADIUS Attributes			
Add RADIUS Attribute			
	429 - USR 539 - Accend 562 - Nortel 762 - Karlivet 800 - Xylan		
	Attribute Id: 231 💌		
At	tribute Value: Users1		
		Create RADIUS Attribute Back	
8 RADIUS attributes will now be assign authenticated users to	e assigned to the Wlanl a VLAN named Users1	EAPUsers group which will	
(Add) Insert Delete			
Id Vendor Id	Attribute Id	Attribute Value	
	221	Licore1	

## 9 Apply and save the changes by clicking *Apply* and then *Apply Changes*.



# 2.2 Ethernet Routing Switch:

This section provides configuration steps required to configure a Nortel Ethernet Switch to support Microsoft Network Access Protection EAP clients. For this section the following configuration steps will be performed:

- 1. IP Addressing (Section 2.2.1)
- 2. Virtual LANs (<u>Section 2.2.2</u>)
- 3. RADIUS Server (Section 2.2.3)
- 4. EAPOL (Section 2.2.4)

## 2.2.1 IP Addressing:

The following IP addressing will be defined on the Nortel Ethernet Routing Switch to support switch management and RADIUS server communications:

- IP Address 192.168.10.10
- Network Mask 255.255.255.0
- Default Gateway 192.168.10.1

IP addressing can be defined on a Nortel Ethernet Switch by using the following procedure:

Specify the IP address of the Ethernet Switch by issuing the *ip address switch <ip-address> netmask <network-mask>* command:

ERS5500(config)# ip address switch 192.168.10.10 netmask 255.255.255.0

2 Specify a default gateway for the Ethernet Switch by issuing the *ip default-gateway* <*router-ip-address>* command:

ERS5500(config)# ip default-gateway 192.168.10.1

## 2.2.2 Virtual LANs:

The following VLAN configuration will be defined on the Nortel Ethernet Switch:

- In compliance with Nortel's best practice implementation recommendations all ports will be removed from the default VLAN id 1.
- Three port based VLANs will be defined:
  - VLAN 10 Dedicated management VLAN.
  - VLAN 40 User VLAN used for authenticated EAP users.
- The uplink port 48 will be configured to TagAll frames and will be added as a member of VLANs 10 and 40.
- In compliance with Nortel's best practice implementation recommendations the uplink port 48 will be configured to discard untagged frames.

VLAN configuration can be defined on a Nortel Ethernet Switch by using the following procedure:

1 Rename the default VLAN by issuing the *vlan name <vlan-id> <vlan-name>* command:

ERS5500(config)# vlan name 1 Default

2 Create a management VLAN by issuing the *vlan create <vlan-id> name <vlan-name> type port* command:

ERS5500(config)# vlan create 10 name SERVICES type port

3 Create a Green VLAN for trusted users by issuing the *vlan create <vlan-id> name <vlan-name> type port* command:

ERS5500(config)# vlan create 40 name USERS1 type port

4 Enable 802.1Q tagging on the uplink port by issuing the *vlan ports <port-list> tagging tagall* command:

ERS5500(config)# vlan ports 48 tagging tagall

5 Remove all port from the default VLAN by issuing the *vlan members remove <vlan-id> all* command.

ERS5500(config)# vlan members remove 1 all

6 Add the management, Green and Yellow VLANs to the uplink port by issuing the *vlan members add <vlan-id> <port-list>* command.

ERS5500(config)# vlan members add 10 48

ERS5500(config)# vlan members add 40 48

7 Enabled the discard untagged frames feature on the uplink port by issuing the *vlan ports <port-list> filter-untagged-frame enable* command:

ERS5500(config)# vlan ports 48 filter-untagged-frame enable

8 Specify the management VLAN ID created in step 2 by issuing the *vlan mgmt <vlan-id>* command:

v2.0

ERS5500(config)# vlan mgmt 10

### 2.2.3 RADIUS Server:

The following RADIUS configuration will be defined on the Ethernet Routing Switch to authenticate NAP enabled Windows Vista and XP clients:

- RADIUS Server Host 192.168.20.11 (Management IP Address of the SNAS)
- RADIUS Key sharedkey

A RADIUS server host and shared key can be defined on a Nortel Ethernet Switch by using the following procedure:

1 Create a RADIUS server host entry specifying the Secure Network Access Servers management IP address by issuing the *radius-server host <ip-address>* command:

ERS5500(config)# radius-server host 192.168.20.11

```
2 Enter and confirm a RADIUS shared key by issuing the radius-server key command:
```

ERS5500(config)# radius-server key

Enter key: \*\*\*\*\*

Confirm key: \*\*\*\*\*



The RADIUS shared key must match the shared secret defined on the Secure Network Access Switch.

## 2.2.4 EAPOL:

The following EAPOL configuration will be defined on the Ethernet Routing Switch to authenticate NAP enabled Windows Vista and XP clients:

- EAPOL will be enabled on access ports 1 47 with the following parameters defined:
  - Re-authentication will be enabled with a re-authentication period of 300 seconds (5 minutes).
  - The quiet period will be lowered from 60 seconds to 10 seconds.
- EAPOL will be globally enabled on the switch.

EAPOL port settings and global status can be defined on a Nortel Ethernet Switch by using the following procedure:

1 Enable EAP support on access ports by issuing the eapol status auto command:

ERS5500(config)# interface fastEthernet 1-47

ERS5500(config-if)# eapol status auto

<sup>2</sup> Enable EAP re-authentication support by issuing the *eapol re-authentication enable* 

Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.

command:

ERS5500(config-if)# eapol re-authentication enable

3 Specify a re-authentication period by issuing the *eapol re-authentication-period <interval>* command:

ERS5500(config-if)# eapol re-authentication-period 300

4 Specify a EAP quiet-interval by issuing the eapol quiet-interval <interval> command:

ERS5500(config-if)# eapol quiet-interval 10

5 Globally enable EAPOL support on the Ethernet Switch by issuing the *eapol enable* command:

ERS5500(config-if)# exit

ERS5500(config)# eapol enable

# 2.3 Nortel Wireless LAN 2300 Controller:

This section provides the minimum configuration steps required to configure a Nortel WLAN 2300 Controller to support 802.1X enabled clients and forward authentication requests to the Nortel Secure Network Access Switch.

For this section the following configuration steps will be performed:

- 1. Base Configuration (<u>Section 2.3.1</u>)
- 2. VLAN Configuration (Section 2.3.2)
- 3. RADIUS Server Configuration (Section 2.3.3)
- 4. Service-Profile Configuration (Section 2.3.4)
- 5. Radio-Profile Configuration (<u>Section 2.3.5</u>)
- 6. Access Point Configuration (Section 2.3.6)

### 2.3.1 Base Configuration:

The following baseline configuration will performed on the Nortel WLAN 2300 Controller:

- The system name will be set to WSS2350-1.
- The country of operation will be set to US.
- The management IP address 192.168.10.22 will be defined as the System-IP address which will be used for AP / Controller communications.
- An admin username and password will be created for management access.
- The enable password required for configuration access will be set.
- The default IP interface 1 will be removed.
- All ports will be removed from VLAN 1.

A minimum baseline configuration may be established on a Nortel WLAN 2300 Controller using CLI with the following steps:

#### 1 Specify the name of the

NT2350-30E0E1# set system name WSS2350-1

# 2 Specify the country of operation which determines the regulatory operation of the 2.4Ghz and 5Ghz radios based on region.

#### WSS2350-1# set system countrycode US

This will cause all APs to reboot. Are you sure? (y/n) [n] y

<sup>3</sup> Specify the System-IP address which determines the interface used for management and AP communications.

#### WSS2350-1# set system ip-address 192.168.10.22

This will cause all APs to reboot. Are you sure? (y/n) [n] y

Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.

#### 4 Create and admin username and specify a password.

WSS2350-1# set user admin password adminpassword

```
5 Set the enable password.
```

WSS2350-1# set enablepass

Enter old password: <Enter>

Enter new password: *enablepassword* 

Retype new password: enablepassword

6 Remove the default interface 1 which is assigned to VLAN 1.

WSS2350-1# clear interface 1 ip

7 Remove VLAN 1 membership from ports 1 – 2.

WSS2350-1# clear vlan 1 port 1-2

This may disrupt user connectivity. Do you wish to continue? (y/n) [n] y

8 Save the changes.

WSS2350-1# save config

### 2.3.2 VLAN Configuration:

Two VLANs will be created on the Nortel WLAN 2300 Controller to be used for controller management and users. Additionally the management and user VLANs will be 802.1Q tagged to the uplink port 1 to provide connectivity to the core network:

- VLAN 10 Named SERVICES will be used for switch management and will be 802.1Q tagged on port 1.
- VLAN 40 Named USERS1 will be used for users upon successful authentication and will be 802.1Q tagged on port 1.
- A management IP Address 192.168.10.22 and Subnet Mask 255.255.255.0 will be defined on VLAN 10.
- The default route 192.168.10.1 with a cost of 1 will be created.

VLANs may be created on a Nortel WLAN 2300 Controller using CLI with the following steps:

```
1 Create a management VLAN. ID 10 named SERVICES and add the uplink port 1 as a 802.1Q tagged member.
```

WSS2350-1# set vlan 10 name SERVICES port 1 tag 10

2 Create a user VLAN ID 40 named USERS1 and add the uplink port 1 as a 802.1Q tagged member.

```
WSS2350-1# set vlan 40 name USERS1 port 1 tag 40
```

3 Specify the management IP Address and Network Mask on Interface 10 which will be tied to the management VLAN ID 10.

WSS2350-1# set interface 10 ip 192.168.10.22 255.255.255.0

4 Create a default route.

WSS2350-1# set ip route default 192.168.10.1 1

5 Save the changes.

WSS2350-1# save config

### 2.3.3 RADIUS Server Configuration:

The Nortel Secure Network Access Switch will be defined on the Nortel WLAN 2300 Controller as a RADIUS server host:

- A RADIUS server named NSNAS1 will be created with the IP address 192.168.20.11 with a shared key that matches the shared key specified in the RADIUS client configuration on the Secure Network Access Switch in <u>Section 2.1.5</u>.
- A RADIUS server group named NSNA will be created and the server NSNAS1 added.
- The System-IP Address will be specified as the source of any RADIUS requests.

A RADIUS server, RADIUS group and Client IP Address may be created on a Nortel WLAN 2300 Controller using CLI with the following steps:

1 Create a RADIUS Server named NSNAS1 with the IP Address 192.168.20.11 and key sharedsecret.

 $\mathsf{WSS2350}\text{-}1\#\, \texttt{set}$  radius server <code>NSNAS1</code> address <code>192.168.20.11</code> key sharedsecret

<sup>2</sup> Create a RADIUS Server Group named NSNA with the RADIUS Server NSNAS1 as a member server.

WSS2350-1# set server group NSNA members NSNAS1

3 Specify the System-IP Address as the source of all RADIUS authentication requests.

WSS2350-1# set radius client system-ip

4 Save the changes.

WSS2350-1# save config

### 2.3.4 Service-Profile Configuration:

A Service-Profile and SSID named Data will be created using WPA Enterprise to support 802.1X wireless clients:

• Service-Profile Name: Data

v2.0

- SSID Name: Data
- Encryption: TKIP
- Authentication: 802.1X

A Service-Profile may be created on a Nortel WLAN 2300 Controller with CLI using the following steps:

```
1 Create a Service-Profile and SSID named Data.
```

```
WSS2350-1# set service-profile Data ssid-name Data
```

2 Define the encryption cipher to be used by the Service-Profile. In this example TKIP encryption will be used.

```
WSS2350-1# set service-profile Data cipher-tkip enable
```

3 Enable WPA for the Service-Profile.

```
WSS2350-1# set service-profile Data wpa-ie enable
```

4 Create an authentication rule which will forward all 802.1X authentication requests to the Nortel Secure Network Access Switch.

```
WSS2350-1# set authentication dot1x ssid Data ** pass-through NSNA
```

5 Assign the Service-Profile to the default Radio-Profile. The Radio-Profile defines which Radios and Access Point will service the SSID.

```
WSS2350-1# set radio-profile default service-profile Data
```

6 Save the changes.

```
WSS2350-1# save config
```

## 2.3.5 Radio-Profile Configuration:

The default Radio-Profile configuration will be modified to disable Auto Channel and Auto Tuning and allow for static Channel and Power configuration. The Radio-Profile Auto Tuning parameters may be modified on a Nortel WLAN 2300 Controller with CLI using the following steps:

```
1 Disable Auto Channel Tuning on the default Radio Profile.
```

WSS2350-1# set radio-profile default auto-tune channel-config disable

```
2 Disable Auto Power Tuning on the default Radio Profile.
```

```
WSS2350-1# set radio-profile default auto-tune power-config disable
```

## 2.3.6 Access Point Configuration:

An 802.11a/b/g Access Point profile will be created on the Nortel WLAN Security Switch and the radios added to the default Radio-Profile:

Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.

v2.0

- Access Point Model: 2330A
- Serial Number: 0771100119
- Access Point Name: WAP2330A-1
- 802.11b/g Channel / Power: 8 / 18
- 802.11a Channel / Power: 36 / 19
- Radio Profile (Both Radios): default

An Access Point profile may be created on a Nortel WLAN 2300 Controller using CLI with the following steps:

```
1 Create an Access Point and define the Serial Number and Model.
```

```
WSS2350-1# set ap 1 serial-id 0771100119 model 2330A
```

```
2 Specify a name for the Access Point.
```

```
WSS2350-1# set ap 1 name WAP2330A-1
```

3 Specify the 2.4Ghz radios channel and power settings, assign a Radio-Profile and enable the radio.

```
WSS2350-1# set ap 1 radio 1 radio-profile default mode enable
```

4 Specify the 5Ghz radios channel and power settings, assign the Radio-Profile and enable the radio.

WSS2350-1# set ap 1 radio 2 radio-profile default mode enable

5 Save the changes.

WSS2350-1# save config

# 2.4 Microsoft Windows Server 2003:

This section provides the minimum configuration steps required to configure a Nortel Ethernet Switch to support 802.1X enabled clients and forward authentication requests to the Nortel Secure Network Access Switch. For this section the following configuration steps will be performed:

- 1. Active Directory Users (Section 2.4.1)
- 2. Active Directory Groups (Section 2.4.2)

NN48500-566

eselab.com



Figure 2.4 – Active Directory Tree

### 2.4.1 Active Directory Users:

The following Active Directory Users will be created on the Windows 2003 Domain Controller:

- A user named 'nsnas' used by the Nortel Secure Network Access Switch to perform the LDAP group search.
- A user named 'wireduser' to test EAP authentication on the Nortel Ethernet Switch.
- A user named 'wlanuser' to test EAP authentication on the WLAN 2300 Controller.

Active Directory Users may be created in Windows 2003 Server using the following steps:

<sup>1</sup> Open the Active Directory Users Snap-In. Click on the Users container and then click Action, New and then User.

NN48500-566

🀗 Activ	e Directory Users and Co	omputers				
🎻 Eile	Action View Window	Help				_ 8 ×
$\leftrightarrow \rightarrow$	D <u>e</u> legate Control	0 🗈 😫 🗉	I   🦉 🖉 ៉ 💎	🤹 🗑		
Activ	Find	Users 38 object	s			
<u>+</u> <u></u> 5   ⊡ <b>∯</b>   e	All Tas <u>k</u> s	Computer     Contact     Group	2	Type Security Group	Description	
. ÷.	New <u>W</u> indow from Here	InetOrgPerson		Security Group	Designated administrators	
÷ 6	Refresh	MSMQ Queue Alia	as Owners	Security Group	Members in this group can Built-in account for quest	
	Export List	Printor		User	bait in account for gaost in	
1	P <u>r</u> operties	User		Security Group	Group for the Help and Su	
	Help		VER 1	Security Group	IIS Worker Process Group Built-in account for apopy	
I 1		IWAM_W3KSEP	RVER1	User	Built-in account for Intern	
		🛛 💆 Kevin L. Marsha	all	User		
		😰 Kristin D. Marsh	nall "	User		
		🙎 Maddie Marsha		User		
				User Convitor Conver	Company in this succession	
		Schema Admin	ervers :	Security Group	Designated administrators	
		SUPPORT 388	, 945a0	User	This is a vendor's account	
		Switch Administ	trator	User		
		🕵 Switch Administ	trators	Security Group		
		🚮 TelnetClients		Security Group	Members of this group ha	
		🕵 Wired User		User		
		WiredEAPUsers	;	Security Group		
		📓 Wlan User		User		
•		VlanEAPUsers		Security Group		•
Create a r	new object					

In the *First Name* and *User logon name* fields enter the user name *nsnas* as defined in
the *iSD Bind Name* field on the Nortel Secure Network Access Switch in Section
2.1.4.1. Click *Next*.

Create in: eselab.com/Users     Eirst name:	w Object - User		
Eirst name: Initials: Initials: I Last name: I Full ngme: Initials: I Ser logon name: Iser logon name (pre-₩indows 2000): ESELAB\ Initials: I Iser logon name (pre-₩indows 2000):	Create	in: eselab.com/Users	
Eris hame: Last name: Full name: Iser logon name: nsnas User logon name (pre-₩indows 2000): ESELAB\ nsnas	First server		
Last name: Full name: Iser logon name: Iser logon name (pre-₩indows 2000): ESELAB\ nsnas	rist name:	Instas Initials:	_
Full name: Insnas User logon name: Insnas @eselab.com ▼ User logon name (pre- <u>W</u> indows 2000): ESELAB\ Insnas	Last name:		
User logon name: nsnas User logon name (pre-Windows 2000): ESELAB\ nsnas	Full n <u>a</u> me:	nsnas	
Insnas @eselab.com ▼ User logon name (pre-Windows 2000) ESELAB\ Insnas	User logon name:		
User logon name (pre- <u>W</u> indows 2000); ESELAB\ nsnas	nsnas	@eselab.com	•
ESELAB\ nsnas	User logon name	pre- <u>W</u> indows 2000):	
	ESELAB\	nsnas	_
	,	,	
		Z Back Nevt N	Cancel

3 In the *Password* fields enter and confirm the password as defined in the *iSD Bind Password* field on the Nortel Secure Network Access Switch in section 2.1.4.1. Check

# the option Password never expires and click *Next*. Verify the new account information and click *Finish*.

New Object - User		×
Create in: eselab.com/Users		
Password:     •••••••••       Confirm password:     •••••••••••		
User must change password at next logon		
Password never expires     Account is disabled		
- Pask		
< <u>B</u> ack	<u>N</u> ext > Ca	incel

4 In the Active Directory Users Snap-In highlight the user name *nsnas*, right click and then select *Properties*.

nsnas	_	Jser	
RAS and IAS Se	<u>C</u> opy	Security Group	Servers in this group can
Schema Admins	Add to a group	Security Group	Designated administrators
SUPPORT_3889	Disable Account	Jser	This is a vendor's account
Switch Administi	Reset Password	Jser	
Switch Administi	MU <u>ve</u> Open Home Bage	Security Group	
TelnetClients	Open Home Page Send Mail	Security Group	Members of this group ha
Wired User	Dena m <u>a</u> li	Jser	
WiredEAPUsers	All Tas <u>k</u> s 🔹 🕨	• Security Group	
Wlan User	Out	Jser	
WIanEAPUsers	Delete	Security Group	
selection.	Rename		
	P <u>r</u> operties		
	Help		

### 5 Click on the Account tab and in Account Options check the option Store password

NN48500-566

### using reversible encryption. Click OK.

nsnas Properties
Member Of         Dial-in         Environment         Sessions           Remote control         Terminal Services Profile         COM+           General         Address         Account         Profile         Telephones         Organization
User logon name: nsnas @eselab.com
User logon name (pre- <u>W</u> indows 2000): ESELAB\ nsnas
Log On Io
Account options:
User must change password at next logon User cannot change password  Password never expires  Store password using reversible encryption
Account expires © Never © End of: Sunday , July 27, 2008
OK Cancel Apply

6 In the Active Directory Users Snap-In highlight the user name *nsnas*, right click and then select *Reset Password*.

nsnas	_	Jser	
RAS and IAS Se		Security Group	Servers in this group can
Schema Admins	Add to a group Disable Assourt	Security Group	Designated administrators
SUPPORT_388	Reset Password	User	This is a vendor's account
Switch Administ	Move	Jser	
Switch Administi TelnetClients	Open Home Page Send Mail	5ecurity Group 5ecurity Group	Members of this group ha
Wired User	Dena M <u>a</u> n	Jser	
WiredEAPUsers	All Tas <u>k</u> s ►	Fecurity Group	
Wian User WianEAPUsers	Cu <u>t</u> Delete	bser Security Group	
	– Rena <u>m</u> e		
	<b>P</b> roperties	_	
	<u>H</u> elp		

In the *Password* fields enter and confirm the password as defined in the *iSD Bind Password* field on the Nortel Secure Network Access Switch in section 2.1.4.1. Check the option Password never expires and click *OK*.

Reset Password	? ×
<u>N</u> ew password:	•••••
Confirm password:	•••••
User must change pas	sword at next logon
The user must logoff and t	hen logon again for the change to take effect.
	OK Cancel

8 In the *Active Directory Users* Snap-In add a new user. Enter the appropriate user information for the Wired EAP test user and click Next.

w Object - User				
Create in:	eselab.com/	/Users		
<u>F</u> irst name:	Wired		Initials:	
Last name:	User			
Full n <u>a</u> me:	Wired User			
User logon name:				
wireduser		@eselab.co	m	•
User logon name (pre	e- <u>W</u> indows 2001	D):		
ESELAB		wireduser		
		( Baali	Nexts	Coursel
		< <u>B</u> ack	<u>N</u> ext>	Lancel

Enter and confirm a password for the Wired EAP test user. Check the option *Password never expires* and click *Next*. Verify the new account information and click *Finish*.

Password:	•••••	
<u>C</u> onfirm password:	•••••	
User <u>m</u> ust change	e password at next logon	
🔲 U <u>s</u> er cannot char	nge password	
Pass <u>w</u> ord never e	expires	
Account is disable	ed	

<sup>10</sup> In the *Active Directory Users* Snap-In add a new user. Enter the appropriate user information for the Wireless LAN EAP test user and click Next.

v Object - User		
Create	in: eselab.com/Users	
<u>F</u> irst name:	Wlan Initials:	7
Last name:	User	-
Full n <u>a</u> me:	Wlan User	
User logon name:		
wlanuser	eselab.com	]
User logon name (	pre- <u>W</u> indows 2000):	
ESELAB\	wlanuser	
	Z Reck Next >	Cancel
	Z DODY INCK >	Caricer

Enter and confirm a password for the Wired EAP test user. Check the option
11 Password never expires and click Next. Verify the new account information and click Finish.

Create in: eselab.com/L Bassword: Confirm password:	Jsers		
Password:	•••••		
Lonfirm password:	•••••		
Hear must change password at pa	wtlogon		
User cannot change password	xclogon		
<ul> <li>Password never expires</li> <li>Account is disabled</li> </ul>			
	( Deels	News	Council

### 2.4.2 Active Directory Groups:

The following Active Directory Groups will be created on the Windows 2003 Domain Controller:

- A group named 'WiredEAPUsers' used for Wired EAP User authentication which matches the group name defined on the Nortel Secure Network Access Switch.
- A group named 'WlanEAPUsers' used for Wireless EAP User authentication which matches the group name defined on the Nortel Secure Network Access Switch.
- The user named 'wireduser' will be added as a member to the group 'WiredEAPUsers'.
- The user named 'wlanuser' will be added as a member to the group 'WlanEAPUsers'.

Active Directory Groups may be created in Windows 2003 Server using the following steps:

1 Open the Active Directory Users Snap-In. Click on the Users container and then click Action, New and then Group.



2 In the Group name field enter the name WiredEAPUsers and click OK.

v Object - Group	
Create in: eselab.com	n/Users
Group name:	
WiredEAPUsers	
Group name (pre-Windows 2000):	
WiredEAPUsers	
C Domain local	Security
Global	O Distribution
C Universal	
	OK Cancel

<sup>3</sup> In *Active Directory Users* Snap-In create a new group. In the Group name field enter the name *WlanEAPUsers* and click *OK*.

Create in: esel	ab.com/Users
Group name:	
WlanEAPUsers	]
Froun name (pre-Windows 2	000):
WlanEAPUsers	,-
- Crown 20000	
Group scope	G Committee
Oumain local     Outain	
O Universal	E Elstribution

4 In Active Directory Users Snap-In highlight the group *WiredEAPUsers*, right click and select *Properties*.

WiredEAPU Wlan User WlanEAPUs	Mo <u>v</u> e Send M <u>a</u> il	Security Group User Security Group
selection.	All Tas <u>k</u> s 🕨 🕨	
	Cu <u>t</u> Delete Rena <u>m</u> e	
	P <u>r</u> operties	]
	Help	

# 5 Select the Members tab and click *Add*. Type the name of the Wired EAP test user and click *OK* to add the user to the group. Click *Apply*.

WiredEAPUsers Prop	erties	? ×
General Members	Member Of Managed By	
Members:		
Name	Active Directory Folder	
😰 Wired User	eselab.com/Users	
A <u>d</u> d	<u>R</u> emove	
	OK Cancel	

In Active Directory Users Snap-In highlight the group WlanEAPUsers, right click and
select Properties. Select the Members tab and click Add. Type the name of the Wlan
EAP test user and click OK to add the user to the group. Click Apply.

WlanEAPUsers Prope	erties	? ×
General Members	Member Of Managed By	
Members:		
Name	Active Directory Folder	
🕵 Wlan User	eselab.com/Users	
		_ []
A <u>d</u> d	<u>R</u> emove	
	OK Cancel <u>A</u> r	ply

# 2.5 Microsoft Windows XP Professional:

This section provides the minimum configuration steps required to enable 802.1X authentication on a Windows XP Professional workstation. For this section the following configuration steps will be performed:

- 1. Windows Services (Section 2.5.1)
- 2. Local Area Network Configuration (Section 2.5.2)
- 3. Wireless Network Connection Configuration (Section 2.5.3)

### 2.5.1 Windows Services:

To support 802.1X authentication the following services need to be enabled on the Windows XP Professional workstation:

Windows XP Version	Interface Type	Required Service Name
Service Pack 2 and below	Ethernet & Wireless LAN	Wireless Zero Configuration
Service Pack 3 and above	Ethernet	Wired AutoConfig
Service Pack 3 and above	Wireless LAN	Wireless Zero Configuration

Services may be enabled on a Windows XP Professional workstation using the following steps:

1 Open the Services Snap-In by clicking *Start* and then *Run*. In the *Open* field type *services.msc* and then click *OK*.



Locate the services named Wireless Zero Configuration and if-applicable Wired
AutoConfig. Access the properties for each service and set the Startup type to Automatic. If a service is stopped click Start to enable the service. Click OK.

Wired AutoConfig	; Properties (Local Computer) 📀 🗷	Wireless Zero Configuration Properties (Local Computer) 📀 💈
General Log On	Recovery Dependencies	General Log On Recovery Dependencies
Service name:	Dot3svc	Service name: WZCSVC
Display name:	Wired AutoConfig	Display name: Wireless Zero Configuration
Description:	This service performs IEEE 802.1X authentication	Description: Provides automatic configuration for the 802.11
Path to executal	ble:	Path to executable:
C:\WINDOWS\	System32\svchost.exe -k dot3svc	C:\WINDOWS\System32\svchost.exe -k netsvcs
Startup type:	Automatic	Startup type: Automatic
Service status:	Started	Service status: Started
Start	Stop Pause Resume	Start Stop Pause Resume
You can specify from here.	the start parameters that apply when you start the service	You can specify the start parameters that apply when you start the service from here.
Start parameters	:	Start parameters:
	OK Cancel Apply	OK Cancel Apply

### 2.5.2 Local Area Network Configuration:

The following configuration will be performed on the Local Area Network Connection to support PEAP authentication to the Nortel Ethernet Switch:

- IEEE 802.1X authentication will be enabled.
- Protected EAP (PEAP) with EAP-MSCHAPv2 will be selected.
- Certificate verification will be configured.

802.1X may be enabled on a Local Area Network Connection in Windows XP Professional using the following steps:

Access the Local Area Connection Properties and select the Authentication tab.
Check the option Enable IEEE 802.1X authentication and set the authentication method to Protected EAP (PEAP). Click Settings.

🚣 Local Area Connection Properties 🛛 🔹 🔀
General Authentication Advanced
Select this option to provide authenticated network access for this Ethernet adapter. Enable IEEE 802.1X authentication Choose a network authentication method: Protected EAP (PEAP) Settings
Cache user information for subsequent connections to this network
OK Cancel

In the Protected EAP Properties window optionally check the options *Validate server* certificate and Connect to these servers. If validating the server certificate enter the appropriate domain name and select the root certificate. Select the Authentication Method Secure password (EAP-MSCHAP v2). Click Configure.

Protected EAP Properties 2 💈
When connecting:
✓ Validate server certificate
Connect to these servers:
eselab.com
Trusted Root Certification Authorities:
Entrust pet Server Certification Authority
Equifax Secure Certificate Authority
Equifax Secure eBusiness CA-1
Equifax Secure eBusiness CA-2
Equifux Secure Clobal eBusiness Ch 1
ESELAB CA
Cunet International Root CA
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2) Configure
Enable Fast Reconnect
Enable Quarantine checks
Disconnect if server does not present cryptobinding TLV
OK Cancel

Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.

For single sign-on support check the option Automatically use my Windows logon *name and password (and domain if any)*. Uncheck this option to manually enter a username / password each time you connect to the switch. Click OK.

EAP MSCHAPv2 Properties
When connecting:
Automatically use my Windows logon name and password (and domain if any).
OK Cancel

If the *Connect to these servers* option was enabled and a specific host entry not specified, the following dialog will be displayed when you first connect to the

Ethernet Switch requesting that you validate the connection. Click *OK* to accept the connection which will add the host to the connection list.

You have reach	ned server named:
If this is the cor message again.	rect server, click OK to connect and you will not see this . Click CANEEL to drop the connection.
	~
	View Server Certificate

### 2.5.3 Wireless Network Connection Configuration:

The following configuration will be performed on the Wireless Network Connection to support PEAP authentication to the Nortel WLAN 2300 Controller:

- A Wireless Network Profile will be created.
- IEEE 802.1X authentication will be enabled.
- Protected EAP (PEAP) with EAP-MSCHAPv2 will be selected.
- Certificate verification will be configured.

802.1X may be enabled on a Wireless Network Connection in Windows XP Professional using the following steps:

Access the *Wireless Network Connection Properties* and select the *Wireless Networks* tab. Click *Add* to create a new Wireless Profile.

	: 2 (
General Wireless Networks Advanced	
☑ Use Windows to configure my wireless netw	vork settings
Available networks:	
To connect to, disconnect from, or find out n about wireless networks in range, click the b	nore information utton below.
ViewW	/ireless Networks
below:	Move up Move down
Add Remove Propert	ies
Add Remove Proper Learn about <u>setting up wireless network</u> <u>configuration.</u>	Advanced

2 Type the Network Name (SSID) and select the Network Authentication and Data Encryption types.

fireless network properties		?
Association Authentication C	onnection	
Network name (SSID):	SNA	
Connect even if this netw	ork is not broadcasting	
This network requires a key f	or the following:	
Network Authentication:	WPA	•
Data encryption:	TKIP	•
Network key:		
Confirm network key:		
Key index (advanced): 1	A V	
The key is provided for me	e automatically	
This is a computer-to-compu access points are not used	iter (ad hoc) network; wireless	
	ОК С	ancel

Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.

Wireless network properties 📀 💈	
Association Authentication Connection	
Select this option to provide authenticated network access for wireless Ethernet networks.	
Enable IEEE 802.1x authentication for this network	
EAP type: Protected EAP (PEAP)	
Properties	
Authenticate as computer when computer information is available	
Authenticate as guest when user or computer information is unavailable	
OK Cancel	

In the Protected EAP Properties window optionally check the options *Validate server certificate* and *Connect to these servers*. If validating the server certificate enter the appropriate domain name and select the root certificate. Select the Authentication Method *Secure password (EAP-MSCHAP v2)*. Click *Configure*.

Protected EAP Properties 💿 🔞
When connecting:
Validate server certificate
✓ Connect to these servers:
eselab.com
Trusted Root Certification Authorities:
Equifax Secure Global eBusiness CA-1
ESELAB CA
Concentrational Root Ch
FESTE, Public Notary Certs
FESTE, Verified Certs
First Data Digital Certificates Inc. Certification Authority
FNMT Clase 2 CA
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2) Configure
✓ Enable Fast Reconnect
Enable Quarantine checks
Disconnect if server does not present cryptobinding TLV
OK Cancel



NN48500-566

For single sign-on support check the option Automatically use my Windows logon *name and password (and domain if any)*. Uncheck this option to manually enter a username / password each time you connect to the WLAN. Click OK.

EAP MSCHAPv2 Properties	×
1) (han connacting)	
when connecting.	
Automatically use my Windows logon nan password (and domain if any).	ie and
OK Cancel	

If the *Connect to these servers* option was enabled and a specific host entry not specified, the following dialog will be displayed when you first connect to the

6 Ethernet Switch requesting that you validate the connection. Click *OK* to accept the connection which will add the host to the connection list.

F	Validate Server Certificate
	You have reached server named:  nsnas-vip.eselab.com
	If this is the correct server, click OK to connect and you will not see this message again. Click CANCEL to drop the connection.
	✓
	View Server Certificate
	OK Cancel

## 2.6 Microsoft Windows Vista:

This section provides the minimum configuration steps required to enable 802.1X authentication on a Windows Vista workstation. For this section the following configuration steps will be performed:

- 1. Windows Services (Section 2.6.1)
- 2. Local Area Network Configuration (Section 2.6.2)
- 3. Wireless Network Connection Configuration (Section 2.6.3)

### 2.6.1 Windows Services:

To support 802.1X authentication the following services need to be enabled on the Windows Vista workstation:

Windows XP Version	Interface Type	Required Service Name
All Versions	Ethernet	Wired AutoConfig
All Versions	Wireless LAN	Wireless Zero Configuration

Services may be enabled on a Windows Vista workstation using the following steps:

v2.0

NN48500-566



# Locate the services named Wireless Zero Configuration and Wired AutoConfig. Access the properties for each service and set the Startup type to Automatic. If a service is stopped click Start to enable the service. Click OK.

Wired AutoConfig Properties (Local Computer)		
General Log On Recovery Dependencies	General Log On Recovery Dependencies	
Service name: dot3svc	Service name: Wlansvc	
Display name: Wired AutoConfig	Display name: WLAN AutoConfig	
Description: This service performs IEEE 802.1X authentication on Ethemet interfaces	Description: This service enumerates WLAN adapters, manages WLAN connections and profiles.	
Path to executable: C:Windows\system32\svchost.exe -k LocalSystemNetworkRestricted	Path to executable: C:\Windows\system32\svchost.exe +k LocalSystemNetworkRestricted	
Startup type:	Startup type:	
Help me configure service startup options.	e configure service startup options. Help me configure service startup options.	
Service status: Started	Service status: Started	
Start Stop Pause Resume	Start Stop Pause Resume	
You can specify the start parameters that apply when you start the service from here. You can specify the start parameters that apply when you start the service from here.		
Start parameters:	Start parameters:	
OK Cancel Apply	OK Cancel Apply	

### 2.6.2 Local Area Network Configuration:

The following configuration will be performed on the Local Area Network Connection to support PEAP authentication to the Nortel Ethernet Switch:

- IEEE 802.1X authentication will be enabled.
- Protected EAP (PEAP) with EAP-MSCHAPv2 will be selected.
- Certificate verification will be configured.

802.1X may be enabled on a Local Area Network Connection in Windows Vista using the following steps:

Access the Local Area Connection Properties and select the Authentication tab.
Check the option Enable IEEE 802.1X authentication and set the authentication method to Protected EAP (PEAP). Click Settings.

Local Area Connection Properties	
Networking Authentication Sharing	
Select this option to provide authentic: this Ethemet adapter.	ated network access for
Microsoft: Protected EAP (PEAF -	Settings
Cache user information for subsequite this network	uent connections
	OK Cancel

In the Protected EAP Properties window optionally check the options *Validate server certificate* and *Connect to these servers*. If validating the server certificate enter the appropriate domain name and select the root certificate. Select the Authentication Method *Secure password (EAP-MSCHAP v2)*. Click *Configure*.

Protected EAP Properties
When connectina:
- 🗹 Validate server certificate
Connect to these servers:
eselab.com
Trusted Root Certification Authorities:
Class 3 Public Primary Certification Authority
Entrust.net Secure Server Certification Authority
SELAB CA
Go Daday class 2 Certification Authority
GTE CyberTrust Global Root
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Enable Fast Reconnect
Enable Quarantine checks
Disconnect if server does not present cryptobinding TLV
OK Cancel

For single sign-on support check the option Automatically use my Windows logon *name and password (and domain if any)*. Uncheck this option to manually enter a username / password each time you connect to the switch. Click OK.

EAP MSCHAPv2 Properties	×
When connecting: Automatically use my W password (and domain	Vindows logon name and if any).
ОК	Cancel

If the *Connect to these servers* option was enabled and a specific host entry not

4 specified, the following dialog will be displayed when you first connect to the Ethernet Switch requesting that you validate the connection. Click *OK* to accept the connection which will add the host to the connection list.

Validate Server Certificate	-
You have reached server named: nsnas-vip.eselab.com If this is the correct server, click OK to connect and you will not see this message again. Click CANCEL to drop the connection.	*
View Server Certifica	ate
OK Cancel	

### 2.6.3 Wireless Network Connection Configuration:

The following configuration will be performed on the Wireless Network Connection to support PEAP authentication to the Nortel WLAN 2300 Controller:

- A Wireless Network Profile will be created.
- IEEE 802.1X authentication will be enabled.
- Protected EAP (PEAP) with EAP-MSCHAPv2 will be selected.
- Certificate verification will be configured.

802.1X may be enabled on a Wireless Network Connection in Windows XP Professional using the following steps:

1 Click *Start, Control Panel* then *Manage Wireless Networks*. Create a new Wireless LAN profile by clicking *Add*.



2 Click Manually create a network profile.

() all N	fanually connect to a wireless network
	the short of the second s
How o	do you want to add a network?
*	Add a network that is in range of this computer This shows you a list of networks that are currently available and lets you connect to one. Once you connect, a profile for the network is saved on your computer.
2	Manually create a network profile This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).
4	Create an ad hoc network This creates a temporary network for sharing files or an Internet connection
	Cancel

3 Type the Network Name (SSID) and select the Network Authentication and Data Encryption types. Click Next.

v2.0

ن الله Manually connect to a wi	ireless network					
Enter information for the wireless network you want to add						
Network name:	NSNA					
Security type:	WPA-Enterprise					
Encryption type:	ТКІР					
Security Key/Passphrase:	Display characters					
V Start this connection automatically						
Connect even if the netw	vork is not broadcasting					
Warning: If you select th	iis option, your computer's privacy might be at risk.					
	Next Cancel					

4 Click Change connection settings.

la. 📀	Manually connect to a wireless network	
Su	ccessfully added NSNA	
	Connect to Open the "Connect to a network" dialog so I can connect.	
	Change connection settings Open the connection properties so that I can change the settings.	
		Close

Access the Local Area Connection Properties and select the Authentication tab.
Check the option Enable IEEE 802.1X authentication and set the authentication method to Protected EAP (PEAP). Click Settings.

NSNA Wireless Network	properties	×
Connection Security		
Security type: Encryption type:	WPA-Enterprise	
Choose a petwork aut	theotication method:	
Microsoft: Protected	EAP (PEAP)    Settings ation for subsequent connections	
	OK Can	cel

In the Protected EAP Properties window optionally check the options *Validate server certificate* and *Connect to these servers*. If validating the server certificate enter the appropriate domain name and select the root certificate. Select the Authentication Method *Secure password (EAP-MSCHAP v2)*. Click *Configure*.

Protected EAP Properties	×
When connecting:	
Validate server certificate	
Connect to these servers:	
eseiab.com	
Trusted Root Certification Authorities:	
Class 3 Public Primary Certification Authority	<u>^</u>
Entrust.net Secure Server Certification Authority	=
SELAB CA	
Go Duddy Class 2 Certification Authority	
GTE CyberTrust Global Root	*
۲ III III III III III III III III III I	•
Do not prompt user to authorize new servers or tru certification authorities.	sted
Select Authentication Method:	
Secured password (EAP-MSCHAP v2)	Configure
Enable Fast Reconnect	
Enable Quarantine checks	
Disconnect if server does not present cryptobinding T	LV
ОК	Cancel

For single sign-on support check the option Automatically use my Windows logon
 name and password (and domain if any). Uncheck this option to manually enter a username / password each time you connect to the switch. Click OK.

EAP MSCHAPv2 Properties	×
When connecting:	
Automatically use my Windows logon name and password (and domain if any).	
OK Cancel	

If the Connect to these servers option was enabled and a specific host entry not

8 specified, the following dialog will be displayed when you first connect to the WLAN requesting that you validate the connection. Click *OK* to accept the connection which will add the host to the connection list.

Val	lidate Server Certificate	
) I n	You have reached server named: nsnas-vip.eselab.com If this is the correct server, click OK to connect and you will not see this message again. Click CANCEL to drop the connection.	*
	View Server Certifica	ite

# 3. Verification:

This section provides some example CLI commands and output to verify operation after configuration has been completed.

# 3.1 Nortel Secure Network Access Switch:

The following CLI commands can be issued on the Nortel Secure Network Access Switch to view sessions and debug RADIUS operations:

# Active 802.1X session information can be viewed by issuing the *info/sessions* command.

>> Main# info/sessions

Number of currently active sessions: 2

Domai n	Switch	Port	User	Source IP	Source Mac
	Logi n	Туре	VI an	Portal IP	Session Type
1	0	1	ESELAB\wi reduser	0.0.0.0	00: 09: 6b: 13: 23: 89
	15: 23	dn_pc	red(0)	-	802. 1x
1	0	503	ESELAB\wl anuser	0.0.0.0	00: 16: e3: 2b: 68: f9
	24Jun08	dn_pc	red(0)	-	802. 1x

2 Debugging may be enabled by issuing the *maint / starttrace* command. Note that tracing may be disabled by issuing *stoptrace*.

#### >> Main# maint/starttrace

Enter tags (list of all, aaa, dhcp, dns, ssl, nha, snas, patchlink, radius, nap) [all]: Enter Domain (or 0 for all Domains) [0]: Output mode (interactive/tftp/ftp/sftp) [interactive]:

>> Maintenance#
15:55:26.579662: Trace started

# 3.2 Nortel Ethernet Switch:

The following NNCLI commands can be issued on the Nortel Ethernet Switch to verify configuration and debug failed 802.1X authentications.

```
The EAP configuration and authentication status of a switch port may be viewed by
1
   issuing the show eapol port <port-number> command.
ERS5500-2# show eapol port 1
EAPOL Administrative State: Enabled
EAPOL User Based Policies: Disabled
EAPOL User Based Policies Filter On MAC Addresses: Disabled
               Admin Oper ReAuth ReAuth Quiet Xmit Supplic Server Max
    Admi n
Port Status Auth Dir
                    Dir Enable Period Period Period Timeout Timeout Reg
3600 10
           Yes Both Both Yes
                                         30
                                               30
                                                      30
                                                             2
1
   Auto
    The VLAN membership of a specific port may be viewed by issuing the show vlan
2
    interface vids <port-number> command.
ERS5500-2# show vlan interface vids 1
Port VLAN VLAN Name
                      VLAN VLAN Name
                                        VLAN VLAN Name
---- ---- ----- ---- ---- ---- ----
       USERS1
1
   40
---- ---- ----- ---- ----- ----- -----
   The RADIUS Server configuration may be viewed by issuing the show radius-server
3
    command.
```

ERS5500-2# show radius-server

Password Fallback: Disabled Primary Host: 192.168.20.11 Secondary Host: 0.0.0.0 Port: 1812 Time-out: 2 Key: \*\*\*\*\*\*\*\*\*\*\*\* Radius Accounting is Disabled AcctPort: 1813

# 4 The list of configured VLANs and port membership may be viewed by issuing the show vlan command.

#### ERS5500-2# show vlan

١d	Name		Туре	Protocol	User PID	Acti ve	IVL/SVL	Mgmt
1	DEFAULT		Port	None	0x0000	Yes	IVL	No
	Port	Members:	NONE					
10	SERVI CES		Port	None	0x0000	Yes	IVL	Yes
	Port	Members:	47-48					
40	USERS1		Port	None	0x0000	Yes	I VL	No
	Port	Members:	47-48					

Total VLANs: 3

# <sup>5</sup> Advanced EAPOL diagnostics for a port may be viewed by issuing the *show eapol auth-diags interface <port-number>* command.

#### ERS5500-2# show eapol auth-diags interface 1

#### Port: 1

EntersConnecting:	5
EapLogoffsWhileConnecting:	0
EntersAuthenti cati ng:	2
AuthSuccessWhileAuthenticating:	2
AuthTimeoutsWhileAuthenticating:	0
AuthFailWhileAuthenticating:	0
AuthReauthsWhileAuthenticating:	0
AuthEapStartsWhileAuthenticating:	0
AuthEapLogoffWhileAuthenticating:	0
AuthReauthsWhileAuthenticated:	0
AuthEapStartsWhileAuthenticated:	0
AuthEapLogoffWhileAuthenticated:	0
BackendResponses:	22
BackendAccessChallenges:	20
BackendOtherRequestsToSupplicant:	20
BackendNonNakResponsesFromSupplicant:	18
BackendAuthSuccesses:	2
BackendAuthFails:	0
## 6 EAPOL statistics for a port may be viewed by issuing the *show eapol auth-stats interface <port-number>* command.

ERS5500-2T# show eapol auth-stats interface 1

Port: 1

Eapol FramesRx:	24
BackendAuthFails:	0
Eapol FramesTx:	29
EapolStartFramesRx:	2
Eapol LogoffFramesRx:	0
Eapol Respl dFramesRx:	2
Eapol RespFramesRx:	20
Eapol ReqIdFramesTx:	3
Eapol ReqFramesTx:	26
InvalidEapolFramesRx:	0
EapLengthErrorFramesRx:	0
LastEapol FrameVersion:	1
LastEapol FrameSource:	0009: 6B13: 2389

#### **3.3 Nortel Wireless LAN Controller:**

The following CLI commands can be issued on the Nortel Wireless LAN 2300 Controller to verify configuration and debug failed 802.1X authentications.



Nortel Confidential Information Copyright © 2008 Nortel Networks. All Rights Reserved.

NSNA 2.0 802.1X Authentication TCG

1 total users

# <sup>3</sup> The RADIUS server status and server groups may be viewed by issuing the *show radius* command.

WSS2350-1# show radius

Radius Servers Default Values Auth-Port=1812 Acct-Port=1813 Timeout=5 Acct-Timeout=5 Retrans=3 Deadtime=0 Key=(null) Author-Pass=(null)

Radius Servers

		Auth	Acct	Ti me		Dead	
Server	IP address	Port	Port	0ut	Retry	Ti me	State
NSNAS	192. 168. 20. 11	1812	1813	5	3	0	UP

Server groups

NSNA: NSNAS

4 The list of configured VLANs, state, 802.1Q tag and port membership may be viewed by issuing the *show vlan* command:

WSS2350-1# show vlan

C + - + -
State
Up
Up

# 4. Appendix:

### 4.1 Stackable Ethernet Switch Return Attributes:

Port Based Priority Attributes			
Attribute Name	Vendor-ID	Attribute-ID	Value
Port-Priority	562	1	0 – 7 (802.1P Priority)
Remote Management	Access		
Attribute Name	Vendor-ID	Attribute-ID	Value
Service-Type	0	6	6 - Administrator (RW Access)
Service-Type	0	6	7 - NAS-Prompt (RO Access)
Used Based Policies			
Attribute Name	Vendor-ID	Attribute-ID	Value
User-Role	562	110	UROL <role-name></role-name>
VLAN Attributes			
Attribute Name	Vendor-ID	Attribute-ID	Value
Tunnel-Type	0	64	13 – (Virtual LANs)
Tunnel-Medium-Type	0	65	6 - (802)
Tunnel-Private-Group-ID	0	81	VLAN-ID which the client belongs

Table 4.1 – Stackable Ethernet Switch RADIUS Attributes

## 4.2 Modular Ethernet Switch Return Attributes:

Port Based Priority Attributes				
Attribute Name	Vendor-ID	Attribute-ID	Value	
Port-Priority	562	1	0 – 7 (802.1P Priority)	
Remote Management Access				
Attribute Name	Vendor-ID	Attribute-ID	Value	
None-Access	1584	192	0	
Read-Only-Access	1584	192	1	
L1-Read-Write-Access	1584	192	2	
L2-Read-Write-Access	1584	192	3	
L3-Read-Write-Access	1584	192	4	
Read-Write-Access	1584	192	5	
Read-Write-All-Access	1584	192	6	
Used Based Policies				
Attribute Name	Vendor-ID	Attribute-ID	Value	
User-Role	562	110	UROL <role-name></role-name>	
VLAN Attributes				
Attribute Name	Vendor-ID	Attribute-ID	Value	
Tunnel-Type	0	64	13 – (Virtual LANs)	
Tunnel-Medium-Type	0	65	6 - (802)	
Tunnel-Private-Group-ID	0	81	VLAN-ID which the client belongs	

Table 4.2 – Modular Ethernet Switch RADIUS Attributes

## 4.3 WLAN 2300 RADIUS Return Attributes:

Remote Management Access				
Attribute Name	Vendor-ID	Attribute-ID	Value	
Service-Type	0	6	2 - Framed (Network User Access)	
Service-Type	0	6	6 - Administrative (Enable Mode)	
Service-Type	0	6	7 - NAS-Prompt (Non Enable Mode)	
Identity Based Networ	king			
Attribute Name	Vendor-ID	Attribute-ID	Value	
Filter-ID	0	11	Name of ACL	
VLAN-Name	562	231	Name of the VLAN to which the client belongs	
Mobility-Profile	562	232	Name of the Mobility Profile used by the authorized client	
Encryption-Type	562	233	Type of encryption used to authenticate the client.	
Time-Of-Day	562	234	Day(s) and time(s) during which a user can log into the network.	
SSID	562	235	Name of the SSID you want the user to use.	
End-Date	562	236	Date and time after which the user is no longer allowed to be on the network	
Start-Date	562	237	Date and time at which the user becomes eligible to access the network	
URL	562	238	URL to which the user is redirected after successful Web- based AAA	

#### Table 4.3 – WLAN 2300 RADIUS Attributes

### 4.1 Realms:

Realms provide the ability for the Secure Network Access Server to route an authentication request to a specific authentication server (local, LDAP, NTLM etc) based on the user information contained within the RADIUS access request packet.

When a RADIUS client sends user credentials for authentication, a user name is often included. Within the user name are two elements:

- 1. Identification of the user account name
- 2. Identification of the user account location

For example the user name kmarshall@eselab.com includes the account name *kmarshall* and the account location *eselab.com*.

A realm name may be a prefix or suffix depending on the operating system, authentication type and client. Before defining a realm name it's important to understand the formatting of the authentication request to ensure that the authentication request will be processed correctly by the Nortel Secure Network Access Switch.

For example a PEAP authentication request from a Microsoft Windows XP client may include the Windows Domain name as a prefix such as *ESELAB*/*username*. To authenticate users in this example a realm named *ESELAB* or *eselab* would need to be created.

An EAP-TLS authentication request as well as host authentication will include the realm name in the suffix such as *user@eselab.com* or host/computer *@eselab.com*. To authenticate users in this example a realm named *eselab.com* would need to be created.

Username	Realm Name
kmarshall@eselab.com	eselab.com
host/ibm-t30-1@eselab.com	eselab.com
ESELAB\kmarshall	ESELAB or eselab

Table 4.1	-	Example	Realms
-----------	---	---------	--------

## 5. Software Baseline:

The following table provides the individual software releases for each Nortel Ethernet Routing Switch used in this document:

Nortel Platform	Software Release
Nortel Secure Network Access Switch 4050	v2.0.0.55
Nortel Ethernet Routing Switch 5500	v5.1.0.015
Nortel WLAN 2300 Controller	V6.0.7.2
Microsoft Platform	Software Release
Microsoft Platform Windows Server 2003 Enterprise Edition	Software Release Service Pack 2
Microsoft Platform Windows Server 2003 Enterprise Edition Windows XP Professional	Software ReleaseService Pack 2Service Pack 3



## 6. Reference Documentation:

Table 7.0 provides a list of additional Nortel and Microsoft Publications which may be referenced to for additional information:

Nortel Document Title	Location
Nortel Ethernet Routing Switch 5500 Series Configuration - Security (217463-C)	http://www.nortel.com/support
Nortel WLAN Security Switch 2300 Series Configuration Guide (320657-F)	http://www.nortel.com/support
Nortel WLAN Security Switch 2300 Series Command Line Reference (320658-F)	http://www.nortel.com/support

 Table 6.0 – Reference Documentation

#### Contact us

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 for assistance.

If you purchased a Nortel Networks service program, contact Nortel Technical Support. To obtain contact information online, go to <u>www.nortel.com/contactus</u>.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to <u>www.nortel.com/erc</u>.