

Nortel Secure Network Access 2.0 Engineering

> > Nortel Secure Network Access 2.0 802.1X Authentication with Nortel Health Agent and Microsoft Network Access Protection Endpoint Inspection Technical Configuration Guide

Enterprise Business Solutions Document Date: August 5, 2008 Document Number: NN48500-567 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 and provide inspection of Microsoft Windows XP and Vista workstations running the Microsoft EAP Quarantine Enforcement and Nortel Health Agent Clients.

### **Revision Control**

No	Date	Version	Revised by	Remarks
1	07/09/2008	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:**

FIGURE	S:	. 4
TABLES	5:	. 4
DOCUM	ENT UPDATES:	. 5
CONVE	NTIONS:	. 5
1. OV	ERVIEW:	. 6
1.1 1.2 1.3	NHA / NAP 802.1X ENFORCEMENT OVERVIEW: TOPOLOGY: PRE-REQUISITES:	.6 10 11
2. CO	NFIGURATION:	12
2.1 2.2 2.3 2.4 2.5	NORTEL SECURE NETWORK ACCESS SWITCH: ETHERNET ROUTING SWITCH: MICROSOFT WINDOWS SERVER 2003: WINDOWS XP PROFESSIONAL: WINDOWS VISTA:	12 45 48 55 59
3. VEF	RIFICATION:	66
3.1 3.2 3.3 3.4 3.5	WINDOWS WORKSTATION COMPLIANT NAP / NHA STATE:	56 57 58 59 70
4. API	PENDIX:	73
4.1	REALMS:	73
5. SO	FTWARE BASELINE:	74
6. REI	FERENCE DOCUMENTATION:	75

## Figures:

Figure 1.1 – NHA / NAP 802.1X Enforcement Framework	6
Figure 1.1.2.1 – Microsoft NAP Agent States	7
Figure 1.1.2.2 – Nortel Health Agent States	8
Figure 1.1.3 – VLAN States	9
Figure 1.2 – Topology	10
Figure 2.1.3 – Server Certificate	16
Figure 2.1.4 – LDAP and NTLM Servers	21
Figure 2.3 – Active Directory Tree	48

v2.0

### Tables:

Table 1.1.3 – Standard RADIUS Return Attributes	8
Table 5.2 – Windows XP SP3 NAP Enforcement Clients	. 57
Table 6.2 – Windows Vista NAP Enforcement Clients	. 62
Table 4.1 – Example Realms	. 73
Table 5.0 – Software Baseline	. 74
Table 6.0 – Reference Documentation	. 75

NN48500-567

### **Document Updates:**

### **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 and provide end-point inspection of wired Microsoft Windows XP and Vista workstations running the Microsoft EAP Quarantine Enforcement Client and Nortel Health Agent Client.

Microsoft Network Access Protection (NAP) delivers a new set of operating system components that provide a platform for protected access to private networks. The NAP platform provides an integrated way of detecting the state of a network client that is attempting to connect to a network and restricting the access of the network client until the policy requirements for connecting to the network have been met.

The NSNA/NAP interoperability architecture allows customers to deploy both the NSNA solution and the Network Access Protection (NAP) concurrently. These components interoperate, allowing customers to enforce security policies for network access using both NSNA and NAP. This architecture allows deployment of NAP clients with or without a Windows 2008 Server based Network Policy Server (NPS) present on the network. If the Microsoft NPS server is present, it will be consulted and its response will be used in a configurable way to augment the access decision made by the SNAS. If a Microsoft NPS server is not in place, the Secure Network Access Switch can communicate with the NAP client components.

This configuration guide describes a solution that does not use or require a Windows 2008 Server with NPS. Integrating Windows 2008 Server with NPS can be performed by specifying a "Remote Policy Server" in the NAP settings on the Secure Network Access Switch.

### 1.1 NHA / NAP 802.1X Enforcement Overview:

This section provides a brief overview of how 802.1X enforcement functions on the Nortel Secure Network Access Switch with the Microsoft Network Access Protection and Nortel Health Agent Clients.



Figure 1.1 – NHA / NAP 802.1X Enforcement Framework

#### **1.1.1 Authentication Process:**

- 1. The Windows XP / Vista workstation initiates 802.1X authentication.
- Using Protected EAP the workstation sends its user and/or computer authentication credentials to the Nortel Secure Network Access Switch providing RADIUS services for the Nortel Ethernet Switch. The credentials are either authenticated locally or using NTLM against authenticated against Active Directory.
- 3. If the authentication credentials are not valid, the 802.1X connection attempt is terminated.
- 4. If the authentication credentials are valid, the Network Policy Server on the Nortel Secure Network Access Switch requests the health state from the Windows XP / Vista workstation.
- 5. The Windows XP / Vista workstation sends the Network Access Protection and Nortel Health Agent health state information to the Nortel Secure Network Access Switch.
- The Nortel Secure Network Access Switch evaluates the health state information of the Windows XP / Vista workstation, determines whether the workstation is compliant, and forwards a RADIUS Access Accept with the appropriate VLAN information to the Nortel Ethernet Switch.
  - a. If the workstation is non-compliant, the Nortel Secure Network Access Switch forwards RADIUS return attributes to the Nortel Ethernet Switch which places the workstation in a remediated Yellow VLAN.

Optionally the Network Policy Server may re-provision the workstation with the required updates to be compliant with health policy. If successful the workstation restarts 802.1X authentication and sends its updated health state information to the Network Policy Server. The Nortel Secure Network Access Switch forwards RADIUS return attributes to the Nortel Ethernet Switch which places the workstation in an unrestricted Green VLAN.

b. If the Windows XP / Vista workstation is compliant, the Nortel Secure Network Access Switch forwards RADIUS return attributes to the Nortel Ethernet Switch which places the workstation in an un-restricted Green VLAN.

#### 1.1.2 Health Agent States:

As shown in figure 1.1.2.1 the Microsoft EAP Quarantine Enforcement Client can be in two states depending on the workstation's compliance state compared to the policy defined on the Network Policy Server.

Taskbar Icon	Client State Description
۲	Policy checks have been performed and the Microsoft EAP Quarantine Enforcement Client is in a non-compliant state. In this state the workstation will be placed into a Yellow remediated VLAN.
	Policy checks have been performed and the Microsoft EAP Quarantine Enforcement Client is in a compliant state.
<b>v</b>	Assuming the Nortel Health Agent policies are compliant the workstation will be placed into an unrestricted Green VLAN.

As shown in figure 1.1.2.2 the Nortel Health Agent may be in one of three states depending on the workstations compliance state compared to the Nortel Health Policy assigned to the group.

Taskbar Icon	Client State Description
<b>e</b>	No policy checks have been performed and the Nortel Health Agent is idle state.
	Policy checks have been performed and the Nortel Health Agent is in non- compliant state. In this state the workstation will be placed into a Yellow remediated VLAN.
<b>e</b>	Policy checks have been performed and the Nortel Health Agent is in compliant state. Assuming the Microsoft policies are compliant the workstation will be placed into an unrestricted Green VLAN.

Figure 1.1.2.2 – Nortel Health Agent States

#### 1.1.3 VLAN States:

The Nortel Secure Network Access Switch uses standard IETF RADIUS return attributes upon successful PEAP authentication to place workstations into the appropriate VLAN based on Microsoft Network Access Protection and Nortel Health Agent compliance states.

During configuration Green and Yellow VLAN Names and IDs are created on the Nortel Secure Network Access Switch. These VLANs are then combined with Filters in an Extended Profile to define the VLAN membership based on NAP and NHA policy compliance state. Table 1.1.3 shows the standard RADIUS return attributes forwarded by the Nortel Secure Network Access Switch to the Nortel Ethernet Switch to assign the VLANs:

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	Numeric VLAN-ID assigned to the port based on compliance state

#### Table 1.1.3 – Standard RADIUS Return Attributes

A workstation with the Microsoft Network Access Protection and Nortel Health Agent clients may be in one of three VLAN states depending on authentication status and policy compliance state:

- Pre-Authentication Windows XP / Vista workstations that have not performed PEAP user or computer authentication will be in an isolated state and not assigned a VLAN. The only communication that may occur between the workstation and Switch is EAP authentication and no other traffic will be passed.
- Non-Compliant Windows XP / Vista workstations that have performed PEAP user and/or computer authentication but fail policy checks will be placed into a remediated Yellow VLAN. The remediated VLAN is intended to provide restricted access to the network to allow the workstation to obtain the required updates to become compliant. Once compliant the workstation is transitioned to the un-restricted Green VLAN.
- Compliant Windows XP / Vista workstations that have performed PEAP user and/or computer authentication and pass policy checks will be placed into an unrestricted Green VLAN with full access to the network. If the workstations compliance state changes the workstation is transitioned to the remediated Yellow VLAN.



Figure 1.1.3 – VLAN States

### 1.2 Topology:

Figure 1.2 shows the topology that will be used in this configuration guide using the following Nortel and Microsoft platforms:



WINDOWS AF 3F3 / VIS

Figure 1.2 – 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 Active Directory using NTLM. Additionally the Nortel Secure Network Access Switch will be configured to provide NAP / NHA compliance verification and assign the users to unrestricted (Green) or restricted (Yellow) VLAN based on the workstations compliance state.
- 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 Green and Yellow VLANs will be created on the switch which will be dynamically assigned to EAPOL NAP users based on compliance state 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 as well as exchange NAP compliance state with the Nortel Secure Network Access Switch. Based on NAP / NHA compliance state the workstation will either be placed in a remediated VLAN (Yellow) or unrestricted VLAN (Green).

This document provides configuration details for Nortel and Microsoft components shown in figure 1.2 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.

### **1.3 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.
  - d. The Nortel Health Agent with appropriate Java Runtime Engine is installed and operational on the Workstation.
- 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 support Microsoft Network Access Protection EAP clients. For this section the following configuration steps will be performed:

- 1. Base Configuration (<u>Section 2.1.1</u>)
- 2. VLANs (Section 2.1.2)
- 3. Certificates (<u>Section 2.1.3</u>)
- 4. Authentication Servers (Section 2.1.4)
- 5. Filters (Section 2.1.5)
- 6. Groups (<u>Section 2.1.6</u>)
- 7. Extended Profiles (Section 2.1.7)
- 8. RADIUS Server (Section 2.1.8)
- 9. Network Access Protection (Section 2.1.9)
- 10. Nortel Health Agent Policy (Section 2.1.10)

#### 2.1.1 Base Configuration:

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

- IP Addressing The Interface, 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.
- 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]

- join Join an existing cluster
- new Initialize host as a new installation
- boot Boot menu
- info Information menu
- exit Exit [global command, always available]
- >> Setup# new

2 Define the following 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 VLAN but a smaller subnet with fewer host addresses could be utilized to save 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: yes	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: eselab.com	The DNS domain name for the system. For this example the domain name is eselab.com.
Create http to https redirect server: yes	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: no	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: <i>yes</i>	The browser based interface (BBI) will be enabled to perform the remaining configuration on the NSNAS.

#### 2.1.2 VLANs:

Two VLANs will be defined on the Nortel Secure Network Access Switch that will determine the NAP client VLAN membership based on compliance state. The VLAN membership will be forwarded to the Nortel Ethernet Switch using standard IETF RADIUS return attributes during EAPoL authentication upon successful Active Directory user authentication:

VLAN ID	VLAN Name	Purpose
30	GREEN	Will be assigned to compliant devices and will provide unrestricted access to the network.
50	YELLOW	Will be assigned to non-compliant devices and will provide remediated restricted access to the network.

VLANs 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 Secure Access Domain, VLANs and then Add.

Managing: 2.0.0.53 Secure Access Domain » VLANs	Logged as admin 🔒
VLANs	
_	Secure Access Domain: 1 eselab.com - Refresh
Add	
Vlan ID Name	
N0 VL	ans contigured.
2 Enter the name YELLOW and specify t	he VLAN Id <i>50</i> . Click <i>Creat</i> e VLAN.
Managing: 2.0.0.53 Secure Access Domain » VLANs	Logged as admin 🔒
Add VLAN	
Nam	e: YELLOW
	Create VLAN Back
3 Click Add. Enter the name GREEN and	specify the VLAN Id 30. Click Create VLAN.

NICNIA 20 002 1W Authoritication		
Endpoint Inspection TCG	v2.0	NN48500-567
Managing: 2.0.0.53 Secure Access Domain »	VLANs	Logged as admin 🖉 🔒
VLANs		
Add VLAN		
	Name: GREEN1 Vlan Id: 30	
		Create VLAN Back
4 The Yellow and G Access Switch.	reen VLANs will now be defined on the I	Nortel Secure Network
Add Delete		
Vian ID Name		
30 GREEN1		
5 Apply and save th	e changes by clicking <i>Apply</i> and then A	Apply Changes.
Nortel Secure Ne	twork Access Switch	Apply   Diff   Revert   Logout   Help
Managing: 2.0.0.53		Logged as admin 🖉 🔒
Apply Pending Cont	iguration Changes	
Warning: Applying change	s will save them to the configuration.	
Apply Changes		
Back		

#### 2.1.3 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.



NN48500-567



v2.0



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

NØRTEL	Nortel Se	cure Network	Access Sv	vitch		Apply   Diff   Rever	Logout   He
Monitor <b>Config</b>	Managing: 2.0.0.53	52					Logged as admin
Wizards Portal Launch Network Secure Access Domain	Certificate	S					
Cluster Certificates	Add Edit	Delete Show					
+ Import			Cart	CA Cort	Key	Koy Sizo	Key Match
+ Conorato		Name	Сеп	CACER		Ney Size	itoj mator
<ul> <li>Generate</li> <li>Export</li> <li>Specify a un</li> </ul>	ique name fo	test cert r the server	Yes Certificate	Yes and then	Yes	1024	Yes
Generate     Export     Specify a un     Ianaging: 2.0.0.53     Certificates	ique name fo	test cert	Yes	Yes and then	Yes	1024	Yes
Generate     Export     Specify a un Anaging: 2.0.0.53 Certificates Certificates	ique name fo	test cert	Yes	and then	ricy Yes	1024	Yes
+ Generate + Export Specify a un fanaging: 2.0.0.53 Certificates Certificates Add New Certifica	ique name fo	test cert	ves	and then	ricy Yes	1024	Yes
• Generate • Export Specify a un Managing: 2.0.0.53 Certificates Certificates Add New Certifica	te	test cert the server	certificate	and then	click U	Incy size 1024	Yes

#### 3 Click Add and specify unique a name for the CA root certificate and then click

v2.0

NN48500-567

Update.	
Managing: 2.0.0.53	Logged as admin 🔒
Certificates	
Add New Certificate	
Add New Certificate	3
Name:	ESELAB-CA
Warning: New certificates are directly applied to the database.	Update Back
Using the navigation tree click <i>Certificat</i> pull-down menu select the server certific locate the PKCS#12 server certificate iss verify the <i>Private Key Password</i> then clic	es, <i>Import</i> and then <i>File</i> . In the <i>Certificate</i> ate name created in step 2. Click Browse and sued from the Certificate Authority. Enter and ck <i>Import</i> .
naging: <b>2.0.0.53</b> Certificates » Import » File	Logged as admin 🔒
ile	
Certificate: 2 ESELAB-Server  Refresh	
e current certificate is Not set, and the current key is Not set.	
ertificate and/or Key File	
File System:	Protocol   Local
Certificate and/or Key File:	\\mages\ESELAB_Ro Browse
rivate Key Password (if required)	
Private Key Password:	****
Confirm Private Key Password:	*****

5 Using the navigation tree click *Certificates*, *Import* and then *File*. In the *Certificate* pull-down menu select the CA root certificate name created in step 3. Click Browse

#### and locate the CA certificate issued from the Certificate Authority then click Import. Note that the CA root certificate does not require a Private Key Password. Logged as admin 🖉 🔒 Managing: 2.0.0.53 Certificates » Import » File File Certificate: 3 ESELAB-CA Refresh The current certificate is Set, and the current key is Not set. Certificate and/or Key File File System: Protocol Local 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. The server and CA root certificates will now be installed on the Secure Network 6 Access Switch.

Add	Edi	t Delete Show					
	ID	Name	Cert	CA Cert	Key	Key Size	Key Match
1	1	test cert	Yes	Yes	Yes	1024	Yes
1	2	ESELAB-Server	Yes	No	Yes	1024	Yes
	3	ESELAB-CA	Yes	Yes	No		

Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain, Server and then SSL. Click on the Certificate Number pull-down menu and select the Server Certificate name installed in the previous steps.

NSNA 2.0 802.1X Au	hentication	with NA	P / NHA
Endpoint Inspection 7	'CG		

NN48500-567

Logged as admin 🔒

Managing: 2.0.0.53

Secure Access Domain » Server » SSL

#### SSL

Secure Access Domain: 1 eselab.com - Refresh

General   CA Certificate List	
General Settings	
Certificate Number:	2 ESELAB-Server 👻
Status:	enabled -
Protocol:	ssl3 🔻
Ciphers:	ALL@STRENGTH
Verify Level:	none 🔻
SSL Cache Size:	4000 (0-10000, 0=unlimited)
SSL Cache Timeout:	300 (seconds)

8 In the CA Certificate List remove the default CA certificate named *test\_cert* and add the CA Certificate installed in the previous steps. Click *Update*.

#### CA Certificate List

	Available	Selected
CA Certificates List:	1 test_cert 2 ESELAB-Server	3 ESELAB-CA
CA Chain List:	Available	Selected
		Update

Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain
then Server. In the DNS Name field enter the fully qualified name of the host as specified in the Common Name field in the Server Certificate. Click Update.

NSNA 2.0 802.1X Authentication with NAP / NHA Endpoint Inspection TCG	v2.0 NN48500-567	
Managing: 2.0.0.53 Secure Access Domain » Server	Logged as admin	8
Server		_
Secure Access Domain: 1 eselab.com - <u>Refresh</u>		
Listen Port: DNS Name :	443 nsnas-vip.eselab.com	
	Update	
10 Apply and save the changes by clicking	Apply and then Apply Changes.	
Nortel Secure Network Access Swite	Ch Apply   Diff   Revert   Logout   Help	
Managing: 2.0.0.53	Logged as admin 🧖	h .
Apply Pending Configuration Changes		_
Warning: Applying changes will save them to the configuration	on.	
Back		_

#### 2.1.4 Authentication Servers:

An LDAP and NTLM server will be created on the Secure Network Access Switch to authenticate RADIUS access requests against Active Directory. The NTLM server will be used for user authentication and LDAP server used for group association:

- An LDAP authentication server entry will be created which will be used for Active Directory group association.
- An 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.

NN48500-567



Figure 2.1.4 – 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: <u>http://support.microsoft.com/kb/942564</u>.

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 AAA, Au	e Browser Based Interi thentication, LDAP and	ace (BBI) navigation I then <i>Add</i> .	tree click Secur	e Access Domain,
Managing: <b>2.0.0.53</b> Secure Ad	ccess Domain » AAA » Authentication	» LDAP		Logged as admin 🔒
LDAP		Secure A	Access Domain: 1 ess	elah com 💌 Refresh
Add				
ID	Name	Display Name	Mechanism	Servers Created
	No LE	AP Authentication servers configu	red.	

ົ	Specify an LDAP Server Name,	Display Name and set the Mechanism to LDAP Click
2	Update.	

NN48500-567

Logged as admin 🔒

#### Managing: 2.0.0.53

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

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 with NAP	/ NHA
Endpoint Inspection TCG	

lpoint Inspection TCG	Р / NHA v2.0	NN48500-567
Managing: <b>2.0.0.53</b> Secure Access Domain » AAA » /	Authentication » LDAP » LDAP Settings	Logged as admin 🖉 🔒
LDAP Settings		
Secure Access Domain: 1 eselab.	com 💌 <u>Refresh</u> Auth ID: 2 💌 <u>Refresh</u>	
Search Base Entry:	ers.DC=eselab.DC=com (example: ou=People.dc=	bluetail.dc=com)
Group Attribute:	memberOf	Substan, do borny
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:	enabled 💌	
Cut Domain from User Name:	disabled 💌	
		Update
Using the Browser Bas AAA, Authentication, L Address and click Upda	ed Interface (BBI) navigation tree cl DAP and then <i>Servers</i> . Specify the <i>l</i> ate.	ick Secure Access Doma Active Directory Servers
lanaging: 2.0.0.53		Logged as admin 🖉 🔒
Secure Access Domain » AAA » /	Authentication » LDAP » Servers	
Servers		
Add New LDAP Server		
	Domain: 1	
	Auth Id: 2	
	IP Address: 192.168.10.5	
	Port: 389	

#### Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain, 5

Update Back

K

NN48500-567

AAA, Authentication, NTLM and then Ad	d.
Managing: 2.0.0.53 Secure Access Domain » AAA » Authentication » NTLM	Logged as admin 🖉 🔒
Authentication	
	Secure Access Domain: 1 eselab.com 💌 Refresh
(Add	
ID Name Display Nat No NTLM Authenticat	ne Mechanism Servers Created ion servers configured.
/anaging: 2.0.0.53 Secure Access Domain » AAA » Authentication	Logged as admin 🔒
Managing: 2.0.0.53 Secure Access Domain » AAA » Authentication	Logged as admin 🚦
Authentication	
Add Now Authentication Sonver	
Domain:	1
Auth Id:	3 🗸
Name:	w3kserver-ntlm
Display Name:	w3kserver-ntlm
Mechanism:	ntim 💌
Group Authentication Servers:	Available Selected
	Update

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

NN48500-567

Domain Controller then click <i>Update</i> .
Managing: 2.0.0.53 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
Password Expired Group:None
Update
8 Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain, AAA, Authentication, NTLM, Servers and click Add.
Managing: 2.0.0.53 Logged as admin 2 is admin a secure Access Domain » AAA » Authentication » NTLM » Servers
Authentication
Secure Access Domain: 1 eselab.com 💌 Refresh Auth ID: 3 💌 Refresh
Add
ID IP Address Reorder
9 Specify the IP Address of the Domain Controller and click <i>Update</i> .
Managing: 2.0.0.53 Secure Access Domain » AAA » Authentication » NTLM » Servers
Authentication
Add New NTLM Server
Domain: 1
IP Address: 192.168.10.5 (format: 10.10.1.75)
Update Back

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

SNA 2.0 802.1X Authentication with NAP / dpoint Inspection TCG	NHA v2.0		NN48500-567	
Managing: 2.0.0.53 Secure Access Domain » AAA » Auth	entication » NTLM » Join		Logged as admin 😰	
Authentication				
Secure Access Demain:	Defreeb Auth Dr 2	Defreeb		
Secure Access Domain: T eselab.com	n ▼ <u>Reliesh</u> Autilio: 3	▼ <u>Reifesh</u>		
Domain ad	ministrator account: admin	istrator		
Domain adm	inistrator password:	*****		
	n password (again).			
				_
The LDAP and NTLM serv	ers will now be inst	alled on the Secur	e Network Access	
Switch.				
Add Edit Delete				_
	Display Namo	Mechanism	Servers Created	
	local	LOCAL	Not applicable	
2 w3kserver1-ldap	w3kserver1-ldap	LDAP	Yes	
3 w3kserver-ntim	w3kserver-ntim	NTLM	Yes	
2 AuthOrder. In the Availab click move and then Upda	<i>le</i> list highlight the n ate.	ame of the NLTM	authentication server	
anaging: 2.0.0.53			Logged as admin 🔒	
Secure Access Domain » AAA » Authe	entication » AuthOrder			
uthOrder				
Secure Access Domain: 1 eselab.com	Refresh			
allback Order				
	Available	Selected		
2 w3	kserver1-ldap 🔺	1 local 🔺		
		3 w3kserver-ntlm		
	<<			
	V	T		
			Update	

NN48500-567



Back

#### 2.1.5 Filters:

Four filters will be defined on the Nortel Secure Network Access Switch that will be later associated with the extended profiles to determine user VLAN membership based on the endpoints NHA and NAP compliance state:

Filter Name	NHA Checks Passed	NAP Checks Passed	Application
NHA_NAP_Passed	True	True	Filter will be matched when both NHA and NAP compliance checks pass.
NHA_Passed_NAP_Failed	True	False	Filter will be matched when NHA compliance checks pass and NAP compliance checks fail.
NHA_Failed_NAP_Passed	False	True	Filter will be matched when NHA compliance checks fail and NAP compliance checks pass.
NHA_NAP_Failed	False	False	Filter will be matched when both NHA and NAP compliance checks fail.

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

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

NN48500-567

	Managing: 2.0.0.53 Logged as admin 🔒
	Filters
	Secure Assess Demain: 1 could com - Defrach
	Secure Access bomain: T eserab.com V Refresh
	ID Name Nortel Health Agent Checks Passed PatchLink Checks Passed NAP Checks Passed No Filters configured.
2	Specify the name NHA_NAP_Passed and set both the Nortel Health Agent Checks Passed and Nap checks passed fields to true. Click Update.
	Managing: 2.0.0.54 Logged as admin 1 Secure Access Domain » AAA » Filters
	Filters
	Add New Filter
	Filter Id: 1 -
	Name: NHA_NAP_Passed
	Nortel Health Agent Checks true
	Passed:
	NAP checks passed: true
	Comment:
	Update Back
	Click Addte exects a second filter Specify the name NUA Deceed NAD Failed and
3	set the Nortel Health Agent Checks Passed field to true and the Nap checks passed
	field to false. Click Update.
	Managing: 2.0.0.54 Logged as admin [2] 1 Secure Access Domain » AAA » Filters
	Filters
	Add New Filter
	Filter Id: 2 -
	Name: A_Passed_NAP_Failed
	Nortel Health Agent Checks true
	Passed:
	NAP checks passed: false -
	Comment:
4	Click Add to create a third filter. Specify the name NHA_Failed_NAP_Passed and set
	the Nortel Health Agent Checks Passed field to false and the Nap checks passed field

NN48500-567

Logged as admin 🖉 🔒

to true. Click Update.

#### Managing: 2.0.0.54

Secure Access Domain » AAA » Filters

#### Filters

#### Add New Filter

Filter Id:	3 -
Name:	A_Failed_NAP_Passed
Nortel Health Agent Checks Passed:	false 🔻
atchLink Check Passed:	ignore 👻
NAP checks passed:	true 👻
Comment:	
	Update

Click Add to create a fourth filter. Specify the name NHA\_ NAP\_Failed and set both the Nortel Health Agent Checks Passed and Nap checks passed fields to false. Click Update.

Managing: 2.0.0.54 Secure Access Domain » AAA » Filters	Logged as admin 🖉 🔒
Filters	

#### Add New Filter

Filter Id:	4 🔻
Name:	NHA_NAP_Failed
Nortel Health Agent Checks Passed:	false 🔻
PatchLink Check Passed:	ignore 👻
NAP checks passed:	false 🔻
Comment:	

6 Four filters will now be defined on the Nortel Secure Network Access Switch.

Ad	Add Edit Delete				
	ID	Name	Nortel Health Agent Checks Passed	PatchLink Checks Passed	NAP Checks Passed
	1	NHA_NAP_Passed	true	ignore	true
	2	NHA_Passed_NAP_Failed	true	ignore	false
	3	NHA_Failed_NAP_Passed	false	ignore	true
	4	NHA_NAP_Failed	false	ignore	false

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

NN48500-567



Warning: Applying changes will save them to the configuration.

Apply Changes

Back

#### 2.1.6 Groups:

A local group named *NAPUsers* will be defined on the Secure Network Access Switch which will have Extended Profiles to determine user VLAN membership based on NAP / NHA compliance state.

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

Using the Browser Based Int AAA, Groups and then Add.	erface (BBI) navigation tree click Secure Access Domain,
Managing: 2.0.0.53 Secure Access Domain » AAA » Groups	Logged as admin 🔒
Groups	
	Secure Access Domain: 1 eselab.com 💌 Refresh
Add	
ID Name	Maximum Login Sessions
	No Groups configured.

#### 2 In the Group Name field enter the name NAPUsers and then click Update.

NSNA 2.0 802.1X Authentication with NAP / NHA			
Endpoint Inspection TCG			

NN48500-567

Logged as admin 🔒

Managing: 2.0.0.53

Secure Access Domain » AAA » Groups

#### Groups

Group Id:	1 -	Available Selected
Group Name:	NAPUsers	*
Maximum Login Sessions:	0	>>
Maximum Session Length:	31 d 0 h 0 m 0 s	ins:
SRS Rule:	<no selection=""> 👻</no>	
MAC Trust Level:	none 🔻	*
rtel Health Agent running mode:	continuous 👻	
Enable MAC Registration:	disabled 👻	
Enable User Registration:	disabled -	
Enforcement Type:	vlan_filter 👻	
Cacho Password Locally:	displad -	
cache i assword Locarry.	disabled +	
The "runonce" option for Nortel Heal and is not applicable for the Nortel H	th Agent running mode is for browser based authenticatio ealth Desktop Agent	n only Update Back
The "runonce" option for Nortel Heal and is not applicable for the Nortel H Apply and save the char	th Agent running mode is for browser based authenticatio ealth Desktop Agent anges by clicking <i>Apply</i> and then <i>App</i> Access Switch	n only Update Back Daly Changes.
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 authenticatio ealth Desktop Agent Ages by clicking <i>Apply</i> and then <i>App</i>	n only Update Back Doly Changes. pply Diff   Revert   Logout   Help Logged as admin 🏹
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 authentication ealth Desktop Agent Ages by clicking <i>Apply</i> and then <i>App</i> Access Switch	n only Update Back Daly Changes. pply Diff   Revert   Logout   Hel; Logged as admin 🖉
The "runonce" option for Nortel Heal and is not applicable for the Nortel H Apply and save the char rtel Secure Network ging: 2.0.0.53 ply Pending Configurat	th Agent running mode is for browser based authenticatio ealth Desktop Agent Ages by clicking <i>Apply</i> and then <i>App</i> Access Switch	n only Update Back Dly Changes. pply Diff   Revert   Logout   Hel Logged as admin 2
Comments: The "runonce" option for Nortel Heal and is not applicable for the Nortel H Apply and save the char ortel Secure Network Iging: 2.0.0.53 ply Pending Configurat Warning: Applying changes will save	th Agent running mode is for browser based authentication ealth Desktop Agent Ages by clicking <i>Apply</i> and then <i>App</i> Access Switch	n only Update Back DIY Changes. pply Diff   Revert   Logout   Hel Logged as admin

#### 2.1.7 Extended Profiles:

Two extended profiles will be defined on the Nortel Secure Network Access Switch that will associate Groups and Filters to determine user VLAN membership based on NAP / NHA compliance state:

Group	Filter Name	VLAN Name
NAPUsers	NHA_NAP_Passed	GREEN1
NAPUsers	NHA_Passed_NAP_Failed	YELLOW
NAPUsers	NHA_Failed_NAP_Passed	YELLOW
NAPUsers	NHA_NAP_Failed	YELLOW

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

Using the Browser Base AAA, Groups, Extended	ed Interface (BBI) navi d Profiles and then Ad	gation tree click <i>Secure Access Domain,</i> d.
Managing: 2.0.0.53 Secure Access Domain » AAA » (	Groups » Extended Profiles	Logged as admin 🔒
Extended Profiles		
Secure Access Domain: 1 eselab.c	com ▼ <u>Refresh</u> Group: 1 N	APUsers ▼ <u>Refresh</u>
D Name	No Profiles config	red.
2 Select the filter name N Update. Managing: 2.0.0.54 Secure Access Domain » AAA » (	HA_NAP_Passed and Groups » Extended Profiles	set the VLAN Name to <i>GREEN1</i> . Click
Extended Profiles Add New Profile		
ld:	1 •	
Filter Name:	NHA_NAP_Passed -	
Vlan Name:	GREEN1 -	
Access Control List ID:		
		Update Back

# Click Add to create a second profile. Select the filter name *NHA\_Passed\_NAP\_Failed* and set the VLAN Name to *YELLOW*. Click *Update*.

v2.0

	inaging: 2.0.0.54
	Secure Access Domain » AAA » Groups » Extended Profiles
	xtended Profiles
	dd New Profile
	ld: 2 -
	Filter Name: NHA_Passed_NAP_Failed 🔻
	VIan Name: YELLOW -
	Access Control List ID:
	Update
4	Click Add to create a third profile. Select the filter name NHA_Failed_NAP_Passed
	and set the VLAN Name to YELLOW. Click Update.
Ì	and set the VLAN Name to YELLOW. Click Opdate.
	and set the VLAN Name to YELLOW. Click Opdate.
	and set the VLAN Name to YELLOW. Click Opdate.  Inaging: 2.0.0.54 Secure Access Domain » AAA » Groups » Extended Profiles  Xtended Profiles  dd New Profile
	and set the VLAN Name to YELLOW. Click Opdate.  Inaging: 2.0.0.54 Secure Access Domain » AAA » Groups » Extended Profiles  Xtended Profiles  Id: 3
	and set the VLAN Name to YELLOW. Click Opdate.  Inaging: 2.0.0.54 Secure Access Domain * AAA * Groups * Extended Profiles  Xtended Profiles  Id: 3 - Filter Name: NHA_Failed_NAP_Passed -
	and set the VLAN Name to YELLOW. Click Opdate.  Inaging: 2.0.0.54 Secure Access Domain » AAA » Groups » Extended Profiles  Xtended Profiles  Id: 3  Filter Name: NHA_Failed_NAP_Passed  Vlan Name: YELLOW
	and set the VLAN Name to YELLOW. Click Opdate.
	and set the VLAN Name to YELLOW. Click Opdate. Inaging: 2.0.54 Secure Access Domain * AAA * Groups * Extended Profiles Xtended Profiles dd New Profile Id: 3 • Filter Name: NHA_Failed_NAP_Passed • Vlan Name: YELLOW • Access Control List ID: Update Back

Managing: 2.0.0.54 Secure Access Domain » AAA » Groups » Extended Profiles	Logged as admin 🖉 🔒
Extended Profiles	
Add New Profile	

Id:	4 -
Filter Name:	NHA_NAP_Failed -
Vlan Name:	YELLOW -
Access Control List ID:	
	Update Back

NN48500-567

#### 6 Four Extended Profiles will now be defined on the Nortel Secure Network Access Switch.

ID	Name
1	NHA_NAP_Passed
2	NHA_Passed_NAP_Failed
3	NHA_Failed_NAP_Passed
4	NHA_NAP_Failed

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.	

Back

Apply Changes

#### 2.1.8 RADIUS Server:

The RADIUS server needs to be configured on the Secure Network Access Switch to support PEAP authentication requests from the Nortel Ethernet Switch:

- 1. Certificates The Server and Root CA Certificates created in Section 2.1.3 will be selected for use with PEAP authentication.
- Clients The Ethernet Routing Switch 5500 will be defined as a RADIUS client.
- Realms A realm will be defined to direct authentication requests to the NTLM 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 Server certificate added in section 2.1.3. Click Update.

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
Using the Browser Based Interface (BBI) <i>RADIUS Server</i> then <i>Client</i> . Click <i>Add</i> .	navigation tree click Secure Access Domai
Using the Browser Based Interface (BBI) RADIUS Server then Client. Click Add. Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Client	navigation tree click Secure Access Domain
Using the Browser Based Interface (BBI) RADIUS Server then Client. Click Add. Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Client Client	navigation tree click Secure Access Domain
Using the Browser Based Interface (BBI) RADIUS Server then Client. Click Add. Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Client Client	navigation tree click Secure Access Domain Logged as admin 😭 Secure Access Domain: 1 eselab.com 💌 <u>Refresh</u>
Using the Browser Based Interface (BBI) RADIUS Server then Client. Click Add. Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Client Client	navigation tree click Secure Access Domain Logged as admin 😭 Secure Access Domain: 1 eselab.com 💌 <u>Refresh</u>
Using the Browser Based Interface (BBI) RADIUS Server then Client. Click Add. Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Client Client	navigation tree click Secure Access Domain Logged as admin

<sup>3</sup> Enter the *IP Address* and *Shared Secret* of the Ethernet Routing Switch 5500. Click *Update.*
NSNA 2.0 802.1X Authentication with NAP / NHA Endpoint Inspection TCG	v2.0 NN48500-567	
Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Client	Logged as admin 🔒	
Client		
Add Radius Client		
Domain: Client IP Address: Shared Secret:	1 192.168.10.10 sharedsecret	
	Update Back	
4 The Nortel Ethernet Switch will now be li	isted as a RADIUS client.	
Add Insert Delete		-
D ID IP Address	Shared Secret	
1 192.168.10.10	sharedsecret	
The RADIUS shared key must match th Switch.	ne shared secret defined on the Nortel Ethernet	
<sup>5</sup> Using the Browser Based Interface (BBI) <i>RADIUS Server</i> then <i>Realms</i> . Click <i>Add</i> .	navigation tree click Secure Access Domain	<b>)</b> ,
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 No Realms	Authentication server ID s configured.	

Active Directory Authentication – In the Name field type enter the name of the Active
Directory Domain *ESELAB*. In the *Authentication Server* pull-down menu select the name of the NTLM authentication server created in section 2.1.4 then click *Update*.

SNA 2.0 802.1X Authentication with NAP / NHA ndpoint Inspection TCG	v2.0	NN48500-567	
Managing: 2.0.0.53 Secure Access Domain » RADIUS Server » Realms		Logged as admin 🔒	
Realms			
Add RADIUS Proxy Realm			
	Domain: 1		
Authoptication	Name: ESELAB	_	
Autrentication	Server: 5 wokserver-hum	Update Back	
Additional details on Realms ma	y be located in the App	endix.	
	_		
Apply and save the changes by cl	icking <i>Apply</i> and ther	Apply Changes.	
Nortel Secure Network Access	Switch	Apply   Diff   Revert   Logout   Help	
Managing: 2.0.0.53		Logged as admin 🖉 🔒	
<u>.</u>			
Apply Pending Configuration Chan	ges		
Warning: Applying changes will save them to the co	onfiguration.		
Apply Changes			

### 2.1.9 Network Access Protection:

The NAP settings will be configured to define the criteria that the Nortel Secure Network Access Switch uses to determine NAP compliance state. Optionally auto-remediation may be enabled to automatically correct client issues and a troubleshooting URL provided to non-compliant users if desired.

NAP configuration 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
	then NAP. Modify base NAP settings as needed and then click Update.

Managing: 2.0.0.53 Secure Access Domain » NAP	Logged as admin 🔒
NAP	
General Settings	Secure Access Domain: 1 eselab.com   Refresh e enabled when at least one Remote NPS server is configured.
Automatic Remediation: false  Policy Decision Point: local	Trouble Shooting URL:
Probation Settings	bled only when Full Access for a Limited Time is enabled.
Full Access for a Limited Time: disa	In the second se
utomatic Remediation true   false>	When true will automatically apply the necessary settings to allow a non-compliant computer to become compliant.
rouble Shooting URL	Provides the NAP client with a URL to provide details for becoming compliant as well as obtaining the latest patches.
ull Access for a Limited Time true   false>	When true provides full access for non-compliant devices for a limited time.
ate YYYY-MM-DD>	Specifies a date where limited access for non-compliant devices starts.
ime HH:MM:SS>	Specifies a time where limited access for non-compliant devices starts.
For each NAP setting r	nodified click I Indate in the respected section to apply the

(1)

For each NAP setting modified click Update in the respected section to apply the changes.

Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain,
NAP then Windows System Health Validator. Modify the Windows System Health
Validator settings as required and then click Update.

NN48500-567



#### Managing: 2.0.0.53 Logged as admin 🔒 Secure Access Domain » NAP » Windows System Health Validator Windows System Health Validator **General Settings** Refresh Secure Access Domain: 1 eselab.com Firewall application: on 👻 Automatic update: on 👻 Virus Protection Antivirus is up to date: Antivirus: true • true -Spyware Antispyware: false 🔻 Antispyware is up to date: true $\overline{\mathbf{v}}$ Upda Security Updates Protection Security Updates Protection: false -Security Updates Severity: critical $\mathbf{T}$ Updates from WSUS: true -Duration allowed since last sync: 86400 (Seconds) Windows Update: true -Update Firewall application When on verifies that a Firewall is present and operational on the client <on | off> Automatic update When on verifies that automatic updates are enabled for the firewall <on | off> Antivirus When true verifies that Antivirus is present and operational on the client <true | false> When true verifies that automatic updates are enabled for Antivirus is up to date Antivirus <true | false> Antispyware When true verifies that Antispyware is present and operational on the client. <true | false> Antispyware is up to date When true verifies that Antispyware is up to date and has the latest updates installed <true | false>

Security <true fa<="" th=""  =""><th>Updates Protection lse&gt;</th><th>When true the Windows System Health Verifier (WSHV) will validate the Windows endpoint's current software security patch levels.</th></true>	Updates Protection lse>	When true the Windows System Health Verifier (WSHV) will validate the Windows endpoint's current software security patch levels.
Security < Critical Moderate	Updates Severity   Important   e   Low   All >	Instructs the windows System Health Verifier (WSHV) to validate the minimum level of all Windows security update patches on the Windows endpoint.
Duration sync <3600 - 3	allowed since last	Designates the duration of time allowed to pass since the Windows endpoint was last updated its own copy of its Windows security update list from its security update source (Windows Update or Windows Server Update Service)
Updates <true fa<="" td=""  =""><td>from WSUS lse&gt;</td><td>Designates whether Windows Server Update Service (WSUS) is an acceptable source for endpoints to obtain their Windows security update information.</td></true>	from WSUS lse>	Designates whether Windows Server Update Service (WSUS) is an acceptable source for endpoints to obtain their Windows security update information.
Windows <true fa<="" td=""  =""><td>Update lse&gt;</td><td>Designates whether Microsoft's Windows Update is an acceptable source for endpoints to obtain their Windows security update information.</td></true>	Update lse>	Designates whether Microsoft's Windows Update is an acceptable source for endpoints to obtain their Windows security update information.
E)	For each NAP setting m changes.	odified click Update in the respected section to apply the

3 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	

### 2.1.10 Nortel Health Agent Policy:

A Nortel Health Agent policy will be created on the Nortel Secure Network Access Switch and assigned to the NAPUsers group. The Nortel Health Agent Policy can be used to augment the NAP policy checks and in this example will be configured to check for the existence of a local file which must reside on the end-point for the Nortel Health Policy to pass.

A Nortel Health Agent Policy can be defined on the Secure Network Access Switch using the Browser Based Interface with the following steps:





In the Create New On Disk SRS Entry window click Browse Local System and select the location and name of the file to check (in this example c:\nha.txt). Optionally enable the option Enable Hash Checking and set the From Date/Time and To Date/Time options to Any. Click OK.

NN48500-567

reate New On Disk SRS Entry				×
File (OR Module) Path	C:\nha.txt		Browse	Local System
	(in "C:\Program Fil	es\Nortel" format)		
E Fetch Module Path from Registry			Key Value	
📝 Enable Hash Checking	-0BFE2508E68C36	22F459A2B4DFF693	SHA1	
Vendor API Call Check				
Min Version:	Max Version:			
Any	Any			
Specify Min Version:	Specify Max V	ersion:		
0.0.0.0	0.0.0.0			
(in "x.x.x.x" format; 0 <x<65536)< th=""><th>(in "x.x.x.x" format; (</th><th>D<x<65536)< th=""><th></th><th></th></x<65536)<></th></x<65536)<>	(in "x.x.x.x" format; (	D <x<65536)< th=""><th></th><th></th></x<65536)<>		
Relative Date/Time Range	Not Older Than	(in days)		
Specific Date/Time Range				
From Date/Time:		To Data (Time:		
Any		Any		
O Specify Date/Time:		Specify Dat	e/Time:	
05/14/2008 08:33	:20	05/14/2008	08:33:	20
MM/DD/YYYY HH:MM	/I:SS (hour: 0~23)	MM/DD/YYYY	HH:MM	l:SS (hour: 0~23)
Operating System		🔽 All Windows		
Vindows 2000 Vindows 2000	lows XP	Vindows 2003	👽 Wi	ndows Vista
Ok	cel	Save and More	Check	Validity

<sup>5</sup> A new Nortel Health Policy named NAPUsers has now created on the Secure Network Access Switch. Click *Save* and then exit the *Nortel Health Policy Administrator*.

File Edit Predefined Software Definition Custom S	oftware Definition So	ftware Definition E	intry Rule 1	ool Help						
Predefined Software Definitions Custom Software Definitions Rule Definitions										
[1] 🗶 🗎 🕹 📓 📁 🚰 💥 🏹 🚔 💼										
Software Definition	Path	Process	Version	Date/Time	Registry Key	Registry Expr	DiskOnly	API	Has	Hash
NAPUsers	C:\nha.txt	<none></none>	Any	Any	<none></none>	<none></none>	V		SHA1	5F0BFE25

Optionally specify a message that will be displayed to users in the event of policy failure. To specify a failure message click the *Rule Definition Tab*, expand the *NAPUsers* policy definition and then click *Display Message On Failure*. Type a message in the *Display Message Editor Content* field and click *Set* then *Save*.

**1** 

NAPUsers

v2.0

NN48500-567

Predefined Software Definitions       Rule Definitions         Predefined Software Definitions       Rule Definitions         Rule Expression Editor       Display Message Editor         Rule Expression       Display Message Contents:         Display Messages       The Nortel Health Agent did not detect a required file on your computer.         Please contact Information Services at 555-1212 for resolution.	File Edit Predefined Software Definition Custom Software Definition	1 Software Definition Entry Rule Tool Help
Image: Second	Predefined Software Definitions Custom Software Definitions	Rule Definitions
To NAPUsers       Display Message Contents:         The Nortel Health Agent did not detect a required file on your computer.         Display Message S         Display Message On Failure	🎦 💢 📄 🔶 Expand	Rule Expression Editor Display Message Editor Trigger Action Editor
The Nortel Health Agent did not detect a required file on your computer. Please contact Information Services at 555-1212 for resolution. Please contact Information Services at 555-1212 for resolution.	NAPUsers	Display Message Contents
C Display Message On Failure	🖬 🔛 Display Messages	The Nortel Health Agent did not detect a required file on your computer. Please contact Information Services at 555-1212 for resolution.
	Display Message On Failure	
Set		Set

# Using the Browser Based Interface (BBI) navigation tree click Secure Access Domain, AAA and then Groups. Click on the group named NAPUsers.

Managing: 2.0.0.54 Secure Access Domain » AAA » Groups	Logged as admin 🔒
Groups	
	Secure Access Domain: 1 eselab.com 💌 <u>Refresh</u>
Add Edit Delete	
D ID Name	Maximum Login Sessions

0

# 8 Using the SRS Rule pull-down menu select the Nortel Health Policy named *NAPUsers* then click *Update*.

NSNA 2.0 802.1X Authentication with NAP	/ NHA
Endpoint Inspection TCG	

NN48500-567

Logged as admin 🔒

Managing: 2.0.0.54

Secure Access Domain » AAA » Groups

#### Groups

Group Id:	1	Available Selected
Group Name:	NAPUsers	A .
Maximum Login Sessions:	0	>>
Maximum Session Length:	31 d 0 h 0 m 0 s	
SRS Rule:	NAPUsers	<<
MAC Trust Level:	none 🔻	~
Enable MAC Registration:	disabled -	
Enable User Registration:	disabled -	
Nortel Health Agent running mode:	continuous 🔻	
Enforcement Type:	vlan_filter 👻	
Cache Password Locally:	enabled -	
Comments:		
Apply and save the char	nges by clicking <i>Apply</i> and then <i>Appl</i> y	y Changes.
ortel Secure Network	Access Switch	y   Diff   Revert   Logout   Help
anaging: 2.0.0.53		Logged as admin 🖉 🔒
lanaging: 2.0.0.53		Logged as admin 🖉 🔒
Anaging: 2.0.0.53	ion Changes	Logged as admin 🖉 🔒
lanaging: 2.0.0.53 Apply Pending Configurat	ion Changes	Logged as admin 🖉 🔒
lanaging: 2.0.0.53 Apply Pending Configurat	ion Changes	Logged as admin 🖉 🔒
Anaging: 2.0.0.53 Apply Pending Configurat Warning: Applying changes will save	ion Changes	Logged as admin 🕅 🚹
Apply Pending Configurat	ion Changes	Logged as admin 🖉 🔒

Back

# 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 (<u>Section 2.2.1</u>)
- 2. Virtual LANs (<u>Section 2.2.2</u>)
- 3. RADIUS Server (<u>Section 2.2.3</u>)
- 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:

1 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 30 Unrestricted VLAN for workstations that pass NAP policy checks.
  - o VLAN 50 Remediated VLAN for workstations that fail NAP policy checks.
- The uplink port 48 will be configured to TagAll frames and will be added as a member of VLANs 10, 30 and 50.
- 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:

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 30 name GREEN type port

4 Create a Yellow VLAN for remediated users by issuing the *vlan create <vlan-id> name <vlan-name> type port* command:

ERS5500(config)# vlan create 50 name YELLOW type port

5 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

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

ERS5500(config)# vlan members remove 1 all

7 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 30 48

ERS5500(config)# vlan members add 50 48

8 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

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

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* 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 Microsoft Windows Server 2003:

This section provides the minimum configuration steps required to configure a Windows 2003 Domain Controller to support authentication NTLM authentication requests and LDAP group associations from a Nortel Secure Network Access Switch. For this section the following configuration steps will be performed:

- 1. Active Directory Users (Section 2.3.1)
- Active Directory Groups (<u>Section 2.3.2</u>)



Figure 2.3 – Active Directory Tree

#### 2.3.1 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 lookup and associations.
- A user named 'wireduser' to test EAP authentication on the Nortel Ethernet Switch.

Active Directory Users 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 User.

Eile	Action	⊻iew	<u>W</u> indow	H	elp				_8>
■ → Delegate Control		ntrol		0 🗈 😫 🖬 🎽	: 😼 🛍 💎	- 🧟 🗑			
Activ -	Fina				Users 38 objects				
اء 🚞	New			►	Computer		Type	Description	
စ္နာရီ	All Tas	iks		•	Contact	2	Security Group		
<u>+</u>	New V	vindow	from Here		Group	ſ	Security Group	Designated administrators	
					InetOrgPerson	Owners	Security Group	Members in this group can	
	Refres	;h			MSMQ Queue Alias		User	Built-in account for quest	
T.A	Export	: <u>L</u> ist			Printor	h	User		
	Proper	ties			User	J	Security Group	Group for the Help and Su	
-	. Cobor			_	phared rolder		Security Group	IIS Worker Process Group	
	<u>H</u> elp				IUSR W3KSERVER1		User	Built-in account for anony	
_					IWAM W3KSERVER1		User	Built-in account for Intern	
					Kevin L. Marshall		User		
					🕵 Kristin D. Marshall		User		
					😨 Maddie Marshall		User		
					🕵 nsnas		User		
					RAS and IAS Servers		Security Group	Servers in this group can	
					Schema Admins		Security Group	Designated administrators	
					5UPPORT_388945a0		User	This is a vendor's account	
					😨 Switch Administrator		User		
					🛛 🕵 Switch Administrators	;	Security Group		
					TelnetClients		Security Group	Members of this group ha	
					🕵 Wired User		User		
					WiredEAPUsers		Security Group		
					🕵 Wlan User		User		
				F	WanEAPUsers		Security Group		1

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 2.4. Click *Next*.

Create	: in: eselab.com/Users
-	
<u>F</u> irst name:	nsnas <u>I</u> nitials:
Last name:	
Full n <u>a</u> me:	nsnas
User logon name:	
nsnas	@eselab.com
User logon name	(pre- <u>W</u> indows 2000):
ESELAB\	nsnas

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

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*.

Password:			
 Confirm passwor	d:		-
User <u>m</u> ust ch	nange password at	next logon	
User cannot	change password		
Password ne	ver expires		
Account is di	sabled		

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 Schema Admins SUPPORT_3889 Switch Administr Switch Administr	<u>C</u> opy Add to a group Di <u>s</u> able Account R <u>e</u> set Password Mo <u>v</u> e Open Home Page	Security Group Security Group Jser Jser Security Group	Servers in this group can Designated administrators This is a vendor's account
TelnetClients Wired User WiredEAPUsers Wlan User WlanEAPUsers selection.	Send Maji All Tasks Cut	Security Group _ Jser - Security Group - Jser Security Group	Members of this group ha
	Delete Rena <u>m</u> e P <u>r</u> operties		]]
	Help		

nsnas Properties 🔋 🗙
Member Of         Dial-in         Environment         Sessions           Remote control         Terminal Services Profile         COM+           General         Address         Account         Profile         Telephones         Organization
User logon name: nsnes @eselab.com
User logon name (pre- <u>W</u> indows 2000): ESELAB\ nsnas
Log On Io 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          Image: Never         Image: 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	<u>C</u> opy	Security Group	Servers in this group can
Schema Admins	Add to a group	Security Group [	Designated administrators
SUPPORT_3887	Reset Password	Jser	This is a vendor's account
Switch Administ	Move	Jser	
Switch Administr	Open Home Page	Fecurity Group	
TeinetClients	Send M <u>a</u> il	Security Group	Members of this group ha
Wired User	-	User	
Wan User	All Tas <u>k</u> s V	liser	
WIanEAPUsers	Cu <u>t</u>	Security Group	
	<u>D</u> elete		
	Rena <u>m</u> e		J
	P <u>r</u> operties		
	Help		

NN48500-567

#### 51

7

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. Click *OK*.

Reset Password	? X
<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*.

Create	e in: eselab.com/Users	
<u>F</u> irst name:	Wired <u>I</u> nitials:	
Last name:	User	í 📘
Full n <u>a</u> me:	Wired User	
User logon name:		
wireduser	@eselab.com 💌	
User logon name	(pre- <u>W</u> indows 2000):	
ESELAB\	wireduser	ĺ

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*.

New Object - User	x
Create in: eselab.com/Users	
Eassword:     ••••••       Confirm password:     •••••••	
User <u>m</u> ust change password at next logon     User cannot change password     ✓ Password never expires     Account is disabled	
	_
< <u>B</u> ack <u>N</u> ext> Cancel	

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

### 2.3.2 Active Directory Groups:

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

- A group named 'NAPUsers' used for Wired PEAP user authentication will be created which matches the local group name defined on the Nortel Secure Network Access Switch.
- The user named 'wireduser' will be added as a member to the group 'NAPUsers'.



Windows does not return a specific group attribute for users that only belong to the Domain Users group. If the Domain Users group is used the default group setting on the Nortel Secure Network Access Switch is required.

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 NAPUsers and click OK.

ew Object - Group		
Create in: eselab.c	om/Users	
Group pame:		
NAPUsers		
Group name (pre-Windows 2000)	);	
NAPUsers	, 	
Group scope		
C Domain local	<ul> <li>Security</li> </ul>	
<ul> <li>Global</li> </ul>	C Distribution	
C <u>U</u> niversal		
	ок	Cancel

NN48500-567

<sup>3</sup> In Active Directory Users Snap-In highlight the group NAPUsers, right click and select *Properties.* 

v2.0



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

NAPUsers	Properties	:		? ×
General	Members	Member Of Managed By		
<u>M</u> ember	'S:			
Name S Wi	red User	Active Directory Folder eselab.com/Users eselab.com/Users		
25 ***		Coold Commonstance		
Ad	d	Bemove		
		ОК С	ancel	Apply

## 2.4 Windows XP Professional:

This section provides configuration steps required on a Windows XP Professional SP3 Workstation to enable the Network Access Protection EAP client. For this section the following configuration tasks will be performed:

- 1. Services (<u>Section 2.4.1</u>)
- 2. NAP Enforcement Clients (Section 2.4.2)
- 3. Local Area Network Connection Properties (Section 2.4.3)

#### 2.4.1 Services:

The following services need to be enabled on the Windows XP Professional SP3 workstation to support 802.1X authentication and Network Access Protection:

- Network Access Protection Agent Allows the workstation to provide health information to the Network Policy Server on the Nortel Secure Network Access Switch.
- Wired AutoConfig Provides 802.1X authentication services for wired interfaces.
- Nortel Health Agent Allows the workstation to provide health information to the Nortel Health Policy Agent on the Nortel Secure Network Access Switch.

Network Access Protection and 802.1X services can be enabled on a Windows XP Professional SP3 workstation by using the following procedure:

1 Click Start and then Run. Next to Open type services.msc and then click OK.

Run	23
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	services.msc
	OK Cancel Browse

<sup>2</sup> In the list of services, right-click *Network Access Protection Agent* and select *Properties.* Set the *Startup type* to *Automatic* and then click *OK*.

Network Access Pr	otection Agent Properties (Local Com 🖻 🔀
General Log On R	Recovery Dependencies
Service name: N	lapAgent
Display name:	Network Access Protection Agent
Description: 4	Allows windows clients to participate in Network
Path to executable: C:\WINDOWS\Sys	tem32\svchost.exe -k netsvcs
Startup type:	Automatic
Service status: S	itarted
Start	Stop Pause Resume
You can specify the from here.	start parameters that apply when you start the service
Start parameters:	
	OK Cancel Apply

<sup>3</sup> In the list of services, right-click *Wired AutoConfig* and select *Properties*. Set the *Startup type* to *Automatic* and then click *OK*.

Wired AutoConf	ig Properties (Local Computer)	? 🔀
General Log On	Recovery Dependencies	
Service name:	Dot3svc	
Display name:	Wired AutoConfig	-
Description:	This service performs IEEE 802.1X authentication on Ethernet interfaces	~ ~
Path to executab C:\WINDOWS\S	le: jystem32\svchost.exe -k dot3svc	_
Startup type:	Automatic	•
Service status:	Started	-
Start	Stop Pause Resume	
You can specify I from here.	he start parameters that apply when you start the servic	e
Start parameters:		
	OK Cancel App	oly

#### <sup>4</sup> In the list of services, right-click Nortel Health Agent and select Properties. Set the

NN48500-567

Startup type to Automatic and then click OK.

Nortel Health Ag	ent Properties (Local Computer) 🛛 ? 🔀
General Log On	Recovery Dependencies
Service name:	tunnelguardservice
Display <u>n</u> ame:	Nortel Health Agent
<u>D</u> escription:	Nortel Health Agent Service
Pat <u>h</u> to executabl "C:\Program Files	le: 
Startup typ <u>e</u> :	Automatic
Service status:	Started
<u>S</u> tart	Stop Pause Resume
You can specify t from here.	he start parameters that apply when you start the service
Start parameters:	
	OK Cancel Apply

### 2.4.2 NAP Enforcement Clients:

The Network Access Protection Enforcement and Nortel NAP Enforcement Clients need to be enabled in Windows XP Professional SP3 to support endpoint inspection in an 802.1X Network Access Protection environment. Table 5.2 lists the Network Access Protection Enforcement Clients supported by a Windows XP SP3:

Enforcement Client	Client ID
DHCP Quarantine Enforcement Client	79617
Remote Access Quarantine Enforcement Client	79618
IPSec Relying Party	79619
Wireless Eapol Quarantine Enforcement Client	79620
TS Gateway Quarantine Enforcement Client	79621
EAP Quarantine Enforcement Client	79623
Nortel NAP Enforcement Client	10260993

#### Table 5.2 – Windows XP SP3 NAP Enforcement Clients

The EAP Quarantine Enforcement Client and Nortel NAP Enforcement Client can be enabled on a Windows XP Professional SP3 workstation by using the following procedure:

## <sup>1</sup> Click Start, All Programs, Accessories and then Command Prompt. At the command

prompt enable the EAP Quarantine Enforcement Client by entering the following:

C:> netsh nap client set enforcement ID = 79623 ADMIN = "ENABLE"

2 At the command prompt enable the Nortel NAP Enforcement Client by entering the following:

C:\> netsh nap client set enforcement ID = 10260993 ADMIN = "ENABLE"

### 2.4.3 Local Area Connection Properties:

The following 802.1X configuration will be defined on a Windows XP Professional SP 3 workstation's Local Area Connection:

- IEEE 802.1X authentication will be enabled
- The EAP authentication method will be set to Protected EAP (PEAP) using MSCHAPv2
- User credential caching will be enabled
- TLS certificate validation will be enabled
- Quarantine checks will be enabled
- Single sign-on using domain credentials will be enabled

802.1X configuration can be configured on Windows XP Professional SP3 workstations Local Area Connection by using the following procedure:

Click *Start*, *Control Panel* and then *Network Connections*. In the list of Network Connections right-click *Local Area Connection* and click *Properties*. Click on the

Authentication tab and check the options Enable IEEE 802.1X authentication and
 Cache user information for subsequent connections to this network. Set the authentication method to Protected EAP (PEAP) and then click Settings.

<sup>2</sup> Check the options Validate server certificate, Connect to these servers, Enable Fast



Protected EAP Properties	Protected EAP Properties	
When connecting:	When connecting:	
Validate server certificate	Validate server certificate	
Connect to these servers:	Connect to these servers:	
eselab.com	nsnas-vip.eselab.com	
Trusted Root Certification Authorities:	Trusted Root Certification Authorities:	
Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	
Equifax Secure eBusiness CA-1	Equifax Secure eBusiness CA-1	
Equifax Secure eBusiness CA-2	Equifax Secure eBusiness CA-2	
Equifax Secure Global eBusiness CA-1	Equifax Secure Global eBusiness CA-1	
SELAB CA	ESELAB CA	
eSign Imperito Primary Root CA	eSign Imperito Primary Root CA	
📃 EUnet International Root CA 🛛 🗸	📃 EUnet International Root CA 🛛 🗸	
Do not prompt user to authorize new servers or trusted certification authorities.	Do not prompt user to authorize new servers or trusted certification authorities.	
Select Authentication Method:		
Secured password (EAP-MSCHAP v2)  Configure	Secured password (EAP-MSCHAP v2)	
Disconnect if server does not present cryptobinding TLV	Disconnect if server does not present cryptobinding TLV	
OK Cancel	OK Cancel	

<sup>3</sup> Check the option *Automatically use my Windows logon name and password (and domain if any)*. Click *OK*. Close the Local Area Connection properties window.

EAP MSCHAPv2 Properties
When connecting:
password (and domain if any).
OK Cancel

## 2.5 Windows Vista:

This section provides configuration steps required on a Windows Vista Workstation to enable the Network Access Protection EAP client. For this section the following configuration tasks will be performed:

- 1. Services (Section 2.5.1)
- 2. NAP Enforcement Client (Section 2.5.2)
- 3. Local Area Network Connection Properties (Section 2.5.3)

## 2.5.1 Services:

The following services need to be enabled on the Windows Vista workstation to support 802.1X authentication and Network Access Protection:

• Network Access Protection Agent – Allows the workstation to provide health information to the Network Policy Server on the Nortel Secure Network Access Switch.

v2.0

- Wired AutoConfig Provides 802.1X authentication services for wired interfaces.
- Nortel Health Agent Allows the workstation to provide health information to the Nortel Health Policy Agent on the Nortel Secure Network Access Switch.

Network Access Protection and 802.1X services can be enabled on a Windows Vista using the following procedure:

1 Click *Start*, *All Programs*, *Accessories* and then *Run*. Next to *Open* type *services.msc* and then click *OK*.

📼 Run	
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	services.msc 🔹
	OK Cancel Browse

<sup>2</sup> In the list of services, right-click *Network Access Protection Agent* and select *Properties.* Set the *Startup type* to *Automatic* and then click *OK*.

NN48500-567

Vetwork Access Pr	otection Agent Properties (Local Computer)	
General Log On	Recovery Dependencies	
Service name:	napagent	
Display name:	Network Access Protection Agent	
Description:	Enables Network Access Protection (NAP)	
Path to executab C:\Windows\Sys	le: tem32\svchost.exe +k NetworkService	
Startup type:	Automatic	
Help me configure service startup options.		
Service status:	Started	
Start	Stop Pause Resume	
You can specify t from here.	he start parameters that apply when you start the service	
Start parameters:		
	OK Cancel Apply	

3 In the list of services, right-click *Wired AutoConfig* and select *Properties*. Set the *Startup type* to *Automatic* and then click *OK*. Close the Services window.

Wired AutoConfig	Properties (Local Computer)	×
General Log On	Recovery Dependencies	
Service name:	dot3svc	
Display name:	Wired AutoConfig	
Description:	This service performs IEEE 802.1X authentication . on Ethemet interfaces	*
Path to executabl C:\Windows\syst	e: m32\svchost.exe +k LocalSystemNetworkRestricted	
Startup type:	Automatic	-
Help me configure	e service startup options.	
Service status:	Started	
Start	Stop Pause Resume	
You can specify the from here.	ne start parameters that apply when you start the service	•
Start parameters:		
	OK Cancel Appl	y

4 In the list of services, right-click *Nortel Health Agent* and select *Properties*. Set the *Startup type* to *Automatic* and then click *OK*. Close the Services window.

NN48500-567

Nortel Health A	Agent Proprtied (Local Computer)	3	
General Lo	g On Recovery Dependencies		
Service nar	ne: tunnelguardservice		
Display nan	e: Nortel Health Agent		
Description	Nortel Health Agent Service		
Path to exe ''C:\Program	cutable: n Files\Nortel\TunnelGuard\CueAgent_srv.exe''		
Startup type	E: Automatic		
Help me configure service startup options.			
Service stat	tus: Started		
Start	Stop Pause Resume		
You can specify the start parameters that apply when you start the service from here.			
Start param	eters:		
	OK Cancel Apply		

### 2.5.2 NAP Enforcement Client:

The Network Access Protection Enforcement and Nortel NAP Enforcement Clients need to be enabled in Windows Vista to support endpoint inspection in an 802.1X Network Access Protection environment. Table 6.2 lists the Network Access Protection Enforcement Clients supported by a Windows Vista:

Enforcement Client	Client ID
DHCP Quarantine Enforcement Client	79617
Remote Access Quarantine Enforcement Client	79618
IPSec Relying Party	79619
TS Gateway Quarantine Enforcement Client	79621
EAP Quarantine Enforcement Client	79623
Nortel NAP Enforcement Client	10260993

#### Table 6.2 – Windows Vista NAP Enforcement Clients

The EAP Quarantine Enforcement Client and Nortel NAP Enforcement Client can be enabled on a Windows Vista workstation by using the following procedure:

Click *Start*, *All Programs*, *Accessories* and then *Command Prompt*. At the command prompt enable the EAP Quarantine Enforcement Client by entering the following:

C:\> netsh nap client set enforcement ID = 79623 ADMIN = "ENABLE"

# At the command prompt enable the Nortel NAP Enforcement Client by entering the following:

C:\> netsh nap client set enforcement ID = 10260993 ADMIN = "ENABLE"

6)

NAP enforcement client configuration may also be performed using Group Policy.

#### 2.5.3 Local Area Connection Properties:

The following 802.1X configuration will be defined on a Windows Vista workstation's Local Area Connection:

- IEEE 802.1X authentication will be enabled.
- The EAP authentication method will be set to Protected EAP (PEAP) using MSCHAPv2.
- User credential caching will be enabled.
- TLS certificate validation will be enabled.
- Quarantine checks will be enabled.
- Single sign-on using domain credentials will be enabled.

Click Start, Control Panel, Network and Internet and Network and Sharing Center. In the left pane click Manage Network Connections. Right-click Local Area Connection and then click Properties. Click on the Authentication tab and check the options

v2.0

<sup>1</sup> Enable IEEE 802.1X authentication and Cache user information for subsequent connections to this network. Set the authentication method to Protected EAP (PEAP) and then click Settings.

📱 Local Area Connection Properties 🛛 💌
Networking Authentication
Select this option to provide authenticated network access for this Ethemet adapter.
Protected EAP (PEAP)
Cache user information for subsequent connections to this network
OK Cancel

Check the options Validate server certificate, Connect to these servers, Enable Fast Reconnect and Enable Quarantine checks. Below Connect to these servers enter the domain name for the network or common name of the server certificate installed on the SNAS. Click Configure.

NN48500-567

Protected EAP Properties	Protected EAP Properties
When connecting:	When connecting:
Validate server certificate	- I Validate server certificate
Connect to these servers:	Connect to these servers:
Trusted Root Certification Authorities:	Trusted Root Certification Authorities:
Class 3 Public Primary Certification Authority Equifax Secure Certificate Authority ESELAB CA GTE CyberTrust Global Root Microsoft Root Authority Thawte Premium Server CA	Class 3 Public Primary Certification Authority Equifax Secure Certificate Authority Escuab CA GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Thawte Premium Server CA Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure Configure Configure Configure Disconnect if server does not present cryptobinding TLV	Select Authentication Method: Secured password (EAP-MSCHAP v2)  Configure  Fable Fast Reconnect Fable Quarantine checks Disconnect if server does not present cryptobinding TLV
OK Cancel	OK Cancel

Check the option Automatically use my Windows logon name and password (and domain if any). Click OK. Close the Local Area Connection properties window.

EAP MSCHAPv2 Properties								
When connecting:								
A described was an Windows losse some and								
Automatically use my Windows logon name and password (and domain if any).								
OK Cancel								

# 3. Verification:

## 3.1 Windows Workstation Compliant NAP / NHA State:

The following behavior will be seen on a Windows XP / Vista workstation upon successful PEAP authentication with compliant Network Access Protection and Nortel Health Agent client states:

The following message and icons will be displayed in the Windows toolbar upon
successful PEAP authentication with compliant Network Access Protection and Nortel Health Agent client states.



The *ipconfig* command can be issued on the workstation to view the current IP addressing configuration which can be used to verify VLAN membership. In this

2 example the DHCP scope for the Green VLAN *30* has been configured to provide the DNS suffix *green.eselab.com* which provides an easy way to identify VLAN membership.

C: \>i pconfi g

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connecti on-speci	fi	С	D١	IS	Sι	uff	٦i)	(		:	green. esel ab. com
IP Address										:	192. 168. 30. 100
Subnet Mask									•	:	255. 255. 255. 0
Default Gateway										:	192. 168. 30. 1

On the Ethernet Switch the *show vlan interface vids <port-number>* NNCLI command can be used to view which VLANs are assigned to switch port. In this example a compliant Windows Workstation is connected to port *1* and has been placed in an unrestricted VLAN id *30* named *GREEN*.

#### 5500-1# show vlan interface vids 1

 Port VLAN VLAN Name
 VLAN VLAN Name
 VLAN VLAN Name

 1
 30
 GREEN1

## 3.2 Windows Workstation Non-Compliant NAP State:

The following behavior will be seen on a Windows XP / Vista workstation upon successful PEAP authentication with non-compliant Network Access Protection and compliant Nortel Health Agent client states:

The following message and icons will be displayed in the Windows toolbar upon
successful PEAP authentication with non-compliant Network Access Protection and compliant Nortel Health Agent client states.

👔 This computer does not meet the requirements of this network	×		
Network access is limited.			
	V	� =" • <b>秋</b> 帰の ∛ 品  ≥	10:44 AM

The *ipconfig* command can be issued on the workstation to view the current IP addressing configuration which can be used to verify VLAN membership. In this

2 example the DHCP scope for the Yellow VLAN 50 has been configured to provide the DNS suffix *yellow.eselab.com* which provides an easy way to identify VLAN membership.

#### C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connecti on-speci	fi	С	DN	S	Sι	ıff	ì>	(	:	yellow.eselab.com
IP Address									:	192. 168. 50. 100
Subnet Mask									:	255. 255. 255. 0
Default Gateway									:	192. 168. 50. 1

On the Ethernet Switch the *show vlan interface vids <port-number>* NNCLI command can be used to view which VLANs are assigned to switch port. In this example a compliant Windows Workstation is connected to port *1* and has been placed in an unrestricted VLAN id *30* named *GREEN*.

5500-1# show vlan interface vids 1

1	50	YELLOW	

# **3.3 Windows Workstation Non-Compliant NHA State:**

The following behavior will be seen on a Windows XP / Vista workstation upon successful EAP authentication with compliant Network Access Protection and non-compliant Nortel Health Agent client states:

The following message and icons will be displayed in the Windows toolbar upon
successful PEAP authentication with compliant Network Access Protection and noncompliant Nortel Health Agent client states.

	Nortel Health Agent Check Error There is an error during health check. You can right click Nortel Health Agent icon or hit 'Show Status' button below to view status information. Rule Message:
	The Nortel Health Agent did not detect a required file on your computer. Please contact Information Services at 555 -1212 for resolution.
This computer does not meet the requirements of Network access is limited.	f this network Show Status

The *ipconfig* command can be issued on the workstation to view the current IP addressing configuration which can be used to verify VLAN membership. In this
example the DHCP scope for the Yellow VLAN 50 has been configured to provide the DNS suffix *yellow.eselab.com* which provides an easy way to identify VLAN membership.

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connecti on-speci	fi	С	D١	١S	Sι	uft	fi)	ĸ	•	:	yellow.eselab.com
IP Address										:	192. 168. 50. 100
Subnet Mask										:	255. 255. 255. 0
Default Gateway										:	192. 168. 50. 1

3

1

On the Ethernet Switch the *show vlan interface vids <port-number>* NNCLI command can be used to view which VLANs are assigned to switch port. In this example a compliant Windows Workstation is connected to port *1* and has been placed in an unrestricted VLAN id *30* named *GREEN*.

```
5500-1# show vlan interface vids 1
```

1	50	YELLOW						
Port	VLAN	VLAN Name	VLAN	VLAN	Name	VLAN	VLAN	Name

## 3.4 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	Sessi on 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

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

## 3.5 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 issuing the show eapol port <port-number> command. ERS5500-1# show eapol port 1 EAPOL Administrative State: Enabled EAPOL User Based Policies: Disabled EAPOL User Based Policies Filter On MAC Addresses: Disabled Admi n Admin Oper ReAuth ReAuth Quiet Xmit Supplic Server Max Port Status Auth Dir Dir Enable Period Period Period Timeout Timeout Req Yes Both Both Yes 3600 10 30 30 1 Auto 30 2 The VLAN membership of a specific port may be viewed by issuing the show vlan 2 *interface vids <port-number>* command. ERS5500-1# show vlan interface vids 1-2 Port VLAN VLAN Name VLAN VLAN Name VLAN VLAN Name ---- ---- ----- ---- ----- -----1 30 GREEN 2 40 YELLOW \_\_\_\_\_ \_\_\_\_ 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

ERS5500-1# show vlan

١d	Name		Туре	Protocol	User PID	Acti ve	IVL/SVL	Mgmt
1	DEFAULT		Port	None	0x0000	Yes	I VL	No
	Port	Members:	NONE					
10	SERVI CES		Port	None	0x0000	Yes	I VL	Yes
	Port	Members:	48					
30	GREEN		Port	None	0x0000	Yes	I VL	No
	Port	Members:	48					
50	YELLOW		Port	None	0x0000	Yes	I VL	No
	Port	Members:	48					

Total VLANs: 3

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

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

#### Port: 1

EntersConnecting:				
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:				
BackendAuthSuccesses:				
BackendAuthFails:	0			

NN48500-567
# 6 EAPOL statistics for a port may be viewed by issuing the show eapol auth-stats interface <port-number> command.

### ERS5500-1# 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

## 4. Appendix:

### 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 Health Agent	vV5.0.0.33
Nortel Ethernet Routing Switch 5500	v5.1.0.015
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 Release Service Pack 2 Service 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 Secure Network Access Switch Configuration - Using BBI (323857-B)	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>.