

Ethernet Switch Ethernet Routing Switch Engineering

> Wired PEAP Machine Authentication for ERS and ES Technical Configuration Guide

Enterprise Solutions Engineering Document Date: January 31, 2008 Document Number: NN48500-547 Document Version: 1.0

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:

The document provides an overview on how to configure Wired PEAP computer and user authentication on Nortel Ethernet Switches in a Microsoft environment. This document demonstrates configuring the Microsoft Internet Authentication Service on a Windows 2003 server, the Microsoft Windows XP 802.1X supplicant and the Nortel Ethernet Switch. This document does not address Certificate Services or Active Directory as this is well documented on Microsoft's web site.

Revision Control:

No	Date	Version	Revised by	Remarks
1	Apr 30 th 2007	1.0	Brad Black	Final Version for Release
2	Nov 14 th 2007	2.0	Kevin Marshall	Revised and reformatted.

Acknowledgements:

Table of Contents:

DOCUMENT UPDATES:	4
CONVENTIONS:	4
1. OVERVIEW:	5
 1.1 WHAT IS COMPUTER AUTHENTICATION:	5 6 7 7
2. INTERNET AUTHENTICATION SERVICE:	8
 2.1 Add Radius Clients: 2.2 Create a Remote Access Policy: 	8 11
3. NORTEL ETHERNET SWITCH:	16
 3.1 DEFINE A RADIUS SERVER: 3.2 SET THE EAPOL ADMIN STATE: 3.3 GLOBALLY ENABLE EAPOL: 	16 17 17
4. WINDOWS XP WORKSTATION:	18
 4.1 CERTIFICATES:	18 21 23
5. VERIFICATION:	25
 5.1 WINDOWS SYSTEM EVENT LOGS: 5.1 ETHERNET SWITCH EAPOL PORT STATUS: 	25 26
6. APPENDIX:	27
 6.1 EAPOL USERS ACTIVE DIRECTORY GROUP 6.2 ACTIVE DIRECTORY REMOTE ACCESS PERMISSIONS 6.3 WINDOWS XP REGISTRY SETTINGS 6.4 WIRELESS ZERO CONFIGURATION SERVICE	27 28 29 30
7. REFERENCE DOCUMENTATION:	32

Document Updates:

None.

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.



Caution – 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 Lucida 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

enabl e

configure terminal

1. Overview:

The document provides an overview on how to configure Wired PEAP computer and user authentication on Nortel Ethernet Switches in a Microsoft environment. This document demonstrates configuring the Microsoft Internet Authentication Service on a Windows 2003 server, the Microsoft Windows XP 802.1X supplicant and the Nortel Ethernet Switch. This document does not address Certificate Services or Active Directory as this is well documented on Microsoft's web site.

1.1 What is Computer Authentication:

User authentication is a natural choice when considering identification to Wired or Wireless infrastructure. However, in most cases Enterprises will also want to also implement computer (or machine) authentication to ensure a complete solution.

There are a number of features in Windows that will only work correctly with an active network connection. Leveraging 802.1X computer authentication ensures that this network connection is established during the Windows boot sequence and prior to end users seeing the initial Windows logon screen. The following table provides a list of some of the common Windows features that require such a connection:

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

Table 1.1 – Scenarios Requiring Machine Authentication

1.2 Windows XP Boot Process:

Unlike 802.1X user authentication which occurs after the end user has logged into Windows, computer authentication occurs during the boot process before the end user is presented with the Windows Logon screen:

- 1. When machine authentication is enabled, the computer will authenticate to the switch port using its machine credentials as soon as an Ethernet link becomes active. If computer authentication is successful the EAPOL Ethernet port status will change to Authorized and the user placed in the appropriate VLAN which may be statically assigned or provided dynamically from the authentication server.
- 2. When a user logs onto the computer, the user authentication will supersede the computer authentication. The Ethernet switch will assign the user to the appropriate VLAN which may be statically assigned or provided dynamically from the authentication server.
- 3. When a user logs off the computer, computer authentication will re-occur and the Ethernet Switch will assign the computer to the appropriate VLAN which may be statically assigned or provided dynamically from the authentication server.



Figure 1.2.1 – Wired Machine Authentication Process

NN48500-546

1.3 **Pre-Requisites:**

This document makes the following assumptions in regards to the Windows 2003 server, Windows XP workstation and Nortel Ethernet Switch:

- 1. A Windows 2003 Advanced or Enterprise Server is installed with the following:
 - a. Latest service pack and updates installed
 - b. Configured as an Active Directory Domain Controller.
 - i. One or more Active Directory User accounts have been created.
 - ii. A unique Group such as **EAPOL Users** has been created with User and Computer accounts that will be performing EAP authentication and has been added as members to the Group (**see** <u>Appendix 6.1</u>)
 - iii. The Remote Access Permission for each of the User and Computer accounts performing EAP authentication are set to Allowed Access (see <u>Appendix 6.2</u>).
 - c. Certificate Services is installed as an Enterprise Root CA.
 - d. Internet Authentication Service is installed.
 - e. IP communication with the Nortel Ethernet Switch.
- 2. Windows XP Workstation with the following:
 - a. Latest service pack and updates installed.
 - b. Is a member of the Windows Domain.
 - c. The Microsoft Wireless Zero Configuration service is running (see <u>Appendix</u> <u>6.4</u>).
- 3. Nortel Ethernet Switch with the following:
 - a. One VLAN with a management IP address assigned.

1.4 Topology:



Figure 1.4.1 – Topology

2. Internet Authentication Service:

For the Microsoft Internet Authentication Service (IAS) to be able to authenticate PEAP users connected to a Nortel Ethernet switch the following configuration steps need to be performed:

- 1. The Nortel Ethernet Switch that will be forwarding RADIUS authentication requests to IAS will need to be defined as a RADIUS client.
- 2. A Remote Access Policy needs to be defined so that IAS knows how to authenticate the users as well as which authentication protocols to support.

2.1 Add Radius Clients:

To add a Nortel Ethernet Switch as a RADIUS client to IAS:

- 1. Open the IAS snap-in by clicking **Start**, **Programs**, **Administrative Tools** then **Internet Authentication Service**.
- 2. In the IAS snap-in, right click RADIUS Clients and then click New RADIUS Client.



3. In the **Friendly name** field specify the hostname of the Ethernet switch. In the **Client** address (IP or DNS) field specify the management IP address of the Ethernet switch. Click Next.

ew RADIUS Client		×
Name and Address		
Type a friendly name and	either an IP Address or DNS name fo	or the client.
Eriendly name:	ers5520-48t	
Client address (IP or DNS).	
192.168.1.10		⊻erify
	Z Back	Nevt > Cancel
	<u>v D</u> ack	

4. Select the default **Client-Vendor** option **RADIUS Standard**. Specify and confirm a **Shared secret** which will match the shared secret defined on the Ethernet switch (for example **Nortel**). Click **Next**.

RADIUS Client				
dditional Information				
fyou are using remote access rendor of the RADIUS client.	policies based o	n the client vend	or attribute, specifj	y the
<u>C</u> lient-Vendor:				
RADIUS Standard				-
<u>S</u> hared secret:	*****			
Confirm shared secret:	*****			
n <u>n</u> equest must contain the	: Message Autri	snucator attribute		
			20. 20.	

5. The Nortel Ethernet switch has now been added to IAS as a RADIUS client.



2.2 Create a Remote Access Policy:

To create a Remote Access Policy in IAS to authenticate computers and users using EAP-TLS:

- 1. Open the IAS snap-in by clicking **Start**, **Programs**, **Administrative Tools** then **Internet Authentication Service**.
- 2. In the IAS snap-in right click **Remote Access Policies** and then click **New Remote Access Policy**.

🐓 Internet Authenticatior) Service		_ 🗆 ×
Eile Action View Help			
← → 🔁 💽 🛃	1 😫		
Internet Authentication Se	ervice (Local)	Name	Order
🕀 🧰 RADIUS Clients		S Connections to Microsoft Routing and Remote	1
🕀 🔲 Remote Access Loggin	g	S Connections to other access servers	2
E Connection Request	New Remote Access Policy		
	<u>N</u> ew	•	
	⊻iew	•	
	Refresh Export List		
	Help		
New Remote Access Policy			

3. Click Next.

Wired PEAP Machine Authentication for ERS and ES TCG

v1.0

NN48500-546



4. Select the option **Use the wizard to set up a typical policy for a common scenario**. In the **Policy name** field enter in the name for the policy (for example **EAPOL Users**). Click **Next**.

Policy Configu	ration Method
The wizard o	can create a typical policy, or you can create a custom policy.
How do you v	vant to set up this policy?
	e wizard to set up a typical policy for a common scenario
C Set up	a custom policy
Type a name t	hat describes this policy.
Type a name t <u>P</u> olicy name:	hat describes this policy. EAPOL Users
Type a name t <u>P</u> olicy name:	hat describes this policy. EAPOL Users Example: Authenticate all VPN connections.
Type a name t <u>P</u> olicy name:	hat describes this policy. EAPOL Users Example: Authenticate all VPN connections.
Type a name t <u>P</u> olicy name:	hat describes this policy. EAPOL Users Example: Authenticate all VPN connections.

5. Select the **Access Method** option **Ethernet** then click **Next**. This sets the match criteria in the policy to only authenticate requests from Ethernet devices.

Wired PEAP Machine Authentication for ERS and ES TCG

v1.0

NN48500-546

Rem	ote Access Policy Wizard
Acces Po	ss Method Dicy conditions are based on the method used to gain access to the network.
Sele	ct the method of access for which you want to create a policy.
C	〕 ⊻PN
	Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
C	Dial-up Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
C	∑ <u>W</u> ireless
	Use for wireless LAN connections only.
G	Ethernet
	Use for Ethernet connections, such as connections that use a switch.
	< Back Next > Cancel

6. Specify the domain users or groups which the policy will apply to. For this example the domain group called **EAPOL Users** has been added. This sets the match criteria in the policy to only authenticate Users and Computers that are a member of this Domain Group. Click **Next**.

lew Rer	mote Access Policy Wizard		×
User	r or Group Access You can grant access to individual users, or you can grant acc groups.	cess to selected	ŷ
Gra C	ant access based on the following: User User access permissions are specified in the user account. Group Individual user permissions override group permissions. Group name:		
	JCLAB\EAPOL Users		Add
	< <u>B</u> ack [<u>N</u> ext >	Cancel

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

NN48500-546

7. Select the EAP type **Protected EAP (PEAP)**. Click **Configure** to specify a server certificate to be used by the policy.

Authentication Methods			Æ
EAP uses different types of security de	vices to authenticate use	ers.	Ŋ
Select the EAP type for this policy.			
<u>I</u> ype:			
Protected EAP (PEAP)			Configure

8. In the **Certificate issued to** pull down menu, select the server certificate you wish to use for the policy. For this example the default server certificate installed on the Windows 2003 Advanced server named **w3kserver.jclab.com** is used. Click **OK** and then **Next**.

Friendly name:		
ssuer: J	ICLAB	
Expiration date: 1	/8/2008 11:44:36 AM	
Enable Fast Reconnect		
ap Types		
and the second		and the

9. Verify the information is correct and then click **Finish**.

Wired PEAP Machine Authentication for ERS and ES TCG

NN48500-546



10. The Remote Access Policy EAPOL Users has now been created.



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

NN48500-546

3. Nortel Ethernet Switch:

For a Nortel Ethernet Switch to be able to support Windows XP workstations authenticating using EAP-TLS the following configuration steps need to be performed:

- 1. A RADIUS server IP addresses, port and shared key needs to be defined.
- 2. The EAPOL admin state for user ports needs to be set.
- 3. EAPOL needs to be globally enabled.

3.1 Define a RADIUS Server:

To add Microsoft IAS as a RADIUS authentication server to a Nortel Ethernet switch using NNCLI:

1 Enter the User EXEC mode by issuing the following command:

ers5510-48t> *enable*

ers5510-48t#

```
2 Enter the Privilege EXEC command mode by issuing the following command:
```

ers5510-48t# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

ers5510-48t(config)#

Define a primary RADIUS server IP address, port and shared key. For this example the 3 IP address of the IAS server is 192.168.1.5, the port is 1812 and the shared key is Nortel (Note: the shared key must match what was defined on IAS in section 2.1):

ers5510-48t(config)# radius-server host 192.168.1.5 port 1812 key Nortel

4 You can verify the RADIUS server configuration by issuing the following command:

ers5510-48t(config)# show radius-server

Password Fallback: Disabled Primary Host: 192.168.1.5 Secondary Host: 0.0.0.0 Port: 1812 Time-out: 2 Key: Nortel Radius Accounting is Disabled AcctPort: 1813

3.2 Set the EAPOL Admin State:

By default all Ethernet ports on a Nortel Ethernet switch are configured with the EAPOL admin state set to **Forced Authorized** which grants access to clients without EAP authentication. To enable EAP authentication the EAPOL admin state for user ports needs to be changed to **Auto**.

Please note that the Windows 2003 Advanced Server in this example is connected to port 48. To maintain connectivity with the server the EAPOL admin state on port 48 will remain set to **Forced Authorized**.

1 To change the EAPOL admin state for user ports 1-47 issue the following commands:

```
ers5510-48t(config-if)# interface fastEthernet 1-47
```

```
ers5510-48t(config-if)# eapol status auto
```

2 To verify the EAPOL admin state for all ports issue the following command:

ers5510-48t(config-if)# show eapol port 1-48

	Admi n		Admi n	0per	ReAuth	ReAuth	Quiet	Xmi t	Suppl i c	Server	Max
Port	Status	Auth	Dir	Dir	Enabl e	Peri od	Peri od	Peri od	Ti meout	Ti meout	Req
1	Auto	Yes	Both	Both	No	3600	60	30	30	30	2
2	Auto	Yes	Both	Both	No	3600	60	30	30	30	2
45	Auto	Yes	Both	Both	No	3600	60	30	30	30	2
46	Auto	Yes	Both	Both	No	3600	60	30	30	30	2
47	Auto	Yes	Both	Both	No	3600	60	30	30	30	2
48	F Auth	Yes	Both	Both	No	3600	60	30	30	30	2

3.3 Globally Enable EAPOL:

To globally enable EAPOL on a Nortel Ethernet switch using NNCLI:

```
1 Globally enable EAPOL mode issue the following command:
```

ers5510-48t(config)# eapol enable

```
2 You can verify the EAPOL global state by issuing the following command:
```

ers5510-48t(config)# show eapol

EAPOL Administrative State: Enabled

4. Windows XP Workstation:

For Windows XP to be able to support computer and user authentication the following configuration steps need to be performed:

- 1. Install CA certificate.
- 2. IEEE 802.1X needs to be enabled on the Local Area Network Connection.
- 3. The Windows XP 802.1X supplicant default behavior needs to be modified by adding two registry entries.

4.1 Certificates:

For PEAP computer and user authentication a CA certificate is recommended (but not required) to be installed on the Windows XP workstation:

• CA Certificate – Allows all parties in the certificate chain to validate the identity of the certificates issued from the enterprise CA. It is recommended that a CA certificate be installed into the **Users Personal Trusted Root Certification Authority** certificate store to all Windows XP to validate the identity of the IAS authentication server.

4.1.1 Issuing CA certificates using Web Enrollment:

If a CA certificate is already present for users accounts this step may be skipped.

To issue a CA certificate using Web Enrollment:

- 1. On the Windows XP workstation open the web browser.
- In the Address field type in the IP address or hostname of the Windows 2003 server that is running Certificate Services using the following format: http://server-ipaddress/CertSrv or http://servername.domain.com/CertSrv.



3. Enter in the domain **User name** and **Password** for the user that will be requiring the certificate.



It is important that you login to the web enrollment tool using the username and password of the user that will be using the user certificate. This ensures that the user certificate is issued to the correct username.

Connect to w3	kserver.jclab.com 🛛 🕐 🔀
	GR
Connecting to w3	kserver.jclab.com
<u>U</u> ser name:	😰 jclab\\harshal2 🛛 🔽
Password:	•••••
	Remember my password
_	OK Cancel

1. Click Download a CA certificate, certificate chain or CRL.



2. Click install this CA certificate chain.

🗿 Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	<u>A</u> 2
🕞 Back 🔹 💿 🔹 📓 🚮 🔎 Search 🤺 Favorites 🤣 🎯 - 🚔 🚍	
Address 💩 http://w3kserver1.jclab.com/certsrv/certcarc.asp	🅞 Go 🛛 Links 🎽 Norton AntiVirus 🛃 👻
Microsoft Certificate Services JCLAB	Home
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certification	ate chain.
To download a CA certificate, certificate chain, or CRL, select the certificate and	d encoding method.
CA certificate:	
Encoding method:	
⊙ DER ⊙ Base 64	
Download CA certificate	
Download CA certificate chain	
Download latest base CRL	com.
Download latest delta CRI	
er ovino	Theorem

- 3. You may see a **Potential Scripting Violation** and **Security Warning** dialog windows. Click **Yes**.
- 4. If successful you will see a **CA Certificate Installation** message displayed on the web page.

 Wird PEAP Machine Authentication for ERS and ES TCG
 1.0
 NM4800-546

 Image: State State

5. A CA certificate for the Enterprise CA should now be displayed in the **Certificates -Current User Trusted Root Certification Authorities Certificates** store.

Internet

🕘 Done

🚡 Certificates - [Console Root\Certificates -	Current User\Trusted Root Certif	ication Authorities\Certificates]		X
🏠 File Action View Favorites Window Help 中 → 💼 💼 😨 🗒 😭	2		_18	×
📄 Console Root	Issued To 🛛 🗡	Issued By	Expiration Date	^
	텔 http://www.valicert.com/ 텔 http://www.valicert.com/ 텔 http://www.valicert.com/ 텔 IPS SERVIDORES 텔 JCLAB	http://www.valicert.com/ http://www.valicert.com/ http://www.valicert.com/ IPS SERVIDORES JCLAB	6/25/2019 6/25/2019 6/25/2019 12/29/2009 1/8/2012	
Intermediate Certification Authorities Intermediate Certificates Intrusted Publishers Intrusted Certificates Intrusted Period Certification Authorities Intrusted People Trusted People	 Microsoft Authenticode(tm) Root Microsoft Root Authority Microsoft Root Certificate Authority NetLock Expressz (Class C) Tanusi NetLock Kozjegyzoi (Class A) Tanu 	Microsoft Authenticode(tm) Root Au Microsoft Root Authority Microsoft Root Certificate Authority NetLock Expressz (Class C) Tanusitv NetLock Kozjegyzoi (Class A) Tanusit	12/31/1999 12/31/2020 5/9/2021 2/20/2019 2/19/2019	
Certificate Enrollment Requests Gertificates (Local Computer) Trusted Root Certification Authorities store contains 110	certificates.	NetLock Uzieti (Class B) Tanusitvany	2/20/2019	

4.2 Modify Local Area Connection Properties:

To enable 802.1X EAP-TLS computer and user authentication on a Windows XP Workstation:

- Within Windows XP open the Network Connections Window Properties by clicking Start, Control Panel, Network and Internet Connections then Network Connections. Right click on the Local Area Network Connection and click Properties.
- 2. Click on the Authentication tab. In the EAP type pull-down menu select Protected EAO (PEAP).

- 3. Select the option **Authenticate as computer when computer information is available** which enables computer authentication.
- 4. Click Properties.

🕹 Local Area Connection Properties 🛛 🔹 💽
General Authentication Advanced
Select this option to provide authenticated network access for Ethernet networks.
EAP type: Protected EAP (PEAP)
Properties Authenticate as computer when computer information is available Authenticate as guest when user or computer information is unavailable
OK Cancel



If the Authentication tab is not displayed in the Local Area Connection Properties window the Microsoft Wireless Zero Configuration service is not running. The Authentication tab will only display if the Microsoft Wireless Zero Configuration service is running (see <u>appendix 6.4</u>).

- 5. Select the **Validate server certificate** checkbox. This allows Windows to verify the validity of the server certificate on the IAS RADIUS server.
- 6. Select the **Connect to these servers** checkbox and in the field ether type in the domain name upon which the RADIUS server must reside (example **jclab.com**) or the host and domain name of the IAS server (example **w3kserver.jclab.com**). This tells Windows XP to only authenticate against the servers in a domain that you specify.
- 7. Click Configure.

Wired PEAP Machine Authentication for ERS and ES TCG

When connecting: Validate server certificate Connect to these servers: W3kserver1.jclab.com Trusted Root Certification Authorities: ABA.ECOM Root CA Autoridad Certificadora de la Asociacion Nacional del Notaria Autoridad Certificadora del Colegio Nacional de Correduria P Baltimore EZ by DST Belgacom E-Trust Primary CA C&W HKT SecureNet CA Class A C&W HKT SecureNet CA Class B Configure Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Select Authentication Method:	rotected EAP Pro	perties		? 🔀
Validate server certificate Connect to these servers: W3kserver1.jclab.com Trusted Root Certification Authorities: ABA.ECOM Root CA Autoridad Certificadora de la Asociacion Nacional del Notaria Autoridad Certificadora del Colegio Nacional de Correduria P Baltimore EZ by DST Belgacom E-Trust Primary CA C&W HKT SecureNet CA Class A C&W HKT SecureNet CA Class B C Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured paceward (EAB.MSCHADB.v2)	When connecting:			
Connect to these servers: W3kserver1.jclab.com Trusted Root Certification Authorities: ABA.ECOM Root CA Autoridad Certificadora de la Asociacion Nacional de Notaria Autoridad Certificadora del Colegio Nacional de Correduria P Baltimore EZ by DST Belgacom E-Trust Primary CA C&W HKT SecureNet CA Class A C&W HKT SecureNet CA Class B C Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured paceward (ECB.MSCHADB.v2)	Validate server c	ertificate		
w3kserver1.jclab.com Trusted Root Certification Authorities: ABA.ECOM Root CA Autoridad Certificadora de la Asociacion Nacional del Notaria Autoridad Certificadora del Colegio Nacional de Correduria P Balkimore EZ by DST Belgacom E-Trust Primary CA C&W HKT SecureNet CA Class A C &W HKT SecureNet CA Class B On ont prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured paceward (EAB.MSCHAB.v2)	Connect to thes	e servers'		
Trusted Root Certification Authorities: ABA.ECOM Root CA Autoridad Certificadora de la Asociacion Nacional del Notaria Autoridad Certificadora del Colegio Nacional de Correduria P Baltimore EZ by DST Belgacom E-Trust Primary CA C&W HKT SecureNet CA Class A C&W HKT SecureNet CA Class B C Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Secured paceword (EAB.MSCHADB.v2) Confinure.	w3kserver1.jc	lab.com		
ABA.ECOM Root CA Autoridad Certificadora de la Asociacion Nacional del Notaria Autoridad Certificadora del Colegio Nacional de Correduria P Baltimore EZ by DST Belgacom E-Trust Primary CA C&W HKT SecureNet CA Class A C&W HKT SecureNet CA Class B Continue Do not prompt user to authorize new servers or trusted certification authorities. Secured paceword (EAB.MSCHAB.V2)	Trusted Root Certif	cation Authorities:		
Autoridad Certificadora de la Asociacion Nacional del Notaria Autoridad Certificadora del Colegio Nacional de Correduria P Baltimore EZ by DST Belgacom E-Trust Primary CA C&W HKT SecureNet CA Class A C&W HKT SecureNet CA Class B C Do not prompt user to authorize new servers or trusted certification authorities. Secured parcmard (EAR-MSCHAB.v2) Confinure.	ABA.ECOM Ro	ot CA		^
Autoridad Certricadora del Colegio Nacional de Correduna P Baltimore EZ by DST Belgacom E-Trust Primary CA C&W HKT SecureNet CA Class A C&W HKT SecureNet CA Class B Do not prompt user to authorize new servers or trusted certification authorities. Secured parcmard (EAR-MSCHAR u2) Confinure.	Autoridad Cert	ficadora de la Asoci	acion Nacional de	el Notaria
	Baltimore F7 by	ficadora del Colegio / DST	Nacional de Cori	reduria P
Confinue Co	Belgacom E-Tru	ist Primary CA		
C&W HKT SecureNet CA Class B Contemporation authorize new servers or trusted Certification authorities. Secured parameted (SAR-MSCHAR u2) Confinue.	C&W HKT Secu	reNet CA Class A		
Do not prompt user to authorize new servers or trusted certification authorities.	C&W HKT Secu	reNet CA Class B		~
Do not prompt user to authorize new servers or trusted certification authorities.	<			>
Secured parameter (SAR-MSCHAR-u2)	Do not prompt u certification auth	er to authorize nev orities.	v servers or trust	ed
Secured paceword (EAP_MSCHAP v2)	Select Authentication I	Method:		
Decured password (CAPPROCHAP V2)	Secured password (E	AP-MSCHAP v2)	× (Configure
Enable Fast Reconnect	Enable Fast Recon	nect		
OK Cancel			ОК	Cancel

v1.0

8. Select the **Automatically use my Windows logon name and password (and domain if any)** checkbox. This tells Windows to use the domain credentials to authenticate the user which provides single sign-on for the user.

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

9. Click **OK**, **OK** and then **OK** again.

4.3 Modify Registry Settings:

By default the Windows XP 802.1X supplicant may not behave as expected when computer authentication is enabled. The Windows XP 802.1X supplicant behavior can be modified by adding the AuthMode and SupplicantMode registry entries:

4.3.1 AuthMode Registry Setting:

Purpose	Controls the computer and user authentication behavior on Windows XP Workstations.
Registry Path	HKEY_LOCAL_MACHINE\Software\Microsoft\EAPOL\Parameters\General\Globa

0

NN48500-546

NN48500-546

	\AuthMode
Values	• 0 - Computer authentication mode. If computer authentication is successful, no user authentication is attempted. If the user logon is successful before computer authentication, user authentication is performed. This is the default setting for Windows XP (prior to Service Pack 1).
	• 1 - Computer authentication with re-authentication. If computer authentication is successful, a subsequent user logon results in a re-authentication with user credentials. The user logon has to complete in 60 seconds or the existing network connectivity is terminated. The user credentials are used for subsequent authentication or re-authentication. Computer authentication is not attempted again until the user logs off the computer. This is the default setting for Windows XP Service Pack 1 (SP1) and Windows Server 2003.
	• 2 - Computer authentication only. When a user logs on, it has no effect on the connection. Only computer authentication is performed. The exception to this behavior is when a user successfully logs on, and then roams between wireless APs. In that case, user authentication is performed. For changes to this setting to take effect, restart the Wireless Zero Configuration service for Windows XP or Windows Server 2003.

4.3.2 SupplicantMode Registry Setting:

Purpose	Controls the EAPOL-Start message behavior on Windows XP Workstations.
Registry Path	HKEY_LOCAL_MACHINE\Software\Microsoft\EAPOL\Parameters\General\Global \SupplicantMode
Values	 1 - Do not transmit. Specifies that EAPOL-Start messages are not sent. 2 - Transmit. Determines when to send EAPOL-Start messages and, if needed, sends an EAPOL-Start message. 3 - Transmit per 802.1X. Sends an EAPOL-Start message upon association to initiate the 802.1X authentication process.

4.3.3 Nortel Recommendations:

Nortel recommends that the AuthMode registry entry be set to 1 and the SupplicantMode registry entry be set to 3 (see <u>Appendix 6.3</u>).

5. Verification:

5.1 Windows System Event Logs:

When a Windows XP workstation boots or the user logs out of Windows, PEAP computer authentication will occur and the following log entry will be created in the Windows System Event Log:

Event Type: Information Event Source: I AS Event Category: None Event ID: 1 Date: 1/10/2007 2:36:13 PM Time: N/A User: W3KSERVER1 Computer: Description: User host/obsat.jclab.com was granted access. Fully-Qualified-User-Name = jclab.com/Computers/OBSAT NAS-IP-Address = 192.168.1.10 NAS-Identifier = <not present> Client_Friendly_Name = ers5510-48t NAS-Identifier = <not present> Client-Friendly-Name = ers5510-48t Client-IP-Address = 192.168.1.10 Calling-Station-Identifier = 00-A0-D1-3D-A0-5E NAS-Port-Type = Ethernet NAS-Port = 1 Proxy-Policy-Name = Use Windows authentication for all users Authentication-Provider = Windows Authentication Server = windows Authentication-Server = <undetermined> Policy-Name = EAPOL Users Authentication-Type = PEAP EAP-Type = Secured password (EAP-MSCHAP v2)

When a User logs into Windows XP PEAP user authentication will occur and the following log entry will be created in the Windows System Event Log:

Event Type: Information Event Source: I AS Event Category: None Event ID: 1 Date: 1/10/2007 Time: 2:34:37 PM User: N/A Computer: W3KSERVER1 Description: User JCLAB\marshal 2 was granted access. Fully-Qualified-User-Name = **Jclab.com/Users/Kevin L. Marshall** NAS-IP-Address = 192.168.1.10 NAS-Identifier = <not present> Client-Friendly-Name = ers5510-48t Client-IP-Address = 192.168.1.10 Calling-Station-Identifier = 00-A0-D1-3D-A0-5E NAS-Port-Type = Ethernet NAS-Port = 1Proxy-Policy-Name = Use Windows authentication for all users Authentication-Provider = Windows Authentication-Server = <undetermined> Policy-Name = EAPOL Users Authentication-Type = PEAP EAP-Type = Secured password (EAP-MSCHAP v2)

5.1 Ethernet Switch EAPOL Port Status:

When a computer or user is authenticated the EAPOL port status for the port will be displayed with the **Auth** status set to **Yes**. All unauthenticated ports will be displayed with the **Auth** status set to **No**.

```
ers5510-48t# show eapol port 1
```

	Admi n		Admi n	0per	ReAuth	ReAuth	Quiet	Xmi t	Suppl i c	Server	Max
Port	Status	Auth	Dir	Dir	Enabl e	Peri od	Peri od	Peri od	Ti meout	Ti meout	Req
1	Auto	Yes	Both	Both	No	3600	10	30	30	30	2

6. Appendix:

6.1 EAPOL Users Active Directory Group

The example Remote Access Policy used in this document tells IAS to authenticate users that are a member of the Windows Domain Group called **EAPOL Users**.

For EAP-TLS computer and user authentication to occur, the **Kevin L. Marshall** user account and **OBSAT** computer account were added as members to the **EAPOL Users** group as shown in Figure 6.1.1.

	Hankar		
General	Members	Member Of Managed By	
<u>M</u> embe	rs:		
Name		Active Directory Folder	
	evin L. Mars	jclab.com/Users	
0	BSAT	jclab.com/Computers	
L			
	14 T		
Ag	<u>Id</u>	Remove	
Ag	Id	Remove	
A	ld]	<u>R</u> emove	

Figure 6.1.1 – EAPOL Users Active Directory Group

6.2 Active Directory Remote Access Permissions

For EAP-TLS user and computer authentication to be successful, the remote access **Dial-In Access Permissions** for the user and computer accounts need to be set to **Allow access**. IAS cannot authenticate any user or computers unless the Dial-In permissions are set.

Figure 6.1.1 & 6.1.2 show the Remote Access Permission settings for the user account **Kevin L. Marshall** and computer account **OBSAT** used in this document.

memore control	Terminal Service	ces Profile	COM+
neral Address Aco Member Of Dia	count Profile Il-in Env	Telephones	Organization Sessions
emote Access Permission Allow access	n (Dial-in or VPN)	Deler	
Í <u>V</u> erify Caller-ID; allback Options [™] No <u>C</u> allback [™] <u>S</u> et by Caller (Routing [™] Always Callback to;	and Remote Acc	ess Service only	
Assign a Static IP Addr Apply Static Boutes - Define routes to enable fr	ress	Static Roy	
Assign a Static IP Addi Apply Static <u>B</u> outes Define routes to enable fr connection.	or this Dial-in	Static Rou	Ites

Figure 6.2.1 – Example Active Directory User Account Dial-In Permission Settings

CONTRACTOR CONTRACTOR CONTRACTOR CONTRACTOR	Member Of Location Managed By Dial-in
Remote Access Permission	(Dial-in or VPN)
Allow access	
C Deny access	
C Control access through	Remote Access Policy
Verify Caller-ID:	
-Callback Options	,
No Callback	
	and Remote Access Service only)
Set by Caller (Routing a	Ind memote Access Service only
 Set by Caller (Routing a Always Callback to: 	
Set by Caller (Routing a Always Callback to: Assign a Static IP Addre	
Set by Caller (Routing a Always Callback to: Assign a Static IP Addre Apply Static Boutes —	
Set by Caller (Routing a Always Callback to: Assign a Static IP Addre Apply Static Boutes Define routes to enable fo connection.	r this Dial-in Static Roytes

Figure 6.2.2 – Example Active Directory Computer Account Dial-In Permission Settings

6.3 Windows XP Registry Settings

To ensure the correct Windows XP 802.1X supplicant behavior when performing computer and user authentication, the AuthMode and SupplicantMode registry keys were added. Figure 6.3.1 shows the recommended registry keys and DWORD values:



Figure 6.3.1 – Registry Entries

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters\General\Global] "AuthMode" = dword: 00000001

"SupplicantMode"=dword: 00000003

Figure 6.3.2 – Example Registry Entry File

6.4 Wireless Zero Configuration service

The Microsoft Wireless Zero Configuration service provides native Windows support for 802.11 Wireless networking as well as 802.1X support for both Wired & Wireless networks.

Before you can enable or configure 802.1X wired computer and user authentication within Windows XP, the Microsoft Wireless Zero Configuration service has to be running. If the service is not in a Started state you will not be able to enable or configure or enable native 802.1X authentication for the Local Area Network connection.

🍓 Services							
File Action View	Help						
← → 💽 📽 🛛) 🗟 😫 🕨 🔳 💷 🖦						
Services (Local)	🍓 Services (Local)						
	Wireless Zero Configuration	Name 🕖	Description	Status	Startup Type	Log On As	^
	Stop the service Restart the service Description: Provides automatic configuration for the 802.11 adapters	Terminal Services Themes Uninterruptible Pow Universal Plug and Volume Shadow Copy WebClient Windows Audio Windows Firewall/In Windows Firewall/In Windows Image Ac Windows Installer Windows Managem Windows Managem	Allows mult Provides u Manages a Provides s Enables Wi Manages a Provides m Provides m Provides m Provides a Provides a Provides a Provides a Provides a	Started Started Started Started Started Started	Manual Automatic Manual Manual Automatic Automatic Automatic Manual Automatic Manual Automatic Manual Automatic	Local System Local System Local Service Local Service Local System Local System Local System Local System Local System Local System Local System	
		WMI Performance A	Provides p Creates an	Started	Manual Automatic	Local System Local System	~
	\Extended \Standard /						

Figure 6.5.1 – Windows XP Services

By default the Microsoft Wireless Zero Configuration service is configured to automatically start and will have the service **Startup** type set to **Automatic**. If the service is disabled or stopped this may be due to a third-party 802.1X supplicant installed with a Wireless LAN NIC. Some third party 802.1X supplicants will disable or stop the Microsoft Wireless Zero Configuration service to eliminate conflict. Wired PEAP Machine Authentication for ERS and ES TCG

	Un Recovery Dependencies		
Service nam	e: WZCSVC		
Display nam	e: Wireless Zero Configuration		
Description:	cription: Provides automatic configuration for the 802.11 adapters		
Path to exec	sutable:		
C:\WINDO\	VS\System32\svchost.exe -k netsvcs		
Startup type	Automatic		
Service stati	us: Started		
Start	Stop Pause Resume		
You can spe from here.	cify the start parameters that apply when you start the service		

v1.0

Figure 6.5.2 – Wireless Zero Configuration Service Properties

If you have a third-party 802.1X supplicant installed you can disable the third-party 802.1X supplicant on the NIC by disabling it in the Local Area Connection properties for the NIC. This will allow the Microsoft Wireless Zero Configuration service to start and also allow Windows to control the 802.1X authentication.

ieneral	Authentication Advanced	
Connec	t using:	
B F	ealtek RTL8139 Family PCI Fast Et Configure	
This co	nnection uses the following items:	
	File and Printer Sharing for Microsoft Networks	^
	QoS Packet Scheduler	
13	AEGIS Protocol (IEEE 802.1x) v3.4.1.0	-
1 35	Ekahau NDIS Usermode I/O Protocol	~
<u></u>		
Í	nstall Uninstall Properties	
Desci	iption	
Allow	is your computer to access resources on a Microsoft ork.	
- Sho	u icon in notification area when connected	
Moti	when connected when connected	
M NOU	yine when this connection has littlifed of ho connectivit	y
	OK Can	ice

Figure 6.5.3 – Disabling a Third-Party 802.1X Driver

NN48500-546

NN48500-546

7. Reference Documentation:

Document Title	Publication Number	Description
Deployment of IEEE 802.1X for Wired Networks Using Microsoft Windows	N/A	This article describes how to deploy IEEE 802.1X authentication for wired networks using authenticating switches, wired client computers running Microsoft® Windows® XP, Windows Server™ 2003, or Windows 2000, and a wired authentication infrastructure consisting of Windows Server 2003 or Windows 2000 Active Directory® directory service domain controllers, certification authorities, and Internet Authentication Service servers.
802.11 Wireless Tools and Settings	N/A	Microsoft TechNet article that includes details for modifying the 802.1X registry settings.

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>.