# **Configuring Wired 802.1x Authentication on Windows Server 2012**

Johan Loos

johan@accessdenied.be

Version 1.0

# Why 802.1x Authentication?

The purpose of this document is to guide you through the procedure how to enable 802.1x authentication to add an additional level of security when client computers are connecting to your local area network. Before a client computer has access to your network, the client computer needs be authenticated. If authentication is successful, the client computer is granted access. If authentication fails, the client computer has no or limited access. Clients can be authenticated using a password or a certificate.

802.1x authentication offers visibility since all clients are identified and authenticated. Offers security if the strongest authentication method is used and offers transparency because there is no involvement of the end-user.

Without proper access to your network, malicious users can use your network to access private data or launch attacks to servers or client computers on your network. *Example:* 

A consultant enters your company, plugs its computer into a socket wall, the client adapter request an IP address from a DHCP server which is located on the local area network. The client computers now have access to your network.

# 802.1x Authentication Overview

802.1x is an authentication framework to restrict unauthorized devices from connecting to the local area network. The authentication server authenticates each client connected to a switch port before the client can access any network resources.

Before the client can access network resources, only EAPOL traffic is allowed between the switch port and the client. If the client gets finally authenticated, normal traffic can flow through the switch port.

To protect your network, you have to use a proper authentication method:

• Authentication requires that the user provides some valid credentials such as username and password or a certificate stored on the client computer or smartcard.

Some components that you can use to protect the wired environment are:

- One or more 802.1x capable switches which are compatible with RADIUS
- Active Directory Domain Services for user and group management
- Active Directory Certificate Services for certificate management
- Network Policy Server to provide authentication, authorization and accounting

# 802.1x Components



**Supplicant (workstation):** Is a client that request access to the local area network and respond to requests from the switch.

Authentication server (NPS Server): This server actually authenticates the client. The authentication server validates the identity of the client and informs the switch if the client is authorized to access the local area network. The authentication server is basically a RADIUS server configured to support EAP authentication.

**Authenticator (switch, wireless access point, wireless controller):** Controls physical access to the network based on the authentication status of the client. This device relays the supplicant credentials to the authentication server.

# **EAP Protocol**

EAPOL works at Layer 2 to authenticate a supplicant before access is granted on the network. EAPOL creates specialized EAP packets to allow EAP packets in the packet body. The goal of port based authentication is to transport the EAP-Method data which implements the actual authentication method.

# EAP Packet Structure

version Type Length Packet Body
---------------------------------

**Version field** identifies the version of the EAPOL protocol. The value is one octet in length and has the value '0000 0002'.

Type field identifies the type of packet being sent and is one octet in length.

EAP-Packet: '0000 0000' EAPOL-Start: '0000 0001' EAPOL-Logoff: '0000 0010' EAPOL-Key: '0000 0011' EAPOL-Encapsulated-ASF-Alert: '0000 0100' Length field defines the length of the packet body and is two octets in length. For example an EAPOL Length field value of '0000 0000 0001 1010' indicates that the Packet Body field contains 22 octets of data. Packet Body field is the payload portion

# EAP Packet

Extensible Authentication Protocol is an authentication protocol which supports multiple authentication methods. It works at the Data link layer and does not need IP to operate.

# **EAP Header**

Code	Identifier	Length	Data	Туре
------	------------	--------	------	------

**Code field** specifies the type of EAP packet and is one 1 byte long. The six EAP packet types can be used:

Code	Description
x01	EAP-Request
x02	EAP-Response
x03	EAP-Success
x04	EAP-Failure
x05	EAP-Initiate
x06	EAP-Finish

Identifier field to match EAP-Response packets to Request packets and is one byte in length.

**Length field** includes the size of the EAP packets including EAP header and data fields and is two bytes long.

**Data field** is variable in length, can contain zero or more bytes as indicated in the Length field.

Type field defines the EAP packet type and is eight bits long.

Туре	Description
1	Identity
2	Notification
3	NAK
4	MD5-Challenge
5	One-Time password
13	EAP-TLS
21	EAP-TTLS
25	PEAP
26	MS-EAP authentication
29	EAP-MSCHAP-V2
49	MS-IKEv2

# Authentication process

When you enable 802.1x authentication, following events occur:

- If the identity of the client is valid and 802.1x authentication is successful, the switch grants the client access to the network
- If 802.1x authentication times out and MAC authentication bypass is enabled, the switch can use the MAC address of the client for authorization
- If the client cannot be identified and a restricted VLAN is specified, the switch can assign the client to the restricted VLAN



The switch re-authenticates the client when one of the following events occurs:

- Periodic re-authentication is enabled and the re-authentication timer expires
- You manually re-authenticate the client

# User and Computer authentication

Authentication can be performed for a user, computer or both. The user or computer can be authenticated via passwords or certificates.

## EAP-TLS

EAP-TLS requires client-side and server side certificates for mutual authentication.

1. Authentication server submits certificate to supplicant

- Supplicant validates server certificate (check if the FQDN is the same as the name in the certificate and if the certificate is signed by a trusted CA, or that the certificate is not revoked
- 3. Supplicant submits certificate to server
- 4. Server validates the certificate of the supplicant

## PEAP-EAP-MSCHAPv2

PEAP-EAP-MSCHAPv2 requires that the authentication server presents a certificate to the supplicant. The supplicant must have the Root CA of the CA that signed the authentication server certificate. It first creates a secure tunnel between the authentication server and the supplicant. This tunnel is created using a valid server certificate that the authentication server sends to the supplicant. Within this secure channel, a new EAP negotiation takes place to authenticate the client.

Authentication is based on a password, so this type of attack is susceptible to a dictionary attack.

- 1. Authentication server submits certificate to supplicant
- 2. Supplicant validates server certificate
- 3. Supplicant submits password through encrypted tunnel
- 4. Authentication server validates supplicant password

If the authentication server is unavailable, 802.1x fails and all supplicants will be denied access.

# Authentication Initiation and Message Exchange

The connection can be initiated by the switch or by the client. The switch sends an EAPrequest/identity frame to the client to request its identity. The client responds with an EAPresponse/identity frame.

If the switch is not configured to supports 802.1x authentication and the client sends any EAPOL frames, these frames are dropped. If the client is configured to supports 802.1x authentication, and the client does not receive an EAP-request/identity frame after three

attempts, the client transmits frames as if the port is in authorized state. A port in authorized state means that the client has been successfully authenticated.

When the client supplies its identity, the switch passes EAP frames between the client and authorization server until authorization fails or succeeds.

If the client identity is valid and the 802.1x authentication succeeds, the switch grants the client access to the network. If the switch gets an invalid identity from an 802.1x capable client, the switch can assign the client to a restricted VLAN that provides limited services.

The switch can re-authenticate the client at regular times or when the re-authentication timer expires. You can configure the switch to use timers based on Session-Timeout (attribute 27) and the Termination-Action (attribute 29). Session-Timeout specifies the time when re-authentication occurs and Termination-Action specifies the action to take during re-authentication. The action can be *Initialize* or *Re-Authenticate*. When you set the Initialize action, the 802.1x session ends and the client will lose connectivity. When you set Re-Authenticate, the client will not lose the connection and simple re-authenticates.

Do not use Re-authentication and session timers if you are using MAB. The switch does not re-learn the MAC address but sends the previously learned MAC address to the RADIUS server. If you use these timers, MAB succeeds when 802.1x authentication fails. So at this point, the client loses connectivity.

### Message exchange process



## Message Exchange during MAC authentication bypass



# Ports in authorized and unauthorized states

The switch port state determines if the client is authorized to access the local area network or not. The port starts in unauthorized state. In this state, the port disallows all traffic except for 802.1x frames. When a client is successfully authenticated, the port is in authorized state and allows all traffic from the client to the switch. If a client does not support 802.1x authentication and connects to an unauthorized port, the switch request the client's identity. In this case, the client cannot responds to the request and the port remains in unauthorized state. The client is not granted access to the network.

When an 802.1x enabled client connects to a port which is not enabled for 802.1x authentication. The client initiates the authentication process by sending the EAPOL-start frame. When the client does not receive a response from the switch, then client sends the request for a number of times.

You can control the port authorization state by using dot1x port-control interface configuration command:

**Force-authorized:** Disable 802.1x authentication and causes the port to the authorized state without any authentication exchange required.

**Force-unauthorized:** Causes the port to remain in unauthorized state, ignoring all attempts by the client to authenticate.

**Auto:** Enable 802.1x authentication and causes the client to begin in the authorized state, allowing only EAPOL traffic to be sent and receive through the port.

When the client receives an accept frame from the authentication server, the client is successfully authenticated and the state of the switch port is set to authorized. If the authentication fails, the switch port remains in unauthorized state, but the client is able to retry the authentication process.

If the authentication server cannot be reached, the switch will retransmit the request. If the switch does not receive any responses from the authentication server after a specific number of attempts, the authentication will fail and the client is not able to access resources on the local area network.

When a client logs of, the client sends an EAP-logoff message, and the switch changes this port back to unauthorized state.

# Configuring 802.1X authentication on Catalyst 3560 Switch

```
addevsw01#config t
addevsw01(config)#aaa new-model
addevsw01(config)#aaa authentication dot1x default group radius
addevsw01(config)#aaa authorization network default group radius
addevsw01(config)#dot1x system-auth-control
addevsw01(config)#interface fa0/2
addevsw01(config-if)#switchport mode access
addevsw01(config-if)#authentication port-control auto
```

# Configuring switch-to-RADIUS server communication

A RADIUS server is identified with its hostname or IP address and specific UDP port numbers for authentication and accounting.

The following configuration shows how to configure the switch to use a RADIUS server with IP address 10.32.5.15 to use port 1812 as authorization port and 1813 for accounting, and set the RADIUS secret to accessdenied

addevsw01(config) **#radius-server host 10.32.5.15 auth-port 1812** acct-port 1813 key accessdenied

The RADIUS secret must match the secret key on the NPS server.

# Enabling periodic re-authentication

You can also specify periodic 802.1x client re-authentication and how often it needs to be occurred. The number of seconds between re-authentication is by default 3600 seconds. The switch can re-authenticate the client at regular times or when the re-authentication timer expires. If the switch is configured to use a RADIUS server, you can configure the switch to use timers based on the following RADIUS attributes.

RADIUS Attribute	Value
[27] Session-Timeout	Value in seconds
[29] Termination-Action	Value in seconds

The Termination-Action specifies which action to take during re-authentication. Possible actions are Initialize and Re-authenticate. When you use Initialize, the 802.1x session ends

and connectivity is lost during re-authentication. When you use Re-authenticate the session is not affected during re-authentication.

This configuration shows how to enable periodic re-authentication and set the number of seconds between re-authentication attempts to 4800

```
addevsw01(config)#int fa0/2
addevsw01(config-if)#authentication periodic
addevsw01(config-if)#authentication timer reauthenticate 4800
```

You can manually re-authenticate the client computer connected to a specific port at any time by entering the following command:

addevsw01(config)#dot1x re-authenticate int fa0/2

# Configuring the quiet period

When the switch is not able to authenticate the client, the switch remains idle for a period of time, and then tries again. The idle time is determined with the quiet period.

This example shows how to configure the switch with a quiet time of 30 seconds.

```
addevsw01(config)#int fa0/2
addevsw01(config-if)#dot1x timeout quiet-period 30
```

## Configuring the switch-to-client retransmission time

## Dot1x timeout tx-period

Before authentication can take place, the switch sends an EAP-request/identify frame to the client. The client responds with an EAP-response/identity frame. If the switch does not receive a message within a period of time, the switch retransmits the frame.

You can configure the default retransmission time as follow:

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#dot1x timeout tx-period 30
```

## Dot1x max-reauth-req:

The number of times the switch resends the request-identity frame

The default value for dot1x timeout is 30 seconds and dot1xmax-reauth-req is 2. Based on timeout = (max-reauth-req + 1) x tx-period. It takes 90 seconds for a supplicant to get access

through mac authentication bypass on guest vlan. When this timeout expired and MAB is configured, MAC authentication can takes place.

## Authentication timer restart:

If 802.1x timeouts on the fallback mechanism fails or has been configured, the authenticator will wait a period of time. After this time, the authentication process starts over.

# Enabling multiple hosts

You can attach multiple hosts to a single 802.1x enabled port. Only one of the attached hosts must be successfully authorized for all hosts to be granted network access.

If the port becomes un-authorized, all attached clients are denied access to the network.

addevsw01(config)#interface fa0/2

addevsw01(config-if)# authentication host-mode multi-host

# **Display Statistics and Status**

You can use following command to display statistics for a specific port:

addevsw01**#show dot1x authentication int fa0/2** 

# Using 802.1x Authentication with VLAN Assignment

You can limit network access by using VLAN assignment. After the switch authenticates the client on an 802.1x enabled port, the RADIUS server sends the VLAN ID to configure the switch port. This feature can be used to limit network access.

- When no VLAN is supplied by the RADIUS server or 802.1x authentication is disabled, the switch becomes access to its default VLAN.
- When incorrect VLAN information is supplied by the RADIUS server and 802.1x authentication is enabled, the switch place the switch port into unauthorized state to prevents ports to be member of another VLAN.
- When VLAN information is supplied correctly by the RADIUS server and 802.1x authentication is enabled, the switch port is configured with the VLAN after successful authentication.
- If multiple-hosts mode is enabled on the switch port, all hosts are placed in the same VLAN as the first authenticated host.

It is important that VLAN 1 or management VLAN is not the default VLAN. If authentication fails, the wired client can still access the network. Shutdown all switch ports which you don't use.

A RADIUS Server must return these attributes to the switch:

RADIUS Attribute	Value
[64] Tunnel-Type	VLAN
[65] Tunnel-Medium-Type	802
[81] Tunnel-Private-Group-ID	VLAN ID

# Using 802.1x Authentication with Guest VLAN

You can use a Guest VLAN to provide limited access the clients. When you enable a Guest VLAN on the switch, the client becomes a member of the Guest VLAN is authentication cannot be performed. For example the client uses an Operating System that does not contains the 802.1x client.

When the client does not send an EAPOL frame or the switch does not receive a response to an EAP request/identity frame, the switch assigns the 802.1x port to the Guest VLAN. Guest VLANs are supported on single-host or multiple-hosts mode.

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#authentication event no-response action
authorize vlan 100
```

# Using 802.1x Authentication with Restricted VLAN

If for some reason an IEEE 802.1x compliant client computer is not able to authenticate, the authentication process fails and the client can be placed into a restricted VLAN. This allows client computer to access limited resources in the restricted VLAN.

These clients are 802.1x compliant but fail the authentication process. For example, the certificate of the client computer has expired.

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#authentication event fail action authorize
vlan 99
```

When the client is not able to authenticate within 3 times, the switch places the switch port into the restricted VLAN. Users for which authentication fails, remains in the restricted VLAN until the next re-authentication occurs. At configured intervals, the switch port sends a reauthentication message. If re-authentication fails, the switch port remains in the restricted VLAN. Otherwise the switch port is configured in to configured VLAN or the VLAN ID sent by the RADIUS Server. Restricted VLANs are only supported in single-host mode.

# Using a Filter-ID to create a VLAN ACL

You can use this attribute to assign an ACL to a client who is authorized on the RADIUS server. The ACL must exist on the switch before connection is filtered. In the example below, access to the IIS Web Services running on that server are denied. The syntax is as follows: addevsw01(config)#access-list 101 deny tcp any host 10.32.5.3 eq www addevsw01(config)#access-list 101 permit ip any any

# Using Cisco-AV-Pair to create a VLAN ACL

You can also use the Cisco-AV-Pair attribute to configure downloadable ACLs. This means that the ACLs don't need to be exists on the switch, but are downloaded to the authorized client computer. In the example below, access to the IIS Web Services running on that server are denied. The syntax is as follows:

ip:inacl#201=deny tcp any host 10.32.5.3 eq www
ip:inacl#201=permit ip any any

# Using 802.1x Authentication with Port Security

When you enable 802.1x on a switch port and the switch port is additionally configured with port security; first authentication takes place and port security manages network access for all MAC addresses.

Interaction between 802.1x authentication and port security:

- When the client is authenticated and port security table is not full, the MAC address of the client is added to the list of secure hosts. The switch port comes up normally.
- When the client is authenticated and port security table is full, the switch port shuts down.

- When the client logs off, all entries in the secure host table are cleared and the switch port change to unauthenticated state.
- If you administratively shutdown a switch port, all entries are removed from the secure host table and the switch port becomes unauthenticated.

You can configure 802.1x authentication with port security in single-host or multiple-hosts mode.

addevsw01(config-if)#switchport port-security mac-address macaddress

# Using 802.1x authentication using MAC Authentication Bypass (MAB)

You can configure an 802.1x enabled port on the switch to authorize clients based on the MAC address. You can use Active Directory as a MAC address database for which are allowed to access the network. When the client connects to the switch, the RADIUS Server sends a RADIUS access/request message with a username and password based on the MAC address. If authorization is successful, the switch allows the client access to the network. If authorization fails, the switch assigns the client to the Guest VLAN.

If the switch detects an EAPOL frame from an 802.1x capable client, the switch uses 802.1x authentication instead of MAC authentication bypass.

If the switch already authorized a port using MAC authentication bypass and detects an 802.1x capable client, the switch does not unauthorized the client. When re-authentication occurs, the switch uses 802.1x authentication as preferred method.

Clients that where authorized with MAC authentication bypassed can be re-authenticated. If re-authentication is successful, the switch keeps the port in the same VLAN. Otherwise the switch assigns the port to the Guest VLAN.

You need to create a domain user and password in Active Directory for all your clients which need to be authenticated via MAB.

New Object - User	×
Create in: addev.local/Access Denied/Users	
First name: 0080c838e0ca Initials:	
Last name:	
Full name: 0080c838e0ca	
User logon name:	
0080c838e0ca @addev.local 💌	
User logon name (pre-Windows 2000):	
ADDEV\ 0080c838e0ca	
< Back Next > Cano	el

To be able to authenticate those clients with only the MAC information, you need to create a

policy on NPS which includes the **Calling Station ID** as condition.

	Client Computers VLAN 20 - EAP-TLS Properties	x			
Overview Conditions	Constraints Settings				
Configure the conditions If conditions match the connection request, NP	Configure the conditions for this network policy. If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request. NPS skips this policy and evaluates other policies, if additional policies are configured.				
	Select condition	x			
Select a condition,	Calling Station ID				
Framed F The Frame packets, s	Specify the phone number dialed by the access client. You can use pattern matching syntax.	^			
Service T The Servic Point to Pc	e, such as Telnet or				
Tunnel Ty The Tunne L2TP.	OK Cancel such as PPTP or	=			
Calling Sta Calling Sta The Calling Client Frie The Client F	tion ID Station ID condition specifies the network access server telephone number dialed by the access client. <b>ndly Name</b> riendly Name condition specifies the name of the RADIUS client that forwarded the connection request to	~			
	Add Cancel				
	Add Edit Remov	e Apply			

To authenticate users, you need only unencrypted authentication and disable all the others.

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#mab
```

Before MAB is in place, the port enabled for MAB must be timeout on 802.1x authentication first.

# **RADIUS Message Types**

**Access-Request:** Sent by a RADIUS client to request authentication and authorization for a network access connection attempt.

**Access-Accept:** Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is authenticated and authorized.

**Access-Reject:** Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is rejected. A RADIUS server sends this message if either the credentials are not authentic or the connection attempt is not authorized.

**Access-Challenge:** Sent by a RADIUS server in response to an Accept-Request message. This message is a challenge to the RADIUS client that requires a response.

**Accounting-Request**: Sent by a RADIUS client to specify accounting information for a connection that was accepted.

**Accounting-Response:** Sent by the RADIUS server in response to the Accounting-Request message. This message acknowledges the successful receipt and processing of the Accounting-Request message.

# **IP Address Assignment**

After successful authentication, the wired client needs to receive an IP address before further communication can takes place. The client can receives an IP address from a DHCP server available on the network or from a DHCP server configured on your switch or other network device. In this paper, we use a Microsoft DHCP Server and create the necessary scopes.

# **Creating VLANs**

Before you assign VLAN ID attribute via RADIUS you need to configure the required VLANs on your switch.

The following creates a VLAN 5

addevsw01(config)#**vlan 5** 

## The following creates a VLAN 10

addevsw01(config)#vlan 10

### The following creates a VLAN 20

addevsw01(config)#**vlan 20** 

### The following creates a VLAN 99

addevsw01(config)#vlan 99

### The following creates a VLAN 100

addevsw01(config)#**vlan 100** 

# Assigning IP address

#### Assign an IP address to the interface of VLAN 5

```
addevsw01(config)#interface vlan 5
addevsw01(config-if)#ip address 10.32.5.254 255.255.255.0
addevsw01(config-if)#no shutdown
```

#### Assign an IP address to the interface of VLAN 10

```
addevsw01(config)#interface vlan 10
addevsw01(config-if)#ip address 10.32.10.254 255.255.255.0
addevsw01(config-if)#ip helper-address 10.32.5.3
addevsw01(config-if)#no shutdown
```

#### Assign an IP address to the interface of VLAN 20

```
addevsw01(config)#interface vlan 20
addevsw01(config-if)#ip address 10.32.20.254 255.255.255.0
addevsw01(config-if)#ip helper-address 10.32.5.3
```

addevsw01(config-if)#no shutdown

## Assign an IP address to the interface of VLAN 99

```
addevsw01(config)#interface vlan 99
addevsw01(config-if)#ip address 10.32.99.254 255.255.255.0
addevsw01(config-if)#ip helper-address 10.32.5.3
addevsw01(config-if)#no shutdown
```

Assign an IP address to the interface of VLAN 100

```
addevsw01(config)#interface vlan 100
addevsw01(config-if)#ip address 10.32.100.254 255.255.255.0
addevsw01(config-if)#ip helper-address 10.32.5.3
addevsw01(config-if)#no shutdown
```

## VLAN information can be retrieved as follows

addevsw01#**show vlan** 

# **Schematic Design**

For this lab, I use a Cisco Catalyst 3560 switch which also provides inter-VLAN routing between the various networks.

Name	Software	Role
ADDEVDC01	Windows Server 2008 R2	DC,DNS,CA
ADDEVDC04	Windows Server 2012	NPS, DHCP
ADDEVWKS01	Windows 7	Client
ADDEVSW01	Cisco Catalyst 3560	Switch



To enable routing between VLANs, use the following command:

addevsw01(config) #ip routing

The IP address of addevdc01 is 10.32.5.3, the IP address of addevdc04 is 10.32.5.15 and the addevwks01 is configured as a DHCP client.

Table overview of network configuration:

Network ID	VLAN ID	Default Gateway	Description
10.32.5.0/24	5	10.32.5.254	Native vlan
10.32.10.0/24	10	10.32.10.254	Clients vlan
10.32.20.0/24	20	10.32.20.254	Clients vlan
10.32.99.0/24	99	10.32.99.254	Restricted vlan
10.32.100.0/24	100	10.32.100.254	Guest vlan

# Prepare the environment for 802.1x Authentication Task List

You need to prepare the environment with the appropriate groups to support 802.1x based authentication. The next step is to create Active Directory Security Groups for authorized access and certificate enrollment.

- Create a group AutoEnroll Server Authentication Certificate
- Create a group AutoEnroll Client Authentication Certificate
- Create a group Wired Computers VLAN 10

# Create a group AutoEnroll NPS Server Authentication Certificate

- Open Active Directory Users and Computer from Administrative Tools
- Select Organizational Unit you want to create the group
- Right click on the OU, select New Group
- On the **New–Group** window, type the name of the group *AutoEnroll Server Authentication Certificate*, and click **OK**

## Create a group AutoEnroll Client Authentication Certificate

- Select Organizational Unit you want to create the group
- Right click on the OU, select **New Group**
- On the New Group window, type the name of the group AutoEnroll Client Authentication Certificate, and click OK

# Create a group Wired Computers VLAN 10

- Select Organizational Unit you want to create the group
- Right click on the OU, select New Group
- On the New Group window, type the name of the group Wired Computers VLAN
   10, and click OK

# **Configuring and Deploying 802.1x Authentication Certificates Task** List

Before we can use 802.1x authentication we have to enroll for certificates. In this section, you will create and enroll hosts on the network to enroll for a certificate. The client computer will send his identity (computer certificate) to the switch, whereas the switch authenticates the client computer against the Network Policy server.

- Create a NPS Server Authentication Certificate
- Create a Workstation Authentication Certificate
- Adding the certificate templates to the Certificate Authority
- Add the NPS Server account to the autoenrollment group
- Add client computer accounts to the autoenrollment group
- Add client computer accounts to the authorized computers group

• Create a GPO for NPS Server certificate enrollment

## Create a NPS Server Authentication Certificate

- Open Certificate Authority snap-in from Administrative Tools.
- Right click on **Certificate Templates** and select **Manage**.
- Right click on RAS and IAS Server certificate Template and select Duplicate

## Template.

• On the Duplicate Template dialog box, select Windows 2003 Server and click OK

ate Temp	ate				×
i can create all Windows sion of Wind tificate temp	certificate tem CAs support a ows Server (m late.	nplates w all certific ninimum s	ith advanced cate template supported CAs	properties properties ) for the c	. However, Select the Juplicate
Windows <u>2</u> 0	03 Server, En	Iterprise	Edition		
Windows <u>S</u> e	rver 2008, En	iterprise	Edition		
rn more abo	ut <u>Certificate</u>	Template	e Versions.		
			OK		Cancel
	ate Templ can create all Windows sion of Wind tificate temp Windows <u>2</u> 0 Windows <u>S</u> e rn more abo	ate Template can create certificate ten all Windows CAs support sion of Windows Server (n tificate template. Windows <u>2</u> 003 Server, En Windows <u>S</u> erver 2008, En rn more about <u>Certificate</u>	ate Template can create certificate templates w all Windows CAs support all certific sion of Windows Server (minimum s tificate template. Windows <u>2</u> 003 Server, Enterprise Windows <u>S</u> erver 2008, Enterprise rn more about <u>Certificate Template</u>	ate Template can create certificate templates with advanced all Windows CAs support all certificate template sion of Windows Server (minimum supported CAs tificate template. Windows <u>2</u> 003 Server, Enterprise Edition Windows <u>Server</u> 2008, Enterprise Edition rn more about <u>Certificate Template Versions.</u>	can create certificate templates with advanced properties all Windows CAs support all certificate template properties sion of Windows Server (minimum supported CAs) for the o tificate template. Windows <u>2</u> 003 Server, Enterprise Edition Windows <u>Server 2008</u> , Enterprise Edition rn more about <u>Certificate Template Versions</u> .

• On the **General** tab, in the **Template** display name field, type 2012 Server Authentication Certificate.

2012 Server Authentication Certificate Properties	? ×					
Cryptography Subject Name Issuance R	equirements					
Superseded Templates Extensions Security	Server					
General Request Hand	ling (					
Template display name:						
2012 Server Authentication Certificate						
, Minimum Supported CAs: Windows Server 2008 Enterprise						
Template name:						
2012ServerAuthenticationCertificate						
Validity period: Renewal period:						
years  6 weeks						
Publish certificate in Active Directory						
Do not automatically reeprol if a duplicate pertificate e	viste in Active					
Directory	Mata III Motive					
For automatic renewal of smart card cardinates, use the e	wieting key					
if a new key cannot be created	Alsung Key					
OK Cancel Apply	Help					

Click on the Subject Name tab, select Build from this Active Directory information.
 Ensure that the Subject name format is set to Common name and that only DNS
 Name is selected under Include this information in subject alternative name.

2012 Server Authentic	cation Co	ertificate P	roperties	<u>? ×</u>
General		1	Request Handli	ng
Superseded Templat	es 🗎	Extensions	Security	Server
Cryptography	Subjec	ct Name	Issuance Re	equirements
C Supply in the reque	est formation sts.	from existing	certificates for au	toenrollment
Build from this Activ	ve Directo	ory information	n	
Select this option to simplify certificate ad	enforce o dministrati	consistency a on.	mong subject nar	mes and to
Subject name formation	et :			_
Common name				<b>-</b>
🔲 Include e-mail n	ame in su	bject name		
Include this informat E-mail name DNS name User prinicipal n	tion in alte name (UP! al name (S	emate subjec N) iPN)	t name:	
ок		Cancel	Apply	Help

Click on the Security tab, click on the Add button and add AutoEnroll Server
 Authentication Certificate group, assign Enroll and Autoenroll permissions and click
 OK.

	te Properties	?
Cryptography Subject Name General Superseded Templates Extension	Issuance Request Ha ons Securit	e Requirements andling ty Server
Group or user names: Authenticated Users Autoenroll Server Authentication (A Administrator Domain Admins (ADDEV\Domain A Enterprise Admins (ADDEV\Enterprise)	DDEV\Autoenroll Idmins) ise Admins)	Server Authen
	Add	Remove
Permissions for Autoenroll Server Authentication Full Control Read Write Enroll Autoenroll	Allow	Deny
Permissions for Autoenroll Server Authentication Full Control Read Write Enroll Autoenroll For special permissions or advanced sett Advanced. Leam about access control and permissi	Allow	Deny

You should remove any of the other security groups that have permissions to enroll and/or autoenroll this certificate template.

# Create a Workstation Authentication Certificate

A certificate is required to authenticate computers for port based authentication.

- Right click on the Workstation Authentication certificate template and select
   Duplicate Template.
- Click on the **General** tab, in the **Template** display name, type *Workstation Authentication Certificate*.

orkstation Aut	thentication	Certificate Pro	operties	?
Superseded T General Rec	emplates	Extensions Subject Nam	Security	Server Requirements
Template displa	ay name: theotication C	artificata		
Minimum Suppo	orted CAs: Wir	ndows Server 20	03 Enterprise	
WorkstationAu	thenticationCe	tificate		
Validity period: years Publish cert	ificate in Active	Renewal p	eriod: eeks 💌	
Do not a Director	automatically re y	enroll if a duplication	ate certificate exi	sts in Active
For automat if a new key	tic renewal of s / cannot be cre	mart card certific ated	ates, use the exi	sting key
	ОК	Cancel	Apply	Help

Click on the Subject Name tab, ensure to select Built from this Active Directory
 Information. Under Subject name format select Common Name. Ensure that DNS
 name is the only option selected under Include this information in subject alternate
 name

Workstatic	on Authentication (	Certificate Prope	rties	? ×
Superse General	eded Templates	Extensions Subject Name	Security Issuance F	Server Requirements
C Supp □ <sup>1</sup>	<b>Iv in the request</b> Jse subject information enewal requests.	n from existing certi	icates for auto	penroliment
Build Select simplify Subject	from this Active Direc this option to enforce y certificate administra ct name format:	tory information consistency amony tion.	g subject name	es and to
DNS Includ E E- DI Us Se	name clude e-mail name in s e this information in al mail name NS name ser prinicipal name (UF ervice principal name (	ubject name temate subject nam PN) SPN)	le:	
	ок	Cancel	Apply	Help

• Click on the **Security** tab, click on the **Add** button and add **AutoEnroll Client** 

Authentication Certificate group, assign Enroll and Autoenroll permissions and click OK

orkstation Authentication Ce	rtificate P	roperties	?
General Request Handling	Subject Na Extensions	ime Issuar Securit	nce Requirements
Group or user names:			
& Authenticated Users			
Autoenroll Client Authenticat	ion (ADDE\	^Autoenroll C	lient Authentic
🔏 Administrator			
& Domain Admins (ADDEV\Do	main Admin	s)	
& Enterprise Admins (ADDEV)	Enterprise A	dmins)	
		Add	Remove
Permissions for Autoenroll Client		/	
Authentication		Allow	Deny
Full Control			
Read			
Write			
Enroll		$\checkmark$	
Autoenroll		$\checkmark$	
For special permissions or advanced	ed settings,	click	Advanced
navanood.			
Leam about access control and p	emissions		
ок	Cancel	Applu	Heb
		r - 10 0 1	

• Close Certificates Templates snap-in

You should remote any of the other security groups that have permissions to enroll and/or autoenroll this certificate template.

# Adding the Certificate Templates to the Certificate Authority

After you have configured or created new certificate templates, you have to add them to the certificate authority to enable enrollment.

From the Certificate Authority snap-in, right click on Certificate Templates, select
 New – Certificate Template to Issue.

Select following certificate templates: Workstation Authentication Certificate and 2012 Server Authentication Certificate and click OK.

# Add the NPS Server account to the AutoEnroll Server Authentication Certificate group

- Open Active Directory Users and Computers from Administrative Tools
- Double click on AutoEnroll Server Authentication Certificate group.
- Click on the **Member** tab and click **Add**.
- In the Select Users, Contacts, Computers, or Groups dialog box, in the Enter the object names to select add *ADDEVSRV01* computer account and click OK.

# Add client computer accounts to the AutoEnroll Client Authentication Certificate group

- Double click on AutoEnroll Client Authentication Certificate group.
- Click on the **Member** tab and click **Add**.
- In the Select Users, Contacts, Computers, or Groups dialog box, in the Enter the object names to select add *ADDEVWKS01* computer account and click OK.

## Add client computer accounts to the Wired Computers VLAN 10

- Double click on Wired Computers VLAN 10 group.
- Click on the **Member** tab and click **Add**.
- In the Select Users, Contacts, Computers, or Groups dialog box, in the Enter the object names to select add *ADDEVWKS01* computer account and click OK.

# Create a GPO for NPS Server certificate enrollment

- Open Group Policy Management from Administrative Tools.
- Expand Domain, expand Group Policy Objects, and select New Group Policy Objects.
- On the New Group Policy dialog box, type Autoenroll Server Certificate and click OK

New GPO			X
<u>N</u> ame:			
Autoenroll Server Certificate			
Source Starter GPO:			
(none)			•
	(	ок	Cancel

- Right click on Autoenroll Server Certificate, select GPO Status, and select User
   Configuration Settings Disabled
- Right click on Autoenroll Server Certificate and select Edit.
- Expand Computer Configuration | Policies | Windows Settings | Security Settings | Public Key Policies.
- In the right pane, double click on **Certificate Services Client Auto-enrollment**
- On the Certificate Services Client Auto-enrollment Properties dialog box, select
   Enroll Certificates Automatically, select Renew expired certificates and select
   Update certificates that use certificate templates and click OK.

Certificate Services Client - /	Auto-Enrollment Properties	? ×
Define Policy Settings		1
Enroll user and computer cert	tificates automatically	
<u>Configuration Model:</u>	Enabled	•
Renew expired certificates	es, update pending certificates, an	d remove
Dipdate certificates that u	use certificate templates	
Expiration notification		
Show expiry notifications lifetime is	when the percentage of remaining	) certificate
Learn more about <u>Automatic</u>	<u>certificate management</u>	Apply

- Close Group Policy Editor
- Link group policy to the organizational unit which contains the computer account of your NPS server.
- On the **NPS server**, open command prompt and run launch **gpupdate.exe** or restart the server.

# Install and Configure your DHCP Server

Client computers on our network will receive an IP address based on the VLAN where the client computer is a member of. In our lab, we will create a scope for VLAN 10.

- Install the DHCP Server Role
- Configure your DHCP Server with a scope for VLAN 10
- Configure your DHCP Server with a scope for VLAN 20
- Configure your DHCP Server with a scope for VLAN 99
- Configure your DHCP Server with a scope for VLAN 100

## Install the DHCP Server role

- Open Server Manager from the Administrative Tools, expand Roles and select Add Roles
- On the Select Server Role page, select DHCP Server and click Next



• On the DHCP Server page, select Next



- On the Select Network Connection Binding page, select the Network Connection and click Next
- On the Specify IPv4 DNS Server Settings page, type the IP address of your preferred DNS server and click Next
- On the Specify IPv4 WINS Server Settings page, select WINS is not required and click

oforo Vou Ponin	When clients obtain an ID address from the DHCD server, they can be given DHCD entires such as the ID
Server Roles DHCP Server	when there obtain an in a durings from the once server, ney tan be given once options such as the in addresses of WINS servers. The settings you provide here will be applied to clients using IPv4.
Network Connection Bindings IPv4 DNS Settings	WINS is not required for applications on this network
IPv4 WINS Settings	WINS is required for applications on this network
DHCP Scopes	Specify the IP addresses of the WINS servers that clients will use for name resolution. These WINS server will be used for all scopes you create on this DHCP server.
DHCPv6 Stateless Mode	Preferred WINS Server IP Address:
IPv6 DNS Settings	
DHCP Server Authorization	Alternate WINS Server IP Address:
onfirmation	
ogress	
esults	

• On the Add or Edit DHCP Scopes page, click Next

Next

Server Roles	addresses to clients until Scopes:	a scope is created.	cannot distribute IP
OHCP Server	Name	IP Address Range	<u>A</u> dd
IPv4 DNS Settings			<u>E</u> dit
IPv4 WINS Settings			Delete
DHCP Scopes			
DHCPv6 Stateless Mode			
IPv6 DNS Settings			
DHCP Server Authorization			
Confirmation			
Progress			
Results			
	Add or select a scope to	o view its properties.	

• On the **Configure DHCPv6 Stateless Mode** page, select **Disable** and click **Next** 

Add Roles Wizard	<u>×</u>
Configure DHCP	v6 Stateless Mode
Before You Begin Server Roles DHCP Server Network Connection Bindings IPv4 DNS Settings IPv4 WINS Settings DHCP scopes DHCPv6 Stateless Mode DHCP Server Authorization Confirmation Progress Results	<ul> <li>DHCP Server supports the DHCPv6 protocol for servicing IPv6 clients. Using DHCPv6, clients can automatically configure their own IPv6 addresses using stateless mode, or they can acquire IPv6 addresses in stateful mode from the DHCP server. If routers on your network are configured to support DHCPv6, verify that your selection below matches the router configuration.</li> <li>Select the DHCPv6 stateless mode configuration for this server.</li> <li>© gnable DHCPv6 stateless mode for this server</li> <li>IPv6 clients will be automatically configure this thout using this DHCP server.</li> <li>© glable DHCPv6 stateless mode for this server</li> <li>After installing DHCP Server, you can configure the DHCPv6 mode using the DHCP Management console.</li> </ul>
	< <u>Previous</u> Install Cancel

• On the Authorize DHCP Server page, select use Current Credentials and click Next



- On the **Confirm Installation Selection** page, click **Install**
- On the Installation Results page, click Close

Before You Begin Server Roles DHCP Server	The following roles, role services, or 1 warning message below	features were installed successfully:
IPv4 DNS Settings IPv4 WINS Settings DHCP Scopes DHCPv6 Stateless Mode DHCP Server Authorization Confirmation Progress Results	Control Panel to check for up DHCP Server	dates.
	Print, e-mail, or save the installation	report

# Configure DHCP Server with a scope for VLAN 10

- Open DHCP Console from Administrative Tools
- Right click on IPv4 and select New Scope
- On the Welcome to the New Scope Wizard page, click Next

New Scope Wizard		
	Welcome to the New Scope Wizard	
	This wizard helps you set up a scope for distributing IP addresses to computers on your network.	
	To continue, click Next.	
	< Back Next > Cancel	

• On the **Scope Name** page, type a name for the scope and click **Next** 

New Scope Wizard	
Scope Name You have to provide an identifying scope name. You also have the option of providing a description.	
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.	
Name: Client Compute	ers VLAN 10
Description:	
	< Back Next > Cancel

• On the **IP Address Range** page, specify Start and End IP address. Also specify the correct subnet mask and click **Next**
	New Scope Wizard	
IP Address Range You define the scop	e address range by identifying a set of consecutive IP addresses.	J.
Configuration settings	for DHCP Server	
Enter the range of a	ddresses that the scope distributes.	
Start IP address:	10 . 32 . 10 . 50	
End IP address:	10 . 32 . 10 . 60	
-Configuration settings	that propagate to DHCP Client	
Length:	24 -	
Subnet mask:	255.255.255.0	
	< Back Next > (	Cancel

• On the Add Exclusions page, click Next

New Scope Wizard
Add Exclusions and Delay Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.
Start IP address:     End IP address:       I     .       Add
Excluded address range:
Subnet delay in milli second:
< Back Next > Cancel

• On the Lease Duration page, specify a lease duration and click Next

New Scope Wizard
Lease Duration The lease duration specifies how long a client can use an IP address from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate. Set the duration for scope leases when distributed by this server. Limited to:
Days: Hours: Minutes:
< Back Next > Cancel

• On the Configure DHCP Option page, select No, I will configure these options later

#### and click Next



• On the Completing the New Scope Wizard page, click Finish

New Scope Wizard	
S	Completing the New Scope Wizard
	You have successfully completed the New Scope wizard.
	Before clients can receive addresses you need to do the following:
	1. Add any scope specific options (optional).
	2. Activate the scope.
	To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.
	To close this wizard, click Finish.
	< Back Finish Cancel

- Expand Scope, right click on Scope Options and select Configure Options
- On the Scope Options dialog box, select the following: 003 Router 10.32.10.254, 006
   DNS Server 10.32.5.3, 015 DNS Domain Name addev.local and click OK
- Right click on the **Scope** and select **Activate**

### Configure DHCP Server with a scope for VLAN 20

- Open DHCP Console from Administrative Tools
- Right click on IPv4 and select New Scope
- On the Welcome to the New Scope Wizard page, click Next

New Scope Wizard	
5	Welcome to the New Scope Wizard
	This wizard helps you set up a scope for distributing IP addresses to computers on your network.
	To continue, click Next.
	< Back Next > Cancel

• On the Scope Name page, type a name for the scope and click Next

New Scope Wizard	
Scope Name You have to pro a description.	vide an identifying scope name. You also have the option of providing
Type a name an how the scope is	d description for this scope. This information helps you quickly identify s to be used on your network.
Name:	Client Computers VLAN 20
Description:	
	< Back Next > Cancel

• On the IP Address Range page, specify Start and End IP address. Also specify the

correct subnet mask and click Next

New Scope Wizard	
IP Address Range You define the scope address range by identifying a set of consecutive IP addresses.	Ņ
Configuration settings for DHCP Server	
Enter the range of addresses that the scope distributes.	
Start IP address: 10 . 32 . 20 . 50	
End IP address: 10 . 32 . 20 . 60	
Configuration settings that propagate to DHCP Client	
Length: 24 👗	
Subnet mask: 255 . 255 . 0	
< Back Next > Cancel	

• On the Add Exclusions page, click Next

New Scope Wizard
Add Exclusions and Delay Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.
Start IP address:     End IP address:       I     .       Find underse range:
Remove
Subnet delay in milli second:
< Back Next > Cancel

• On the Lease Duration page, specify a lease duration and click Next

New Scope Wizard	
Lease Duration The lease duration specifies how long a client can use an IP address from this scope.	(J)
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate. Set the duration for scope leases when distributed by this server. Limited to:	
Days: Hours: Minutes:	
< Back Next >	Cancel

• On the **Configure DHCP Option** page, select **No, I will configure these options later** and click **Next** 

New Scope Wizard	
Configure DHCP Options You have to configure the most common DHCP options before clients can use the scope.	
When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.	
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.	
Do you want to configure the DHCP options for this scope now?	
O Yes, I want to configure these options now	
No, I will configure these options later	
< Back Next > Cancel	

• On the **Completing the New Scope Wizard** page, click **Finish** 

New Scope Wizard	
	Completing the New Scope Wizard
	You have successfully completed the New Scope wizard.
	Before clients can receive addresses you need to do the following:
	1. Add any scope specific options (optional).
	2. Activate the scope.
	To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover. To close this wizard, click Finish.
	< Back Finish Cancel

- Expand Scope, right click on Scope Options and select Configure Options
- On the Scope Options dialog box, select the following: 003 Router 10.32.20.254, 006
   DNS Server 10.32.5.3, 015 DNS Domain Name addev.local and click OK
- Right click on the **Scope** and select **Activate**

## Configure DHCP Server with a scope for VLAN 99 (Authentication Fail VLAN)

- Open DHCP Console from Administrative Tools
- Right click on IPv4 and select New Scope
- On the Welcome to the New Scope Wizard page, click Next

New Scope Wizard	
	Welcome to the New Scope Wizard
	This wizard helps you set up a scope for distributing IP addresses to computers on your network.
	To continue, click Next.
	< Back Next > Cancel

• On the Scope Name page, type a name for the scope and click Next

New Scope Wizard	
Scope Name You have to p a description.	rovide an identifying scope name. You also have the option of providing
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.	
Name:	Authentication Fail VLAN 99
Description:	
	< Back Next > Cancel

• On the **IP Address Range** page, specify Start and End IP address. Also specify the correct subnet mask and click **Next** 

	New Scope Wizard	
P Address Range You define the scop	e address range by identifying a set of consecutive IP addresses.	Dh
- Configuration settings	for DHCP Server	
Enter the range of ad	dresses that the scope distributes.	
Start IP address:	10 . 32 . 99 . 50	
End IP address:	10 . 32 . 99 . 60	
-Configuration settings Length:	that propagate to DHCP Client	
Subpot mode:	255 255 0	
Subriet Mask.	200.200.200.0	
1		
	< Back Next > (	Cancel

• On the Add Exclusions page, click Next

New Scope Wizard	
Add Exclusions and Delay Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.	
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.	
Start IP address:       End IP address:          Add         Excluded address range:       Remove         Subnet delay in milli second:       0	
< Back Next > Cancel	

• On the Lease Duration page, specify a lease duration and click Next

New Scope Wizard	
Lease Duration The lease duration specifies how long a client can use an IP address from this scope.	
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate. Set the duration for scope leases when distributed by this server. Limited to:	
Days: Hours: Minutes:	
< Back Next > Cancel	

• On the Configure DHCP Option page, select No, I will configure these options later

#### and click Next



• On the Completing the New Scope Wizard page, click Finish

New Scope Wizard	
5	Completing the New Scope Wizard
_7₽	You have successfully completed the New Scope wizard.
	Before clients can receive addresses you need to do the following:
	1. Add any scope specific options (optional).
	2. Activate the scope.
	To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.
	To close this wizard, click Finish.
	< Back Finish Cancel

- Expand Scope, right click on Scope Options and select Configure Options
- On the Scope Options dialog box, select the following: 003 Router 10.32.99.254, 006
   DNS Server 10.32.5.3, 015 DNS Domain Name addev.local and click OK
- Right click on the **Scope** and select **Activate**

## Configure DHCP Server with a scope for VLAN 100 (Guest VLAN)

- Open DHCP Console from Administrative Tools
- Right click on IPv4 and select New Scope
- On the Welcome to the New Scope Wizard page, click Next

New Scope Wizard	
	Welcome to the New Scope Wizard This wizard helps you set up a scope for distributing IP addresses to computers on your network. To continue, click Next.
	< Back Next > Cancel

• On the Scope Name page, type a name for the scope and click Next

New Scope Wizard	
Scope Name You have to provide an identifying scope name. You also have the option of providing a description.	
Type a name and how the scope is	d description for this scope. This information helps you quickly identify to be used on your network.
Name:	Client Computers VLAN 100
Description:	
	< Back Next > Cancel

• On the IP Address Range page, specify Start and End IP address. Also specify the

correct subnet mask and click Next

New Scope Wizard	
IP Address Range You define the scope address range by identifying a set of consecutive IP addresses.	
Configuration settings for DHCP Server	
Enter the range of addresses that the scope distributes.	
Start IP address: 10 . 32 . 100 . 50	
End IP address: 10 . 32 . 100 . 60	
Configuration settings that propagate to DHCP Client	
Length: 24	
Subnet mask: 255.255.255.0	
< Back Next > Cancel	

• On the Add Exclusions page, click Next

New Scope Wizard
Add Exclusions and Delay Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.
Start IP address:     End IP address:       · · · ·     · · · ·
Excluded address range:
Subnet delay in milli second:
< Back Next > Cancel

• On the Lease Duration page, specify a lease duration and click Next

New Scope Wizard	
Lease Duration The lease duration specifies how long a client can use an IP address from this scope.	S
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.	
Set the duration for scope leases when distributed by this server.	
Limited to:	
Days: Hours: Minutes:	
< Back Next > Ca	ancel

• On the **Configure DHCP Option** page, select **No, I will configure these options later** and click **Next** 

New Scope Wizard	
Configure DHCP Options You have to configure the most common DHCP options before clients can use the scope.	
When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.	
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.	
Do you want to configure the DHCP options for this scope now?	
O Yes, I want to configure these options now	
No, I will configure these options later	
< Back Next > Cancel	

• On the **Completing the New Scope Wizard** page, click **Finish** 

New Scope Wizard	
	Completing the New Scope Wizard
	You have successfully completed the New Scope wizard.
	Before clients can receive addresses you need to do the following:
	1. Add any scope specific options (optional).
	2. Activate the scope.
	To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.
	To close this wizard, click Finish.
< Back Finish Cancel	

- Expand Scope, right click on Scope Options and select Configure Options
- On the Scope Options dialog box, select the following: 003 Router 10.32.100.254, 006 DNS Server 10.32.5.3, 015 DNS Domain Name addev.local and click OK
- Right click on the **Scope** and select **Activate**

# Install and configure your NPS Server

The task of the NPS server is the talk with the switch. The NPS server will be configured as a RADIUS server, whereas the switch will be configured as a RADIUS client. Afterwards, we need to create a Connection Request Policy which allows a connection between the switch and the NPS server. Next step is to create Network Policies where we can provide more details on how the client on the network needs to be authenticated.

- Install the NPS Server Role
- Configure RADIUS Clients on NPS Server
- Configure Connection Request Policy
- Configure a Network Policy for EAP-TLS
- Configure a Network Policy for PEAP-EAP-MSCHAPv2
- Configure a Network Policy for PEAP-EAP-TLS

### Install the NPS Server Role

- Open Server Management from Administrative Tools
- On the Select Server Role page, select Network Policy and Access Services, and click

#### Next

Add Roles Wizard		×
Select Server Ro	les	
Before You Begin Server Roles Network Policy and Access Services Role Services Confirmation Progress Results	Select one or more roles to install on this server. Boles: Active Directory Certificate Services Active Directory Johanni Services Active Directory Jiphweight Directory Services Active Directory Liphweight Directory Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services DNS Server DNS Server File Services V Metwork Policy and Access Services Terminal Services UDDI Services UDDI Services Web Server (115) Windows Deployment Services	Description: <u>Network Policy and Access Services</u> provides Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (IRRA), and Host Credential Authority (IRRA), and Host Credent
	More about server roles	
	< Previous	Next > Install Cancel

• On the Network and Access Services page, click Next

Add Roles Wizard	×
Network Policy	and Access Services
Before You Begin Server Roles Network Policy and Access Services Role Services Confirmation Progress Results	<ul> <li>Introduction to Network Policy and Access Services allows you to provide local and remote network access and to define and refrore policies for network access authentication, authorization, and client health using Network Policy Server (NPS), Routing and Remote Access Service, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP).</li> <li>Tongo to Net</li> <li>Ou can deploy NPS as a Remote Authentication Dial-In User Service (RADIUS) server and proxy and as a Network Access Protection (NuP) policy server. After installing NPS using this wizard, you can configure NPS from the NPAS home page using the INPS Console.</li> <li>AlaP helps you ensure that computers connecting to the network are compliant with organization network apes using the INPS console.</li> <li>Additional Information</li> <li>Overview of Network Policy and Access Services</li> <li>Network Access Protection (NuP) in NPS</li> <li>Network Access Protection (NuP) in NPS</li> <li>Network Policy Server</li> </ul>
	< Previous Next > Install Cancel

• On the Select Role Services page, select Network Policy Server

Before You Begin Server Ro <mark>l</mark> es	Select the role services to install for Network Policy and Acce <u>R</u> ole services:	ss Services: Description:
Network Policy and Access Services Role Services Confirmation Progress Results	Vetwork Policy Server     Routing and Remote Access Services     Remote Access Service     Routing     Health Registration Authority     Host Credential Authorization Protocol	Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.
	More about role services	

• On the Confirm Installation Selections page, click Install

Add Roles Wizard		×
Confirm Installati	ion Selections	
Before You Begin Server Roles Network Policy and Access Services Role Services	To install the following roles, role services, or features, click Install.  (1) 1 informational message below  (1) This server might need to be restarted after the installation completes.	
Confirmation	Network Policy and Access Services	
Progress	Network Policy Server	
	Print, e-mai, or save this information	
	< Previous Next > Install Cancel	

### **Configure Accounting**

- From the Network Policy Server console, click on Accounting
- Select Configure Local File Logging
- On the Log File tab, select IAS as format and click OK

### **Configure RADIUS Clients on NPS Server**

- Open Network Policy Server from Administrative Tools
- Expand RADIUS Clients and Servers, right click on RADIUS Clients and select New RADIUS Client
- On the New RADIUS Client dialog box, specify a friendly name and IP address
- From the Vendor list box, select Cisco and specify a Shared Secret

		Cisco 35	560 Pro	pertie	s		×
ettings	Advanced						
Enable	e this RADIUS client						
Sele	ct an existing templat	e:					
							7
Name	and Address						
Friend	y name:						
Cisco	3560						
Addre	s (IP or DNS):						
10.32	5.254					Verify	
Shared	Secret an existing Shared S	ecrets temp	olate:				
None							-
None To ma secret secret	nually type a shared s click Generate. You entered here. Shared nual I secret:	ecret, click must confi I secrets ar	c Manual gure the l e case-se	To auto RADIUS ensitive.	matically ge client with t	enerate a share the same share	- -
None To ma secret secret	nually type a shared s click Generate. You entered here. Shared nual I secret:	ecret, click must confi secrets ar	c Manual gure the l e case-se te	To auto RADIUS msitive.	matically ge client with t	enerate a sharee the same sharee	- -
None To ma secret secret Share Confin	nually type a shared s click Generate. You entered here. Shared nual I secret:	ecret, click must confi I secrets ar	c Manual. gure the l e case-se	To auto RADIUS msitive.	matically ge client with t	enerate a share the same share	-
None To ma secret secret Share Confin	nually type a shared s click Generate. You entered here. Shared nual I secret: n shared secret:	ecret, click must confi I secrets ar	c Manual. gure the le case-se	To auto RADIUS msitive.	matically ge client with t	enerate a share the same share	4

• Click on **Advanced**, uncheck or check the required options

Cisco 3560 Properties
Settings Advanced
Vendor Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.
Vendor name:
RADIUS Standard V
Additional Options
RADIUS client is NAP-capable
OK Cancel Apply

• Click **OK** 

Configure a Connection Request Policy

- From the Network Policy Server Console, right click on Connection Request Policies and select New
- On the Specify Connection Request Policy Name and Connection Type page, type a name for the policy and click Next

	Cisco Switch Properties			
Overview Conditions S	ettings			
Policy name:	Cisco Switch			
Policy State If enabled, NPS evalua	tes this policy while processing connection requests. If disabled, NPS does not evalue this policy.			
Policy enabled				
Network connection method         Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific. but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.         Image: Type of network access server:         Unspecified         Vendor specific:         Image: Type of network access server:				
	OK Cancel Apply			

- On the Specify Conditions page, click Add. Select NAS Port Type (Ethernet)
- On the Select conditions dialog box, select NAS IPv4 Address and click Add
- On the NAS IPv4 Address dialog box, type the management IP address of the switch.

			Cisco Switch Properties
Overview	Conditions	Settings	
Configure	the condition	ne for this r	stunde policy
coningure		15 101 1115 1	etwork policy.
lf conditio	ons match the on request, N	e connectio IPS skips th	in request, NPS uses this policy to authorize the connection request. If conditions do not match the nis policy and evaluates other policies, if additional policies are configured.
Cor	dition	_	Value
NA 😂	S Port Type		Ethemet
BE NA	S IPv4 Addre	ss	10.32.5.254
Condition	description		
The NAS	Port Type co	ondition spe	ecifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual
private ne	etworks, IEEE	E 802.11 w	ireless, and Ethemet switches.
			Add Edit Remove
			OK Cancel Apply

- Click **OK** and click **Next**
- On the Specify Connection Request Forwarding page, select Authenticate requests on this server and click Next
- On the Specify Authentication Methods page, click Next

	Cisco Switch Properties
Overview Conditions Settings	
Configure the settings for this network policy if conditions and constraints match the con Settings:	r. nection request and the policy grants access, settings are applied.
Required Authentication Methods	Override network policy authentication settings
Authentication Methods Forwarding Connection Request	These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.
Authentication     Accounting	EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types:
Specify a Realm Name           P         Attribute           RADIUS Attributes	Move Up Move Down
Standard Vendor Specific	Add Edit Remove
	Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) User can change password after k has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after k has expired Encrypted authentication (CHAP)
	Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method.
	OK Cancel Apply

- On the **Configure Settings** page, click **Next**
- On the Completing Connection Request Policy Wizard page, click Finish

## Configure a Network Policy for EAP-TLS

- From the Network Policy Server Console, right click on Network Policies and select
   New
- On the Specify Network Policy Name and Connection Type page, type a name for

your policy and click Next

	New Network Policy
	<b>Specify Network Policy Name and Connection Type</b> You can specify a name for your network policy and the type of connections to which the policy is applied.
Policy name Client Comput	: ers VLAN 20 - EAP-TLS
Select the type type or Vendo select Unspec	s of network access server that sends the connection request to NPS. You can select either the network access server rspecific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, ified.
Unspecifie O Vendor spe 10	ad v señe: ⇔

- On the Specify Conditions page, click Add
- From the Select Conditions dialog box, select NAS Port Type (Ethernet) and click Add
- From the Select Condition dialog box, add the following Windows Groups Domain

Computers, Domain Users , and click Next

			New Network Policy
		Specify Co Specify the con of one conditio	onditions ditions that determine whether this network policy is evaluated for a connection request. A minimum n is required.
Cond	litions:		
	Condition		Value
<b>S</b>	NAS Port	Туре	Ethemet
1	Windows	Groups	ADDEV\Wired Computers VLAN 20 OR ADDEV\Domain Users
Cond The V	ition descri	ption:	specifies that the connecting user or computer must belong to one of the selected groups.
			Add Edt Remove
			Previous Next Finish Cancel

• On the Specify Access Permissions page, select Access Granted and click Next

	New Network Policy
	Specify Access Permission Configure whether you want to grant network access or deny network access if the connection request matches this policy.
Access grading of the second sec	anted ses if client connection attempts match the conditions of this policy. nied less if client connection attempts match the conditions of this policy. determined by User Dial-in properties (which override NPS policy) my access according to user dial-in properties if client connection attempts match the conditions of this policy.
	Previous Next Finish Cancel

• On the **Configure Authentication Methods** page, clear MS-CHAP, clear MS-CHAP-v2 and click **Add** 

• On the Select EAP dialog box, select Microsoft: Smart card or other Certificate and

click **OK** 

	New Network Policy
	<b>Configure Authentication Methods</b> Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.
EAP types are n EAP Types: Microsoft: Sma	egotiated between NPS and the client in the order in which they are listed. art Card or other certificate Move Up
Add	Edt Remove
Less secure Microsoft E User car User car Encrypted a Unencrypte Allow clients Perform made	authentication methods: ncrypted Authentication version 2 (MS-CHAP-v2) n change password after it has expired ncrypted Authentication (MS-CHAP) n change password after it has expired uthentication (CHAP) d authentication (PAP. SPAP) s to connect without negotiating an authentication method. chine health check only
	Previous Next Finish Cancel

• On the **Configure Constraints** page, click **Next** 

New Network Policy						
Configure Constraints Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional if you do not want to configure constraints, click Next.						
Configure the constraints for this network If all constraints are not matched by the Constraints:	Configure the constraints for this network policy. If all constraints are not matched by the connection request, network access is denied.					
Constraints Left Timeout Session Timeout Called Station ID Day and time restrictions NAS Port Type	Specify the maximum time in minutes that the server can remain idle before the connection is disconnected Disconnect after the maximum idle time 1					
	Previous Next Finish Cancel					

• On the **Configure Settings** page, add the following **Standard Attributes** 

	New Net	work Policy	x		
Configure Settings NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy ar matched.					
Configure the settings for this network If conditions and constraints match the Settings:	policy. e connection request and the	policy grants access, settings are applied.			
RADIUS Attributes  Standard  Vendor Specific  Network Access Protection  NAP Enforcement	To send additional attribut then click Edit. If you do n your RADIUS client docur	es to RADIUS clients, select a RADIUS standard attribute, and ot configure an attribute, it is not serit to RADIUS clients. See mentation for required attributes.			
Extended State	Name	Value			
Routing and Remote Access	Framed-MTU Tunnel-Medium-Type	1344 802 (includes all 802 media plus Ethemet canonical for			
Multilink and Bandwidth Allocation Protocol (BAP)	Tunnel-Pvt-Group-ID Tunnel-Type	20 Virtual LANs (VLAN)			
IP Filters					
A Encryption					
IP Settings	Add Edi	t Remove			
	1 *				
		Previous Next Finish Cancel			

• Click on Vendor Specific attributes and add Microsoft Tunnel-Tag equal to 1, click OK and click Next

	Ne	ew Network Pol	cy	x			
Configure Settings           NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy a matched.							
Configure the settings for this network If conditions and constraints match the Settings:	Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied.						
RADIUS Attributes  Standard  Vendor Specific  Network Access Protection  NAP Enforcement	To send addition then click Edit. If your RADIUS cli	al attributes to RADIL you do not configure ent documentation for	IS clients, select a Vendor Specific attribute, and an attribute, it is not sent to RADIUS clients. See required attributes.				
Extended State	Name Tunnel-Tag	Vendor RADIUS Standard	Value 1				
Multilink and Bandwidth Allocation Protocol (BAP)							
IP Settings	Add	Edit	Remove				
		Previo	us Next Finish Can	cel			

• On the Completing New Network Policy page, click Finish

		New Network Policy	x
Ç	Completing New N	Network Policy	
You have succes	sfully created the following ne	twork policy:	
Client Computer	rs VLAN 20 - EAP-TLS		
Policy condition	18-		
Condition	Value		
NAS Port Type	Ethernet		
Windows Groups	ADDEV\Wired Computers	VLAN 20 OR ADDEV\Domain Users	
Policy settings:			
Condition	- 44 4	Value	_
All thentication IVI	ethod	EAP	^
Access Demissio		Crant Assess	^
Access Permissio	n biant Cliente	Grant Access	< =
Access Permissio Update Noncomp NAP Enforcement	n bliant Clients t	Grant Access True Allow full network access	^
Access Permissio Update Noncomp NAP Enforcement Ignore User Dial-	n pliant Clients It In Properties	Grant Access True Allow full network access False	-
Access Permissio Update Noncomp NAP Enforcemen Ignore User Dial- Extensible Auther	n pliant Clients It In Properties ntication Protocol Method	Grant Access True Allow full network access False Microsoft: Smart Card or other certificate	<
Access Permission Update Noncost NAP Enforcemen Ignore User Dial- Extensible Auther To close this wizar	n Diant Clients In Properties Inication Protocol Method d, click Finish.	Grant Access True Allow full network access False Microsoft: Smart Card or other certificate	*

Configure a Network Policy for PEAP-EAP-MSCHAPv2

- From the Network Policy Server Console, right click on Network Policies and select
   New
- On the Specify Network Policy Name and Connection Type page, type a name for

your policy and click Next

	New Network Policy
	Specify Network Policy Name and Connection Type You can specify a name for your network policy and the type of connections to which the policy is applied.
Policy name: Client Compute	rs VLAN 10 - PEAP-EAP-MSCHAPv2
Network conne Select the type type or Vendorr select Unspecifie Organization Vendor specifie 10	ction method of network access server that sends the connection request to NPS. You can select either the network access server specific, but nether is required. If your network access server is an 802.1X authenticating switch or wireless access point, led.
	Previous Next Finish Cancel

• On the Specify Conditions page, click Add

- From the Select Conditions dialog box, select NAS Port Type (Ethernet) and click Add
- From the Select Condition dialog box, add the following Windows Groups Domain

Computers, Domain Users and click Next

		New Network Policy	X
	Specify C Specify the cor of one conditio	Conditions nditions that determine whether this network policy is evaluated for a connec on is required.	tion request. A minimum
Conditions:			
Condition Windows NAS Port	Groups Type Iption: Type condition sp s, IEEE 802.11 v	Value ADDEV-Wired Computers VLAN 10 OR ADDEV-Domain Users Ethemet  peofiles the type of media used by the access client, such as analog phone lines, li wireless, and Ethemet switches.  Add Edit	SDN, tunnels or virtual
		Previous Next Finis	h

• On the Specify Access Permissions page, select Access Granted and click Next

	New Network Policy
	Specify Access Permission Configure whether you want to grant network access or deny network access if the connection request matches this policy.
Access grading of the second sec	anted ses if client connection attempts match the conditions of this policy. nied less if client connection attempts match the conditions of this policy. determined by User Dial-in properties (which override NPS policy) any access according to user dial-in properties if client connection attempts match the conditions of this policy.
	Previous Next Finish Cancel

- On the **Configure Authentication Methods** page, clear MS-CHAP, clear MS-CHAP-v2 and click **Add**
- On the Select EAP dialog box, select Microsoft: Protected EAP (PEAP)

Client Computers VLAN 10 PEAP-EAP-TLS Properties				
Client Co Overview Conditions Constraints Settings Configure the constraints for this network policy. If all constraints are not matched by the connect Constraints: Constraints: Authentication Methods Session Timeout Called Station ID Day and time restrictions NAS Port Type	Allow access only to those clients that authenticate with the specified methods.       Allow access only to those clients that authenticate with the specified methods.       EAP types are negotiated between NPS and the client in the order in which they are isted.       EAP Types:       Microsoft: Protected EAP (PEAP)       Move Up       Move Down       <			
	Microsoft Distyleted Authentication (MS-CHAP)     User can change password after it has expired     Microsoft Encrypted Authentication (MS-CHAP)     User can change password after it has expired     Encrypted authentication (CHAP)     Unencrypted authentication (PAP, SPAP)     Allow clients to connect without negotiating an authentication method     Perform machine health check only			
L	OK Cancel Apply			

• Configure settings as below and click **OK** 

Edi	t Protected EAP Properties			
Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.				
Certificate issued to:	ADDEVDC04.addev.local			
Friendly name:	ADDEVDC04.addev.local			
Issuer:	addev-ca			
Expiration date:	24/10/2013 14:49:36			
✓ Enable Fast Reconnect Disconnect Clients without Cryptobinding Eap Types				
Secured password (EAP-M	ISCHAP v2) Move Up			
Move Down				
Add Edit	Remove OK Cancel			

• On the **Configure Constraints** page, click **Next** 

New Network Policy					
Co co if	Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.				
Configure the constraints for this network policy. If all constraints are not matched by the connection request, network access is denied.					
Constraints Left Timeou Session Tim Called Stati Called Stati Day and tim restrictions RAS Port Ty	t neout on ID te ype	Specify the maximum time in minutes that the server can remain idle before the connection is disconnected  Disconnect after the maximum idle time  1 ^			
		Previous Next Finish Cancel			

• On the Configure Settings page, add the following Standard Attributes

	New Net	work Policy	×				
Configure Set NPS applies settings matched.	<b>ttings</b> to the connection request if	all of the network policy conditions and constraints for the	policy are				
Configure the settings for this network p If conditions and constraints match the	Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied.						
RADIUS Attributes         Standard         Standard         Vendor Specific         Network Access Protection         NAP Enforcement         Extended State         Routing and Remote         Access         Multilink and Bandwidth Allocation Protocol (BAP)         IP Filters         Encryption         IP Settings	To send additional attribut then click Edit. If you don your RADIUS client docum Attributes: Name Framed-MTU Tunnel-Medium-Type Tunnel-Pty-Group-ID Tunnel-Type Add Edit	es to RADIUS clients, select a RADIUS standard attribute, and ot configure an attribute, it is not sent to RADIUS clients. See entation for required attributes. Value 1344 802 (includes all 802 media plus Ethemet canonical for 10 Virtual LANs (VLAN)					
		Previous Next Finish Canc	el				

• Click on Vendor Specific attributes and add Microsoft Tunnel-Tag equal to 1, click OK and click Next

	New Network Policy	×
Configure Se           NPS applies settings           matched.	2 <b>ttings</b> s to the connection request if all of the network policy conditions and constraints fo	r the policy are
Configure the settings for this network   If conditions and constraints match the	policy. e connection request and the policy grants access, settings are applied.	
RADIUS Attributes Standard Standard Network Access Protection NAP Enforcement	To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. S your RADIUS client documentation for required attributes.	nd ee
Extended State	Name Vendor Value	
Routing and Remote Access     Multilink and Bandwidth Allocation Protocol (BAP)     IP Filters     Encryption     IP Settings	Tunnel-Tag RADIUS Standard 1 Add Edit. Remove	
	Previous Next Finish (	Cancel

• On the **Completing New Network Policy** page, click **Finish** 

	New Network Policy	x
Completing New N	letwork Policy	
You have successfully created the following net	work policy:	
Client Computers VLAN 10 - PEAP-EAP-	MSCHAPv2	
Policy conditions:		
Condition Value		
Windows Groups ADDEV\Wired Computers	/LAN 10 OR ADDEV\Domain Users	
NAS Port Type Ethemet		
Policy settings:		
Condition	Value	
Authentication Method	EAP	
Access Permission	Grant Access	≡
Update Noncompliant Clients	True	
NAP Enforcement	Allow full network access	
Ignore User Dial-In Properties	False	
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)	$\mathbf{v}$
To close this wizzed, click Finish		
to close this wizard, click Finish.		
	Previous Next Finish Cancel	

# Configure a Network Policy for PEAP-EAP-TLS

- From the Network Policy Server Console, right click on Network Policies and select
   New
- On the **Specify Network Policy Name and Connection Type** page, type a name for your policy and click **Next**

	New Network Policy
	<b>Specify Network Policy Name and Connection Type</b> You can specify a name for your network policy and the type of connections to which the policy is applied.
Policy name Client Comput Network conn Select the typ type or Vendo select Unspec	ers VLAN 10 - PEAP-EAP-TLS ection method e of network access server that sends the connection request to NPS. You can select either the network access server r specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, offed.
<ul> <li>Type of ne</li> <li>Unspecifie</li> <li>Vendor specifie</li> <li>10</li> </ul>	twork access server: ed
	Previous Next Finish Cancel

- On the Specify Conditions page, click Add
- From the Select Conditions dialog box, select NAS Port Type (Ethernet) and click Add
- From the Select Condition dialog box, add the following Windows Groups Domain

Computers, Domain Users and click Next

			New Network Policy	1
J		Specify Co Specify the condition	onditions ditions that determine whether this network policy is evaluated for a connection request. A minimu n is required.	m
Ca	onditions:			
	Condition		Value	1
1	🦉 Windows	Groups	ADDEV/Wired Computers VLAN 10 OR ADDEV/Domain Users	
9	NAS Port	Туре	Ethemet	
Co Th pri	ndition descr e NAS Port 1 vate network	iption: Type condition spe s, IEEE 802.11 wi	ecflies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual ireless, and Ethernet switches.           Add         Edit	
			Previous Next Finish Cancel	1

• On the Specify Access Permissions page, select Access Granted and click Next

	New Network Policy
	Specify Access Permission Configure whether you want to grant network access or deny network access if the connection request matches this policy.
Access griphics of the second se	anted uss if client connection attempts match the conditions of this policy. nied ss if client connection attempts match the conditions of this policy. determined by User Dial-in properties (which override NPS policy) any access according to user dial-in properties if client connection attempts match the conditions of this policy.
	Previous Next Finish Cancel

- On the **Configure Authentication Methods** page, clear MS-CHAP, clear MS-CHAP-v2 and click **Add**
- On the Select EAP dialog box, select Microsoft: Protected EAP (PEAP)

Client	Computers VLAN 10 PEAP-EAP-TLS Properties	x
Overview Conditions Constraints Setting Configure the constraints for this network pol if all constraints are not matched by the corr Constraints: Constraints Authentication Methods	s	
<ul> <li>Idle Timeout</li> <li>Session Timeout</li> <li>Called Station ID</li> <li>Day and time restrictions</li> <li>NAS Port Type</li> </ul>	EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types: Microsoft: Protected EAP (PEAP) Move Up Move Up Move Down <	
	OK Cancel Ap	ply

• Configure settings as below and click **OK** 

Edi	it Protected EAP Properties
Select the certificate the s A certificate that is config Policy will override this cer	server should use to prove its identity to the client. ured for Protected EAP in Connection Request rtificate.
Certificate issued to:	ADDEVDC04.addev.local
Friendly name:	ADDEVDC04.addev.local
Issuer:	addev-ca
Expiration date:	24/10/2013 14:49:36
Enable Fast Reconnect     Disconnect Clients with     Eap Types	out Cryptobinding
Smart Card or other certif	ficate Move Up
	Move Down
Add Edit	Remove OK Cancel

• On the Configure Constraints page, click Next

	New Network Policy
Configure Constraints are add constraint is not ma if you do not want t	Denstraints litional parameters of the network policy that are required to match the connection request. If a tched by the connection request, NPS automatically rejects the request. Constraints are optional; o configure constraints, click Next.
Configure the constraints for this netw If all constraints are not matched by th <b>Constraints</b> :	ork policy. e connection request, network access is denied.
Constraints Ide Timeout Session Timeout Called Station ID Day and time restrictions NAS Port Type	Specify the maximum time in minutes that the server can remain idle before the connection is disconnected Disconnect after the maximum idle time 1
	Previous Next Finish Cancel

• On the **Configure Settings** page, add the following **Standard Attributes** 

	New Net	work Policy	x
NPS applies setti matched.	Settings ngs to the connection request i	f all of the network policy conditions and constraints for t	he policy are
Configure the settings for this netwo If conditions and constraints match	ork policy. the connection request and the	policy grants access, settings are applied.	
Settings:			
RADIUS Attributes	To send additional attribut then click Edit. If you do r	es to RADIUS clients, select a RADIUS standard attribute, an not configure an attribute, it is not sent to RADIUS clients. See	ıd
Vendor Specific	your RADIUS client docu	mentation for required attributes.	
Network Access Protection			
NAP Enforcement	Attributes:		
Extended State	Name	Value	
Routing and Remote	Framed-MTU	1344	
Access	Tunnel-Medium-Type	802 (includes all 802 media plus Ethemet canonical for	
Multilink and Bandwidth Allocation Protocol (BAP)	Tunnel-Pvt-Group-ID Tunnel-Type	10 Virtual LANs (VLAN)	
IP Filters			
Encryption			
IP Settings	Add Ed	t Remove	_
	1		
		Previous Next Finish Car	ncel

• Click on Vendor Specific attributes and add Microsoft Tunnel-Tag equal to 1, click OK and click Next

	Ne	w Network Poli	cy	x
Configure Se NPS applies settings matched.	ttings to the connection r	equest if all of the n	etwork policy conditions and constraints for the p	olicy an
Configure the settings for this network if conditions and constraints match the Settings:	policy. connection request	and the policy grants	access, settings are applied.	
RADIUS Attributes     Standard     Vendor Specific     Network Access Protection	To send additiona then click Edit. If your RADIUS clie	al attributes to RADIU you do not configure nt documentation for	IS clients, select a Vendor Specific attribute, and an attribute, it is not sent to RADIUS clients. See required attributes.	
NAP Enforcement	Attributes:	Mandan	Met er	
Routing and Remote Access	Tunnel-Tag	RADIUS Standard	value 1	
Multilink and Bandwidth Allocation Protocol (BAP)				
IP Filters				
IP Settings	Add	Edit	Remove	
		Previo	us Next Finish Cancel	

• On the Completing New Network Policy page, click Finish

	New Network Policy
Completing N	ew Network Policy
You have successfully created the follow	ving network policy:
Client Computers VLAN 10 - PEAF	-EAP-TLS
Policy conditions:	
Condition Value	
Windows Groups ADDEV\Wired Com	outers VLAN 10 OR ADDEV\Domain Users
NAS Port Type Ethemet	
Policy settings:	
Policy settings: Condition	Value
Policy settings: Condition Authentication Method	Value ^ EAP
Policy settings: Condition Authentication Method Access Permission	Value ^ EAP Grant Access
Policy settings: Condition Authentication Method Access Permission Update Noncompliant Clients	Value ^ EAP Grant Access True
Policy settings: Condition Authentication Method Access Permission Update Noncompliant Clients NAP Enforcement	Value  EAP Grant Access True Allow full network access
Policy settings: Condition Authentication Method Access Permission Update Noncomplant Clients NAP Enforcement Ignore User Dial-In Properties Extensible Authentication Protocol Methods Te Jose Shiencard, abla Daich	Value       ^         EAP
Policy settings: Condition Authentication Method Access Permission Update Noncompliant Clients NAP Enforcement Ignore User Dial-In Properties Extensible Authentication Protocol Meti To close this wizard, click Finish.	Value ^ EAP _ Grant Access = True _ Allow full network access _ False _ nod _ Microsoft: Protected EAP (PEAP) _ V

## **Configure your policy with Filter-Id ACL**

addevsw01(config)#access-list 101 deny tcp any host 10.32.5.3 eq www addevsw01(config)#access-list 101 permit ip any any

You need to add the RADIUS attribute into your Network Policy.

- Open Network Policy Server from Administrative Tools
- Right click on the Network Policy, select Properties and click Settings
- On the Add Standard RADIUS Attribute page, select Filter-Id and click Add

Add Standard RADIUS Attribute
To add an attribute to the settings, select the attribute, and then click Add.
To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.
Access type:
Ali
Attributes:
Name
Acct-Interim-Interval
Callback-Number
Class
Filter-Id
Framed-AppleTalk-Link
Framed-AppleTalk-Network
Ersmad Applo Talle Zono
Description:
specifies the name of filter list for the user requesting authentication.
Add Close

• On the Attribute Information page, click String and type the ACL number

Attribute In	formation	x
Attribute name: Filter-Id		
Attribute number: 11		
Attribute format: OctetString		
Enter the attribute value in: String		
○ Hexadecimal		
101		
	OK Cano	el

• Click OK

	Attribute Information			x
Attribute name: Filter-Id				
Attribute number: 11				
Attribute format: OctetString				
Attribute values:				
Vendor	Value		Add	
RADIUS Standard	101		Edit	
			Remove	
			Move Up	
			Move Dow	'n
	0	к	Cancel	

• Click OK

## **Configure your policy with Cisco-AV-Pair ACL**

```
ip:inacl#201=deny tcp any host 10.32.5.3 eq www
ip:inacl#201=permit ip any any
```

You need to add the Vendor attribute into your Network Policy.

- Open Network Policy Server from Administrative Tools
- Right click on the Network Policy, select Properties and click Settings
- On the Add Vendor Specific Attribute page, select Cisco and click on Cisco-AV-Pair and click Add

Attribute Information	x
Attribute name: Cisco-AV-Pair	
Attribute number: 5000	
Attribute format: String	
Attribute values:	
Vendor Value	Add
	Edit
	Remove
	Move Up
	Move Down
ОК	Cancel

• In the **Attribute value** box, type your ACL

Attribute Information	
Attribute name: Cisco-AV-Pair	
Attribute number: 5000	
Attribute format: String	
<u>A</u> ttribute value:	
ip:inacl#201=deny.tcp any host 10.32.5.3 eq.www	
OK Cancel	

- Click OK
- In the Attribute value box, type your ACL
| Attribute In                     | formation × |
|----------------------------------|-------------|
| Attribute name:<br>Cisco-AV-Pair |             |
| Attribute number:<br>5000        |             |
| Attribute format:<br>String      |             |
| Attribute value:                 |             |
| ip:inacl#201=permit ip any any   |             |
|                                  |             |
|                                  | OK Cancel   |

• Click OK

Attribute Information	x		
Attribute name: Cisco-AV-Pair			
Attribute number: 5000			
Attribute format: String			
Attribute values:			
Vendor Value	Add		
Cisco ip:inacl#201=deny tcp any host 10.32.5.3 eq www			
Cisco ip:inacl#201=permit ip any any	Edit		
	Remove		
	Move Up		
	Move Down		
ОК	Cancel		

• Click **OK**, click **Close** and click **OK** 

## **Create a Secure Baseline GPO for Windows 7 client Computers**

- Configure Windows 7 client computers for certificate enrollment
- Configure Windows 7 client computers to enable Wired Authentication
- Configure Windows 7 client computers for 802.1x authentication via Group Policies and PEAP-EAP-TLS

- Configure Windows 7 client computers for 802.1x authentication via Network Sharing Center and PEAP-EAP-MSCHAPv2
- Configure Windows 7 client computers for 802.1x authentication via Network Sharing Center and EAP-TLS
- Configure Windows 7 client computers for 802.1x authentication via Network Sharing Center and PEAP-EAP-TLS

#### Configure Windows 7 client computers for certificate enrollment

- Open Group Policy Management from Administrative Tools
- Expand, Domain | Group Policy Objects | Group Policy, and select New Group Policy
   Object. Type Secure Baseline Client Computers
- Right click on Secure Baseline Client Computers, select GPO Status and select User
   Configuration Settings Disabled.
- Right click on Secure Baseline Client Computers and select Edit.
- Expand Computer Configuration | Policies | Windows Settings | Security Settings |
   Public Key Policies, double click on Certificate Services Client-Auto Enrollment.
- On the Certificate Services Client-Auto Enrollment dialog box, select Enabled.

Certificate Services Client - A	uto-Enrollm	ent Properties	? ×
Define Policy Settings			1
Enroll user and computer certi	ficates automa	tically	
<u>Configuration Model:</u>	Enable	ed	
Renew expired certificates revoked certificates	, update pend	ling certificates, a	nd remove
Update certificates that us	e certificate te	emplates	
Expiration notification			
Show expiry notifications v lifetime is	when the <u>p</u> erce	entage of remainir	ng certificate
10 - %			
Learn more about <u>Automatic c</u>	ertificate mana	agement	
	ОК	Cancel	Apply

• Select Renew expired certificates, select Update certificates and click OK.

#### Configure Windows 7 client computers to enable Wired Authentication

Before we can configure a Windows 7 client computer with 802.1x authentication, we need to enable the Authentication tab, which is part of the local area connection. This Authentication tab will be displayed when the Wired AutoConfig service is started.

- Select System Services, right click on WiredAutoConfig, and select Properties.
- Select **Define this Policy Setting**, and change service startup mode to **Automatic**.

? ×
Apply

• Click OK.

Configure Windows 7 client computers for 802.1x authentication via Group Policy and PEAP-EAP-TLS

- Right click on Wired Network Policies and select Create a New Windows Vista Policy.
- On the New Vista Wired Network Policy Properties dialog box, type a policy name



- Click on the Security tab. Select Enable use of IEEE 802.1x authentication for network access.
- From the Select a network authentication method list box, select Smart Card or certificate.
- On the Authentication Mode list box, select User or Computer authentication.

New Wired Network Policy Properties	×
General Security	
Enable use of IEEE 802.1X authentication for network access	
Select a network authentication method:	
Microsoft: Protected EAP (PEAP)	
Authentication Mode:	
User or Computer authentication	
Max Authentication Failures:	
Cache user information for subsequent connections to this network	
Advanced	
OK Cancel Apply	

- Select Enforce advanced 802.1X settings and click OK.
- Click on Advanced and select Enforce advanced 802.1X settings

2	Enforce advanced 802.1X settings         Max Eapol-Start Msgs:       Held Period (seconds):         3       1         Start Period (seconds):       Auth Period (seconds):         5       18         Eapol-Start Message:       Eapol-Start Message:
	Transmit per IEEE 802.1X
Sing	gle Sign On
Г	Enable Single Sign On for this network
	Perform immediately before User Logon
	Max delay for connectivity(seconds):
	Allow additional dialogs to be displayed during Single Sign On
	This network uses different VLAN for authentication     with machine and user credentials

- Click **OK** and Click **OK**
- Close Group Policy Editor.
- Link GPO to the OU of your workstations
- Restart client computer or launch gpupdate.exe

# Configure Windows 7 client computers for 802.1x authentication via Network and Sharing Center for PEAP-EAP-MSCHAPv2

- Open Network and sharing Center, and select Change adapter settings
- Right click on Local Area Connection and select Properties
- Select Authentication tab and select Enable IEEE 802.1X authentication
- On the Choose a network authentication method list box, select Microsoft:
   Protected EAP (PEAP)
- Click on Settings and select Secured Password (EAP-MSCHAPv2)

Protected EAP Properties				
When connecting:				
Validate server certificate				
Connect to these servers:				
Trusted Root Certification Authorities:				
addev-ca				
AddTrust External CA Root				
Baltmore Cyber Irust Root     Class 2 Public Drimony Cartification Authority				
Entrust pet Certification Authority (2048)				
Entrust net Secure Server Certification Authority				
Equifax Secure Certificate Authority				
<				
Do not prompt user to authorize new servers or trusted certification authorities.				
Select Authentication Method:				
Secured password (EAP-MSCHAP v2)  Configure				
☑ Enable Fast Reconnect				
Enforce Network Access Protection				
Disconnect if server does not present cryptobinding TLV				
Enable Identity Privacy				
	٦			
OK Cancel				

- Click **OK**
- Clear **Remember my credentials for this connection each time I'm logged on** and enable **Fallback to unauthorized network access**

Local Area Connection Properties	23	
Networking Authentication		
Select this option to provide authenticated network access for this Ethemet adapter. Inable IEEE 802.1X authentication		
Choose a network authentication method:		
Microsoft: Protected EAP (PEAP)		
Remember my credentials for this connection each time I'm logged on		
Fallback to unauthorized network access		
Additional Settings		
OK Car	ncel	

• Click Additional Settings, select Specify authentication mode and select Computer authentication from the list

Advanced settings
802.1X settings
Specify authentication mode
User or computer authentication 🔻 Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK Cancel

• Click OK

Configure Windows 7 client computers for 802.1x authentication via Network and Sharing Center for EAP-TLS

- Open Network and sharing Center, and select Change adapter settings
- Right click on Local Area Connection and select Properties
- Select Authentication tab and select Enable IEEE 802.1X authentication
- On the Choose a network authentication method list box, select Microsoft: Smart
   Card or other Certificate
- Clear Remember my credentials for this connection each time I'm logged on and enable Fallback to unauthorized network access

Local Area Connection Properties		
Networking Authentication		
Select this option to provide authenticated network access for this Ethemet adapter.		
Enable IEEE 802.1X authentication		
Choose a network authentication method:		
Microsoft: Smart Card or other certificate   Settings		
Remember my credentials for this connection each time I'm logged on		
Fallback to unauthorized network access		
Additional Settings		
OK Cancel		

• Click Additional Settings, select Specify authentication mode and select Computer authentication from the list

Advanced settings				
802.1X settings				
Specify authentication mode				
User or computer authentication   Save credentials				
Delete credentials for all users				
Enable single sign on for this network				
Perform immediately before user logon				
Perform immediately after user logon				
Maximum delay (seconds):				
Allow additional dialogs to be displayed during single sign on				
This network uses separate virtual LANs for machine and user authentication				
OK Cancel				

• Click OK

Configure Windows 7 client computers for 802.1x authentication via Network and Sharing Center for PEAP-EAP-TLS

- Open Network and sharing Center, and select Change adapter settings
- Right click on Local Area Connection and select Properties
- Select Authentication tab and select Enable IEEE 802.1X authentication
- On the Choose a network authentication method list box, select Microsoft:
   Protected EAP (PEAP) and click Settings

Local Area Connection Properties	×	
Networking Authentication		
Select this option to provide authenticated ne this Ethernet adapter. Enable IEEE 802.1X authentication	twork access for	
Choose a network authentication method:		
Microsoft: Protected EAP (PEAP)	<ul> <li>Settings</li> </ul>	
Remember my credentials for this connection each time I'm logged on		
Fallback to unauthorized network access		
Additional Settings		
	Cancel	

• From the Select Authentication Method list box, select Smart Card or other

certificate and click OK

	Protected EAP Properties
	When connecting:
	Validate server certificate
	Connect to these servers:
l	
	Trusted Root Certification Authorities:
	addev-ca
	AddTrust External CA Root
1	Baltimore CyberTrust Root =
	Class 3 Public Primary Certification Authority
	Entrust.net Certification Authority (2048)
	Entrust.net Secure Server Certification Authority
	Do not prompt user to authorize new servers or trusted certification authorities.
	Select Authentication Method:
	Smart Card or other certificate  Configure
	<ul> <li>Enable Fast Reconnect</li> <li>Enforce Network Access Protection</li> <li>Disconnect if server does not present cryptobinding TLV</li> <li>Enable Identity Privacy</li> </ul>
	OK Cancel

• Clear Remember my credentials for this connection each time I'm logged on and enable Fallback to unauthorized network access

Local Area Connection Properties	X				
Networking Authentication					
Select this option to provide authenticated network access for this Ethernet adapter. Enable IEEE 802.1X authentication					
Choose a network authentication method:					
Microsoft: Protected EAP (PEAP)					
Remember my credentials for this connection each time I'm logged on					
Fallback to unauthorized network access					
Additional Settings					
OK Cancel					

Click Additional Settings, select Specify authentication mode and select User or

Computer authentication from the list

Advanced settings					
802.1X settings					
Specify authentication mode					
User or computer authentication					
Delete credentials for all users					
Enable single sign on for this network					
Perform immediately before user logon					
Perform immediately after user logon					
Maximum delay (seconds):					
Allow additional dialogs to be displayed during single sign on					
This network uses separate virtual LANs for machine and user authentication					
OK Cancel					

Click OK

## Configuring Catalyst 3560 for 802.1x authentication Task List

The next step is to configure the switch to support port-based authentication.

- Enabling 802.1x authentication on the switch
- Configuring switch-to-RADIUS server communication
- Configure Guest VLAN
- Configure Restricted VLAN
- Enabling periodic re-authentication
- Display statistics and status

#### Configuring 802.1x authentication on the switch

```
addevsw01#config t
addevsw01(config)#aaa new-model
addevsw01(config)#aaa authentication dot1x default group radius
```

```
addevsw01(config)#aaa authorization network default group radius
addevsw01(config)#dot1x system-auth-control
addevsw01(config)#interface fa 0/2
addevsw01(config-if)#switchport mode access
addevsw01(config-if)#authentication port-control auto
```

#### Configuring switch-to-RADIUS server communication

addevsw01(config)#radius-server host 10.32.5.15 auth-port 1812
acct-port 1813 key accessdenied

#### **Configure Guest VLAN**

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#authentication event no-response action
authorize vlan 100
```

#### **Configure Restricted VLAN**

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#authentication event fail action authorize
vlan 99
```

#### Enabling periodic re-authentication

```
addevsw01(config)#int fa 0/2
addevsw01(config-if)#authentication periodic
addevsw01(config-if)#authentication timer reauthenticate 4800
```

#### **Display Statistics and Status**

```
addevsw01#show dot1x int fa 0/2
```

#### How to test

Power-on your Windows 7 client computer and configure the correct authentication method. When restart your Windows 7 client, the client sends an authentication request. If authentication is successful, the client computer receives an IP address from your DHCP server. If the client computer is a member of Wired Computers VLAN 10, the client receives an IP address from the network range 10.32.10.50-60.

If authentication fails, the client becomes a member of VLAN 99 and receives an IP address in the range of 10.32.99.50-60

If the client computer is successfully authenticated, you receive an IP address from VLAN 10



After authorization, you receive following message for PEAP-EAP-TLS authentication:



#### VLAN database

addevsw01#sh vlan											
VLAN	Name				Sta	itus	Ports				
1	default				act	ive:	 Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Gi0/1				
5	native	e-vlan			act	ive	Fa0/1				
10	VLAN0010				act	ive	Fa0/2				
99	VLAN0(	099			act	active					
100	VLAN01	100			act	active					
1002	fddi-d	default			act	act/unsup					
1003	3 token-ring-default				act	act/unsup					
1004	fddine	et-default			act	/unsup					
1005	trnet-	-default			act	/unsup					
VLAN	Туре	SAID	MTU	Parent	RingNo	Bridge	No Stp	BrdgMode	Trans1	Trans2	
1	enet	100001	1500	_	_	_	_	-	0	0	
5	enet	100005	1500						0	0	
10	enet	100010	1500						0	0	
99	enet	100099	1500						0	0	
100	enet	100100	1500						0	0	
1002	fddi	101002	1500						0	0	
1003	tr	101003	1500						0	0	
1004	fdnet	101004	1500				ieee	2 -	0	0	
VLAN	Туре	SAID	MTU	Parent	RingNo	Bridge	No Stp	BrdgMode	Trans1	Trans2	
1005	trnet	101005	1500	-	-	_	ibm	-	0	0	
Remot	te SPAN	N VLANs									
Primary Secondary Type Ports											
adder	addewsw01±										

If the client computer fails authentication, you receive an IP address from VLAN 99



If the authentication method is not compatible, the client becomes a member of the authentication fail VLAN

"Mar 1 02:10:12:453: \$A0InmGR-5-51ARI: Starting 'dotix' for client (0080.c638.eUca) on Interface Fa0/2 AuditSessionib 042005F
E000000300764D22
*Mar 1 02:10:16.966: %DOT1X-5-FAIL: Authentication failed for client (0080.c838.e0ca) on Interface Fa0/2 AuditSessionID 0A200
5FE000000300764D22
*Mar 1 02:10:16.966: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'dot1x' for client (0080.c838.e0ca) on Interface Fa
0/2 AuditSessionID 0A2005FE000000300764D22
*Mar 1 02:10:19.231: %DOT1X-5-FAIL: Authentication failed for client (0080.c838.e0ca) on Interface Fa0/2 AuditSessionID 0A200
5FE000000300764D22
*Mar 1 02:10:19.231: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'dot1x' for client (0080.c838.e0ca) on Interface Fa
0/2 AuditSessionID 0A2005FE000000300764D22
*Mar 1 02:11:51.849: %DOT1X-5-FAIL: Authentication failed for client (0080.c838.e0ca) on Interface Fa0/2 AuditSessionID 0A200
5FE000000300764D22
*Mar 1 02:11:51.849: %AUTHMGR-7-RESULT: Authentication result 'timeout' from 'dot1x' for client (0080.c838.e0ca) on Interface
Fa0/2 AuditSessionID 0A2005FE0000000300764D22
*Mar 1 02:11:51.849: %AUTHMGR-5-VLANASSIGN: VLAN 99 assigned to Interface Fa0/2 AuditSessionID 0A2005FE0000000300764D22
*Mar 1 02:11:52.864: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
*Mar 1 02:11:52.889: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (0080.c838.e0ca) on Interface Fa0/2 AuditSessionI
D 0A2005FE000000300764D22
*Mar 1 02:11:52.889: %DOT1X-5-RESULT OVERRIDE: Authentication result overridden for client (0080.c838.e0ca) on Interface Fa0/
2 AuditSessionID 0A2005FE0000000300764D22
*Mar 1 02:12:21.872: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
addevsw01#

#### Per User ACL



## Appendix A: Security Groups

Group	Description
Autoenroll Server	Members of this group receive a certificate with the
Authentication Certificate	purpose of server authentication
Autoenroll Client	Members of this group receive a certificate with the
Authentication Certificate	purpose of client authentication
Wired Computers VLAN 10	Members of this group are placed into VLAN 10
Wired Computers VLAN 20	Members of this group are placed into VLAN 20

#### **Appendix B: Switch Configuration**

```
sh run
Building configuration...
Current configuration : 3581 bytes
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
1
hostname addevsw01
boot-start-marker
boot-end-marker
T
username cisco password 0 cisco
aaa new-model
T
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa session-id common
system mtu routing 1500
ip routing
ip domain-name addev.local
1
crypto pki trustpoint TP-self-signed-1081864448
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1081864448
 revocation-check none
 rsakeypair TP-self-signed-1081864448
I.
I
crypto pki certificate chain TP-self-signed-1081864448
 certificate self-signed 01
  3082024D 308201B6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31303831 38363434 3438301E 170D3933 30333031 30303031
  30315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 30383138
  36343434 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100BF82 23C594F7 C1F04979 E31E819E CFA7B323 F1D827C3 64211110 15FD804F
  9DC25434 E0E63342 95253F16 5A721C51 EAA30216 8B8320A7 C7573A55 684B9F77
  42CB097A 3F8C2A13 21B0C676 51C7B00C C5D781EF 03AA038E BC3E8946 7AE41C17
  9F3A6698 2921AE8F D2C84E5F 8D436AEC 8046208A DB718804 5061306E 921D0A44
  4D0F0203 010001A3 75307330 0F060355 1D130101 FF040530 030101FF 30200603
  551D1104 19301782 15616464 65767377 30312E61 64646576 2E6C6F63 616C301F
```

```
0603551D 23041830 1680149F 143D56F9 389C6F81 F05B0DAE 8B693799 98893530
  1D060355 1D0E0416 04149F14 3D56F938 9C6F81F0 5B0DAE8B 69379998 8935300D
  06092A86 4886F70D 01010405 00038181 00851ACE F2C9718D 5DBA2B67 DF48378D
 704D9DCD 2D6D49FF F3321FA1 42901F2A CFD3B18D 13064E95 B116D74C E943DA73
  53741A11 5FC49F57 4D566F5E A838163D 6408D122 F3A8FE7F D99F6422 AA67F077
  25E8D40D 54915FEA 16309073 79A433C7 B45C2E08 B30198F3 83784498 0788ACFD
  1F67D8B0 C537D680 744EAFD0 FBF60449 AD
      quit
dot1x system-auth-control
I.
T
T
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip ssh version 2
I
T
interface FastEthernet0/1
switchport access vlan 5
switchport mode access
1
interface FastEthernet0/2
switchport mode access
authentication event fail action authorize vlan 99
authentication event no-response action authorize vlan 100
authentication port-control auto
authentication periodic
authentication timer reauthenticate 60
dot1x pae authenticator
1
interface FastEthernet0/3
1
interface FastEthernet0/4
!
interface FastEthernet0/5
1
interface FastEthernet0/6
1
interface FastEthernet0/7
1
interface FastEthernet0/8
!
interface GigabitEthernet0/1
1
interface Vlan1
no ip address
1
interface Vlan5
ip address 10.32.5.254 255.255.255.0
1
interface Vlan10
ip address 10.32.10.254 255.255.255.0
 ip helper-address 10.32.5.15
```

T

```
interface Vlan99
 ip address 10.32.99.254 255.255.2
 ip helper-address 10.32.5.15
Т
interface Vlan100
 ip address 10.32.100.254 255.255.2
ip helper-address 10.32.5.15
1
ip http server
ip http secure-server
1
1
logging esm config
access-list 101 deny tcp any host 10.32.5.3 eq www
access-list 101 permit ip any any
I.
radius server addevdc01
address ipv4 10.32.5.15 auth-port 1812 acct-port 1813
key accessdenied
!
!
!
Т
line con 0
line vty 0 4
password cisco
transport input ssh
line vty 5 15
password cisco
transport input ssh
!
end
addevsw01#
```