Global Information Assurance Certification Paper

Implementing IEEE 802.1x for Wired Networks

GIAC (GCWN) Gold Certification

Author: Johan Loos, johan@accessdenied.be
Advisor: Rodney Caudle

Accepted: TBD
(Date your final draft is accepted by your advisor)

Abstract

Without an extra layer of security, hosts can access resources on the wired network without any form of authentication. Basically there is no way to know who is accessing the wired network infrastructure. To manage this type of connections, IEEE 802.1x port based authentication can be implemented to force wired clients to authenticate. Without proper access to the wired network, malicious users can use the network to access company's data or launch attacks to servers or client computers on the wired network.

1. Introduction

Most companies do not have an extra of security layer in place when client computers are connecting to a wired network. Most of the time, when a client computer connects to the network, the client computer receives an IP address from a DHCP server. At this point, these client computers are not identified or authenticated on the wired network and can launch attacks based on the hacker's knowledge. With the introduction of wireless networks, IEEE 802.1x becomes more popular certainly in enterprise based wireless networks. IEEE 802.1x was implemented on most wireless networks with the goal to have all wireless client computer on the network authenticated and identified. But still, protection of wired networks is left behind (Cisco, 2011).

The goal of this paper is to describe the advantage of an IEEE 802.1x implementation and how it can be used to authenticate client computers on the wired network (Cisco, 2010). At the beginning, the wired client computer does not have an IP address and is not able to connect to network resources. At this point, the client computer can only 'talk' with the switch and no further communication is possible. When the client computer receives an IP address after successful authentication, the client computer can communicate with network resources. But what happens with guest computers? Are these client computers able to connect to the wired network? Well, for most companies, this is not allowed by the company security policy. Because a guest computer is not a managed computer from the company and this guest computer is not allowed to access the resources on the internal network. But help is on the way, guest computers can be placed into a separate network so that only internet access for example is allowed. The technology used to place guest computers in separate networks are Virtual LANs (VLANs). Depends on the design of the internal network, networks can be segmented and inspected as necessary (Cisco, 2007).

Client computers can be authenticated using a password or a certificate. Password based authentication is the easiest form of authentication and can be implemented on client computers which are managed by the organization. Password based authentication can also be used on guest computers.

Johan@accessdenied.be

When a managed client computer connects to the network, the client computer uses the credentials based on the credentials the client computer (in case of computer authentication) got from the domain controller or the credentials received from a domain administrator (in case of user authentication). If a guest computer connects to the network, the user is prompted to enter the proper credentials before authentication can takes place (Microsoft, 2008).

The most secure form of IEEE 802.1x authentication is certificated based authentication. Using this type of authentication, every client computer must have a certificate to proof its identity (University of Oslo, 2011).

It is recommended that the organization installs a Public Key Infrastructure (PKI) to deploy certificates if not already in place (Microsoft, 2013). Certificates can be automatically deployed to client computers with any input of the end user.

2. IEEE 802.1x Authentication

IEEE 802.1x can be used to restrict unauthorized devices from connecting to the company's network. There are three components used is the authentication process. These components are the supplicant, the authentication server and the authenticator (Cisco, 2010).

The supplicant is basically the wired client computer. This can be a managed computer or a guest computer. In the initial phase (before authentication), the client computer can only 'talk' with the switch. The protocol used for communication between the wired client and the switch is EAP (Extensible Authentication Protocol) over LAN (EAPoLAN) (Cisco, 2011). For communication over wireless networks, client computers use the protocol EAP over Wireless (EAPoWLAN).

The Authentication Server is typically a RADIUS server. In this paper a Microsoft Network Policy Server (NPS) is used and configured to perform RADIUS authentication (Microsoft, 2008). The goal of the RADIUS server is to authenticate a wired client computer based on a certain condition. For example: if the client computer is a member of a specific security group in Active Directory, the client computer can be placed into a specific VLAN.

Johan@accessdenied.be

The authenticator is typically a switch or a wireless access point. The task of the authenticator is to forward authentication traffic from an un-authorized client computer to the RADIUS server. Before authentication of the wired client is successful, the authenticator communicates with the client computer using EAP. The authenticator then communicates using the IP protocol or RADIUS messages with the RADIUS server. After successful authentication of the client computer, communication can take place normally, which means IP.

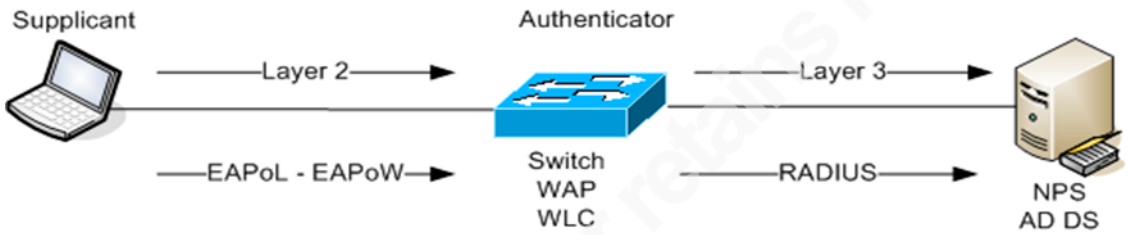


Figure 1: Overview of the IEEE 802.1x components used on a network

Authentication can takes places by either using a certificate or by using a password. If certificate based authentication is used, Group Policy (Microsoft, 2012) from Active Directory can be used to deploy a certificate to the client computer. This is called auto-enrollment (Microsoft, 2013). This basically means that when the client computer starts, a Group Policy is executed on the client computer and the certificate is automatically installed into the local certificate store (Microsoft, 2011).

It doesn't matter if the certificate becomes corrupted or lost. There must be a process in the organization that managed client computers can receive a certificate easily. Certificate enrollment can be part of the computer imaging process, but the client computer must first connect to an unsecured switch port to receive the information from Group Policy. If there is a staging area available, this network is also separated from the internal network and can indeed be used.

The RADIUS server does also needs a certificate. This certificate is used to proof the identity of the RADIUS server to the client computer and to create a secure tunnel if Protected Extensible Authentication Protocol (PEAP) is being used. When first a secure tunnel is created between the client computer and the RADIUS server, the PEAP tunnel ensures that all authentication traffic is encrypted. The recommendation is to use PEAP in

the wired authentication process to encrypt further authentication traffic even if password or certificate based authentication is being used.

If password based authentication is used, client computers don't need a certificate but only the RADIUS server needs one. User or computer credentials can be used to authenticate a client computer on the network. This is the same username and password combination from the Active Directory domain which the user uses to logon to the domain.

2.1.1. IEEE 802.1x Requirements

Depending on the authentication method used as mentioned above, the network needs to have the following components installed.

- One or more 802.1x capable switches which are compatible with RADIUS. The switches used on the network must be able to support IEEE 802.1x and must be able to communicate with a RADIUS server. Verify the currently installed flash image on the switch to verify this functionality.

- Active Directory Domain Services for user and group management (Microsoft, 2000). Used to create the appropriate users and groups which can be used to place a client computer into a VLAN. A separate domain for authentication is not needed; this can be easily integrated into an existing infrastructure.

- Active Directory Certificate Services for certificate management. Used to create certificates for client computers and/or the RADIUS server. The recommended design for a Public Key Infrastructure (PKI) is a two-tier design. This means a Root Certification Authority (Microsoft, 2013) and a Subordinate Certification Authority (Microsoft, 2013). The task of the Subordinate CA is to create certificates which are generated for users and computers. The setup will work with only a Root CA, but is not a best practice.

- Network Policy Server to provide authentication, authorization and accounting (Microsoft, 2012). The Network Policy Server plays the role of RADIUS and is used to authenticate users or computers based on their supplied credentials. The RADIUS server contacts the Active Directory Domain Controller to verify the

credentials. The RADIUS server can also be configured with RADIUS attributes, so that the switch can be configured based on the supplied attributes by the RADIUS server.

2.2. Authentication Process

In normal daily operations, when the client computer uses the password or a certificate of the client computer and these are valid, IEEE 802.1x authentication will be successful and the client computer is granted access to the network (Cisco, 2010).

But what is the client computer is not able to send to correct credentials to perform IEEE 802.1x authentication? In that case the following possibilities exist. The first option is that the IEEE 802.1x client is not enabled on the client computer. This basically means that the client computer is not able to send or receive an authentication request and will be placed into a separate VLAN. The second option is that the certificate on the client computer is not valid (e.g. certificate is expired). This means that authentication still fails and the client computer will be placed into a separate VLAN.

Are client computers placed into the same VLAN when either the certificate is not valid or the IEEE 802.1x client is not enabled? It depends on how the switch is configured and which VLAN is used for which purpose. It is important to know why the authentication is failing. If a managed client computer fails authentication, the client computer probably needs a new certificate, but when a guest client computer fails authentication, the client does not need to access the network servers to request a new certificate. So, the recommend solution is to separate these two VLANs. Based on the vendor of the switch, restricted VLANs and Guest VLANs can be configured for this purpose (Cisco, 2007).

Additionally, a failback authentication method can also be used as a solution by using only the MAC address of the client computer. This can be useful because network printers does not support IEEE 802.1x authentication. But again, it depends on the vendor of the printer. These days, most network cards which can be placed into a printer support this feature. But anyway, when the printer does not support IEEE 802.1x authentication, the device can be authenticated using its MAC address. This is not a bulletproof solution, since a malicious user can easily obtain the MAC address of the printer (by printing a test configuration page). If the malicious user is able to configure the machine with the MAC

address of the printer, this user can gain access to the network. MAC authentication is called MAC Authentication Bypass (MAB) and if enabled on the switch, is active when all other IEEE 802.1x authentication methods fail (Cisco, 2010).

2.3. User and Computer Authentication

Authentication can be performed for a user, computer or both and supplicants can be authenticated via a certificate or a password (Cisco, 2011). If certificate based authentication is used, the client computer must have a valid computer certificate with the purpose of client authentication (Microsoft, 2008).

2.3.1. EAP-TLS

EAP-TLS is a certificate based authentication protocol (Microsoft, 2008) and requires client-side and server-side certificates to perform mutual authentication. A client-side certificate is a certificate stored in the local certificate store on the client computer, and a server-side certificate is a certificate dedicated and stored in the local certificate store on the RADIUS server (Cisco, 2011).

When the client computer starts and tries to authenticate, the RADIUS server sends a computer certificate to the client computer. The client computer checks the validity of the certificate by first checking the Certificate Revocation List (CRL) to see if the certificate is not revoked. The next step is to verify if the name of the RADIUS server is the same as the name in the certificate. This process is needed to be sure that the certificate of the RADIUS server is not spoofed.

The client computer sends a certificate to the RADIUS server for authentication and the RADIUS server will also check the validity of the client certificate.

If both certificates are valid, authentication can be performed, otherwise authentication can fail.

2.3.2. EAP-MSCHAPv2

EAP-MSCHAPv2 is a password based authentication protocol and requires that the authentication server has a certificate and is presented to the supplicant (Microsoft, 2008).

Johan@accessdenied.be

The supplicant must have the whole certificate chain available in its local certificate store. This basically means that the client computer must have a certificate of the Root CA and the certificate of the Sub CA. This is automatically done when the client computer is a member of the domain; because these certificates are deployed automatically via group policy to client computers (Microsoft, 2012). This is not the case for guest computers. Before the validity of the RADIUS server certificate can be checked, the guest computer needs also the certificate chain and needs to be installed manually.

2.3.3. PEAP-EAP-TLS or PEAP-EAP-MSCHAPv2

PEAP creates a secure tunnel between the authentication server and the supplicant (Microsoft, 2008). This tunnel is created using the certificate of the authentication server which the authentications server sends to the supplicant in the beginning of the authentication process. Within this secure tunnel, a new EAP negotiation takes place to authenticate the client computer.

EAP-MSCHAPv2 authentication is based on a password, so this type of authentication is susceptible to a dictionary attack. To protect the password send over the network, PEAP can be implemented to create a secure tunnel (Cisco, 2011).

Otherwise, if the malicious user is able to grab the password hash of the user account, the malicious user is able to launch some Pass-the-Hash attacks (Microsoft Security Intelligence Report, 2013) to gain access to internal network resources without any form of authentication.

2.4. Understanding Switchports

When IEEE 802.1x is configured on the switch, a switch port needs to be configured what will happen when authentication is successful or not (Cisco, 2010).

Depending on the vendor of the switch, a switch port can be placed into what's called unauthorized state. This means that the switch port does not allow traffic to pass and no connection is possible. This situation happens when authentication fails.

A switch port in authorized state means that the client computer is successfully authenticated and the switch port is enabled to allow traffic to pass. The LED color above

the switch port will also change. It will be amber for unauthorized state and becomes green for authorized state.

2.5. Understanding VLAN Assignment

Traffic from client computers can be limited by passing the correct RADIUS attributes to the switch. This allows that client computers which are member of a certain security group can be placed into a specific Virtual LAN (VLAN). For example: when a client computer is a member of the security group Client Computer VLAN 10, the VLAN attribute (Tunnel-Private-Group-ID) with the value of 10 can be passed from the RADIUS server to the switch. At this point, when the switch receives this attribute, the switch port will be placed into the supplied VLAN number. The VLANs has to be created in front on the switch.

The most interesting RADIUS attributes needed for VLAN assignment are listed in the following table. These attributes needs to be configured in the Network Policy on the RADIUS server (Cisco, 2010).

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

2.6. Understanding the Guest VLAN

The Guest VLAN is used to provide limited access to client computers. If guest computers connects to the network and the authentication process fails, the guest client computer is placed into the Guest VLAN. This VLAN has limited or no access to resources on the internal network. For example: a guest VLAN can be used to provide only internet access to visitors (Cisco, 2010).

If a client computer is not enabled for IEEE 802.1x, authentication cannot be performed and the client computer will be placed into the guest VLAN. For example: the client computer uses an operating system that does not have an IEEE 802.1x client enabled or configured. Microsoft Windows operating system has an IEEE 802.1x client

by default, but it is not enabled. The IEEE 802.1x client can be enabled on the client by starting the Wired Autoconfig Service.

2.7. Understanding the Restricted VLAN

When a client computer is enabled, and configured for IEEE 802.1x , and the authentication process fails, the client computer is placed into a restricted VLAN (Cisco, 2010).

A reason why the authentication fails is that the certificate is not valid anymore on the client computer. This can happen when the client computer was not able to renew his certificate within the lifetime period of the certificate or the certificate on the client computer is corrupted. For this reason, there must be a process in place that the client computer is able to receive a new or updated certificate. For example: a restricted VLAN is used for managed client computer who needs to receive an update.

2.8. IP Address Assignment

After successful authentication, the client computer needs to receive an IP address before further communication can takes place. The client computer can receive an IP address from a DHCP server available on the network or from a DHCP server configured on the switch. In this paper, a Microsoft DHCP Server (Microsoft, 2005) is used and the necessary scopes (Microsoft, 2005) are created for each VLAN from which the client computer receives an IP address.

This means if the authentication is successful on the client computer, the client receives an IP address from the internal network range. Using the scope from this paper, the client computer receives an IP address from the network range 10.32.10.0/24. When authentication fails, the client computer receives an IP address from the network range 10.32.99.0/24 or 10.32.100.0/24.

3. Configuration Guide

The configuration guide of the switch and Network Policy Server can be found in Appendix A of this paper.

Johan@accessdenied.be

4. Conclusion

The implementation of IEEE 802.1x authentication is not easy but can be an interesting challenge. Knowledge on different platforms is needed such as Public Key Infrastructure, RADIUS server and switch configuration. Support personal need to be trained into troubleshooting processes. Because if its goes wrong it can be on different components in the authentication process (e.g. certificate expired on either the client of RADIUS server, RADIUS server not available during the time of authentication, IEEE 802.1x client not enabled, etc). To make this troubleshooting process easier, syslog messages generated on the switch can be send to a syslog server. The state of the switch port, why authentication fails, and the VLAN information per switch port are all available into one central place.

After successful implementation, IEEE 802.1x port based authentication can help as an extra layer of security. Remember that the goal is to secure the local area network and by using this technology. This extra layer of security can be part of the defense-in-depth strategy that the organization might have (Microsoft, 2000). All client computers are authenticated and identified and can only access the network after successful authentication. If authentication fails, client computers can be placed automatically into a restricted or guest VLAN to avoid further connection. At this point, only managed client computers are able to access internal network resources and can help to keep malicious users away.

5. References

Configuring IEEE 802.1x Port-Based Authentication, Cisco (2010): http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/sw8021x.html

Wired IEEE 802.1x Deployment Guide, Cisco (2011): http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/Dot1X_Deployment/Dot1x_Dep_Guide.html

Configuring InterVLAN Routing with Catalyst 3560 Series Switches, Cisco (2012):

Johan@accessdenied.be

http://www.cisco.com/en/US/tech/tk389/tk815/technologies_configuration_example09186a008015f17a.shtml

Creating Ethernet VLANs on Catalyst Switches, Cisco (2007):
http://www.cisco.com/en/US/tech/tk389/tk689/technologies_configuration_example09186a008009478e.shtml

Configuring Interfaces, Cisco (2010):
http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_52_se/configuration/guide/swint.html

Configuring Active Directory Certificate Services, Microsoft (2013):
http://technet.microsoft.com/en-us/library/cc772393(v=ws.10).aspx

Configure Certificate auto-Enrollment, Microsoft (2013):
http://technet.microsoft.com/en-us/library/cc731522.aspx

Display Certificate Stores, Microsoft (2011):
http://technet.microsoft.com/en-us/library/cc725751.aspx

Configuring Active Directory Domain Services, Microsoft (2009):
http://technet.microsoft.com/en-us/library/cc755103(v=ws.10).aspx

User and Group Management in Active Directory (2000):
http://technet.microsoft.com/en-us/library/bb727067.aspx

Configuring a DHCP Server, Microsoft (2005):
http://technet.microsoft.com/en-us/library/cc756865(v=ws.10).aspx

Create and Edit a Group Policy Object, Microsoft (2012):
http://technet.microsoft.com/en-us/library/cc754740.aspx

Network Policy Server, Microsoft (2012):
http://technet.microsoft.com/en-us/library/cc732912.aspx

Configuring Network Policy Server, Microsoft (2008):
http://technet.microsoft.com/en-us/library/cc732912(v=ws.10).aspx

Creating Network Policies on the RADIUS server, Microsoft (2012):
http://technet.microsoft.com/en-us/library/cc754107.aspx

Creating EAP Authentication Methods on the RADIUS server, Microsoft (2008):
http://technet.microsoft.com/en-us/library/cc731694(v=ws.10).aspx

How to configure Wired IEEE 802.1x for Windows 7, University of Oslo (2011):

Johan@accessdenied.be

http://www.uio.no/english/services/it/network/student-residential-network/instructions/win7/

Defending against Pass-the-Hash Attacks, Microsoft (2013): http://www.microsoft.com/security/sir/strategy/default.aspx#!password_hashes

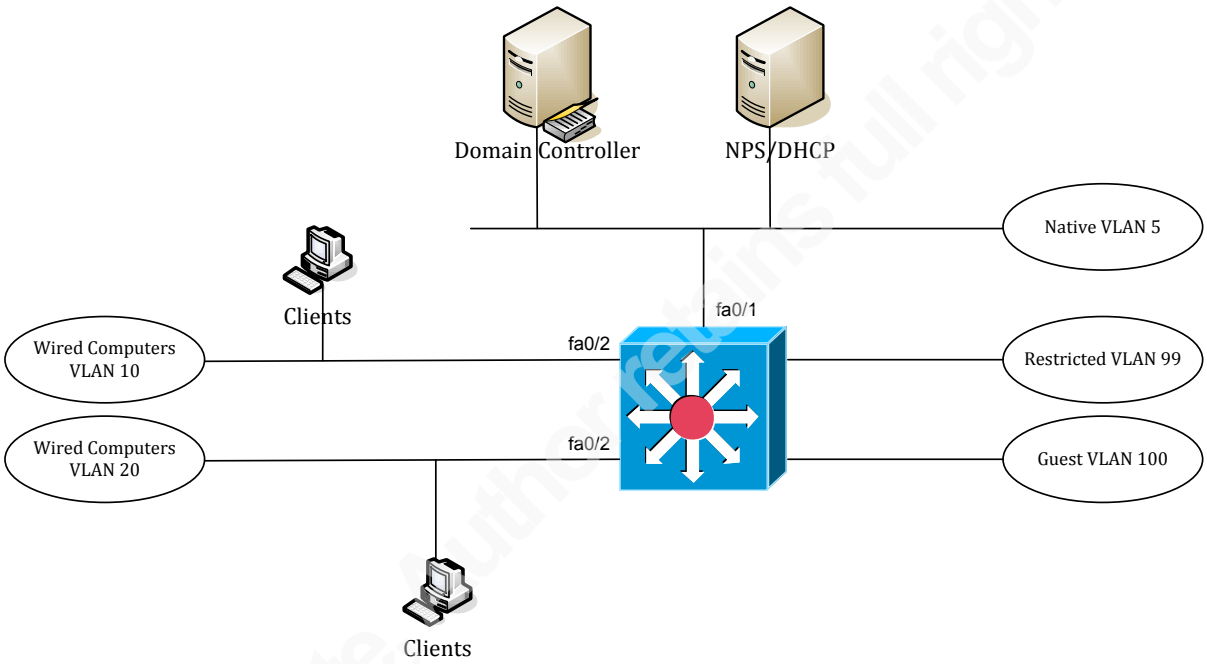
Defense in depth Overview, Microsoft (2000): http://technet.microsoft.com/en-us/library/cc767969.aspx

Johan@accessdenied.be

Appendix A

5.1. Schematic Design

Figure 2: Overview of the network diagram.



For this paper, a Cisco switch 3560 is used which also provides inter-vlan routing (Cisco, 2012). Inter-vlan routing is needed to route traffic between VLANs. This setup also works with a 2960 switch, but then a layer-3 device is needed to perform routing between VLANs. This layer-3 device can be either a router or firewall.

Table 1 List of servers used

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

The IP address of addevdc01 is 10.32.5.3. This server has the following roles installed: Domain controller, DNS Server, DHCP Server and Active directory Certificate Services.

Johan@accessdenied.be

The IP address of addevdc04 is 10.32.5.15. This server has the following role installed: Network Policy Server.

Workstation addevwks01 is configured as DHCP client.

Table 2 shows an overview of the different networks and their purpose

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

Enable routing between VLANs.

```
addevsw01(config)#ip routing
```

5.2. Creating VLANs

VLANs needed to be created in front, before the switch can place any switch port into a specific VLAN. The following commands can be used to create VLANs on the switch (Cisco, 2007).

Create VLAN 5

```
addevsw01(config)#vlan 5
```

Create VLAN 10

```
addevsw01(config)#vlan 10
```

Create VLAN 20

```
addevsw01(config)#vlan 20
```

Create VLAN 99

```
addevsw01(config)#vlan 99
```

Create VLAN 100

Johan@accessdenied.be

```
addevsw01(config)#vlan 100
```

5.3. Assigning IP addresses

Assign an IP address to a VLAN interface so that other network components can use this IP address as default gateway. An IP Helper Address is used which connect to a DHCP Server if wired client computer request for an IP address (Cisco, 2010).

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
```

5.4. Prepare the network for IEEE 802.1x Authentication

To prepare the network to support IEEE 802.1x authentication, several step can be done up front. The next step is to create Active Directory Security Groups for authorized

access and certificate enrollment. Create the following security groups in Active Directory (Microsoft, 2000).

AutoEnroll NPS Server Authentication Certificate: Members of this group receive automatically a server certificate. This certificate is used to authenticate the RADIUS server and to create the PEAP tunnel. Typically RADIUS servers will be added into this group. After creation of this security group, add computer account ADDEVDC04 as a member of this group.

AutoEnroll Client Authentication Certificate: Members of this group receive automatically a computer certificate. This certificate is used to authenticate the client computer. Typically client computers will be added into this group. After creation of this security group, add computer account ADDEVWKS01 as a member of this group.

Wired Computers VLAN 10: Members of this group will be placed in VLAN 10 when authentication is successful. After creation of this security group, add computer account ADDEVWKS01 as a member of this group.

Wired Computers VLAN 20: Members of this group will be placed in VLAN 20 when authentication is successful.

5.4.1. Configuring and Deploying IEEE 802.1x Authentication Certificates

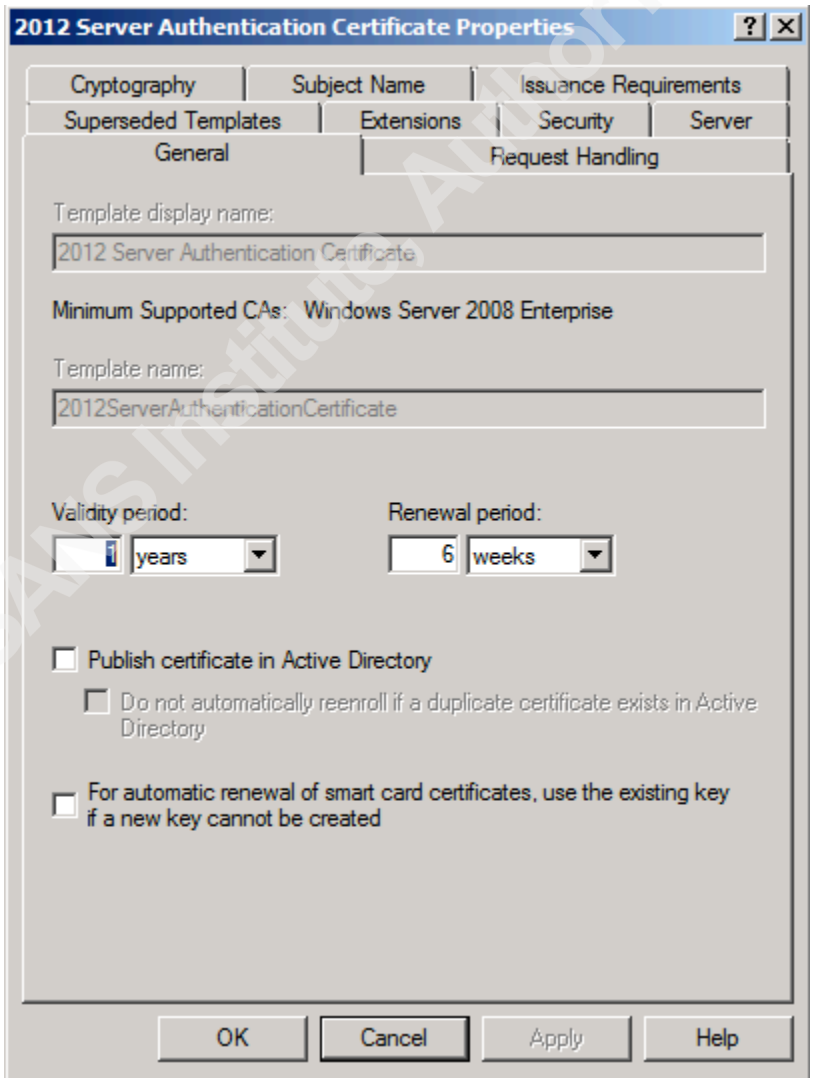
Before IEEE 802.1x authentication can be used, certificates need to be deployed to client computers and RADIUS servers. In this section, the appropriate certificate templates are created (Microsoft, 2013). The client computer sends its identity (computer certificate) to the switch, whereas the switch forwards the authentication request from the client computer to the Network Policy server.

5.4.2. Create a NPS Server Authentication Certificate

- Open **Certificate Authority** snap-in from **Administrative Tools, r**ight 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**

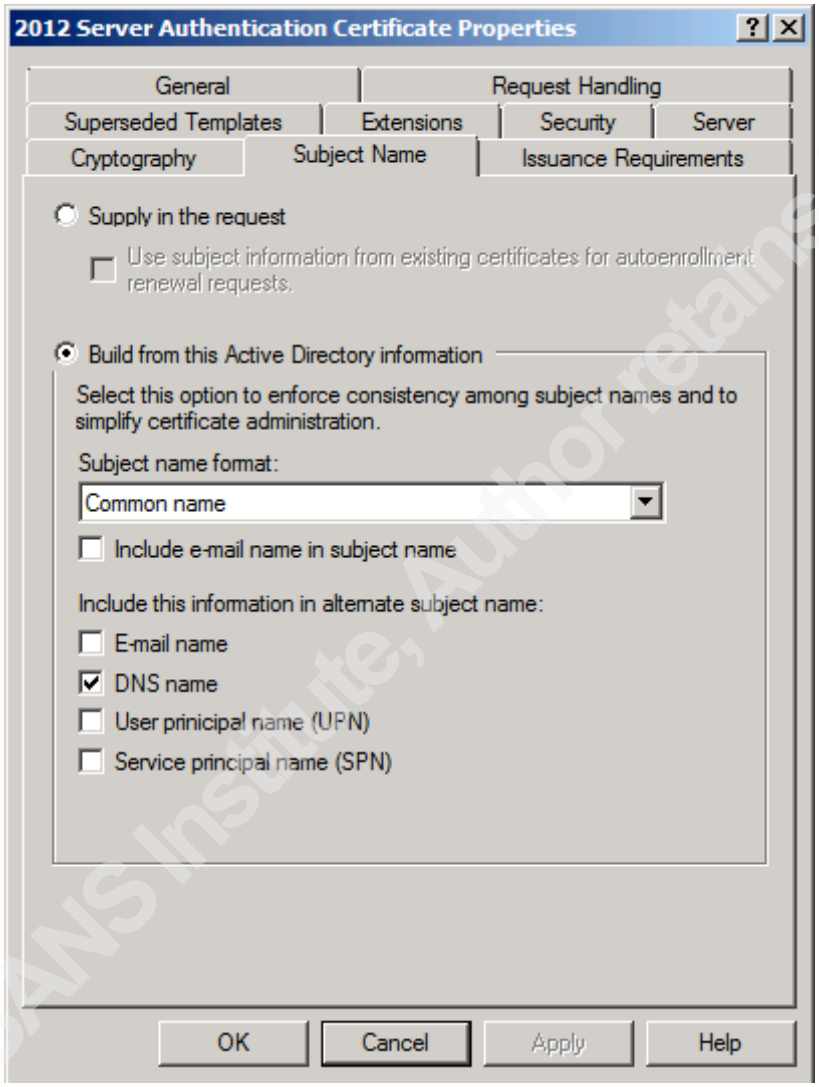
Johan@accessdenied.be

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



Johan@accessdenied.be

- 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**.



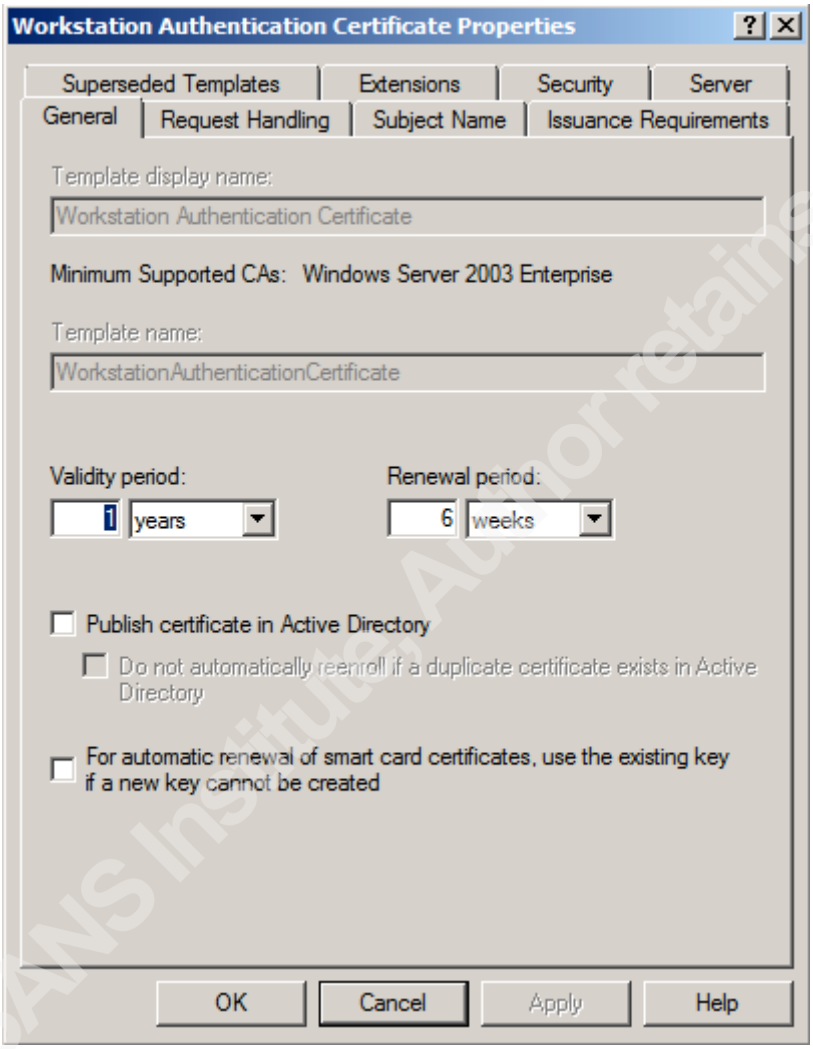
- Click on the **Security** tab, click on the **Add** button and add **AutoEnroll Server Authentication Certificate** group, assign **Enroll** and **Autoenroll** permissions and click **OK**.

5.4.3. Create a Workstation Authentication Certificate

A certificate is required to authenticate computers for IEEE 802.1x port based authentication.

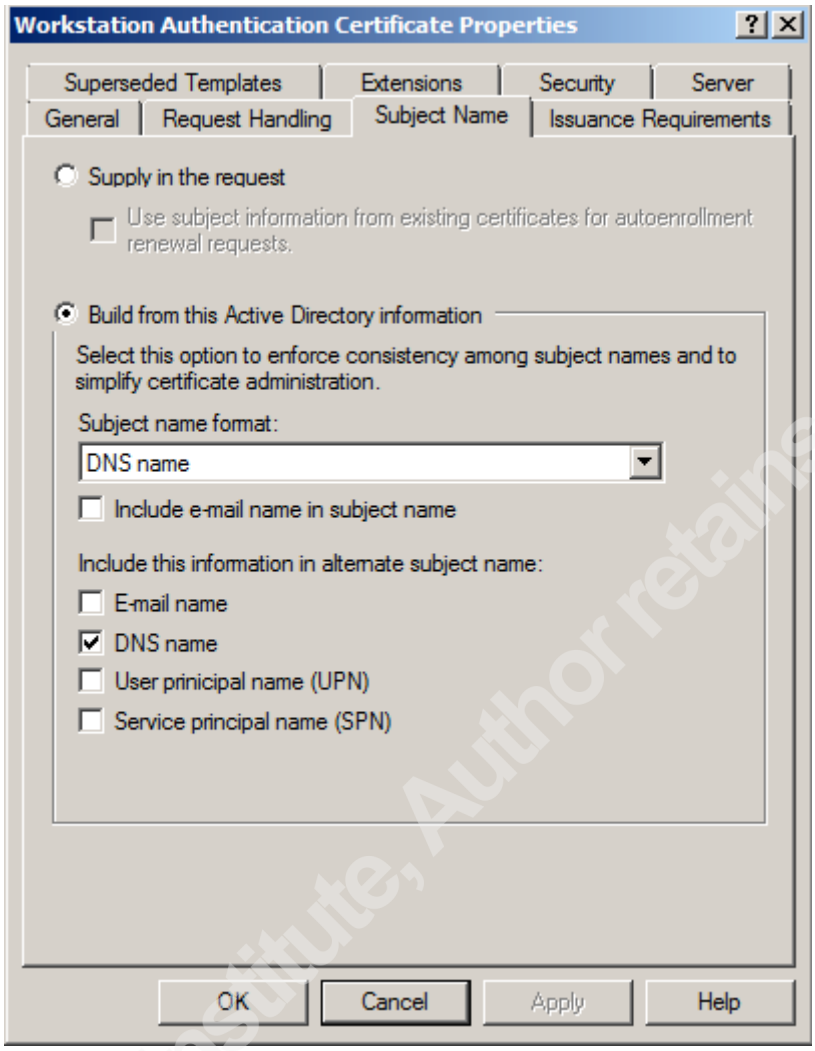
Johan@accessdenied.be

- 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.*



- 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**

Johan@accessdenied.be



- 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**

5.4.4. Adding the Certificate Templates to the Certificate Authority

After the necessary certificate templates are created, these templates needs to be added 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**.

Johan@accessdenied.be

5.4.5. Create a GPO for NPS Server and Client Certificate Enrollment

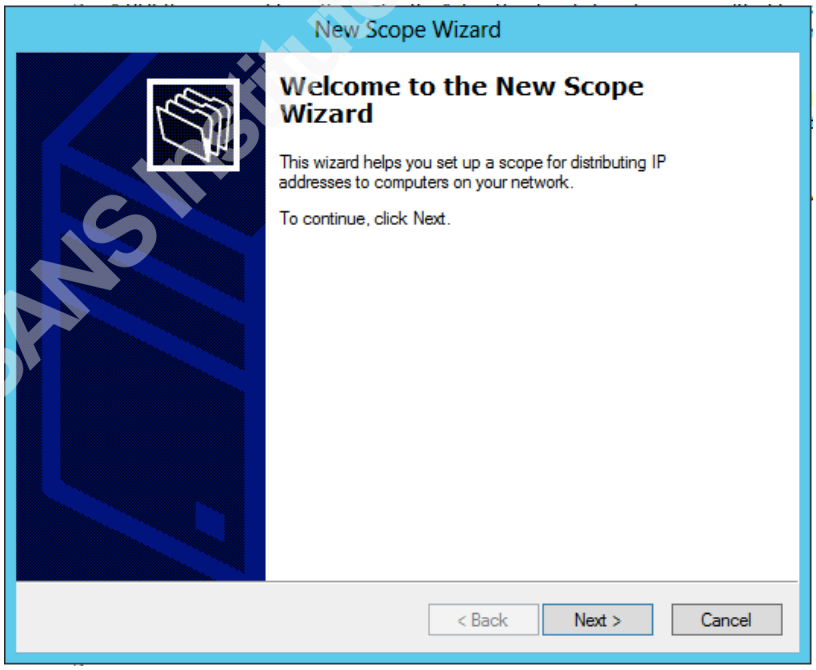
To perform automatically certificate enrollment, create a Group Policy and configure the computer configuration part for auto-enrollment (Microsoft, 2012). Link the GPO to the appropriate organization unit where the computer account resides.

5.5. Configure the DHCP Server

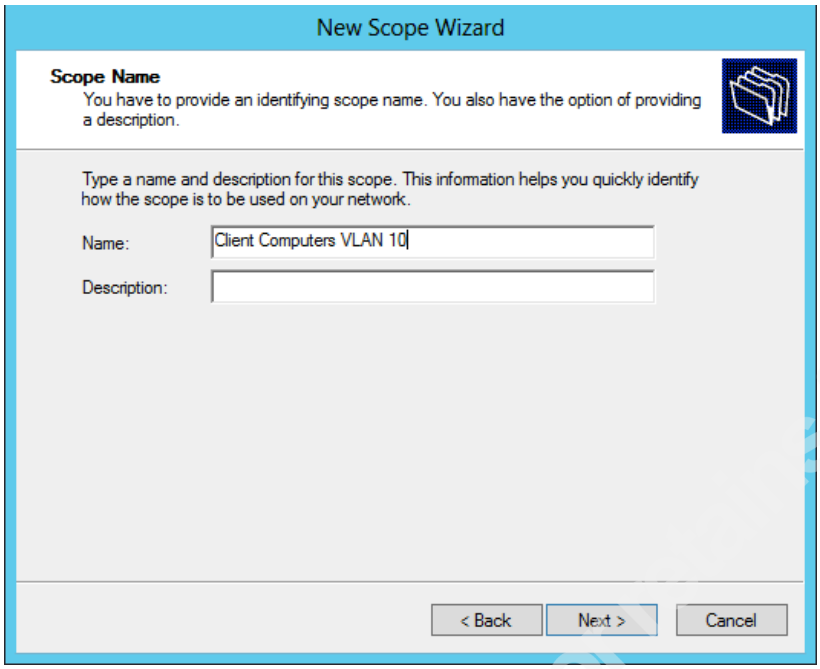
Client computers on the network receive an IP address based on the VLAN where the client is a member of. In this paper several VLAN's are used as mentioned in table 2. The goal is to create several DHCP scopes. Each scope has its range of IP addresses per VLAN. For the ease of use, only IPv4 addresses are being used (Microsoft, 2012). The following example shows how to create a scope for VLAN 10. Repeat this step to create additional scopes for VLAN 20, VLAN 99 and VLAN 100.

5.5.1. Configure DHCP Server with a scope for VLAN 10

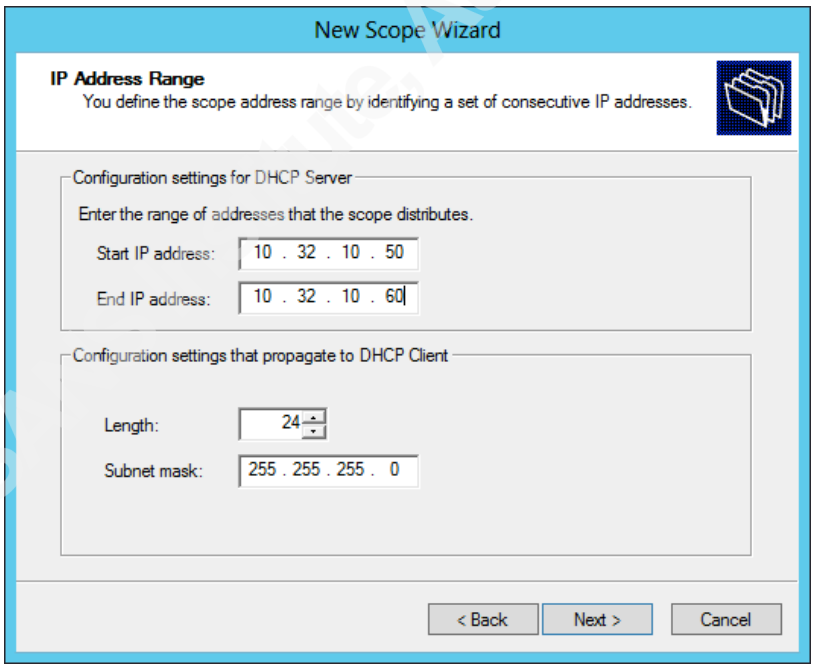
- Open **DHCP Console** from **Administrative Tools,** right click on **IPv4** and select **New Scope**
- On the **Welcome to the New Scope Wizard** page, click **Next**



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

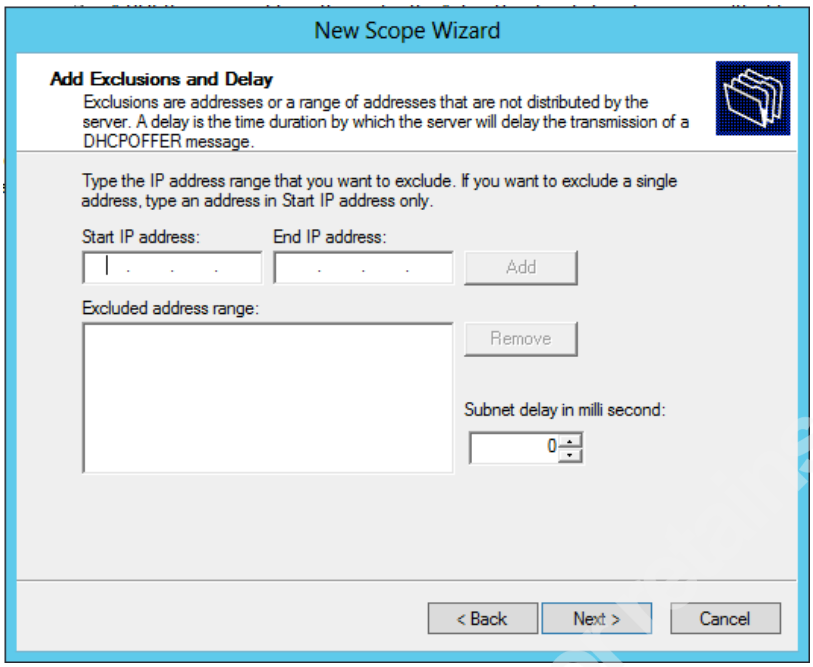


- On the **IP Address Range** page, specify Start and End IP address. Also specify the correct subnet mask and click **Next**

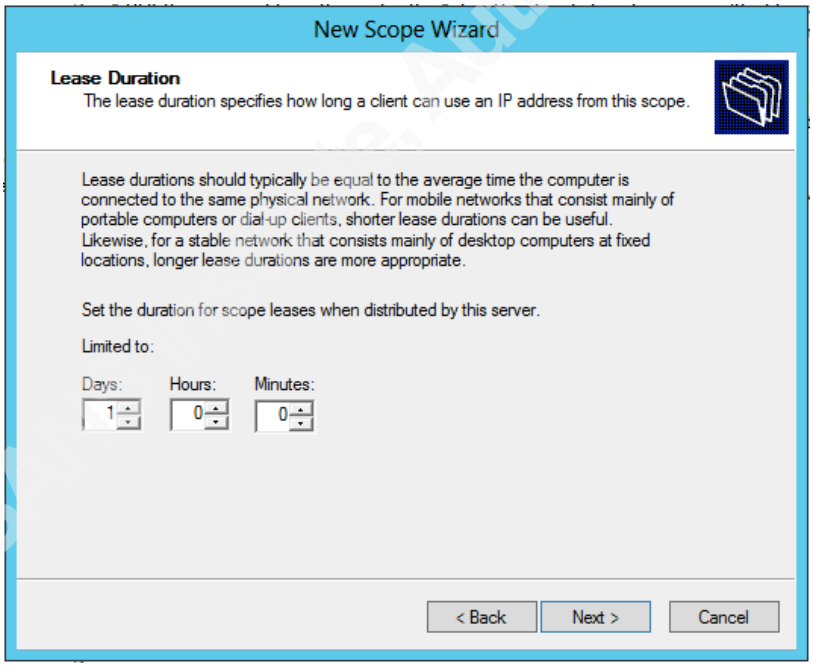


- On the **Add Exclusions** page, click **Next**

Johan@accessdenied.be

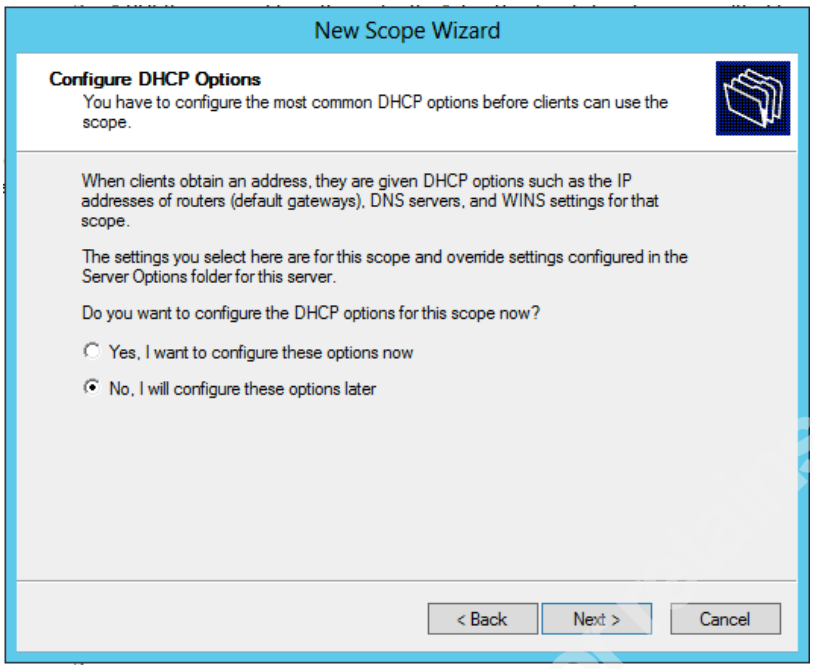


- On the **Lease Duration** page, specify a lease duration and click **Next**



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

Johan@accessdenied.be



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

5.6. Configure the Network Policy Server (RADIUS)

The task of the NPS Server is to talk with the switch to authenticate the client computers. The NPS Server will be configured as a RADIUS server, whereas the switch needs to be configured as a RADIUS client. A Connection Request Policy is created which allows a connection between the switch and the NPS server (Microsoft, 2008).

The next step is to create Network Policies where more details are configured on how the client needs to be authenticated. Client computers can be authenticated using certificate based authentication (EAP-TLS), password based authentication (PEAP-EAP-MSCHAPv2) or certificate based authentication with a secure tunnel (PEAP-EAP-TLS).

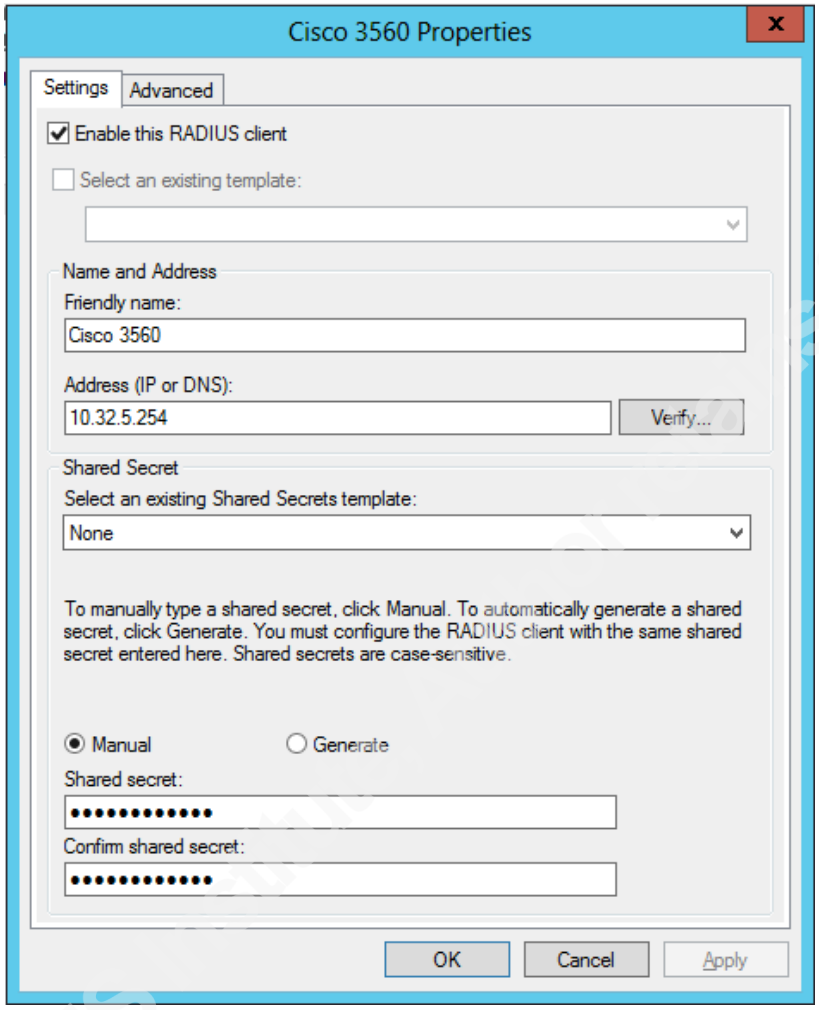
In this paper, certificate based authentication with PEAP is being used to provide to highest level of security. The following step assumes that Windows Server 2012 with the Network Policy Server role is already installed.

5.6.1. Configure RADIUS client on NPS Server

- Open **Network Policy Server** from **Administrative Tools, e**xpand RADIUS Clients and Servers, right click on **RADIUS Clients** and select **New RADIUS Client**

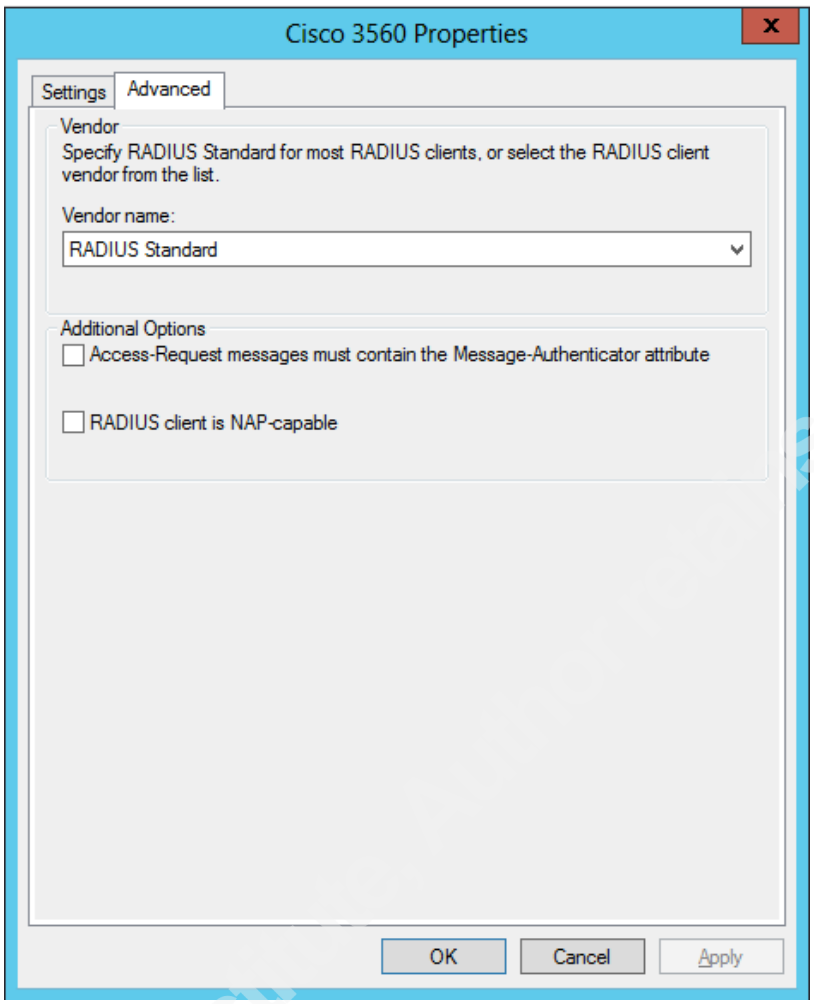
Johan@accessdenied.be

- 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**



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

Johan@accessdenied.be

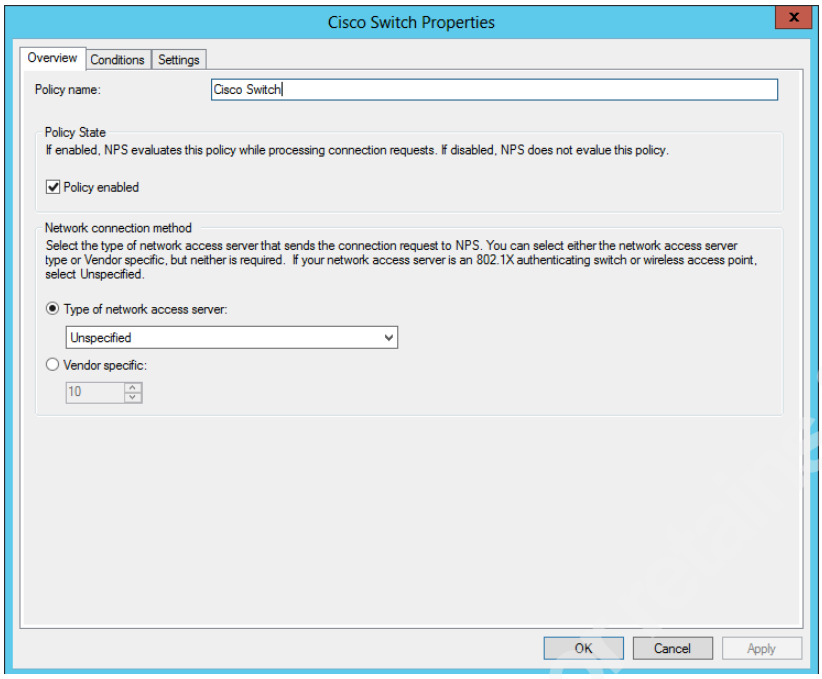


- Click **OK**

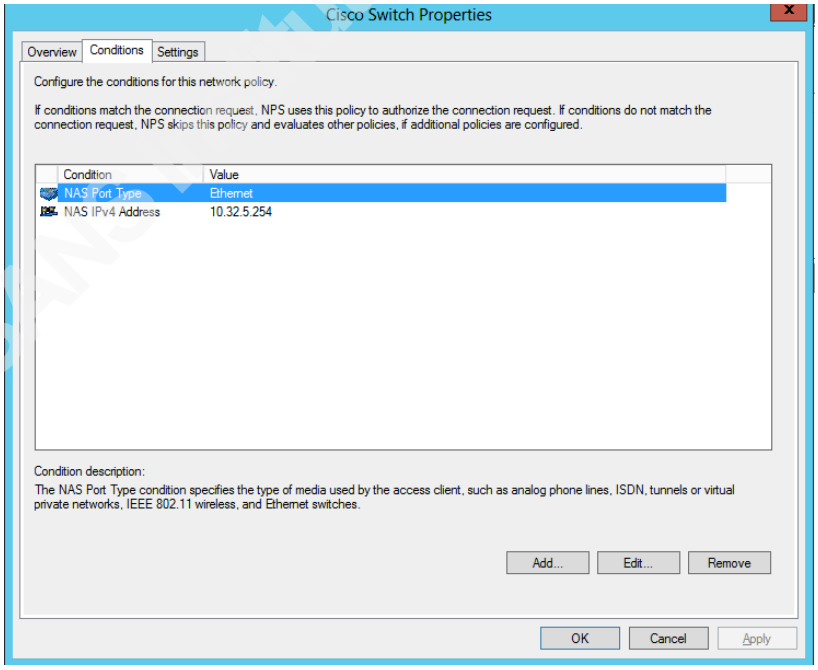
5.6.2. Configure Connection Request Policy

- 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**

Johan@accessdenied.be



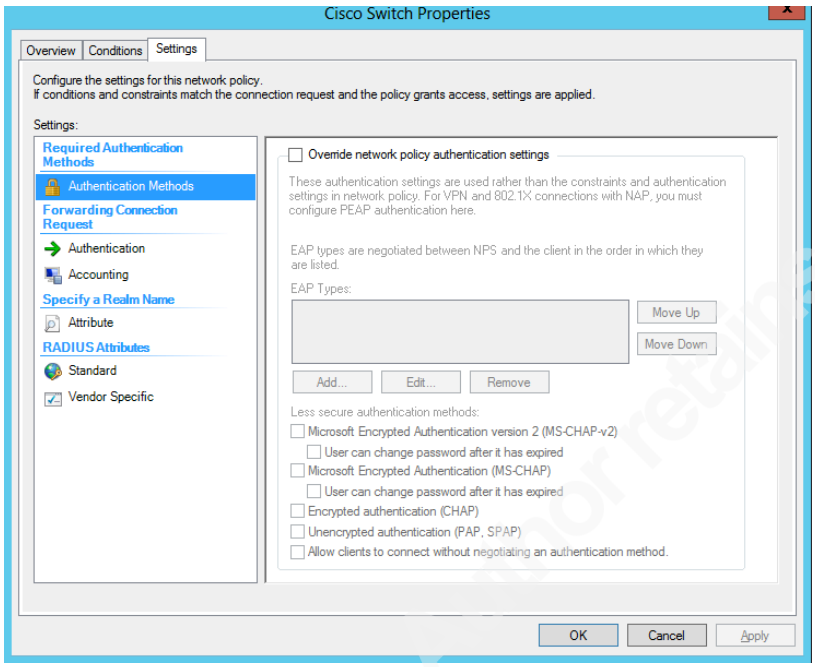
- On the **Specify Conditions** page, click **Add**. Select **NAS Port Type (Ethernet)**
- On the **Select conditions** dialog box, select **NAS IPv4 Address** and click **Add**
- On the **NAS IPv4 Address** dialog box, type the management IP address of the switch.



- Click **OK** and click **Next**

Johan@accessdenied.be

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

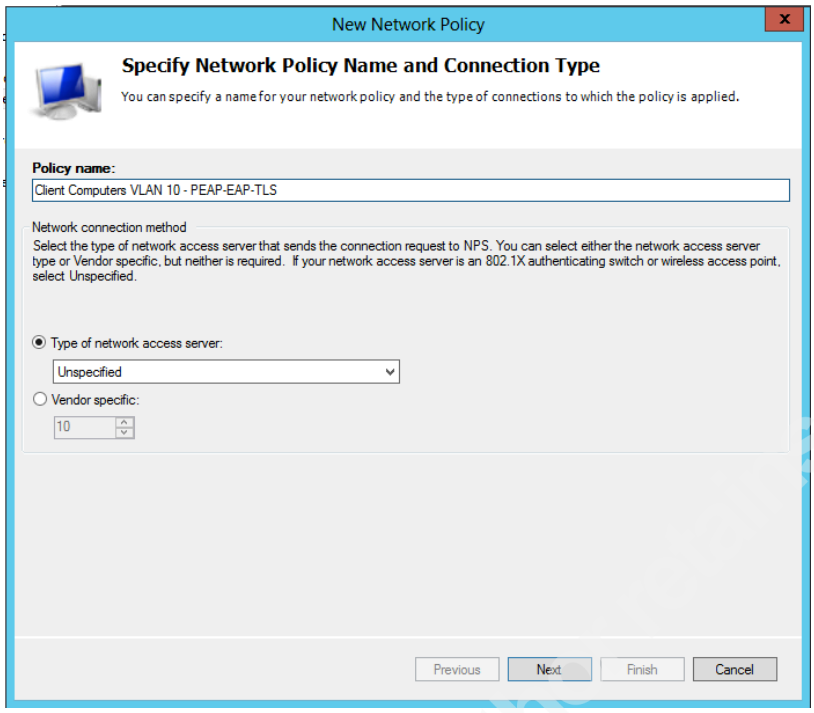


- On the **Configure Settings** page, click **Next**
- On the **Completing Connection Request Policy Wizard** page, click **Finish**

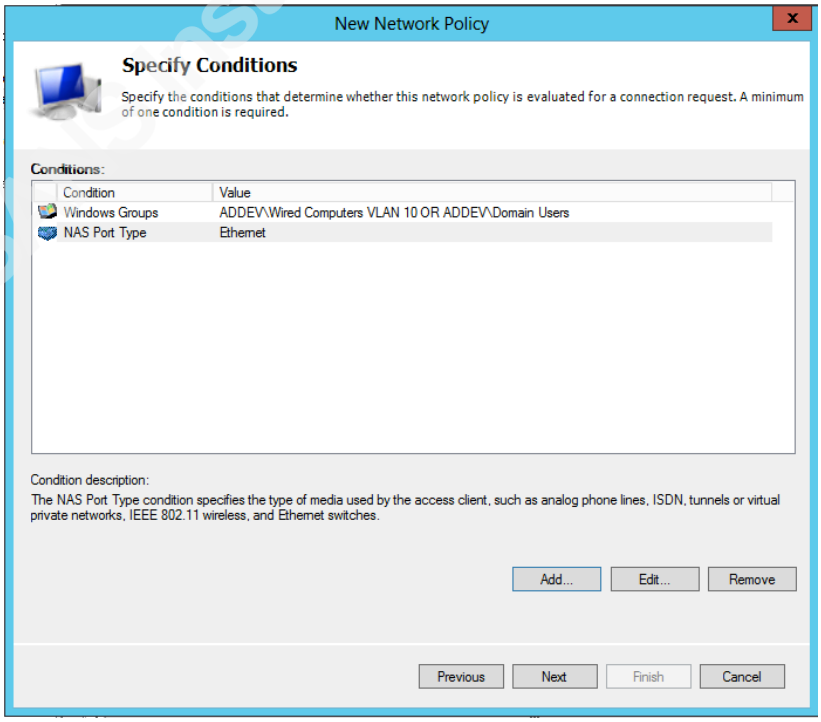
5.6.3. Configure a Network Policy for PEAP-EAP-TLS

- 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 the policy and click **Next**

Johan@accessdenied.be

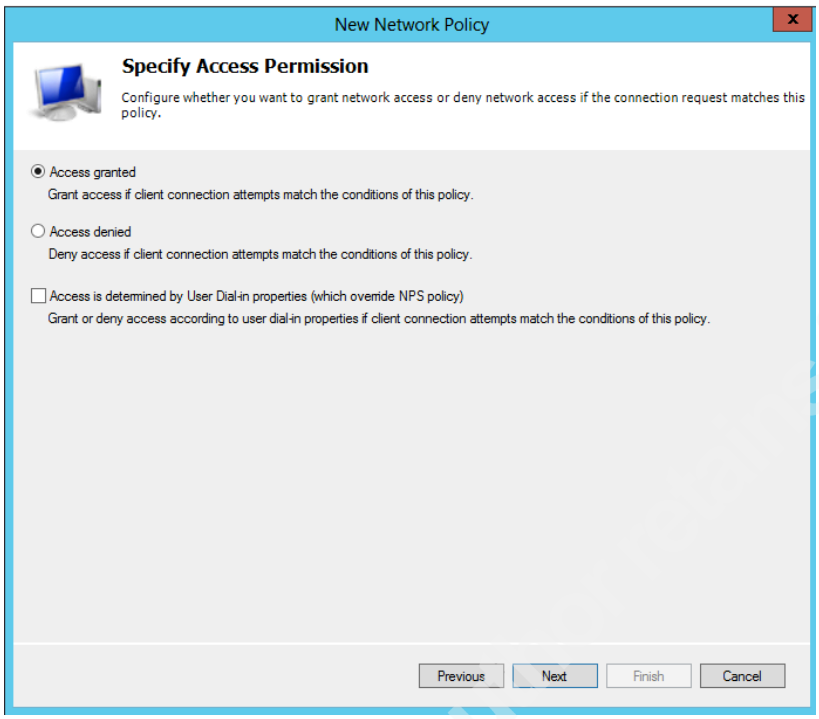


- On the **Specify Conditions** page, click **Add**
- From the **Select Conditions** dialog box, select **NAS Port Type (Ethernet)** and click **Add**
- From the **Select Condition** dialog box, add the following Windows Groups *Wired Computers VLAN 10*, *Domain Users* and click **Next**

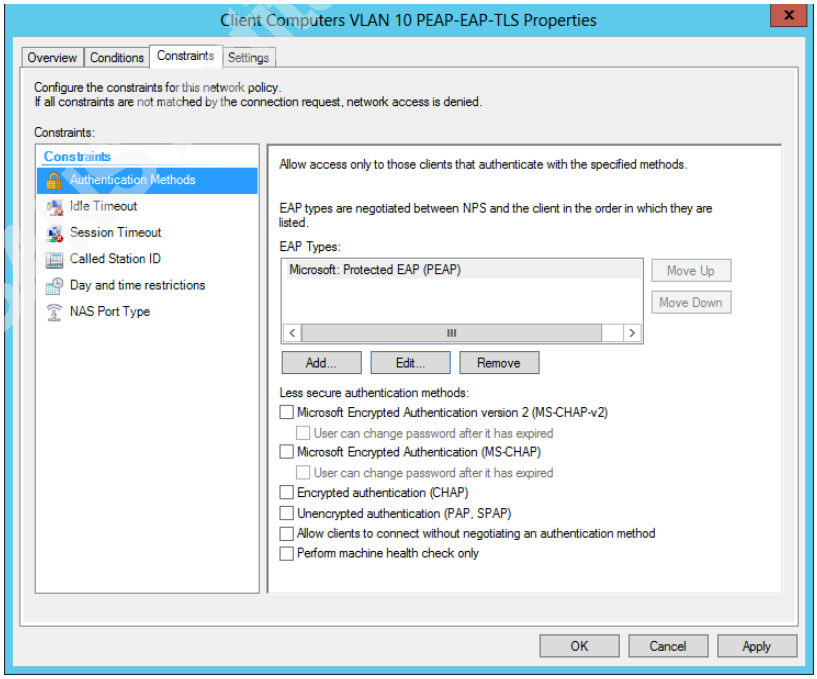


Johan@accessdenied.be

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

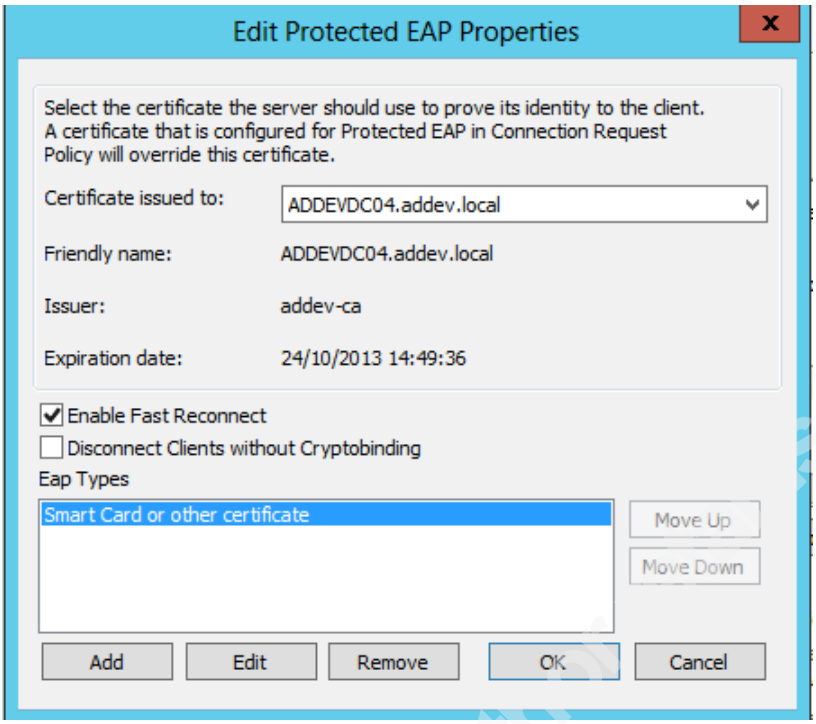


- On the **Configure Authentication Methods** page, clear MS-CHAP, clear MS-CHAP-v2 and click **Add**
- On the **Select EAP** dialog box, select **Microsoft: Protected EAP (PEAP)**

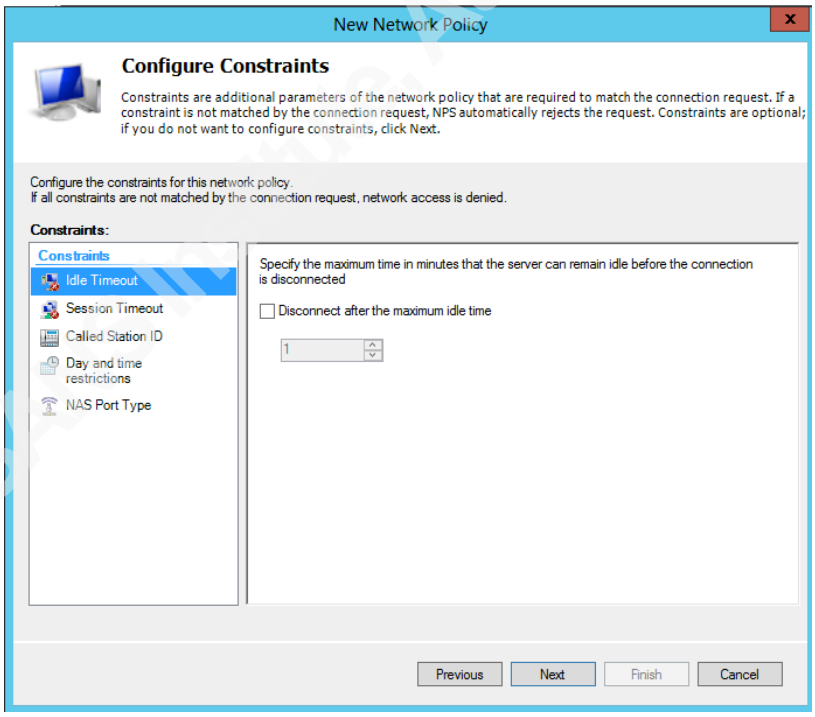


- Configure settings as below and click **OK**

Johan@accessdenied.be

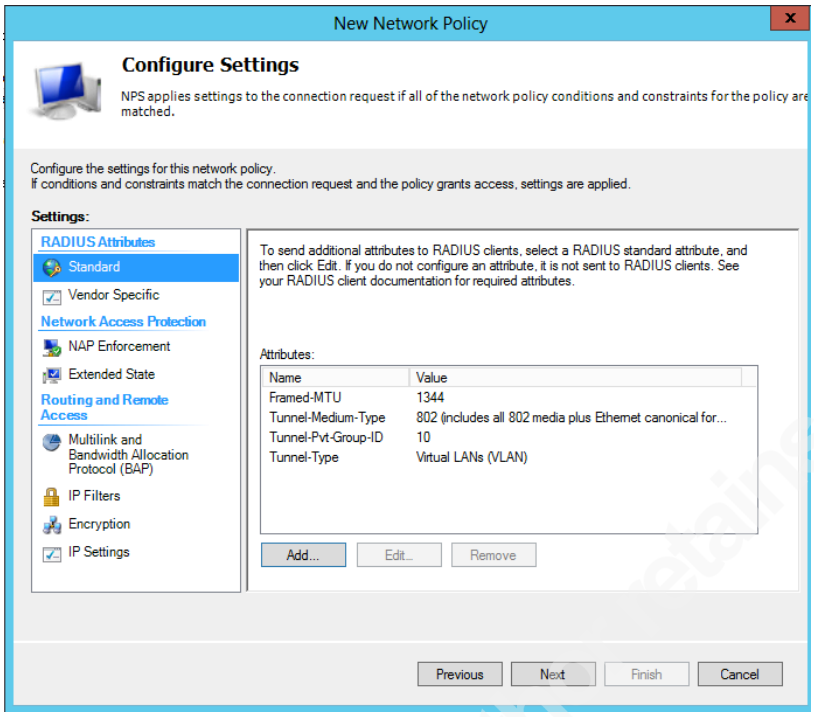


- On the **Configure Constraints** page, click **Next**

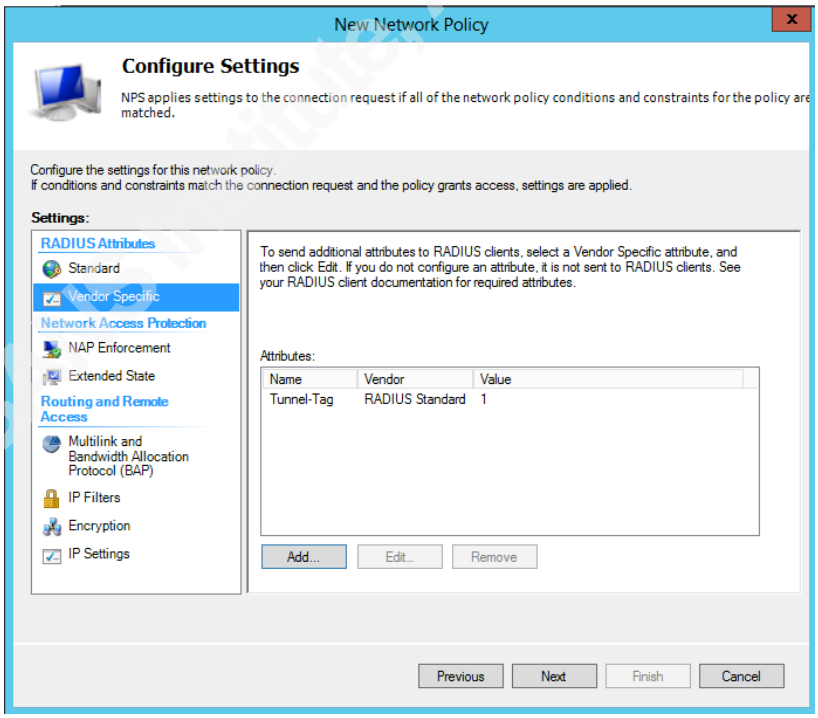


- On the **Configure Settings** page, add the following **Standard Attributes**

Johan@accessdenied.be



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



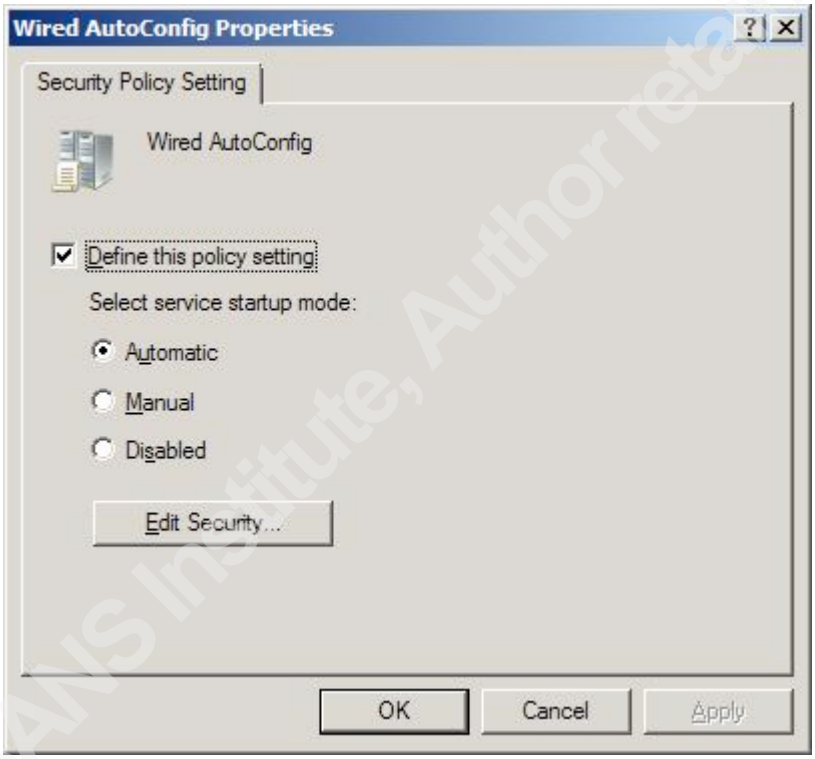
- On the **Completing New Network Policy** page, click **Finish**

Johan@accessdenied.be

5.7. Configuring Windows 7 client computers to enable IEEE 802.1x client

Before a Windows 7 client computer can be configured for IEEE 802.1x authentication, the Authentication tab needs to be enabled (University of Oslo, 2011). After the Wired AutoConfig service is started on the client computer, the authentication tab will be visible on the local area connection adapter.

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



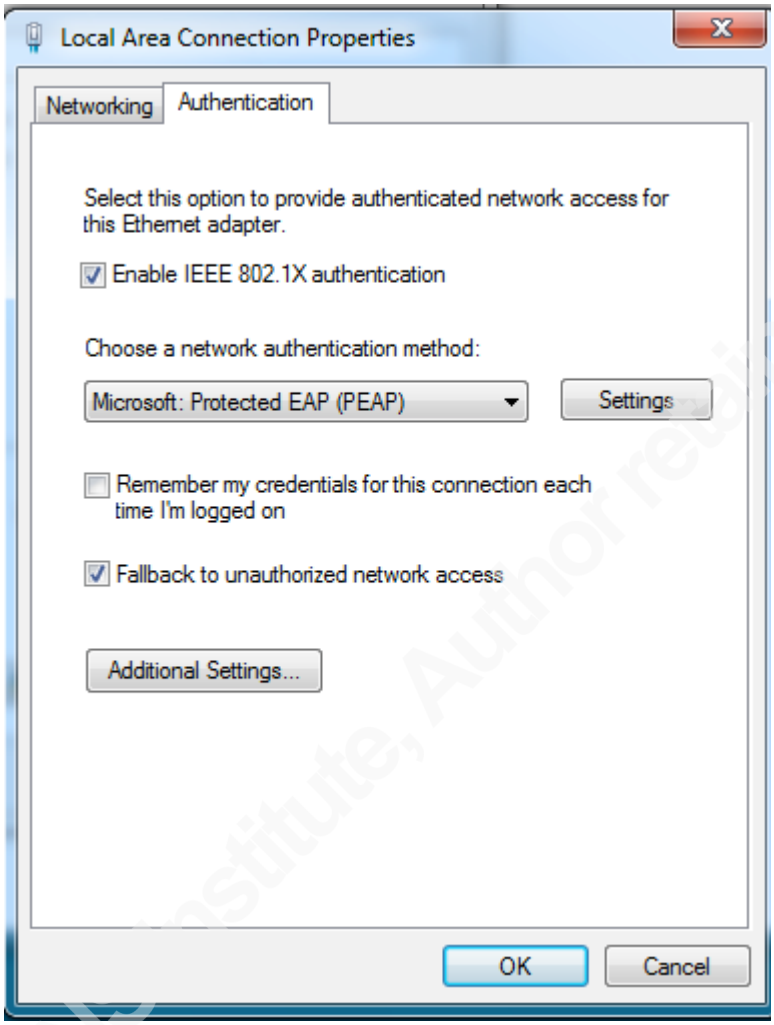
- Click **OK**

5.8. Configure Windows 7 client computer for 802.1x authentication via GPO

- 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**

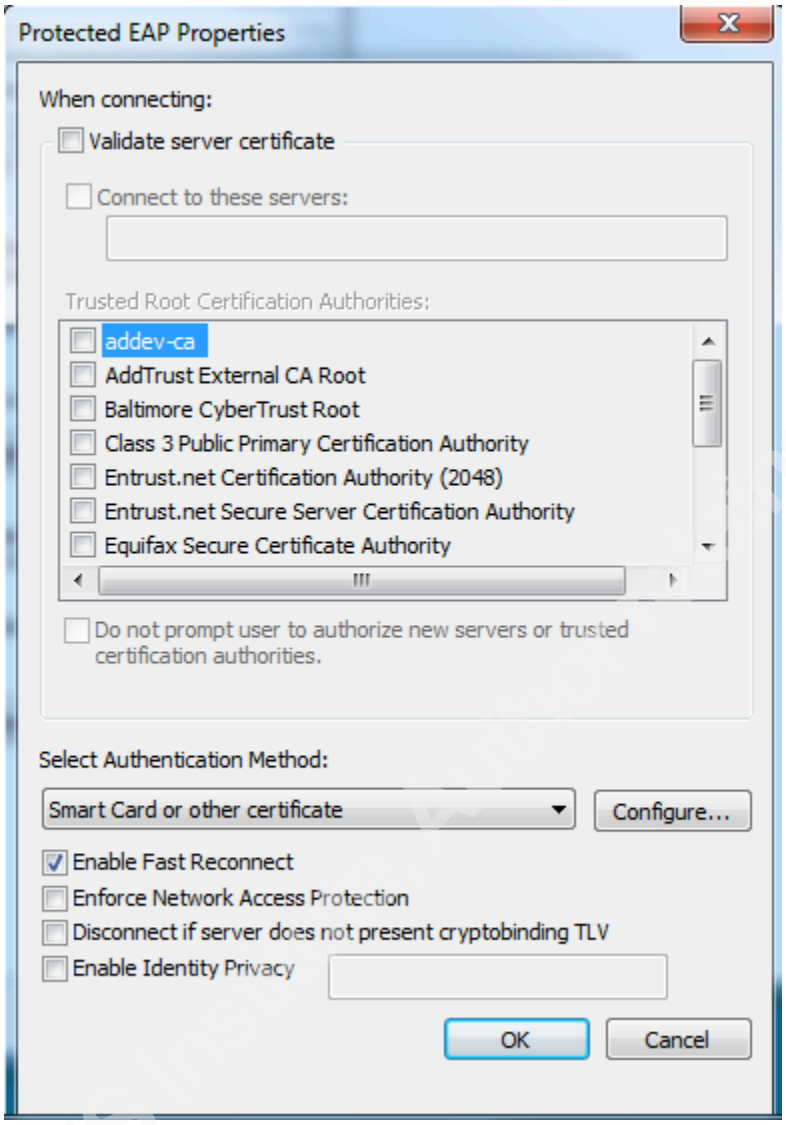
Johan@accessdenied.be

- On the **Choose a network authentication method** list box, select **Microsoft: Protected EAP (PEAP)** and click **Settings**



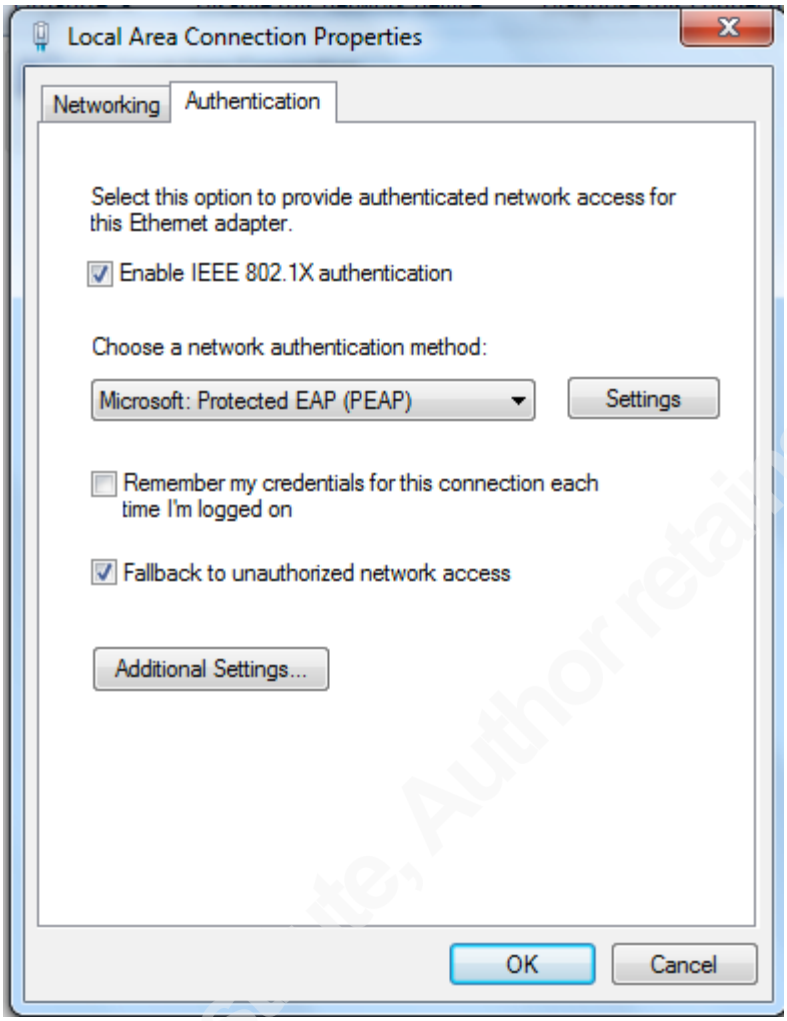
- From the **Select Authentication Method** list box, select **Smart Card or other certificate** and click **OK**

Johan@accessdenied.be



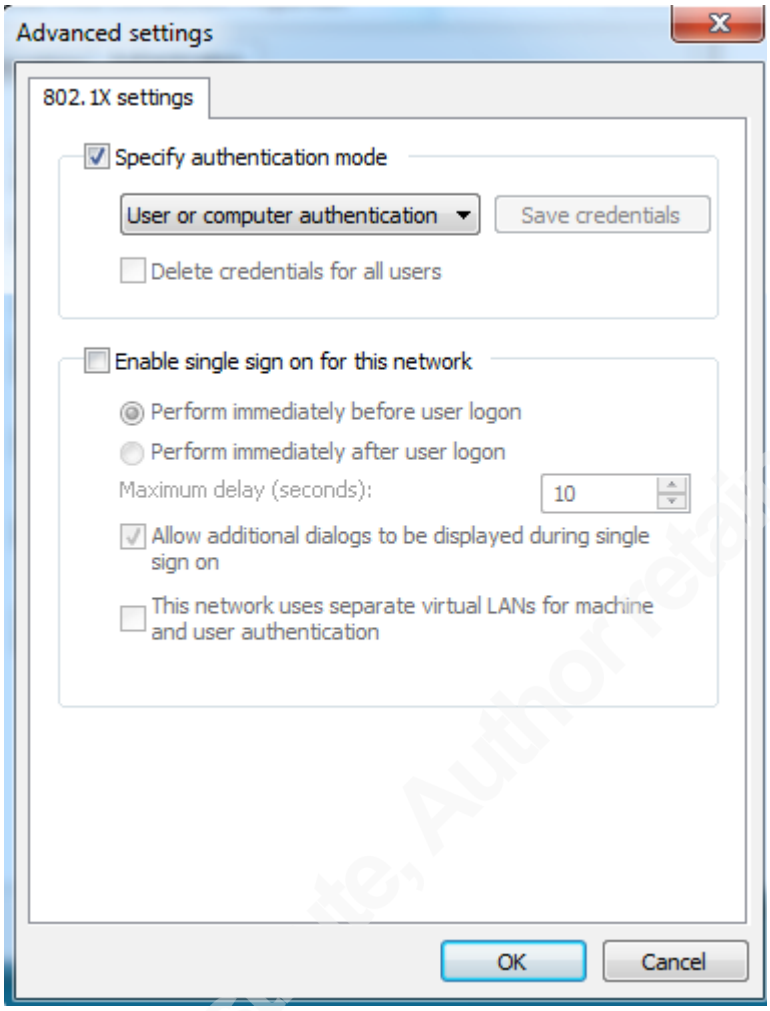
- Clear **Remember my credentials for this connection each time I'm logged on** and enable **Fallback to unauthorized network access**

Johan@accessdenied.be



- Click **Additional Settings**, select **Specify authentication mode** and select **User or Computer authentication** from the list

Johan@accessdenied.be



- Click **OK**

5.9. Configuring Cisco 3560 for IEEE 802.1x authentication

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

5.9.1. Configuring IEEE 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
```

Johan@accessdenied.be

5.9.2. Configuring switch-to-RADIUS server communication

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

5.9.3. Configure a Guest VLAN

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

5.9.4. Configure a Restricted VLAN

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

5.10. Test the configuration

Power-on the Windows 7 client computer. When the Windows 7 client computer starts up, the client sends an authentication request to the switch. If authentication is successful, the client computer receives an IP address from the DHCP server. If the client computer is a member of the security group Wired Computers VLAN 10, the client receives an IP address from the network range 10.32.10.50-10.32.10.60.

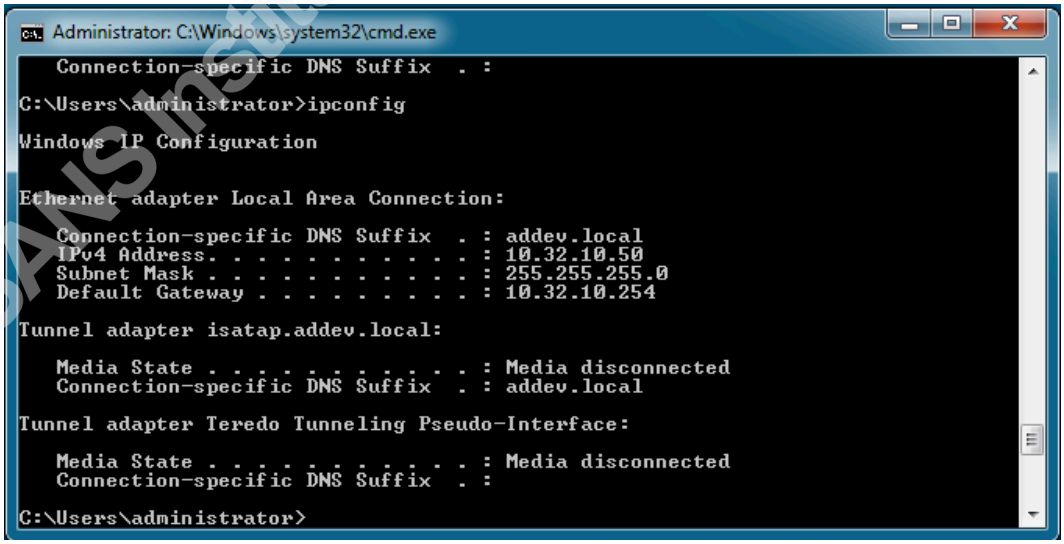


Figure 3: Successful authentication on the Windows 7 client

Johan@accessdenied.be

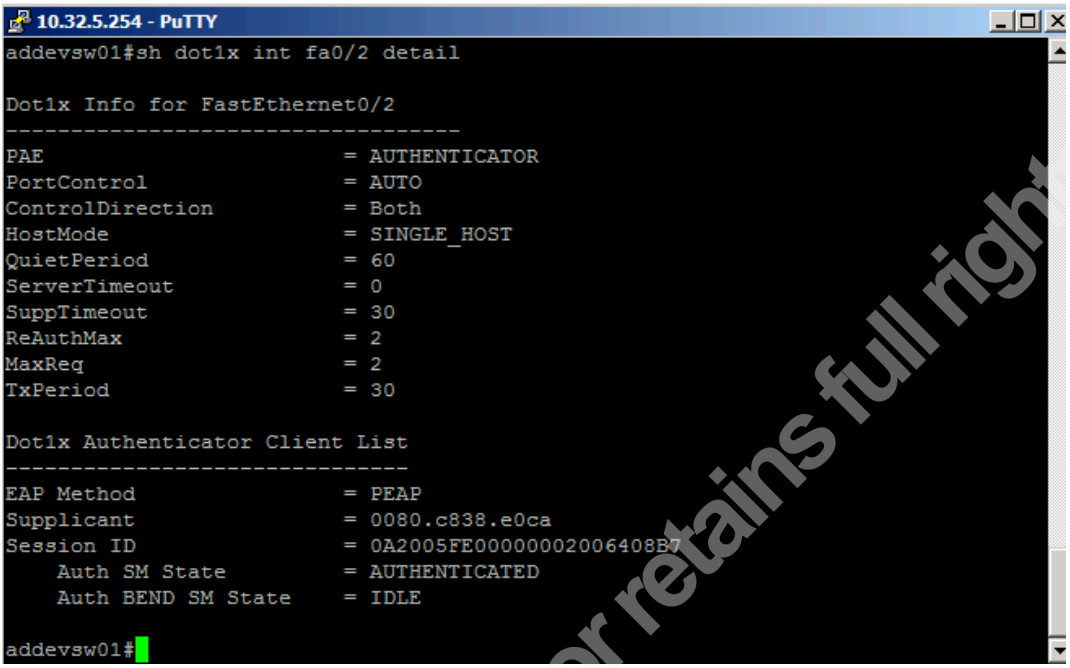


Figure 4: Successful authorization on the switch

If authentication fails, the client becomes a member of VLAN 99 and receives an IP address in the range of 10.32.99.50-10.32.99.60.

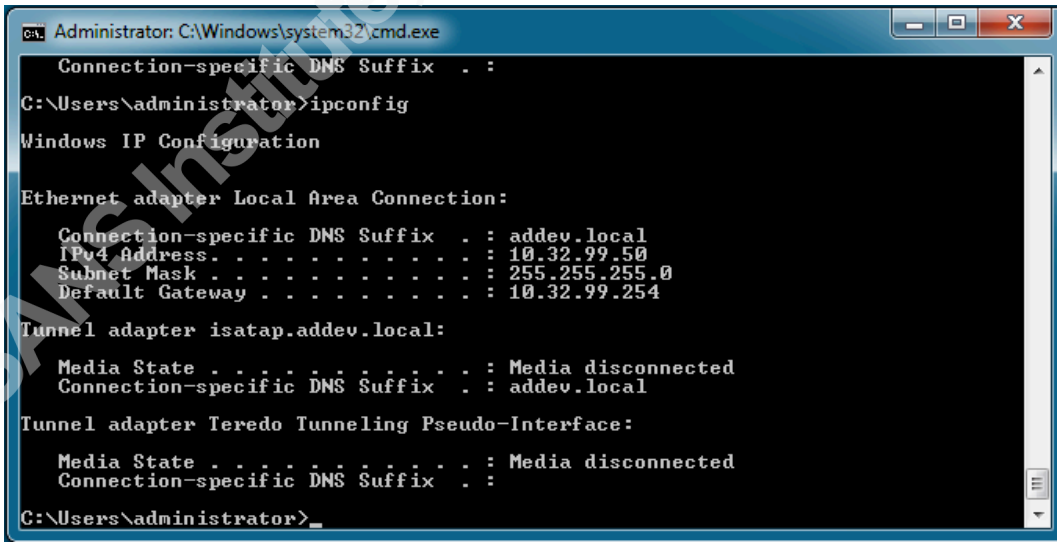


Figure 5: Failed authentication on the Windows 7 client

Johan@accessdenied.be

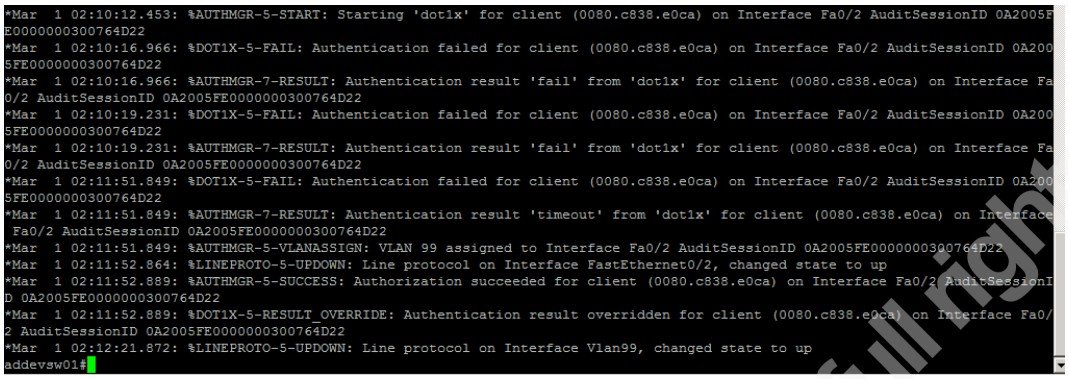


Figure 6: The switch places the switch port into VLAN 99

Johan@accessdenied.be