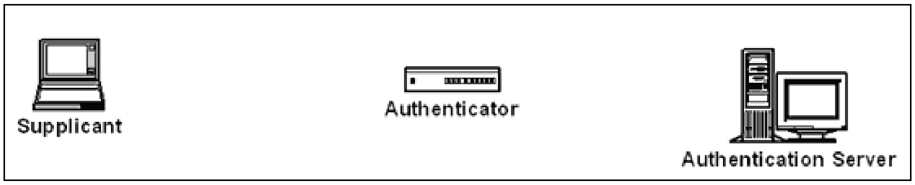
802.1x Port-Security

Setting up 802.1x port-security in your network can restrict non-organization end devices from access the organization’s network. It will secure the resources from any unauthorized users and workstations. Configuring 802.1x port-security consists of 3 sections as there are 3 main devices that constitute the port-security as shown in the figure below;

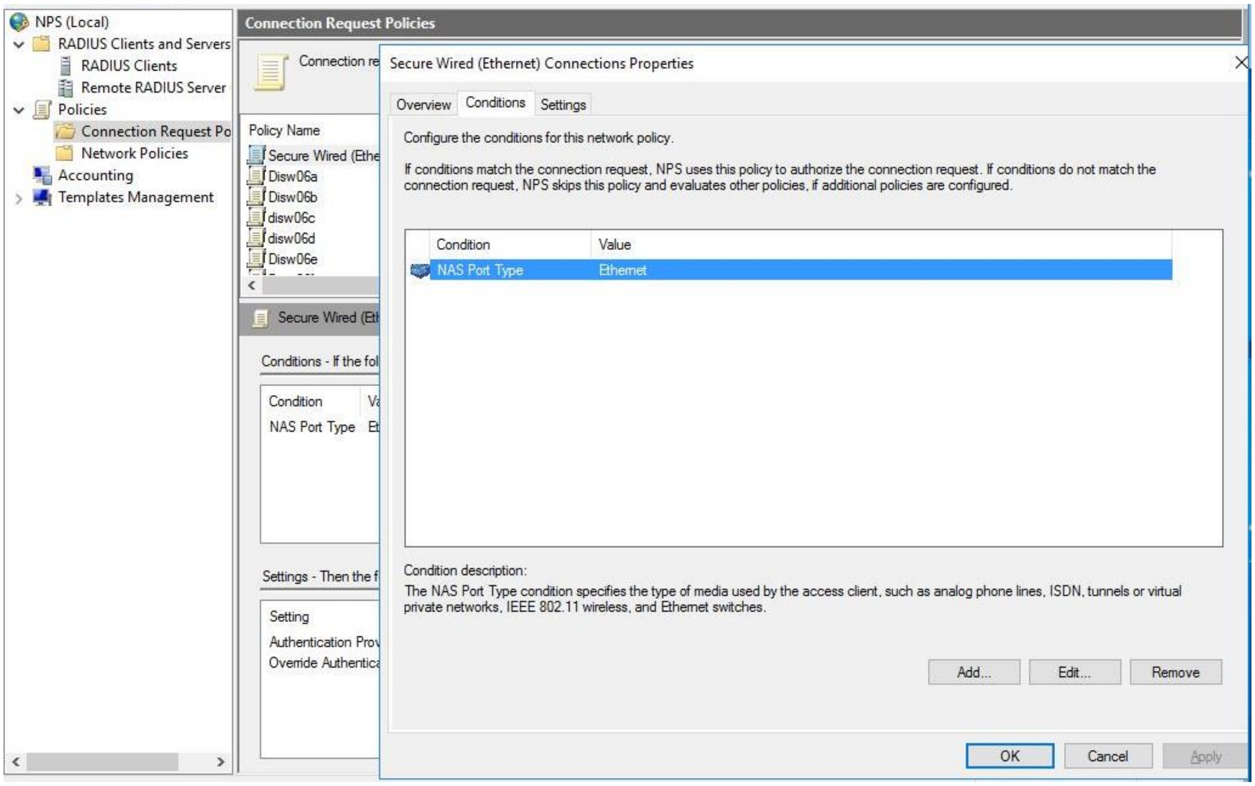


The supplicant is the end devices as desktop, laptops or even mobile devices who needs to access the resources.

Authenticator is generally 802.1x capable network switch which acts as a middle-man that helps the supplicant talk with the authentication server. It is not the one who authenticates the end devices, but it sends authentication traffic from supplicant to the server.

Authentication server is generally a radius server which authenticates (grants or rejects) the requests it receives from the authenticator; based on the condition it is configured for.

1. **Configuring the Radius server:**
   In the radius server, open **Network Policy server**. Create radius clients which are the network switches as has been discussed in the AAA configuration manual.
   Right-click the **Connection Request Policy** and select **New** to create a new Policy.
   Set everything to default except for the **Conditions**. Add a condition **NAS Port Type** with a value of **Ethernet**. Save the policy.



Secure Wired (Ethernet) Connections Properties

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.

Condition	Value
NAS Port Type	Ethernet

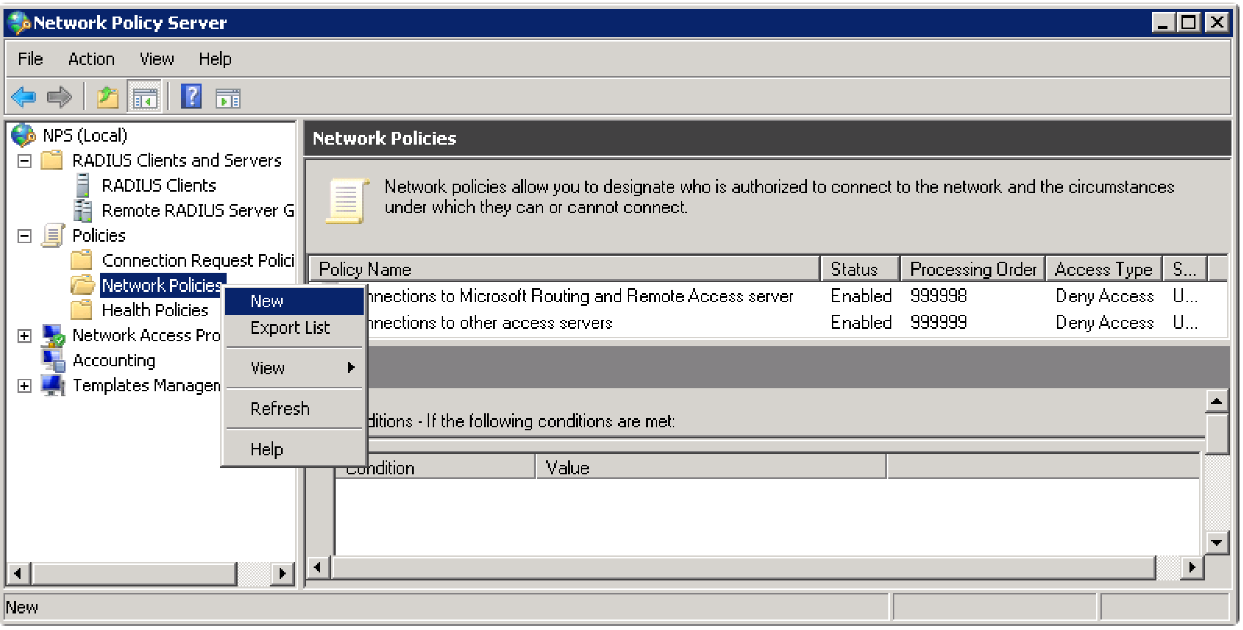
Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

Next step is to configure a **Network Policies** for the authenticating end devices.

-Santosh Bajimaya

802.1x Port-Security

Now we can create a network policy. Click on **Policies** > **Network Policies** (right mouse click) and click on **New**.



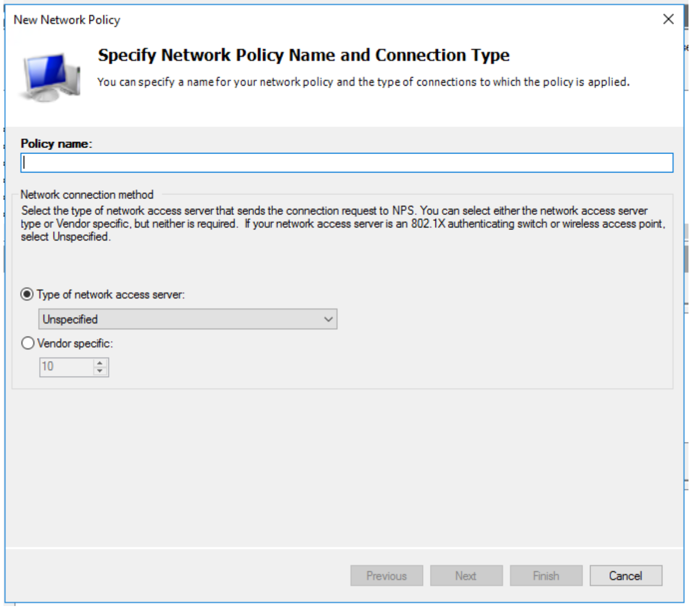
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	S...
nnections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	U...
nnections to other access servers	Enabled	999999	Deny Access	U...

ditions - If the following conditions are met:

Condition	Value

Give the policy a name, I'll call it "Wireless". Leave the type of network access server as **Unspecified**. Click **Next** to continue.



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:

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.

● Type of network access server:
Unspecified

○ Vendor specific:
10

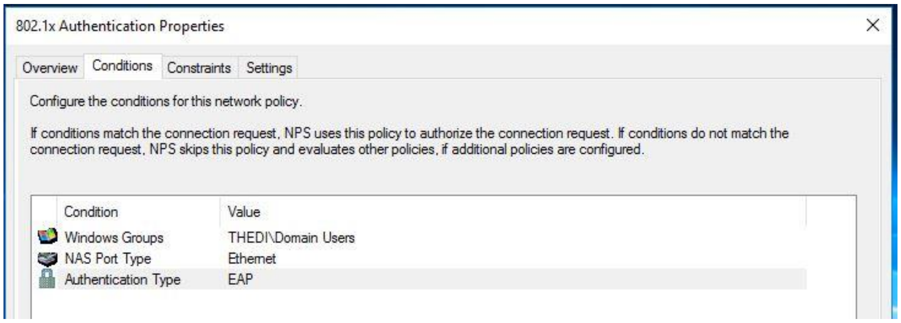
Now we can specify some conditions. I've set the following conditions:

- **Windows Groups**: **thedi/Domain Users**. By default all users in our Active Directory our member of the domain users group. If you only want certain users to be able to connect to the wireless network then it's better to create a new domain group for this.
- **NAS Port Type**: **Ethernet**. This ensures that the network policy only applies to wireless users.
- **Authentication Type**: **EAP**

Click on **Next** to continue.

-Santosh Bajimaya

802.1x Port-Security

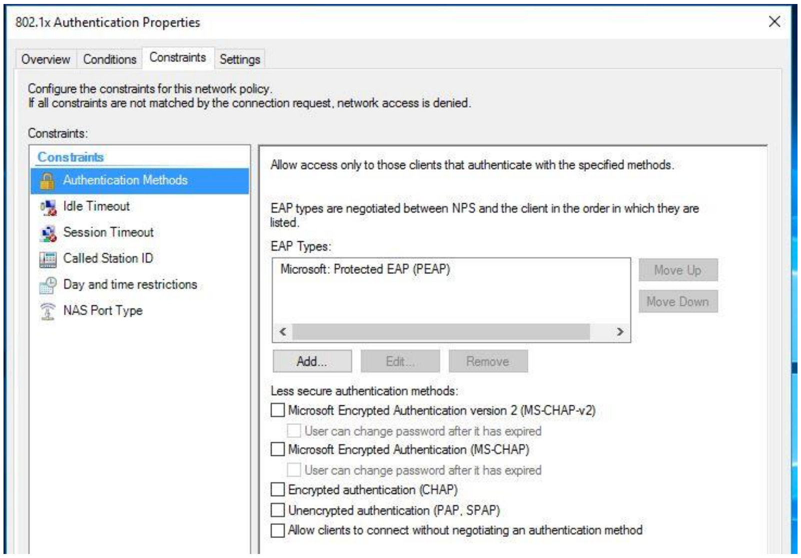


Configure the conditions for this network policy.

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.

Condition	Value
Windows Groups	THEDI\Domain Users
NAS Port Type	Ethernet
Authentication Type	EAP

We will now add PEAP authentication to our wireless policy. Click on **Add**.
Here you can select the authentication types that you want. I'll start with PEAP. Click on **Microsoft: Protected EAP (PEAP)** and click on **OK**.
You will see it in the overview. Select **Microsoft: Protected EAP (PEAP)** and click on **Edit**.



Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

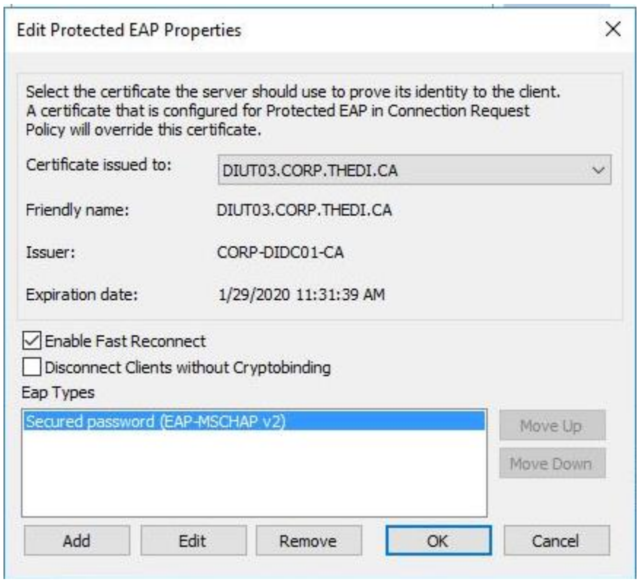
Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:
Microsoft: Protected EAP (PEAP)

Less secure authentication methods:
☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
☐ 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

Make sure you have selected the correct certificate. This is the computer certificate that will be presented to wireless users when they connect using PEAP. It allows our wireless clients to confirm the identity of the RADIUS server. Click **OK** to continue.



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: DIUT03.CORP.THEDI.CA
Friendly name: DIUT03.CORP.THEDI.CA
Issuer: CORP-DIDC01-CA
Expiration date: 1/29/2020 11:31:39 AM

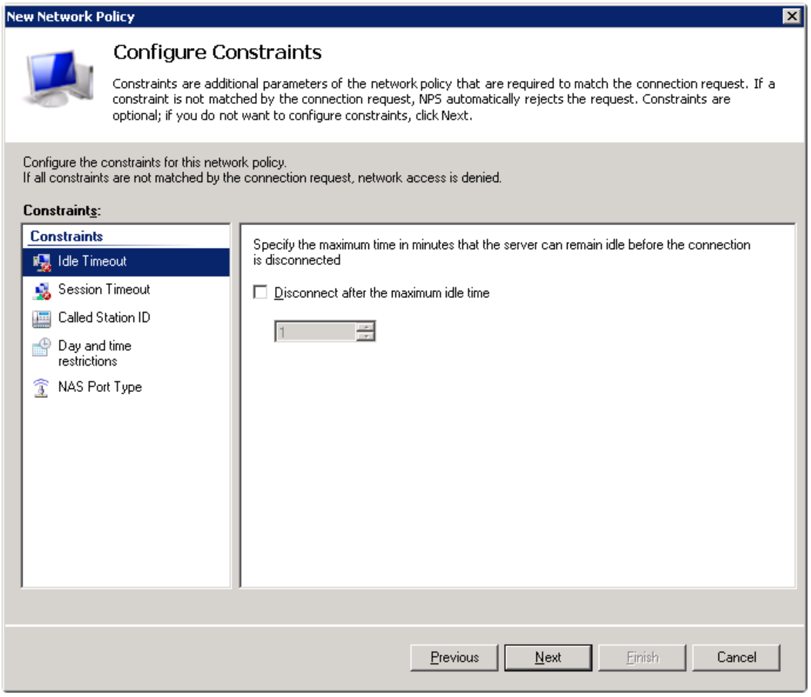
☑ Enable Fast Reconnect
☐ Disconnect Clients without Cryptobinding

Eap Types
Secured password (EAP-MSCHAP v2)

-Santosh Bajimaya

802.1x Port-Security

You will see an option to configure constraints, you can use these if you want to restrict access to the network…for example you can set a day and time restriction. If you want to do this, it's best to leave it alone for now and first make sure that everything is working. Click **Next** to continue.



New Network Policy

Configure Constraints

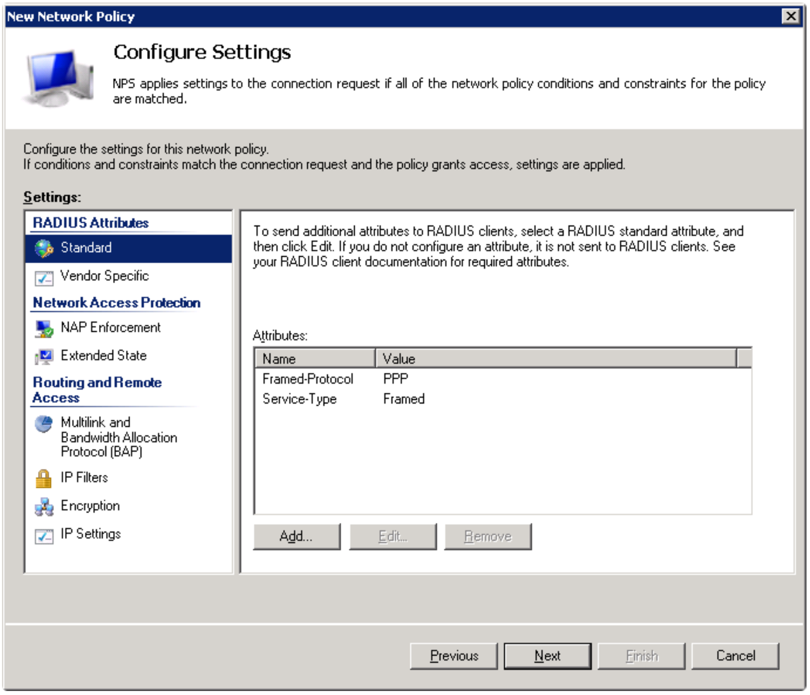
Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

Click **Next** to continue.



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

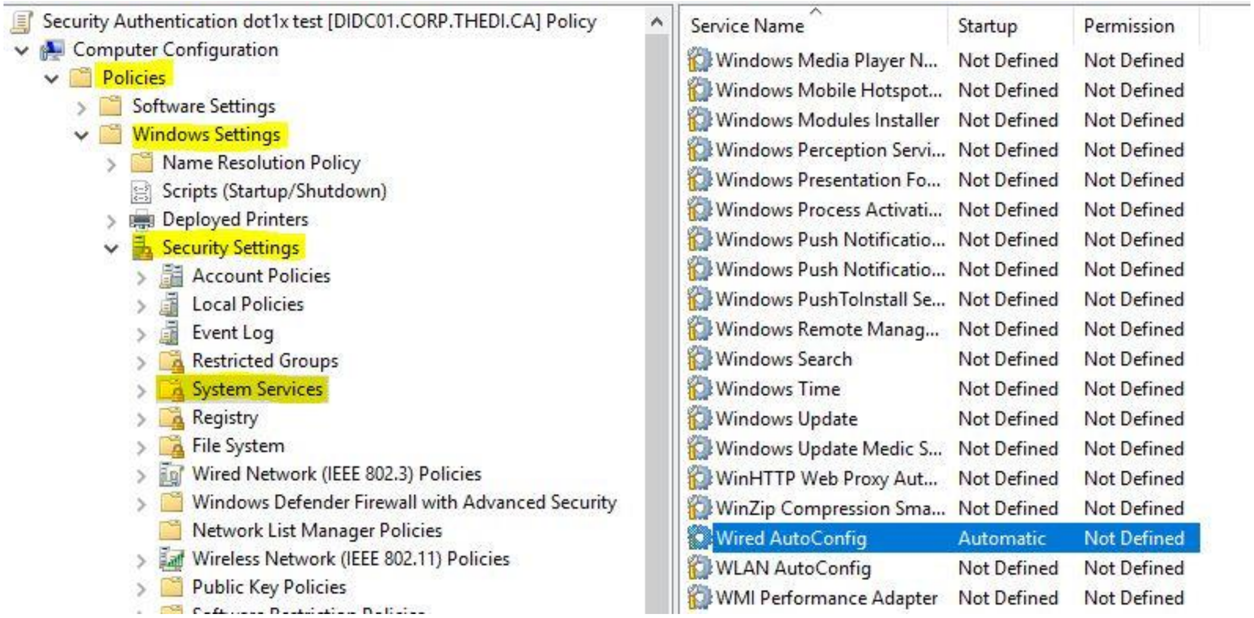
Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Click on **Next**. And click on **Finish** to complete the configuration of our policy.
NPS is running and we have successfully created a policy for network users.

802.1x Port-Security

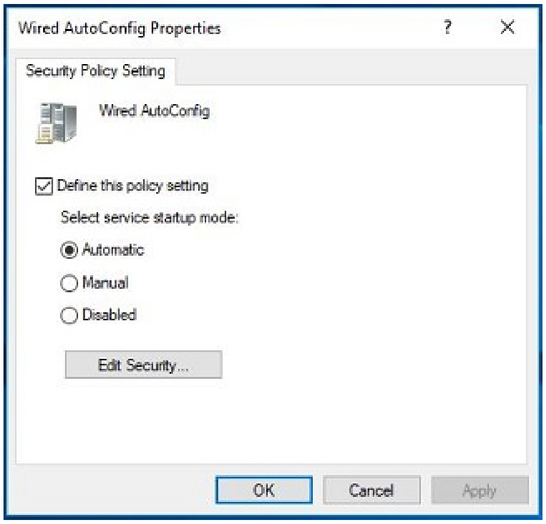
2. **Configuring The Supplicants:**
   Supplicants can be configured one by one but here we will look at configuring end devices through group policy.
   Open Group Policy Management console and target the OU whose end devices you want to configure for the security. Create a group policy within that OU and edit it.
   Go to **Computer configuration > Windows settings > Security Settings > System Services.**
   On the right windows, find "**Wired AutoConfig**" and set it to automatic as shown in the figure.



- Security Authentication dot1x test [DIDC01.CORP.THEDI.CA] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Defender Firewall with Advanced Security
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies

Service Name	Startup	Permission
Windows Media Player N...	Not Defined	Not Defined
Windows Mobile Hotspot...	Not Defined	Not Defined
Windows Modules Installer	Not Defined	Not Defined
Windows Perception Servi...	Not Defined	Not Defined
Windows Presentation Fo...	Not Defined	Not Defined
Windows Process Activati...	Not Defined	Not Defined
Windows Push Notificatio...	Not Defined	Not Defined
Windows Push Notificatio...	Not Defined	Not Defined
Windows PushToInstall Se...	Not Defined	Not Defined
Windows Remote Manag...	Not Defined	Not Defined
Windows Search	Not Defined	Not Defined
Windows Time	Not Defined	Not Defined
Windows Update	Not Defined	Not Defined
Windows Update Medic S...	Not Defined	Not Defined
WinHTTP Web Proxy Aut...	Not Defined	Not Defined
WinZip Compression Sma...	Not Defined	Not Defined
Wired AutoConfig	Automatic	Not Defined
WLAN AutoConfig	Not Defined	Not Defined
WMI Performance Adapter	Not Defined	Not Defined

This setting enables services in Network adaptor for the authentication configuration.



Wired AutoConfig Properties

Security Policy Setting

Wired AutoConfig

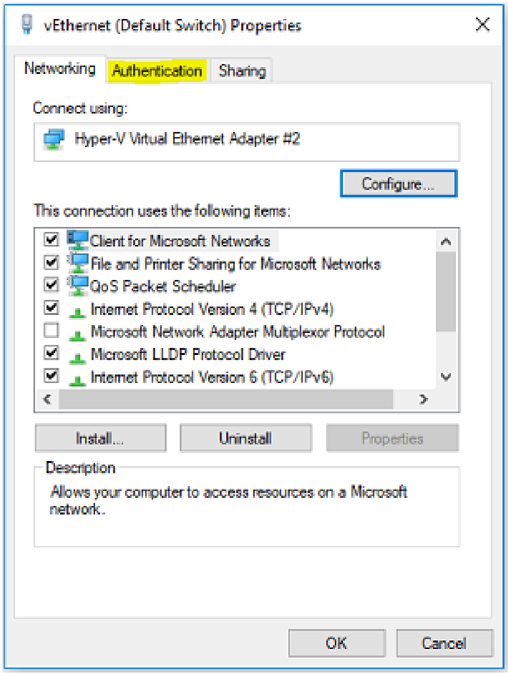
☑ Define this policy setting

Select service startup mode:

● Automatic

○ Manual

○ Disabled



vEthernet (Default Switch) Properties

Connect using:

Hyper-V Virtual Ethernet Adapter #2

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Description

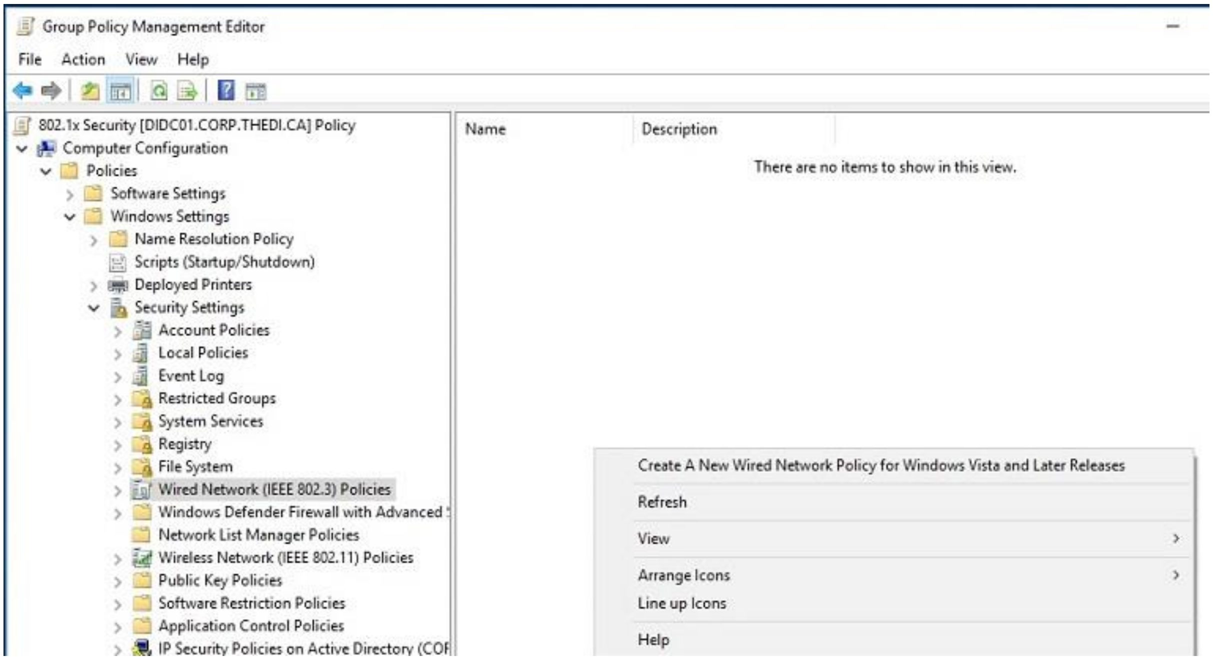
Allows your computer to access resources on a Microsoft network.

-Santosh Bajimaya

802.1x Port-Security

Once enabled, you will be able to see a new "**Authentication**" tab in the properties of your network adaptor as shown in the figure above.

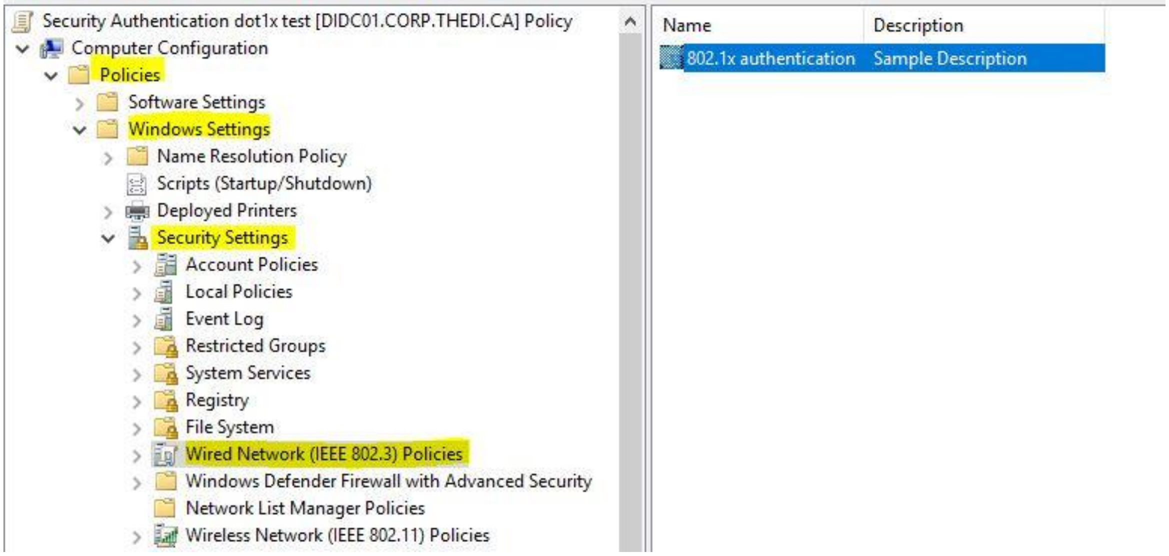
Next step is to configure the network adaptor setting in the end devices so that they are able to send in the authentication traffic (EAPOL) to the switch. We will be configuring the Authentication tab through group policy. You can edit the same group policy you created earlier. Just find "**Wired Network (IEEE 802.3 Policies"** as shown in the figure below:


Group Policy Management Editor
File
Action
View
Help
802.1x Security [DIDC01.CORP.THEDI.CA] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (COF
Name
Description
Create A New Wired Network Policy for Windows Vista and Later Releases
Refresh
View
Arrange Icons
Line up Icons
Help

There are no items to show in this view.

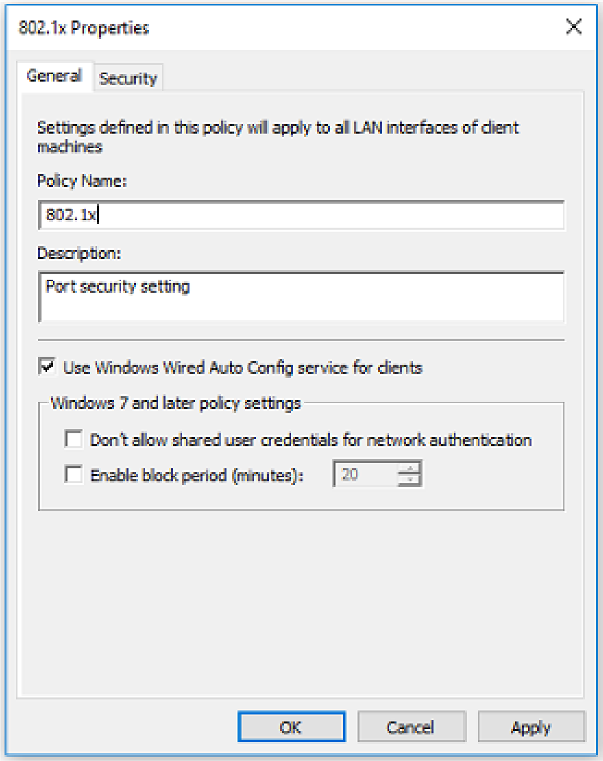
Right click on the right side of the window and select **Create a New Wired Network Policy for Windows Vista and Later Releases.**

Give your policy a name and open it to edit the settings.



802.1x Port-Security

Configure the properties as shown in the figure below:



802.1x Properties

General | Security

Settings defined in this policy will apply to all LAN interfaces of client machines

Policy Name: 802.1x

Description: Port security setting

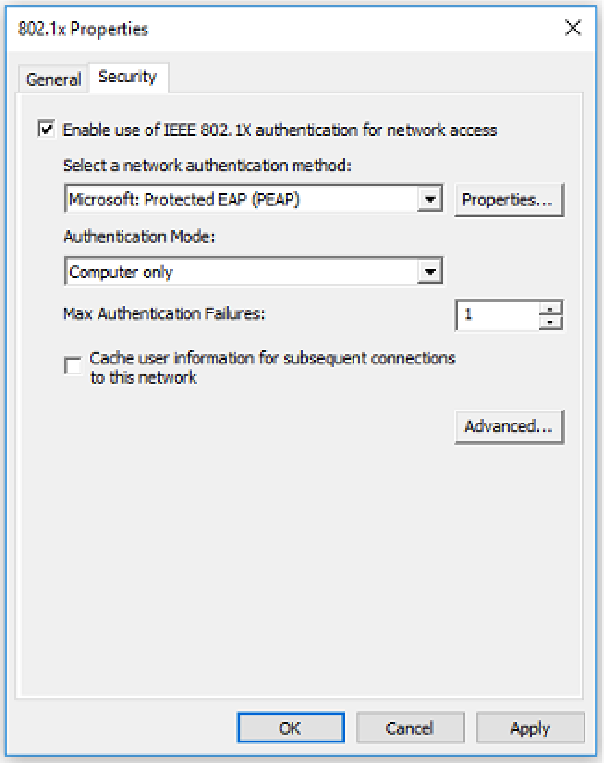
☑ Use Windows Wired Auto Config service for clients

Windows 7 and later policy settings

☐ Don't allow shared user credentials for network authentication

☐ Enable block period (minutes): 20

OK | Cancel | Apply



802.1x Properties

General | Security

☑ Enable use of IEEE 802.1X authentication for network access

Select a network authentication method: Microsoft: Protected EAP (PEAP) | Properties...

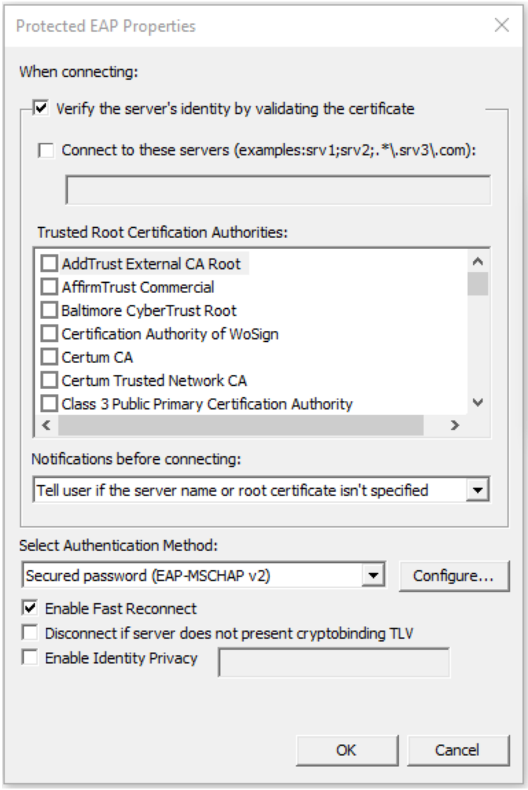
Authentication Mode: Computer only

Max Authentication Failures: 1

☐ Cache user information for subsequent connections to this network

Advanced...

OK | Cancel | Apply



Protected EAP Properties

When connecting:

☑ Verify the server's identity by validating the certificate

☐ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

Trusted Root Certification Authorities:

☐ AddTrust External CA Root
☐ AffirmTrust Commercial
☐ Baltimore CyberTrust Root
☐ Certification Authority of WoSign
☐ Certum CA
☐ Certum Trusted Network CA
☐ Class 3 Public Primary Certification Authority

Notifications before connecting: Tell user if the server name or root certificate isn't specified

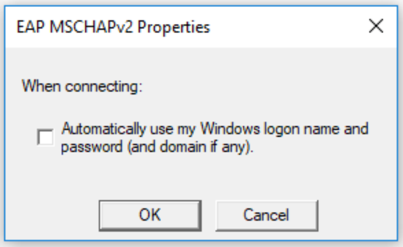
Select Authentication Method: Secured password (EAP-MSCHAP v2) | Configure...

☑ Enable Fast Reconnect

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

OK | Cancel



EAP MSCHAPv2 Properties

When connecting:

☐ Automatically use my Windows logon name and password (and domain if any).

OK | Cancel

-Santosh Bajimaya

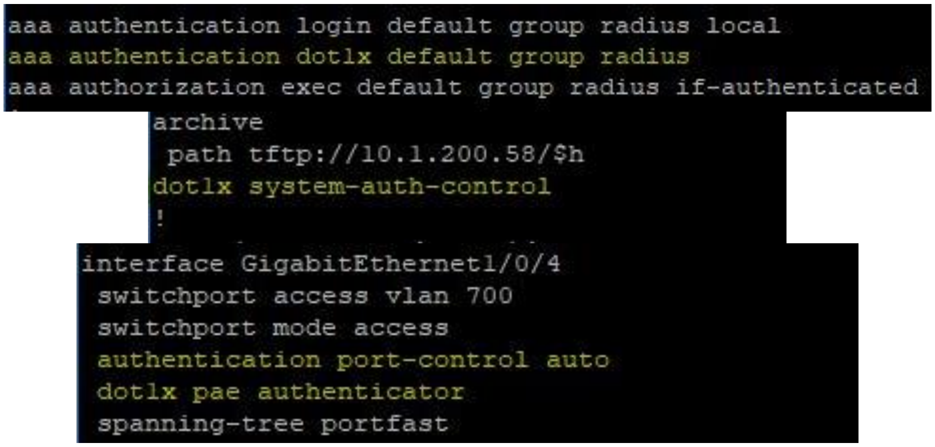
802.1x Port-Security

3. **Configure the Authenticator:**

Now that the Supplicant has been configured, we need to configure the network switches to understand the authentication traffic and send the traffic to radius server for authentication. Most of the commands have been already configured for the AAA authentication setup for switch access. So, for the 802.1x port-security, we basically need 4 more commands.

```
Switch (Config) # aaa authentication dot1x default group radius
Switch (Config) # dot1x system-auth-control
Switch (config-if) # authentication port-control auto
Switch (config-if) # dot1x pae authenticator
```

The first 2 commands are the global configuration commands and the rest 2 are interface configuration commands.



```
aaa authentication login default group radius local
aaa authentication dot1x default group radius
aaa authorization exec default group radius if-authenticated
archive
 path tftp://10.1.200.58/$h
dot1x system-auth-control
!
interface GigabitEthernet1/0/4
 switchport access vlan 700
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
```

Reference:

- https://networklessons.com/uncategorized/peap-and-eap-tls-on-server-2008-and-cisco-wlc#Network-Policy
- https://www.youtube.com/watch?v=jkvayOyoX-E
- https://blogs.technet.microsoft.com/networking/2012/05/30/creating-a-secure-802-1x-wireless-infrastructure-using-microsoft-windows/
- https://www.networkworld.com/article/2940463/it-skills-training/machine-authentication-and-user-authentication.html