

# How to configure 802.1x guest vlan in Windows Server 2008

## [Topology]:

Client(192.168.1.90)-----P11 DES-3200-18 P15----Radius\_Server(192.168.1.100)

Client is used Windows Vista for testing.

Radius Server is used Windows Server 2008.

## [Configuration]:

### [DES-3200-18]:

config vlan default delete 1-18

create vlan v10 tag 10

config vlan v10 add untagged 10-16

create vlan v20 tag 20

config vlan v20 add untagged 1-10

config ipif System ipaddress 192.168.1.1/24 vlan v10

enable 802.1x

create 802.1x guest\_vlan v10

config 802.1x guest\_vlan ports 10-16 state enable

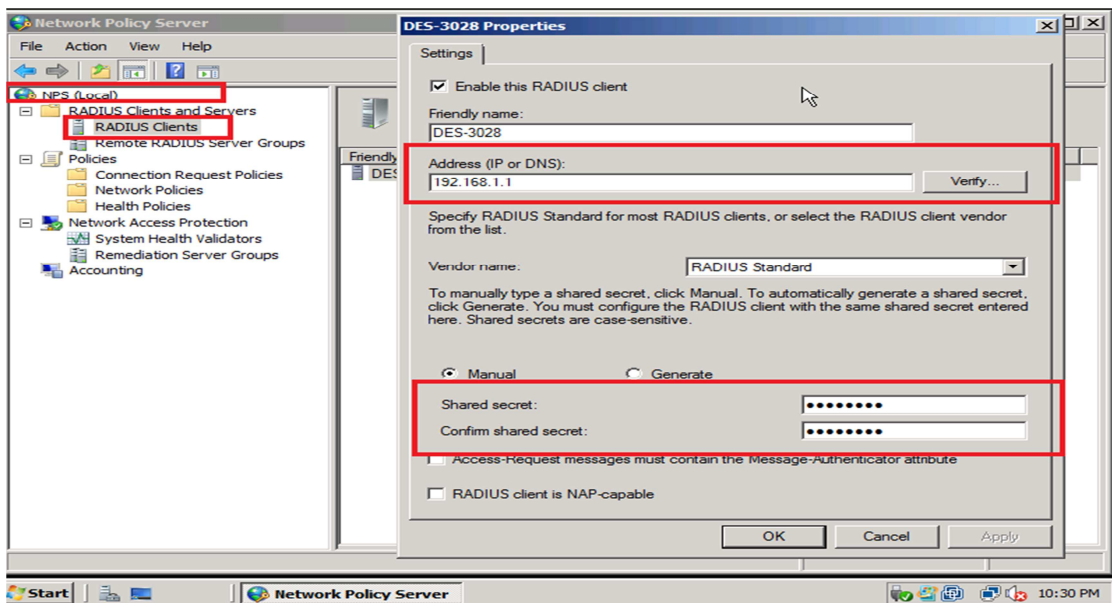
config 802.1x capability ports 10-14 authenticator

config radius add 1 192.168.1.100 key 123456 default

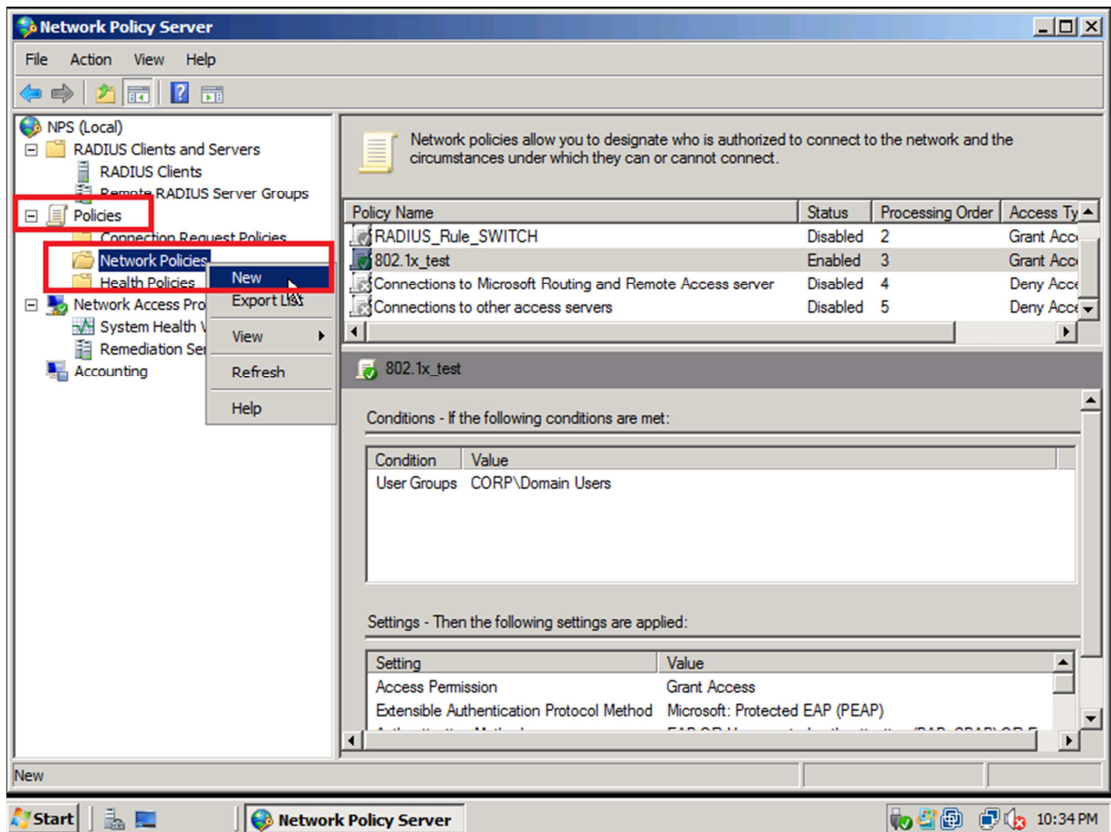
config ipif System ipaddress 192.168.1.1/24

## [Windows Server 2008]:

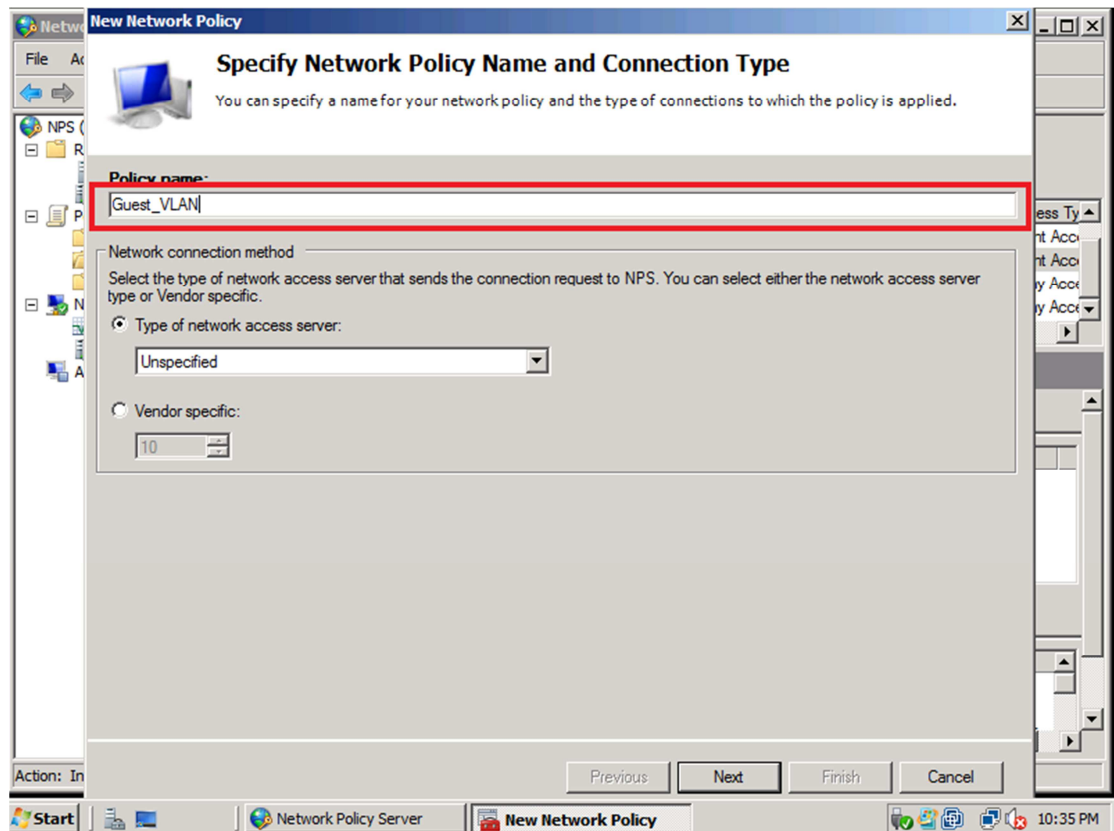
1. Under the **Network Policy Server**-> **RADIUS Clients** and new a RADIUS Client. You have to type the Switch IP address and key in this parts.



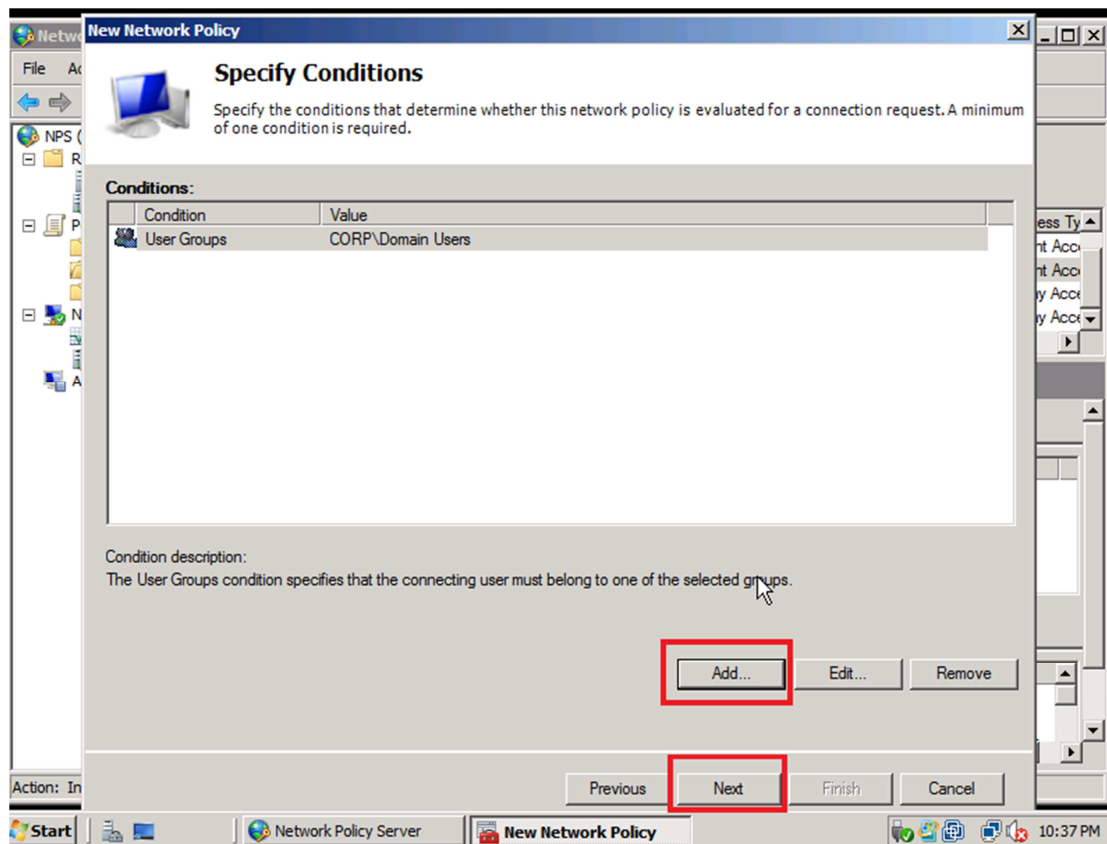
2. Under the **Policies-> Network Policies** and new a policy as follows



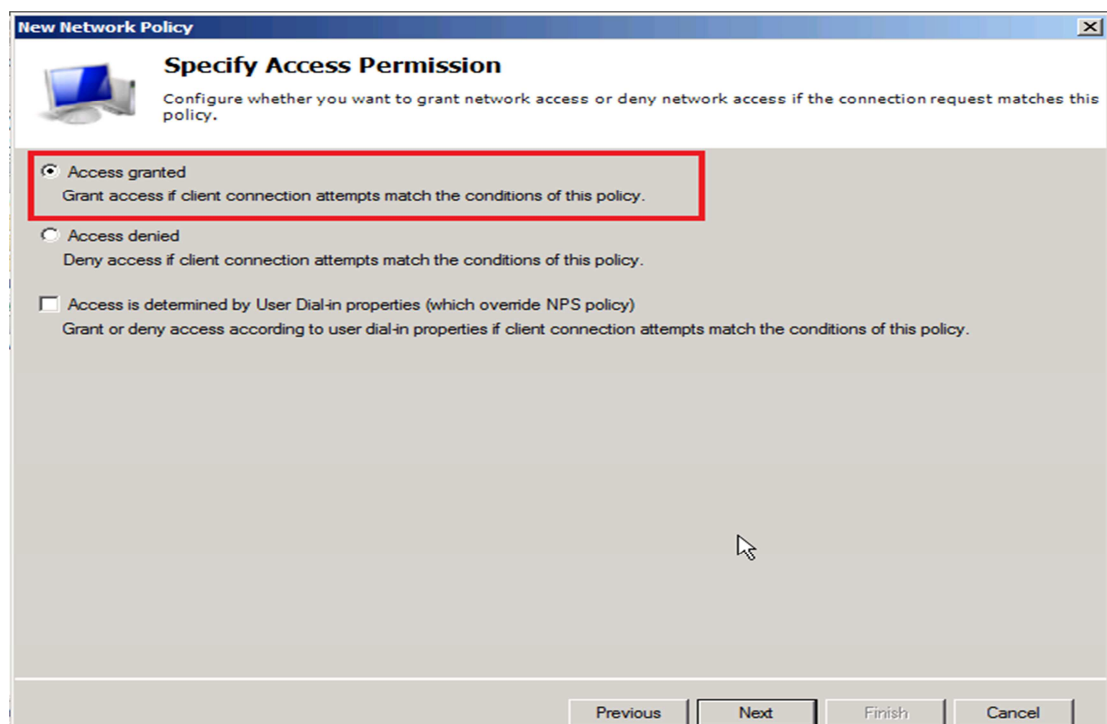
3. Specify the **Policy name** and click the **Next**.



4. Click **Add** button and select the **Domain Users** into the condition and click the **Next**.



5. Select **Access granted** and click the **Next** button.



6.

**New Network Policy**

## Configure Authentication Methods

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

**EAP Types:**

Microsoft: Protected EAP (PEAP) Move Up  
Move Down

Add... Edit... Remove

**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.
- Perform machine health check only

Previous Next Finish Cancel

**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.

**Constraints:**

**Constraints**

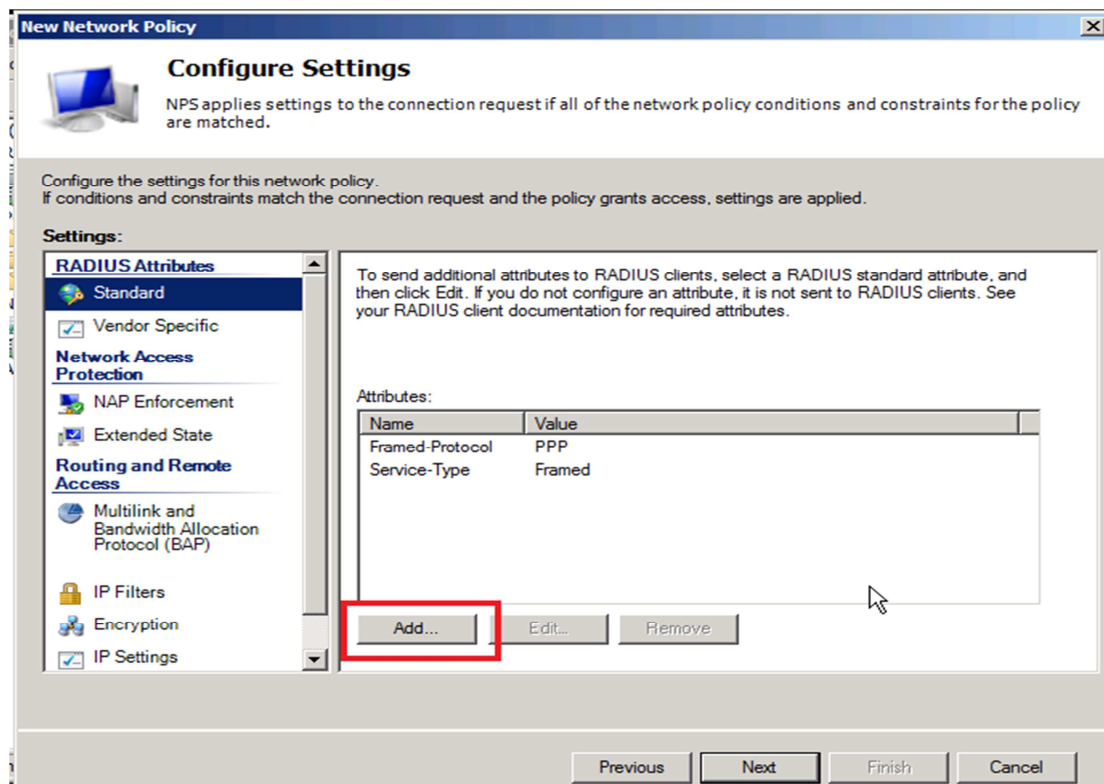
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

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

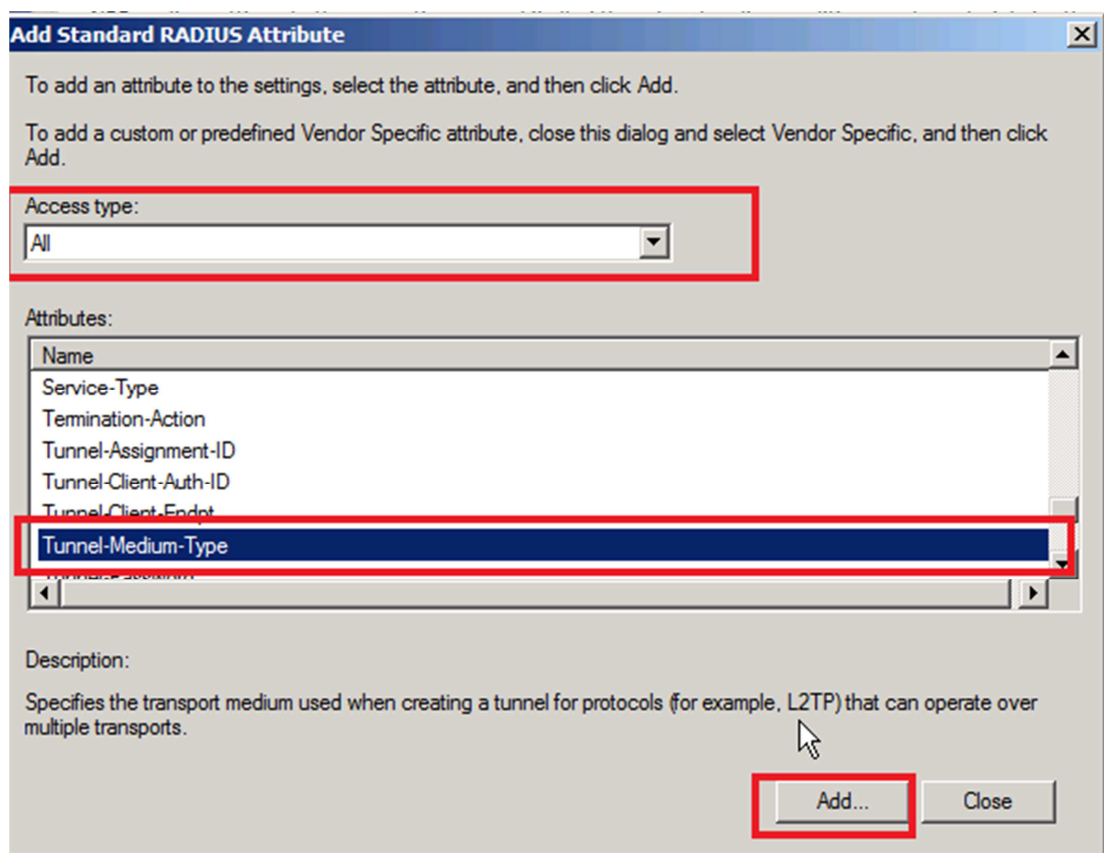
Disconnect after the maximum idle time

Previous Next Finish Cancel

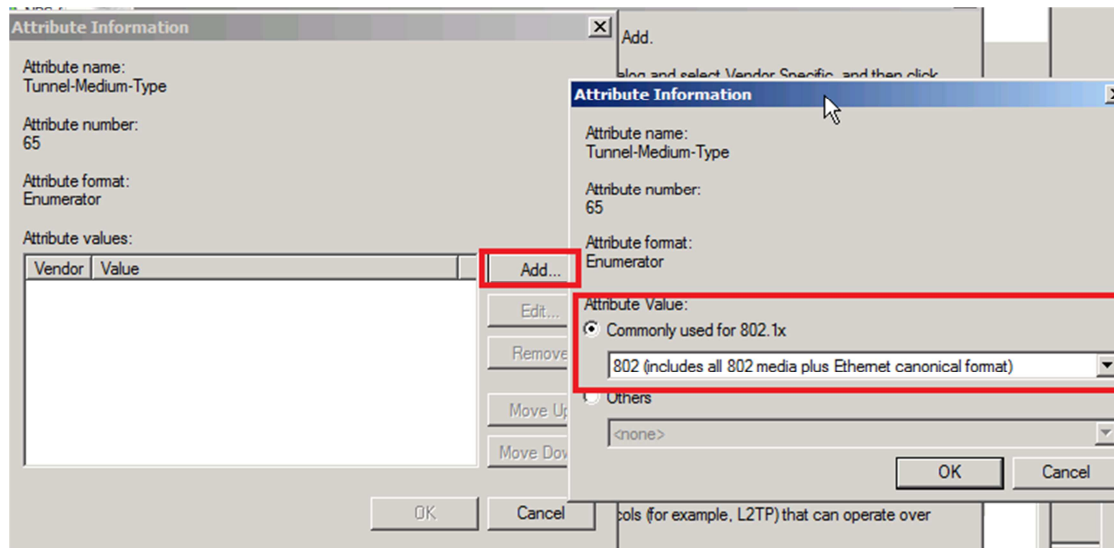
**7. Click Add to add the following information (IMPORTANT):**



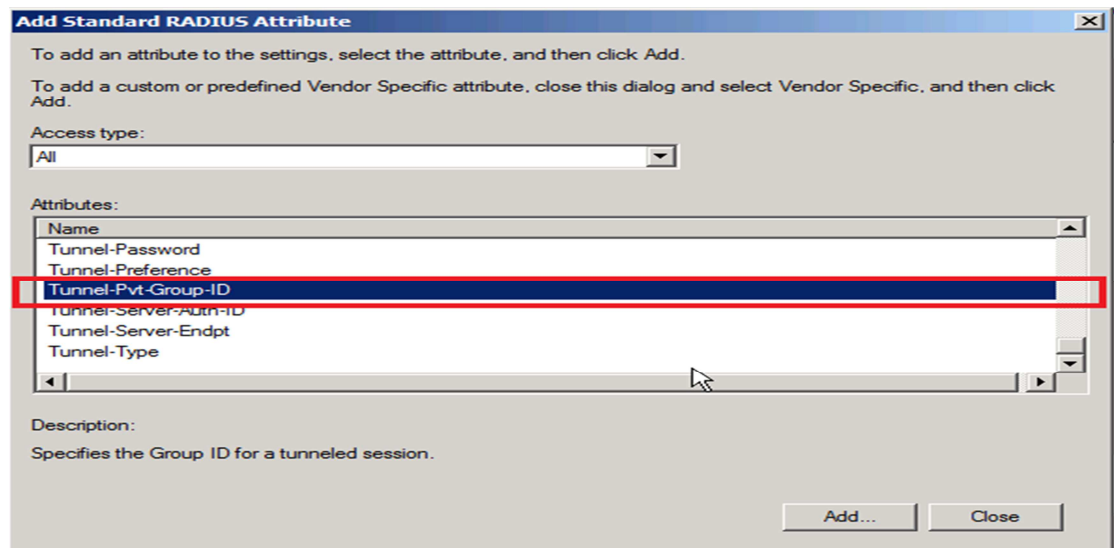
Choose the **Access type** as **All** and find the **Attributes** called **Tunnel-Medum-Type** and click **Add** button as follows.



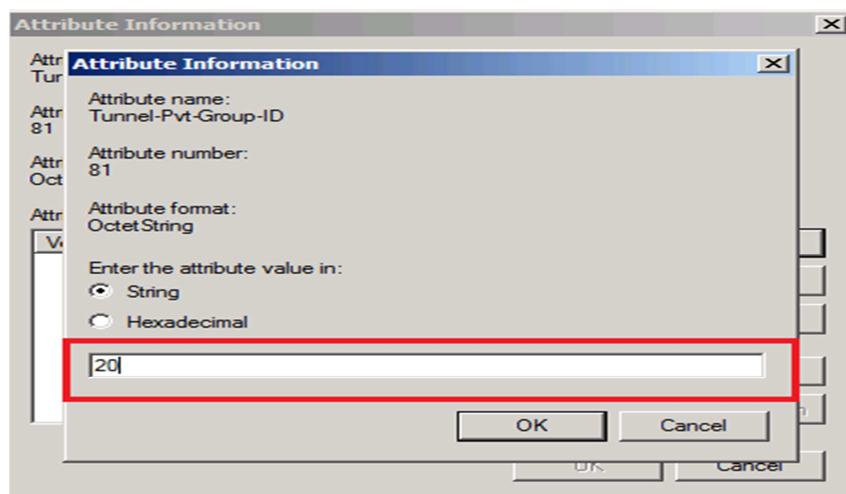
Click Add and select the Attribute Value as follows. Then Click OK



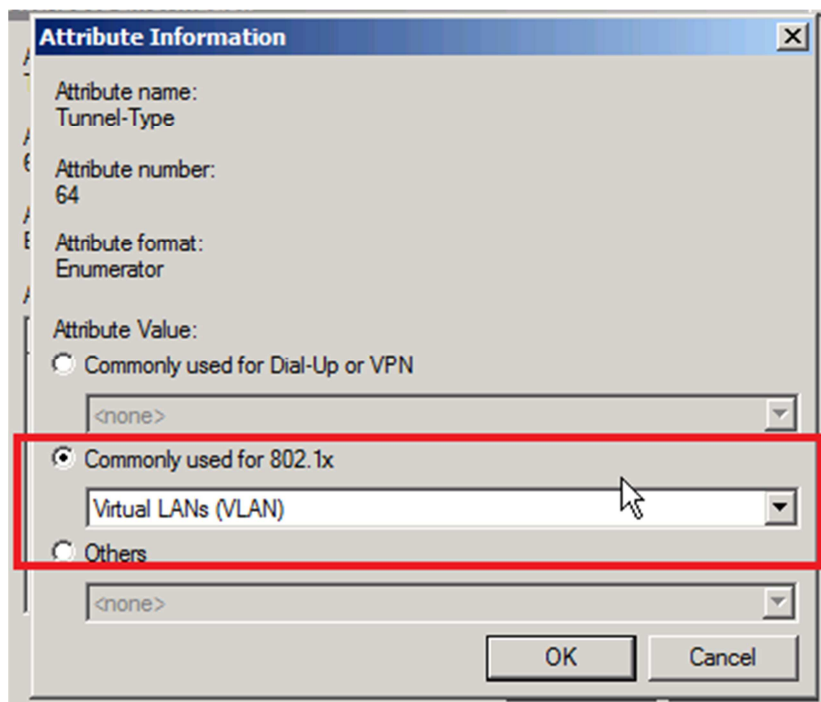
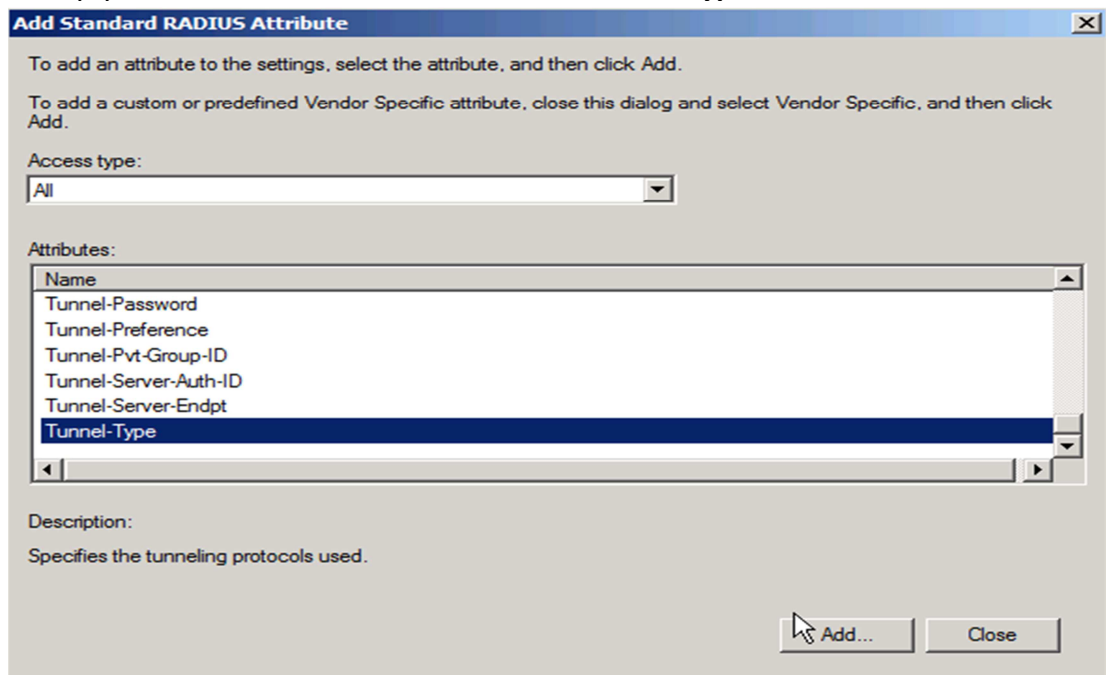
Secondly, you have to find the **Attributes** called **Tunnel-Pvt-Group-ID** and click the **Add**.



Specify the String to 20 as follows

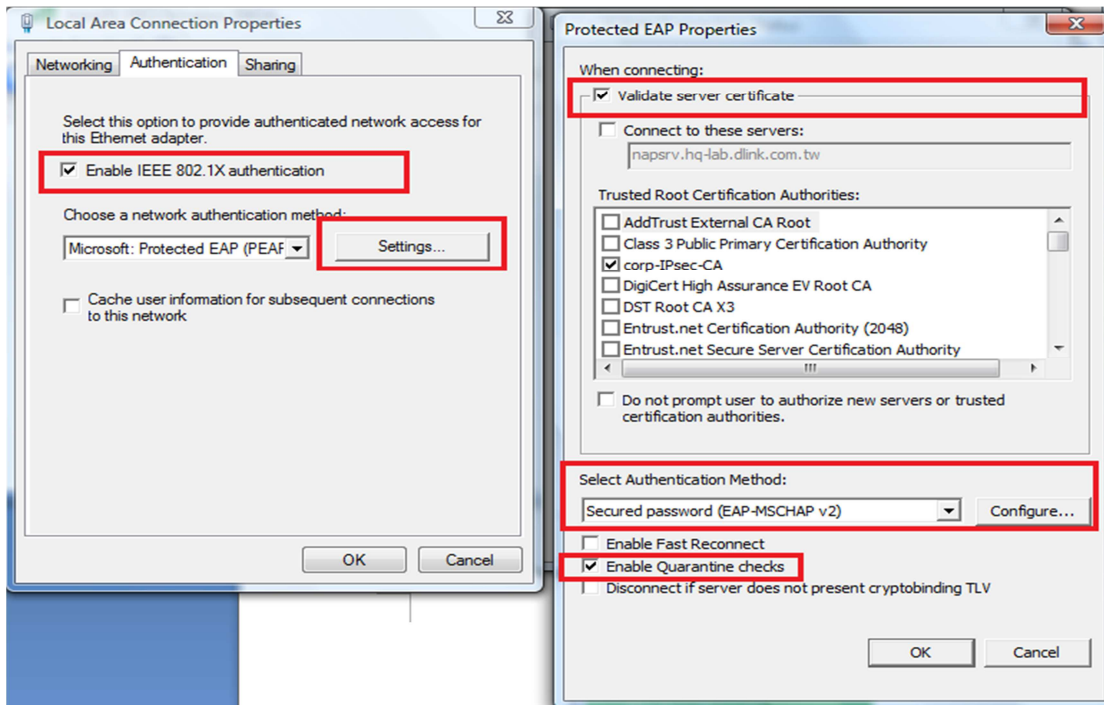


Finally, you have to find the Attributes called **Tunnel Type**:



**[Testing Procedure]:**

1. Client have to download the certificate from the Server through [http://IP\\_address/certsrv](http://IP_address/certsrv) . The IP\_address is the server\_IP. Then import the client
2. For the client's NIC setting, you can refer the following:



3. Plug the cable on the port 11 and type the username/ password for it.

**[Testing result]:**

```
DES-3200-18:4#show vlanshow vlanshow 802.1x auth_state port 11show vlan
show 802.1x auth_state port 11
```

```
Command: show 802.1x auth_state ports 11
```

Port	Auth PAE State	Backend State	Port Status
11	Authenticated	Idle	Authorized

```
DES-3200-18:4#show vlanshow vlan
Command: show vlan
```

```
VID      : 1          VLAN Name      : default
VLAN Type : Static    Advertisement : Enabled
Member Ports :
Static Ports :
Current Tagged Ports :
Current Untagged Ports :
Static Tagged Ports :
Static Untagged Ports :
Forbidden Ports :

VID      : 10         VLAN Name      : v10
VLAN Type : Static    Advertisement : Disabled
Member Ports : 10,12-16
Static Ports : 10,12-16
Current Tagged Ports :
Current Untagged Ports : 10,12-16
Static Tagged Ports :
Static Untagged Ports : 10,12-16
Forbidden Ports :

VID      : 20         VLAN Name      : v20
VLAN Type : Static    Advertisement : Disabled
Member Ports : 1-9,11
Static Ports : 1-9,11
Current Tagged Ports :
Current Untagged Ports : 1-9 11
Static Tagged Ports :
Static Untagged Ports : 1-9 11
Forbidden Ports :
```

```
Total Entries : 3
```



802.1x\_Guest\_VLAN.log