

How to set up 802.1x Port-based with Windows Server 2008

[Topology]:

Client(192.168.0.78)--(p8)DES-3200-18(192.168.0.1/24)(17)—Radius(192.168.0.100)

Radius server is used Windows Server 2008.

DES-3200-18 is used the firmware 1.30B04

[Configuration]:

[DES-3200-18]

config 802.1x capability ports 1:1-1:12 authenticator

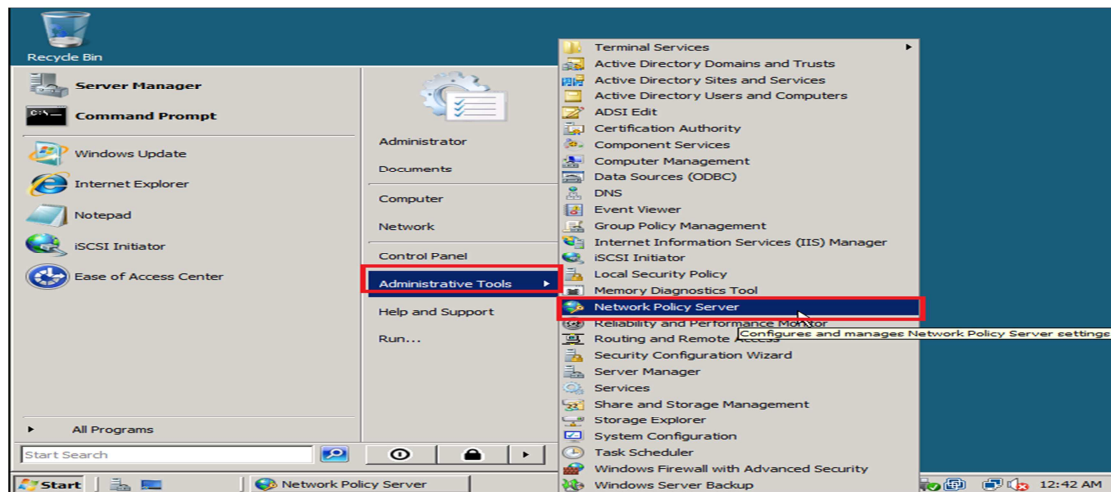
enable 802.1x

config radius add 1 192.168.0.100 key 123456 default

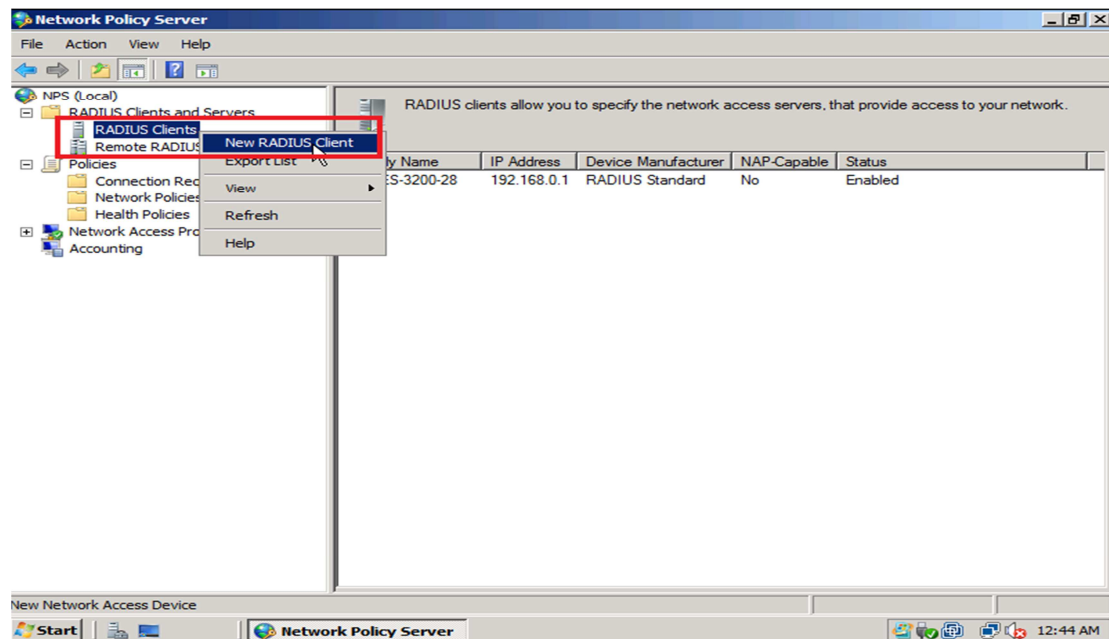
config 802.1x auth_mode port_based

[Windows Server 2008]

1. Click the **Network Policy Server** under **Start->Administrative Tools->Network Policy Server**.



2. Click **New RADIUS Client** under **NPS(Local)-> RADIUS Clients and Servers-> RADIUS Clients**.



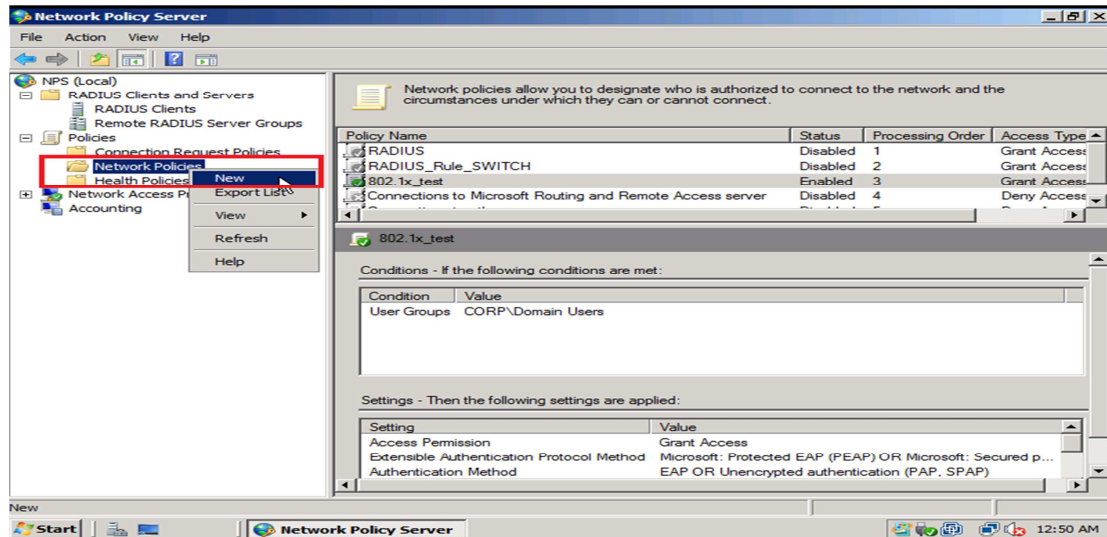
3. Filled the Friendly name, Address, and Shared secret as follows:

The 'New RADIUS Client' dialog box is shown with the following configuration:

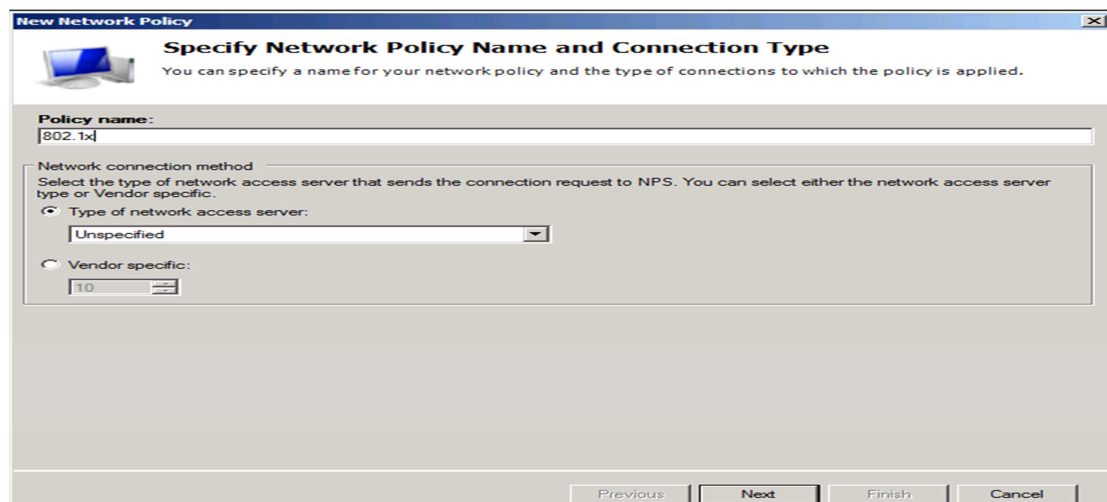
- ☒ Enable this RADIUS client
- Name and Address**
 - Friendly name: DES-3200-28
 - Address (IP or DNS): 192.168.0.1
 - Verify... button
- Vendor**
 - Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.
 - Vendor name: RADIUS Standard (selected from dropdown)
- Shared Secret**
 - To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
 - ☒ Manual ☐ Generate
 - Shared secret: [Redacted]
 - Confirm shared secret: [Redacted]
- Additional Options**
 - ☐ Access-Request messages must contain the Message-Authenticator attribute
 - ☐ RADIUS client is NAP-capable

OK and Cancel buttons are at the bottom.

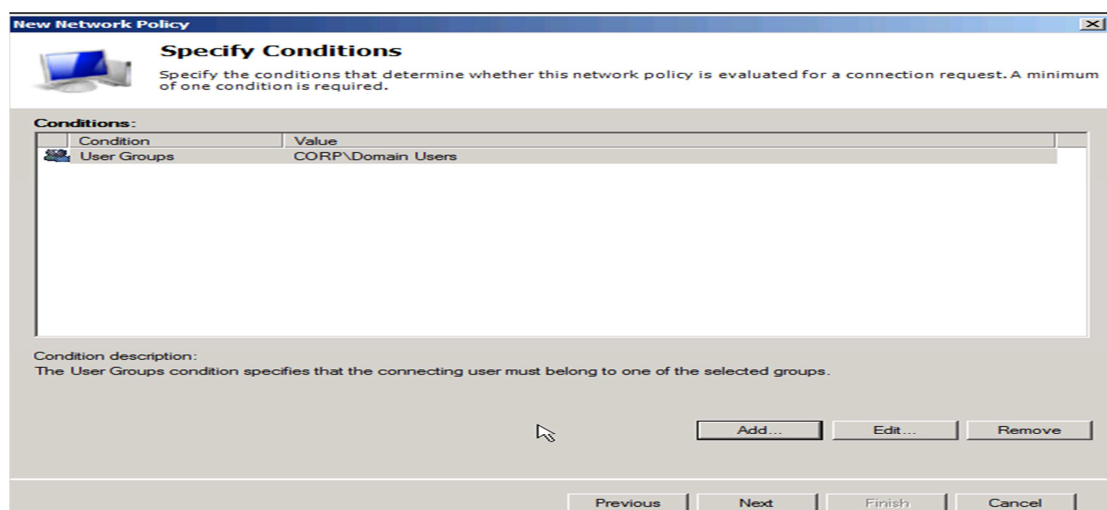
4. Click a **New** under **NPS(Local)->Policies->Network Policies**.



5. Specify the **Policy name** and then click the **Next** button.



6. Add the domain user group in to the condition:



7. Specify **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 granted**
Grant access if client connection attempts match the conditions of this policy.

☐ **Access denied**
Deny access if client connection attempts match the conditions of this policy.

☐ **Access is determined by User Dial-in properties (which override NPS policy)**
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

8. Configure Authentication Methods as follows:

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:

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

1

Previous Next Finish Cancel

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.

Settings:

RADIUS Attributes

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 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.

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add... Edit... Remove

Previous Next Finish Cancel

New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

802.1x

Policy conditions:

Condition	Value
User Groups	CORP\Domain Users

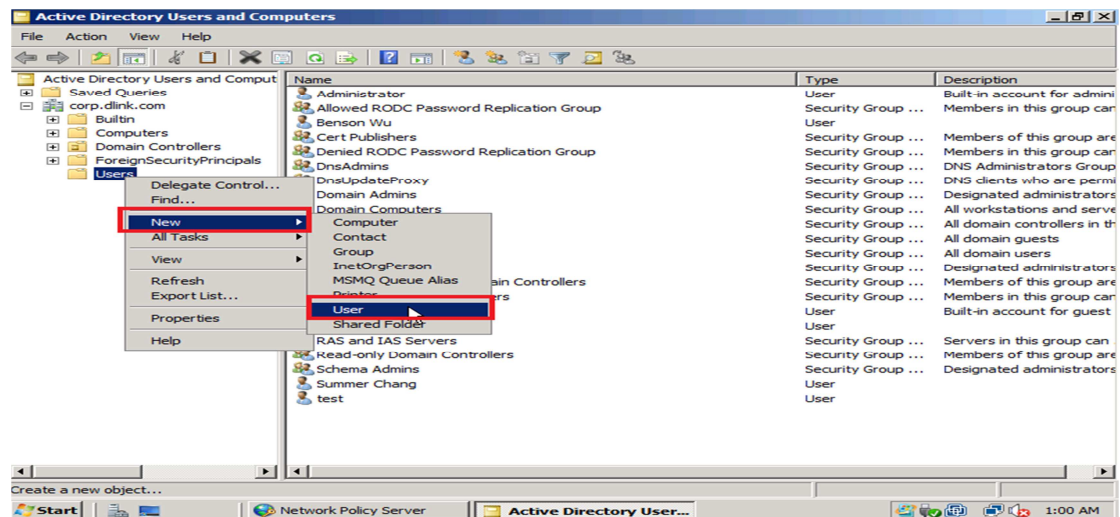
Policy settings:

Condition	Value
Authentication Method	EAP OR Unencrypted authentication (PAP, SPAP)
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

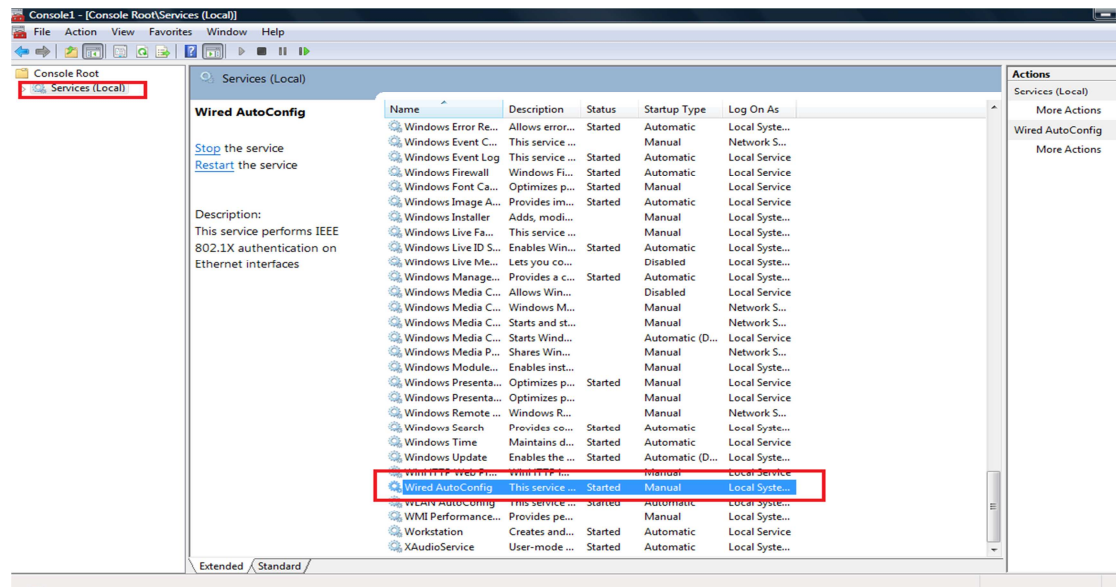
Previous Next Finish Cancel

9. Add user under **Active Directory Users and Computers**.

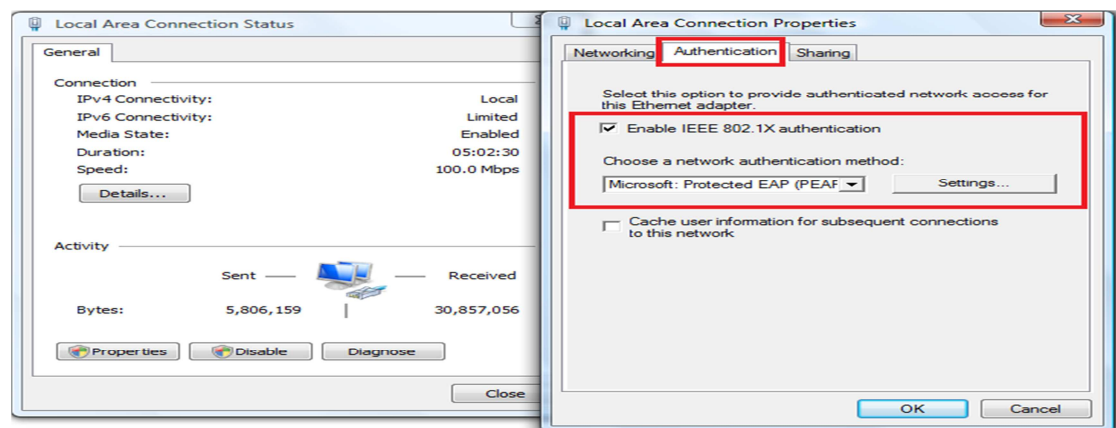


[Client Vista]:

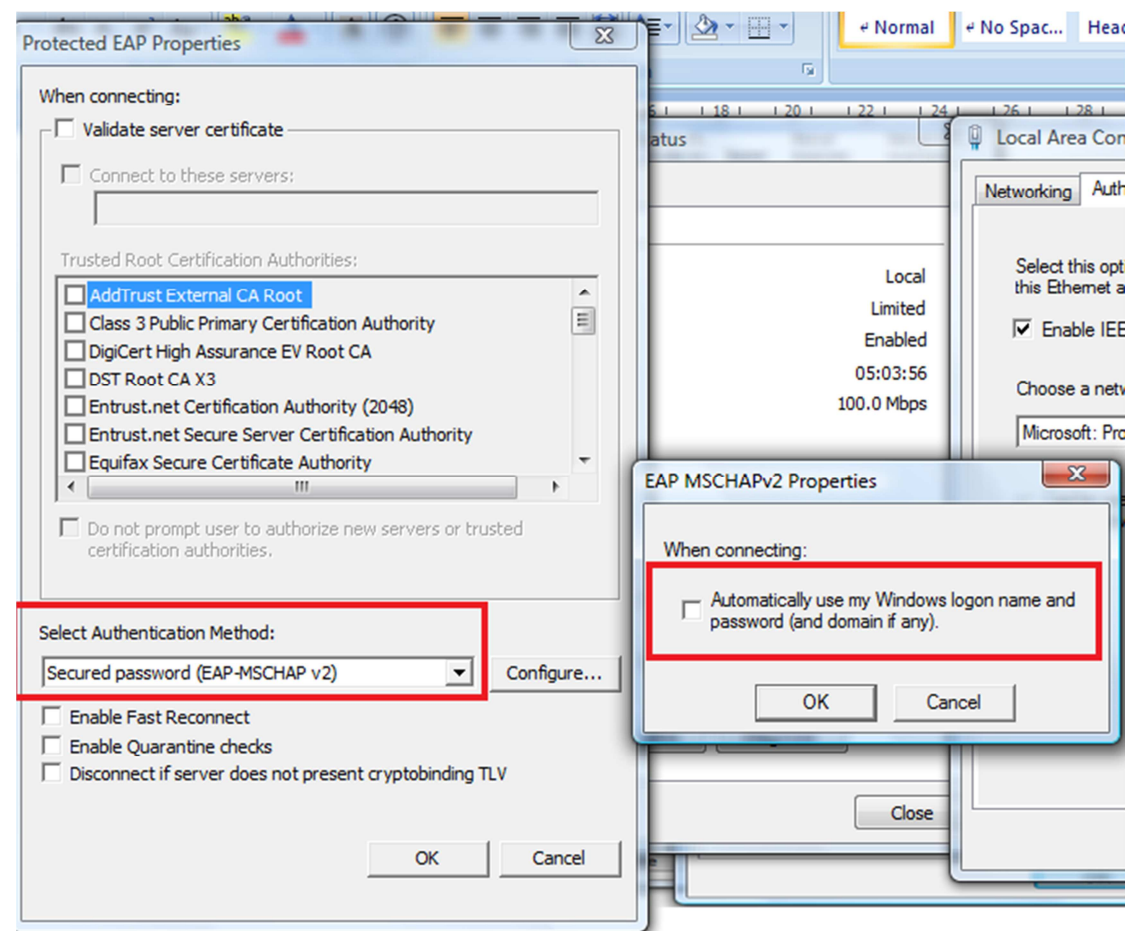
1. Use the MMC and go to the **Services**, check the **Wired AutoConfig** services is Started.



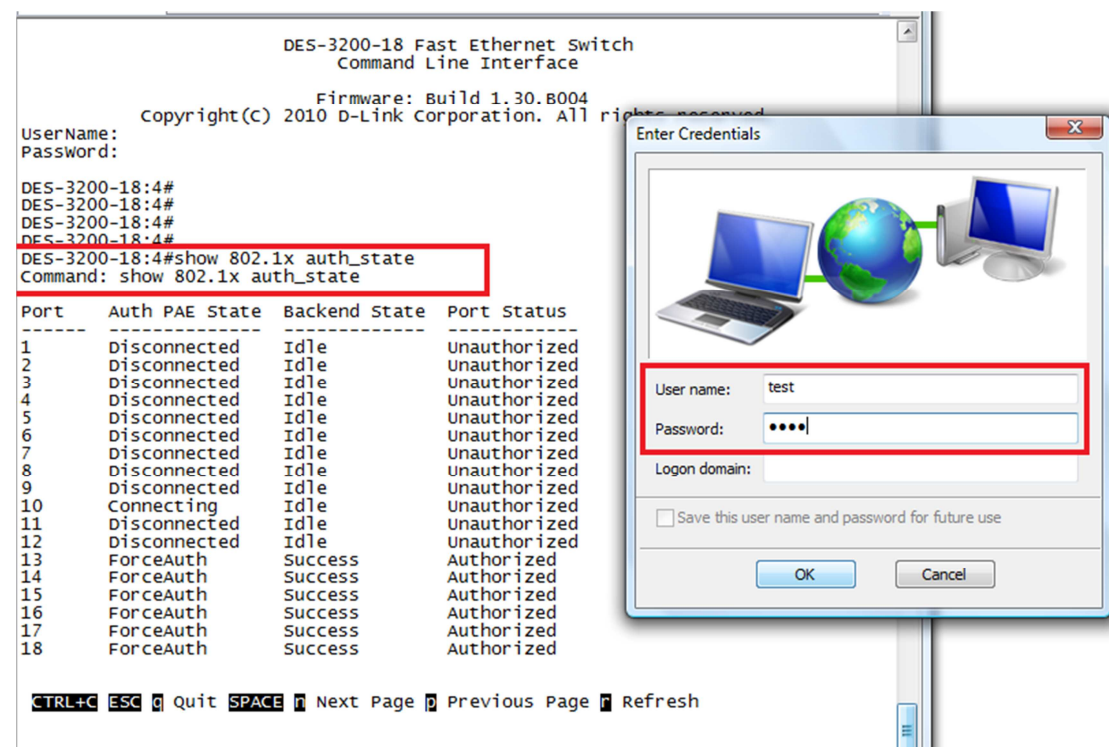
2. Under the NIC setting, make sure the **Authentication** tab come up. Then click the **Settings** button.



3. Click the **Configure..** button and disselect the **Automatically.....**



[Testing Result]:



DES-3200-18:4#show 802.1x auth_state
Command: show 802.1x auth_state

Port	Auth PAE State	Backend State	Port Status
1	Disconnected	Idle	Unauthorized
2	Disconnected	Idle	Unauthorized
3	Disconnected	Idle	Unauthorized
4	Disconnected	Idle	Unauthorized
5	Disconnected	Idle	Unauthorized
6	Disconnected	Idle	Unauthorized
7	Disconnected	Idle	Unauthorized
8	Disconnected	Idle	Unauthorized
9	Disconnected	Idle	Unauthorized
10	Authenticated	Idle	Authorized
11	Disconnected	Idle	Unauthorized
12	Disconnected	Idle	Unauthorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized