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.

🞭 Network Policy Serve	r							_ 8	×
File Action View Hel	lp .								
🧇 🔿 🖄 🔝 👔 i									
NPS (Local) RADIUS Clients and RADIUS Clients RADIUS Clients RADIUS Clients Remote RADIUS	Servers New RADIUS	5 Client	RADIUS cli	ents allow you	to specify the network a	ccess servers, th	hat provide access to	o your network.	
	ExportList	10	ly Name	IP Address	Device Manufacturer	NAP-Capable	Status		
Connection Red	View	•	S-3200-28	192.168.0.1	RADIUS Standard	No	Enabled		
Real Pointes Network Access Pro Accounting	Help								
New Network Access Device]	
😂 Start 🛛 🚠 📃	🔤 😔 Net	work Polic	y Server				🗳 🏟 🕀	🔁 🏚 12:44 Al	м

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

New RADIUS Client	×
Enable this RADIUS client	
Name and Address	
DES-3200-28	
Address (IP or DNS):	
192.168.0.1	Verify
Vendor Specify RADIUS Standard for most RADIUS clients, or select the RAI vendor from the list.	DIUS client
Vendor name:	
RADIUS Standard	-
To manually type a shared secret, click Manual. To automatically gen secret, click Generate. You must configure the RADIUS client with th secret entered here. Shared secrets are case-sensitive. Manual Generate Shared secret:	erate a shared e same shared
•••••	
Confirm shared secret:	
•••••	
Additional Options Access-Request messages must contain the Message-Authentica RADIUS client is NAP-capable	tor attribute
ОК	Cancel

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

Network Policy Server		_ 8 ×
File Action View Help		
🗢 🔿 🖄 📷 🔽 🖬		
NPS (Local) RADUS Clients and Servers RADIUS Clients RADIUS Clients RADIUS Server Groups	Network policies allow you to designate who is authorized t circumstances under which they can or cannot connect.	o connect to the network and the
Policies Connection Request Policies	BADIUS	Disabled 1 Grant Access
Network Policies	RADIUS PUL SWITCH	Disabled 7 Grant Access
Health Policies New	802 1v test	Enabled 3 Grant Access
🕀 🎭 Network Access Pt 🛛 Export List	Connections to Microsoft Routing and Remote Access server	Disabled 4 Deny Access
Accounting		
View P		
Refresh	802.1x_test	
Help	Conditions - If the following conditions are met:	<u> </u>
	Condition Value User Groups CORP\Domain Users	
	Settings - Then the following settings are applied:	
	Setting Value	▲
	Access Permission Grant Access	
	Extensible Authentication Protocol Method Microsoft: Protected	EAP (PEAP) OR Microsoft: Secured p
	Authentication Method EAP OR Unencrypt	ed authentication (PAP, SPAP)
	N	
New		
🎝 Start 📋 🚠 📰 👘 🐼 Networ	k Policy Server	🗳 😡 🗊 🍙 12:50 AM

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

New Network P	'olicy	×
	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	:	
802.1x		_
□ Network conne	ection method	
Select the type type or Vendor	o of network access server that sends the connection request to NPS. You can select either the network access server specific.	
 Type of ne 	twork access server:	
Unspecifie	ed 💌	
C Vendor spe	sofic:	
10		
	Previous Next Finish Cancel	

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

New Network P	olicy		×
	Specify the c	Conditions onditions that determine whether this network policy is evaluated for a connection re ion is required.	quest. A minimum
Conditions:			
Condition	i se	Value	
User Grou	ups	CORP\Domain Users	
Condition descr	ription:		
The User Group	ps condition sp	ecfies that the connecting user must belong to one of the selected groups.	Remove
		Previous Next Finish	Cancel

7. Specify Access granted and click Next:

New Network P	olicy
	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 se	Inted as if client connection attempts match the conditions of this policy. hed is if client connection attempts match the conditions of this policy. Idetermined by User Dial-in properties (which override NPS policy) ny access according to user dial-in properties if client connection attempts match the conditions of this policy.
	L3
	Previous Next Finish Cancel

8. Configure Authentication Methods as follows:

Image: Second	Configure Authentication Methods Explose a constraint of the second of the	w Network Po	olicy	
EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types: Microsoft: Protected EAP (PEAP) Add Edit Remove Add Edit Remove Less secure authentication methods: User can change password after it has expired Encrypted Authentication (CHAP) User can change password after it has expired Encrypted authentication (CPA, SPAP) Allow clients to connect without negotiating an authentication method. Add Particle Protected	EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types: Microsoft: Protected EAP (PEAP) Add Edt Remove Less secure authentication methods: Microsoft Encrypted Authentication (MS-CHAP-v2) User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Forcypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method. Forcypted method charge the authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method.		Configure Authentication Methods Configure one or more authentication methods required for the connection request to match this policy. For EA 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.	P
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) User can change password after it has expired Addemice the secure authentication (CHAP) Unercorpted authentication (CPAP, SPAP) Allow clients to connect without negotiating an authentication method.	Add Edt Remove Less secure authentication methods: Microsoft Encrypted Authentication (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 (PAP, SPAP) Allow clients to connect without negotiating an authentication method. Perform machine health check only	AP types are no AP Types: Microsoft: Prot	ected EAP (PEAP)	
Add Edit Remove Less secure authentication methods: Image: Secure authentication (MS-CHAP-v2) User can change password after it has expired Image: Secure authentication (MS-CHAP) Image: User can change password after it has expired Image: Secure authentication (CHAP) Image: User can change password after it has expired Image: Secure authentication (CHAP) Image: User can change password after it has expired Image: Secure authentication (CHAP) Image: User can change password after it has expired Image: Secure authentication (CHAP) Image: User can change password after it has expired Image: Secure authentication (CHAP) Image: User can change password after it has expired Image: Secure authentication (CHAP) Image: User can change password after it has expired Image: Secure authentication (CHAP) Image: User can change password after it has expired Image: Secure authentication (CHAP) Image: User can change password after it has expired Image: Secure authentication (CHAP) Image: User can change password after it has expired Image: Secure authentication (CHAP) Image: User can change password after it has expired Image: Secure authentication (CHAP) Image: User can change password after it has expired Image: Secure authenticatit has expired Image: U	Add Edit Remove Less secure authentication methods: Microsoft Encrypted Authentication (VIS-CHAP-v2) User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired S Encrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method. Perform machine health check only S		Move Down	
		Add	Edit Remove	
		User car	norpped Authentication Version 2 (MSCHAP-V2) In change password after it has expired	
Unencrypted authentication (FAP, SFAP) Allow clients to connect without negotiating an authentication method. Defense mechanism backter shealth action is a set of the set of	Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method. Perform machine health check only	User car	Inclypted Authentication (IN-S-CHAP) T change persword after it has expired Untertication (CHAP)	
renorm machine health check only		Allow clients	d authentication (rAF, SFAF) s to connect without negotiating an authentication method. chine health check only	

New Network F	Policy	×
	Configure Co Constraints are addii constraint is not mat optional; if you do n	nstraints tional parameters of the network policy that are required to match the connection request. If a ched by the connection request, NPS automatically rejects the request. Constraints are ot want to configure constraints, click Next.
Configure the if all constraints Constraint	constraints for this networks are not matched by the same not matched by the second se	rk policy. a 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 T
		Previous Next Finish Cancel

ew Network Policy	
Configure Se	ettings
NPS applies settings are matched.	a to the connection request if all of the network policy conditions and constraints for the policy
Configure the settings for this network If conditions and constraints match the	policy. e 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	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 Add Edit
IP Settings	
	Previous Next Finish Cancel
Completing	New Network Policy
You have successfully created the for 802.1x	llowing network policy:
Condition Value User Groups CORP\Domain Users	
Policy settings:	
Condition Authentication Method Access Permission Update Noncompliant Clients NAP Enforcement Framed-Protocol Service-Type	Value EAP OR Unencrypted authentication (PAP, SPAP) Grant Access True Allow full network access PPP Framed
To close this wizard, click Finish.	k,

9. Add user under Active Directory Users and Computers.

Active Directory Users and Com	puters		_ <u>=</u> = ×
(= -> <u>2</u> 📰 2 🗀 🗙 🖸] o 🖦 🛛 🖬 🔧 📚 😭 🍸 🗾 🍇		
Active Directory Users and Comput	Name	Type	Description
a) Saved Queries Barrow Computers Computers Domain Controllers PoreignSecurityPrincipals Users Delegate Control Find New Afresh Export List Properties Help	Administrator Administrator Benson Wu Cert Publishers Densd RODC Password Replication Group DonsAdmins Donsid Goog Donsin Admins Domain Computers Computer Computer Contact Group InctorgPerson MSMQ Queue Alias Shared Folder RAS and IAS Servers Kead-only Domain Controllers Summer Chang Lest	User Security Group User Security Group Security Group User User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Bullt-in account for admin Members in this group can Members in this group can DNS deministrators Group DNS deninistrators Group DNS dents who are perm Designated administrator All workstations and serv All domain controllers in t All domain guests All domain users Designated administrator Members of this group an Members of this group can Members of this group an Designated administrator
I	4		•
Create a new object			
reate a new object	(J	

[Client Vista]:

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

Services (Local)								Actions
Services (Local)								Services (Local)
Wired AutoConfig	Name	Description	Status	Startup Type	Log On As		^	More Actio
_	Windows Error Re	Allows error	Started	Automatic	Local Syste			Wired AutoCor
Stop the convice	Windows Event C	This service		Manual	Network S			
Stop the service	🖓 Windows Event Log	This service	Started	Automatic	Local Service			More Acti
Restart the service	Windows Firewall	Windows Fi	Started	Automatic	Local Service			
	🖓 Windows Font Ca	Optimizes p	Started	Manual	Local Service			
	🖓 Windows Image A	Provides im	Started	Automatic	Local Service			
Description:	G Windows Installer	Adds, modi		Manual	Local Syste			
This service performs IEEE	Windows Live Fa	This service		Manual	Local Syste			
802.1X authentication on	Windows Live ID S	Enables Win	Started	Automatic	Local Syste			
Ethernet interfaces	Windows Live Me	Lets you co		Disabled	Local Syste			
	G Windows Manage	Provides a c	Started	Automatic	Local Syste			
	Windows Media C	Allows Win		Disabled	Local Service			
	🖓 Windows Media C	Windows M		Manual	Network S			
	🖓 Windows Media C	Starts and st		Manual	Network S			
	Windows Media C	Starts Wind		Automatic (D	Local Service			
	Windows Media P	Shares Win		Manual	Network S			
	Windows Module	Enables inst		Manual	Local Syste			
	🖓 Windows Presenta	Optimizes p	Started	Manual	Local Service			
	🖓 Windows Presenta	Optimizes p		Manual	Local Service			
	🖓 Windows Remote	Windows R		Manual	Network S			
	G Windows Search	Provides co	Started	Automatic	Local Syste			
	🖓 Windows Time	Maintains d	Started	Automatic	Local Service			
	Windows Update	Enables the	Started	Automatic (D	Local Syste			
	WINI ITTP Web Pl	**********		ivianuai	Local Service			
	🔅 Wired AutoConfig	This service	Started	Manual	Local Syste			
	WEAN Autocoming	This service	Started	Automatic	LOCAL Syste	1	=	
	WMI Performance	Provides pe		Manual	Local Syste			
	Sk Workstation	Creates and	Started	Automatic	Local Service			
	AudioService	User-mode	Started	Automatic	Local Syste		+	

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

Uccal Area Connection Status	Uccal Area Connection Properties
General	Networking Authentication Sharing
Connection IPv4 Connectivity: Local IPv6 Connectivity: Limited Media State: Enabled Duration: 05:02:30 Speed: 100.0 Mbps Details	Select this option to provide authenticated network access for this Ethemet adapter. Enable IEEE 802.1X authentication Choose a network authentication method: Microsoft: Protected EAP (PEAF Settings Cache user information for subsequent connections to this network
Activity Sent Received Received Bytes: 5,806,159 30,857,056	
Properties Tisable Diagnose Close	OK Cancel

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

Protected EAP Properties	e Normal + No Spac Hea
When connecting: Validate server certificate Connect to these servers:	atus
Trusted Root Certification Authorities: AddTrust External CA Root Class 3 Public Primary Certification Authority DigiCert High Assurance EV Root CA DST Root CA X3 Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority	Local Limited Enabled 05:03:56 100.0 Mbps Microsoft: Pro
Equifax Secure Certificate Authority Equifax Secure Certificate Authority Do not prompt user to authorize new servers or trusted certification authorities.	EAP MSCHAPv2 Properties
Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure	Automatically use my Windows logon name and password (and domain if any). OK Cancel
Enable 1 ast Reconnect Enable Quarantine checks Disconnect if server does not present cryptobinding TLV OK Cancel	

[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 2 3 4 5 6 7 8	Disconnected Disconnected Disconnected Disconnected Disconnected Disconnected Disconnected	Idle Idle Idle Idle Idle Idle Idle Idle	Unauthorized Unauthorized Unauthorized Unauthorized Unauthorized Unauthorized Unauthorized Unauthorized
10	Authenticated	Idle	Authorized
11 12 13 14 15 16 17 18	Disconnected Disconnected ForceAuth ForceAuth ForceAuth ForceAuth ForceAuth ForceAuth	Idle Success Success Success Success Success Success Success	Unauthorized Unauthorized Authorized Authorized Authorized Authorized Authorized Authorized

н