How to setup MAC-Based-Access-Control with Microsoft Windows Server 2008 NPS

[Topology] Client-----DGS-3120-----RADIUS Server (p2) (p24) 10.90.90.90 10.90.90.201

1. Install NPS role on Windows Server 2008.

Server Roles Server Roles Confirmation Progress Results	Select one or more roles to install on this server. Roles: Active Directory Certificate Services Active Directory Pederation Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services DHCP Server DHCP Server Fax Server File Services Vietwork Policy and Access Services (Installed) Print Services UDDI Services UDDI Services Web Server (IIS) Windows Deployment Services Windows Server Update Services	Description: Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
	Windows Deployment Services Windows Server Update Services	

2. Create a new username as allowed host MAC address, password is "dlink".

Computer Management File Action View Help						-DX
(= =) 2 📰 G 😖 🚺	•					
Computer Management (Local) System Tools S	Name Name New User User name: Full name: Description: Password: Confirm password User canno User canno V Password n Account is: Help	Full Name F0def1932de2 F0def193 F0def19 F0def193 F0def193 F0def193 F0def19 F0def193 F0def19 F0def193 F0def19 F0def19 F0def193 F0def19 F0def1	logon	2 × rir et	Actions Users More Actions	*
Ctaut 1 2 m	A l	s Antwork B	alicu Saruar			10+57 AM

3. Add RADIUS client (Switch) into NPS, key is 123456.

Network Policy Server	New RADIUS Client	X					
File Action View Help	Enable this RADIUS client						
s - 2 🖬 🛛 🖬	□ Name and Address Friendly name:						
S NPS (Local)	3120						
RADIUS Clients and Serve	Address (IP or DNS):						
Remote RADIUS Serve	10.90.90	Verify					
I Policies Network Access Protection Accounting	Vendor Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.						
	RADIUS Standard	•					
	To manually type a shared secret, click Manual. To automatically generate secret, click Generate. You must configure the RADIUS client with the secret entered here. Shared secrets are case-sensitive.	rate a shared same shared					
	Confirm shared secret:						
	•••••						
	Additional Options Additional Options Access-Request messages must contain the Message-Authenticato	or attribute					
Action: In progress	ОК	Cancel					
灯 Start 📋 🚠 💼 👘 🗍	Network Connections						

4. Create NPS policy as "RADIUS server for 802.1x Wireless or Wired connections".



5. Select Secure Wired (Ethernet) Connections.

🚯 Network Policy S	Configure 802.1X	×	
File Action View	Select 802.1X Connections Type		
RADIUS CI Remote RJ Delices Network Acces	Type of 802.1X connections: C Secure Wireless Connections When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points. C Secure Wired (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet clients connecting through the switches. Name: This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify a.		ard.
1	Secure Wired (Ethemet) Connections Previous Next Firrish Cancel]	s (also called
🖉 Start 🛛 🚠 📼	Network Connections		10:56 AM

6. EAP Type select "EAP-MSCHAP v2".

Network Policy S	Configure 802.1X	× <u> </u>
File Action View	Configure an Authentication Method	
RADIUS C	Select the EAP type for this policy.	ccess policies for
Connectio	Microsoft: Secured password (EAP-MSCHAP v2)	
Accounting		ard.
		es that allow NPS
		s (also called
•	Previous Next Firnish Cancel	
🎊 Start 🗌 🏭 📰	👔 Network Co 📀 Network Pol 🔠 Computer 🚠 Server Man 🎼 Configure	🔄 🚯 🕼 11:05 AM

7. Add user groups.

Network Policy S	Configure 802.1X	×	×
File Action View Image: state s	Specify User Groups Users that are members of the selected group or groups will be allower based on the network policy Access Permission setting.	d or denied access	
RADIUS CI Remote R/ Policies Connection Network P	To select User Groups, click Add. If no groups are selected, this policy applies to all users. Groups	Add	ccess policies for
Health Poli	Select Group Select this object type:	Remove	ard.
	Group Object Ty From this location: VWIN2KS-1 Location	vpes	es that allow NPS s (also called
	Erter the object name to select (<u>examples</u>): VWIN2K8-1\Users Check N	lames	
	Advanced OK Car		
	Previous Next Firith	Cancel	

- 8. Clieck "next" to finish.
- 9. Edit the policy, select "constraints" label. And check below options. Then click "OK" and ignore warning message.

O I C tu Coostminte	e	
Overview Conditions Constraints Configure the constraints for this net if all constraints are not matched by t Constraints:	Settings vork policy. ne connection request, network access is denied.	
Constraints Authentication Methods Session Timeout Called Station ID Day and time restrictions NAS Port Type	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: Secured password (EAP-MSCHAP v2) Move Up Move Down Add Edit Bemove Less secure authentication methods: Where can change password after it has expired Wicrosoft Encrysted Authentication (MS-CHAP) Wicrosoft Encrysted Authentication (MS-CHAP) Wier can change password after it has expired Wicrosoft Encrysted Authentication (MS-CHAP) Wier can change password after it has expired Wicrosoft Encrysted Authentication (PAP) Wier can change password after it has expired Wier can change password after it has expired Wie	

Apply below command on switch:

config mac_based_access_control method radius

config mac_based_access_control password dlink //this password must be the same to step 2

config mac_based_access_control ports 1:1-1:8 state enable

enable mac_based_access_control

config radius add 1 10.90.90.201 key 123456 default //this key must be the same to step 3

After connect client on port 2, you can see RADIUS-Accept packet on Server side.

K Re	altek RTL8139	/810	x Family	Fast	Ether	net N	VIC					ireshi	ark								_
Eile	<u>E</u> dit <u>V</u> iew	Go	Captur	e A	nalyz	e S	tatistic	s T	elep	hony	Io	ols	Help								
			86	*	2	8	10	\$	~	•	3	\$		€ €				¥ 🗹	•	*	
Filter	radius											•	Expression.	Clear	Арр	oły					
No.	Time		Source							C	estin	ation	i				Prot	tocol			Info
	2 18.5547	97	10.90.	. 90.	90					1	.0.9	0.90	0.201				RAE	DIUS			Access-Request(1) (id=1, 1=103)
	5 19.1126	18	10.90	. 90.	201	1				1	.0.9	0.90	0.90				RAI	DIUS			Access-Accept(2) (id=1, 1=78)

🗑 Frame 5: 120 bytes on wire (960 bits). 120 bytes captured (960 bits)	
B Ethernet II, Src: Microsof_40:75:fd (00:03:ff:40:75:fd), Dst: ac:f1:df:b4:ce:20 (ac:f1:df:b4:ce:20)	
B Internet Protocol, Src: 10.90.90.201 (10.90.90.201), Dst: 10.90.90.90 (10.90.90.90)	
🗄 User Datagram Protocol, Src Port: radius (1812), Dst Port: intu-ec-client (8021)	
B Radius Protocol	

And show port status on Switch:

DGS-3120-24TC:admin#show mac_based_access_control auth_state ports 2 Command: show mac_based_access_control auth_state ports 1:2

(P): Port-based

Port	MAC Address	State	VID	Priority	Aging Time/ Block Time
1:2	F0-DE-F1-93-2D-E2	Authenticated	1	-	1440
Tota Tota Tota	l Authenticating Hosts l Authenticated Hosts l Blocked Hosts	5 : 0 : 1 : 0			

DGS-3120-24TC:admin#