

Descripcion – Configuracion de servidor de autenticacion Radius utilizando Windows Server con Active Directory en switches administrables de D-Link (Utilizaremos como ejemplo el DGS-3426)

## Configuración en Windows Server

Paso 1 – Crear usuario

	🛓 🔽 🖬 🔏 🍇	G 7 2 &	
Active Directory Users and Comput	Name	Туре	Description
🗄 🧾 Saved Queries	& Administrator	User	Built-in account for admini
E 📰 test2008.com	Allowed RODC P	Security Group	Members in this group can
🕀 🧾 Builtin	Cert Publishers	Security Group	Members of this group are
Computers	Benied RODC Pa	Security Group	Members in this group can
Domain Controllers	A DnsAdmins	Security Group	DNS Administrators Group
ForeignSecurityPrincipals	& DnsUpdateProxy	Security Group	DNS clients who are permi
Users	& Domain Admins	Security Group	Designated administrators
	Bomain Computers	Security Group	All workstations and serve
	Bomain Controllers	Security Group	All domain controllers in th
	Somain Guests	Security Group	All domain guests
	Somain Users	Security Group	All domain users
	& Enterprise Admins	Security Group	Designated administrators
	& Enterprise Read	Security Group	Members of this group are
	Sroup Policy Cre	Security Group	Members in this group can
	🔒 Guest	User	Built-in account for guest
	A operator	Security Group	
	RAS and IAS Ser	Security Group	Servers in this group can
	Read-only Domai	Security Group	Members of this group are
	Schema Admins	Security Group	Designated administrators
	& test2	User	1111111111



Paso 2 – Abrir la consola NPS y seleccionar **RADIUS for 802.1x wireless or weird connections** y luego haga click en **Configure 802.1X** 



Paso 3 – Seleccione la opcion Secured Wired (Ethernet) Connections



Paso 4 – Agregue el Cliente Radius configurando un nombre, La IP del Switch y una contraseña (en el ejemplo la contraseña sera 123456)

figure.	450 Properties	×	
	Name and Address Friendly name:		
	3450		
0	Address (IP or DNS):		
	10.90.90.90 Verify		
ADIUS	Shared Secret		ot
ent cc	To manually type a shared secret, click Manual. To automatically generate a share	ed	
spec	secret, click Generate. You must configure the RADIUS client with the same shar secret entered here. Shared secrets are case-sensitive.	ed	
150			
100	Manual     O     Generate		8
	Shared secret:		2
	•••••	5	ve
	Confirm shared secret:	ΗË	*•
	OK Const	- 1	
	OK Cancel		

Paso 5 – Seleccione el metodo de autenticacion EAP-MSCHAP v2

onfigure 802.1X	
Configure an Authentication Met	hod
Select the EAP type for this policy.	
Type (based on method of access and network configuration)	
Microsoft: Secured password (EAP-MSCHAP v2)	✓ Configure
Microsoft: Secured password (EAP-MSCHAP v2)	Configure
Microsoft: Secured password (EAP-MSCHAP v2)	Configure
Microsoft: Secured password (EAP-MSCHAP v2)	Configure

Paso 6 – Agregue grupo de usuarios como **Domain User** 

	Specify User Groups Users that are members of the selected group based on the network policy Access Permission	or groups will be allowed o 1 setting,	or denied access
select U	ser Groups, click Add. If no groups are selected, this po	licy applies to all users.	Add
TEST200	8\Domain Users		Remove



Paso 7 – Una vez creada la politica se deben editar algunas opciones

🞭 Network Policy Server					
File Action View Help					
🗢 🧼 🙇 📅 🚺 🖬					
NPS (Local)     ADIUS Clients and Servers     ADIUS Clients     RADIUS Clients     Remote RADIUS Server G	Network policies allow you to designate who is authorized under which they can or cannot connect.	to connect t	o the network and th	ne circumstance	s
E Policies	Policy Name	Status	Processing Order	Access Type	S
Connection Request Polici	Secure Wired (Ethernet) Connections	Enabled	1	Grant Access	U
i Network Policies	Connections to Microsoft Routing and Remote Access server	Enabled	2	Deny Access	U
📔 Health Policies	Connections to other access servers	Enabled	3	Deny Access	U.,

Paso 8 – ingrese a la pestaña **Settings** para añadir atributos adicionales a Radius

anviour   Conditiona   Constraints	tings		
onfigure the settings for this network po conditions and constraints match the co attings:	licy. onnection request and the po	olicy grants access, settings a	are applied.
RADIUS Attributes	To send additional attr then click Edit. If you o	ibutes to RADIUS clients, se do not configure an attribute,	lect a Vendor Specific attribute, and it is not sent to RADIUS clients. See
🚰 Vendor Specific	your notion clone de	camentation for required attr	Dates:
Network Access Protection			
NAP Enforcement	Attributes:		
Network State	Name	Vendor	Value
Routing and Remote Access		41	
🔏 Multilink and Bandwidth			



Paso 9 – Seleccione **Custom** luego ingrese el **D-Link vendor Code** con el valor de **171**. Mas abajo marque la opcion **Yes. It conforms** y luego haga click en **Configure Attributes** 

Add Vendor	Specific Attribute	×
To add an at	tribute to the settings, select the attribute, and then click Add.	
To add a Ver	ndor Specific attribute that is not listed, select Custom, and then click Add.	
Vendor:		
Custom		
Attributes:		
Name	Vendor	
Vendor-Spe	ecific RADIUS Standard	

Attribute name: Vendor Specific	
Specify network access se	erver vendor.
C Select from list:	RADIUS Standard
• Enter Vendor Code:	171 🕂
Specify whether the attribut	te conforms to the RADIUS REC specification for
vendor specific attributes.	
vendor specific attributes.	
<ul> <li>vendor specific attributes.</li> <li>Yes. It conforms</li> <li>No. It does not conform</li> <li>Configure Attribute</li> </ul>	



Paso 10 – En la siguiente ventana configure **Vendor-assigned attribute number** con el valor **1** para autorización de la cuenta de usuario

Attribute Value:

- 3 = Nivel de usuario
- 4 = Nivel de operador
- 5 = Nivel de administrador

En el ejemplo utilizaremos el 4 (operador)

/endor-assigned a	attribute number:	
Attribute format:		
Decimal		
Attribute value:		
4		

Paso 11 – Ingrese a la pestaña Constraints, configure **Authentication Method** como acontinuacion

figure the constraints for this network	policy.
constraints are not matched by the o	connection request, network access is denied.
onstraints	Allow access only to those clients that authenticate with the specified methods
Authentication Methods	y now becease only to a rose circles and barrenticate with the specified methods.
ldle Timeout	EAP types are negotiated between NPS and the client in the order in which they are
Session Timeout	listed.
Called Station ID	EAP Types:
Day and time restrictions	Microsoft: Secured password (EAP-MSCHAP v2)
NAS Port Type	MoveDown
#0 3001	<b>x</b>
	Add Edit Remove
	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
	✓ Unencrypted authentication (PAP, SPAP)
	Allow clients to connect without negotiating an authentication method
	Perform machine health check only

Como configurar Active Directory con NPS (Radius) en switches D-Link



## Configuración en el Switch

Paso 12 – En el Switch aplique los siguientes comandos

## enable authen\_policy

create authen server\_host 10.90.90.201 protocol radius key 123456

config authen application telnet login method\_list\_name radius

create authen\_login method\_list\_name radius

config authen\_login method\_list\_name radius method radius

Paso 13 – Ingresar al switch por telnet con el usuario creado anteriormente test2

