#### Autenticación de acceso inalámbrico integrando RouterOS y Microsoft Windows Server

MUM Bogotá - Colombia 2019

by:

Lucas Aguilera





#### Sobre mi

- Lucas Aguilera
- Ingeniero electrónico
- Trainer de Mikrotik TR
- CTO de la empresa Two Networks
- Dentro del mundo del TI desde el 2000
- Conociendo Mikrotik desde el 2010





#### **Two Networks**

Empresa radicada en Santiago de los Caballeros en República Dominicana. Dedicada a la gestión e integración de sistemas de información. Además, el desarrollo y acompañamiento de proyectos tecnológicos.

Somos partner autorizado de: Google, Microsoft, PRTG, Kaspersky, Acronis, 3CX, entre otros.





#### **Two Networks**

Dentro de nuestro catálogo de servicios, brindamos:

- Gestión de redes de información
- Cableado estructurado
- Implementación de equipos activos (routers y switches)
- Redes inalámbricas indoor y outdoor
- Inteligencia de riesgo
- Copias de respaldo en la nube
- Entrenamientos





#### Contenido

- Objetivos
- Conceptos sobre 802.1X
- Configurando NPS en Windows Server 2012
- Configurando CAPsMAN
- Configurando el CAP
- Configuración de Radius en el Mikrotik





## Objetivos

Dar a conocer sobre el standard 802.1X y su funcionamiento

- Mostrar como realizar la configuración del NPS de Windows Server 2012 para lograr la integración con Mikrotik
- Mostrar al configuración del CAPsMAN de Mikrotik





#### La realidad

- Un solo SSID para todo y para todos
- Se prostituye la clave. Hasta el vecino la tiene
- No existe un control de acceso hacia nuestra red empresarial





#### Los beneficios

Tendremos un control real sobre los usuario que se conectarán

- Si la clave de un usuario se ve comprometida, es fácil de realizar el cambio
- Si el usuario sale de empresa, simplemente en borrar o deshabilitar el usuario





#### Conceptos de 802.1X

Estándar creado por la IEEE para brindar seguridad de la red, mediante la autenticación del dispositivo antes de concederle acceso

Funciona para redes Ethernet e inalámbricas (802.11)

Fue impulsado antes de que WEP saliera al mercado, ya que desde su nacimiento venía por problemas de vulnerabilidad conocidos

En dicho estándar convergen tres entes: suplicante, autenticador y el servidor de autenticación.





#### Conceptos de 802.1X



Fuente: Wikipedia





#### Conceptos de 802.1X

Para que el 802.1X puede funcionar, se requerirán tres protocolos:

**Extensible Authentication Protocol (EAP):** este realizará el proceso de autenticación entre el suplicante hacia el servidor de autenticación

**EAP over LAN (EAPOL):** Transporta la comunicación entre el suplicante y el autenticador

**Remote Authetication Protocol (RADIUS):** se encarga de transportar los mensajes EAP entre el autenticador y el servidor de autenticación





#### Dot1x

- Nuevo módulo de RouterOS agregado en la versión 6.45.1
- Permite que RouterOS sea suplicante y autenticador
- El suplicante soporta varios métodos de EAP
- Implementación en empresas con estándares como la ISO 27002





#### Dot1x







#### Prerrequisitos

Tener instalado el Windows Server 2012 como controlador de dominio, Windows Certified Authority y todos sus patches aplicados

Tener el equipo Mikrotik que será el CAPsMAN y los CAPs actualizados, preferiblemente, con la misma versión de RouterOS











	Add Roles and Features Wizard	
Select server roles Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles and Features Wizard         Select one or more roles to install on the selected server.         Roles         Active Directory Certificate Services         Active Directory Domain Services (Installed)         Active Directory Federation Services         Active Directory Lightweight Directory Services         Active Directory Rights Management Services         Application Server         DHCP Server         DNS Server (Installed)	DESTINATION SERVER 2NLAB.lab.local      Description      Network Policy and Access Services provides Network Policy Server (NPS), Health Registration Authority     (HRA), and Host Credential Authorization Protocol     (HCAP), which help safeguard the health and security     of your network.
	<ul> <li>DNS Server (Installed)</li> <li>Fax Server</li> <li>File and Storage Services (2 of 12 installed)</li> <li>Hyper-V</li> <li>Network Policy and Access Services</li> <li>Print and Document Services</li> <li>Remote Access</li> <li>Remote Desktop Services</li> <li>Volume Activation Services</li> <li>Volume Activation Services</li> <li>Web Server (IIS)</li> <li>Windows Deployment Services</li> <li>Windows Server Essentials Experience</li> <li>Windows Server Update Services</li> </ul>	2
	< P.	revious Next > Install Cancel





6	Add Roles and Features Wizard	- 0 ×
Select role service	es	DESTINATION SERVER 2NLAB.lab.local
Before You Begin Installation Type Server Selection Server Roles Features Network Policy and Acces Role Services Confirmation Results	Select the role services to install for Network Policy and Access Services	3 Description Network Policy Server (NPS) allows you to create and norce organization-wide network access policies for client health, connection request authentication, and abs deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.
		< Previous Next > Install Cancel
	TWO NETWORKS - MUM Colombia	a 2019



17 17

		Serv	er Manager	_ 0 ×
Server Ma	anager • Dashl	ooard		• 😥   🚩 Manage Tools View Help
Dashboard	WELCOME TO SERVE	R MANAGER		Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Module for Windows PowerShell
All Server		1 Config	gure this local serv	Active Directory Sites and Services Active Directory Users and Computers ADSI Edit
B DNS B File and Storage Services ▷	QUICK START	2 Add	I roles and features	Component Services Computer Management Defragment and Optimize Drives
🔥 NAP	WHAT'S NEW	3 Add	l other servers to mana	DNS Embedded Lockdown Manager
		5 Cor	nect this server group	Group Policy Management Health Registration Authority
	LEARN MORE			iSCSI Initiator Local Security Policy 4
	ROLES AND SERVER	GROUPS		Network Policy Server
	Roles: 4   Server group	: 1   Servers total:	1	ODBC Data Sources (32-bit)
	AD DS	1	🛱 DNS	Performance Monitor Resource Monitor
	Manageability	,	<ul> <li>Manageability</li> </ul>	Security Configuration Wizard
	Events		Events	Services System Configuration
	Services		Services	System Information
	Performance BPA results		BPA results	Task Scheduler Windows Firewall with Advanced Security
				Windows Memory Diagnostic









	Network Policy Server	_ 0 ×
File Action View Help		
NPS (Local) RADIUS Clients and Servers RADIUS Clients and Servers Remot Remot View Policies Conne Network Health Health Help Accounting Templates Management	RADIUS Clients         Image: RADIUS clients allow you to specify the network access servers, that provide access to your network.         Friendly Name       IP Address         Device Manufacturer       NAP-Capable         Status	
	<	
New Network Access Device		
	TWO NETWORKS - MUM Colombia 2019	Λ

20 20



Mikrot k 22



Mikrotik 23













»	Secure Wireless Connections Properties	Π
File	Overview Conditions Constraints Settings	-
INF ⊿	Configure the constraints for this network policy. If all constraints are not matched by the connection request, network access is denied. Constraints:	whic
⊿ []	Allow access only to those clients that authenticate with the specified methods.	
۵ 🎝	Idle Timeout       EAP types are negotiated between NPS and the client in the order in which they are listed.         Session Timeout       EAP Types:         EAP Types:       EAP Types:	ecified ecified ecified
▶ 🖣	Image: Control output interesting interestinterestinteresting interesting interesting interesting interesting	
	Add     Edit     Remove       Less secure authentication methods:     Image: Charles of the secure	
	<ul> <li>✓ Microsoft Encrypted Authentication Version 2 (Microsoft Pari 4/2)</li> <li>✓ User can change password after it has expired</li> <li>✓ Microsoft Encrypted Authentication (MS-CHAP)</li> <li>✓ User can change password after it has expired</li> </ul>	
	Encrypted authentication (CHAP)     Unencrypted authentication (PAP, SPAP)	
	Allow clients to connect without negotiating an authentication method     Perform machine health check only	
	OK Cancel Apply	
L	Extensible Authentication Protocol Method Microsoft: Protected EAP (PEAP) Authentication Method EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change passwork NAP Enforcement Allow full network access	■ ord after





















#### Configurando el CAPsMAN

Previo al inicio de la configuración debemos tener:

- Crear una interface bridge en el router que será el CAPsMAN
- Asignarle una dirección IP a la interface bridge creada
- Crear un DHCP Server en la interface bridge
- Actualizar todos los equipos, CAPsMAN y CAPs, con la misma versión del RouterOS.



CAPsMAN										
CAP Interface	Provisioning	Configurations	Channels	Datapaths	Security C	g. Access	List Rates	Remote CAP	Radio Regi	stration Table
<b>+</b> - 🛷	* =	Reselect	Channel	Manager	AAA	]				
Name	Δ	Туре	MTU	l Actua	al MTU L2	1TU Tx		Rx		Tx Packet (p/s)
CAPs Manag	er	CAD Interface		1500		1600		0 bps	0 bp	05
	[	✓ Enabled		ОК						
	Certificate:			Cano	cel					
	CA Certificate:		•	App	dy 🔤					
		Require Peer	r Certificate							
Generat	ed Certificate:			Interra	aces					
Generated	CA Certificate:									
	Package Path:									
U	Ipgrade Policy:	none	₹							







CAPsMAN											
CAP Interface	Provisioning	Configura	tions Channe	els Datapaths	Security Cfg	Access List	Rates	Remote CAP	Radio	Registrati	ion Table
4 - 2	I T										
Name	🛆 Authenti	ication T	Encryption	Group E	ncryption 0	Group Key Upda	te Pas:	sphrase	EAP M	ethods	
LAB_Sec	WPA2 E/	AP	aes com						passth	nrough	
CAPs Security	Configuration	<lab_sec></lab_sec>									
	Name: 🚺	B_Sec									ОК
Authentica	ation Type: 🗌	WPA PSK	WPA2 PSI	K 🗌 WPA EAF	WPA2	EAP 🔺					Cancel
E	incryption: 🔽	aes ccm	tkip 🔺								Apply
Group E	incryption:									-	Comment
Group Ke	ey Update:									•	Сору
Pa	assphrase:									-	Remove
EAP	9 Methods: pa	ssthrough								₹ 🗢	
EAP Radius A	ccounting: 🔽	]								•	
wo	_										
networ	rke			TWO NETWO	orks - MUM	Colombia 2019				IVIII	$\langle U \rangle$

CAP Interface Provisioning	Configurations	Channels	Datapaths	Security Cf	g. 4	Access List	Rate
4 - 4							
Name 🛛 🕹 Bridge	Local For	Client To	VLAN Mo	de VLAN ID			
New CAPs Datapath Configur	ation						×
Name:	datapath_LAB					ОК	
MTU:					•	Cancel	
L2 MTU:					•	Apply	
ARP:					•	Commen	t
Bridge:	bridgeLAB			₹	•	Сору	
Bridge Cost:					•	Remove	:
Bridge Horizon:					•		
Local Forwarding:					•		
Client To Client Forwarding:					•		
VLAN Mode:					•		
VLAN ID:					•		
Interface List:					•		





CAPsMAN										
CAP Interface	Provisioning	Configurations	Channels	Datapaths	Security Cfg.	Access List	Rates	Remote CAP	Radio	Registration Table
+ - =	T									
Name	∆ SSID	Hide	SSID Loa	d Bal Cou	ntry Channe	el Fred	uency	Band		Rate
CAPs Configura	ation <cfg_la< td=""><td>b&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></cfg_la<>	b>								
Wireless Cha	annel Rates	Datapath Sec	curity					ОК		
	Name: cfg	_Lab						Cancel		
	Mode: ap					Ŧ		Apply		
	SSID: LA	B_Wifi						Comment		
Hid	de SSID:						•	Сору		
Load Balancing	g Group:						•	Remove		
D	)istance:						-			
- Ηω.	Retries:						<b>.</b>			
Hw. Protectio	n Mode:						-			
0 works			TW	O NETWORK	(S - MUM Colo	mbia 2019				Mikrc



APSMAN .								
CAP Interface Provisio	ning Configurations	Channels Datap	aths Security Cf	g. Access List	Rates	Remote CAP	Radio	Registration Table
4 - 2 7								
Name 🛆 SSI	D Hide	SSID Load Bal	Country Char	inel Fred	quency	Band		Rate
CAPs Configuration <cf< td=""><td><sup>i</sup>g_Lab&gt;</td><td></td><td></td><td></td><td></td><td>×□</td><td></td><td></td></cf<>	<sup>i</sup> g_Lab>					×□		
Wireless Channel R	Rates Datapath Sec	urity				ОК		
Data	path: datapath_LAB			Ŧ		Cancel		
<b></b>	MTU.				1	Apply		
					]•	Comment		
L2	MTU:					Commenc		
	ARP:				•			
Bi	ridge:				] -	Remove		
Bridge	Cost:				-			
Bridge Ho	rizon:				-			
• <u> </u>				lombia 2010				1 Auro
vorke		I VVO INETV						IVIINI O



etworks

CAPsMAN													
CAP Interface	Provisioning	Configurat	ions Char	nnels Data	apaths	Secur	ity Cfg.	Access	List R	ates	Remote CAP	Radio	Registration Table
+	T												
Name	∆ SSID		Hide SSID	Load Bal.	Cou	ntry	Channe	1	Freque	ncy	Band		Rate
CAPs Configur	ation <cfg_lat< td=""><td>&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></cfg_lat<>	>											
Wireless Ch	annel Rates	Datapath	Security							_	ОК		
	Security: 🛃	AB_Sec							<b>Ŧ</b>		Cancel		
Authentica	ation Type:								•	-	Apply		
E	Encryption:								-	-	Comment		
Group B	Encryption:								•	-	Сору		
Group Ke	ey Update:								•	•	Remove		
Pé	assphrase:								•	•			
EAF	P Methods:								4	•			
EAP Radius A	accounting:								•	•			





tworks

CAPsMAN										
CAP Interface	Provisioning	Configurations	Channels	Datapaths	Security Cfg.	Access List	Rates	Remote CAP	Radio	Registration Table
$+ - \vee \times \square \mathbb{7}$										
# Radio MA	4C	Identity Reg	Common N	la Action	Master C	onfigura S	lave Conf	iguration		
New CAPs Provisioning										
Ra	adio MAC: 🔟	0:00:00:00:00:00		ОК						
Hw. Supporte	ed Modes:		\$	Cancel						
Identity	/ Regexp:			Apply						
Common Name	e Regexp:			Disable						
IP Addres	s Ranges:		÷	Comment	1					
	Action: cr	eate enabled	₹	Copy						
Master Conf	iguration: cf	g_LAB	₹	Remove						
Slave Conf	iguration:		<b></b>							
Nam	e Format: ide	entity	₹							
Nar	me Prefix:		•							
enabled										





	1 🖄 🖆 🦷 CAP	WPS Client	Setup Rep	beater Scanner	Freq. Usage	Alignment	Wireless Sniffer	Wireless Snooper
Name S 🚸wlan1	A Type Wireless (Atheros AR	Actual MTU 1500	Tx	Rx 0 bps	0 bps	Tx Packet (p/s)	Rx Packet (p/s) 0	) FP Tx 0
CAP								
		inabled		ОК				
	Certificate: nor	112		Cancel				
	Discovery Interfaces: eth	er1	∓ ≑					
		ock To CAPsMAN.						
	CAPsMAN Addresses: 10.	99.1.254	<b>+</b>					
	CAPSMAN Names:		₹					
	Bridge: nor	10						
		Static Virtual						
	Requested Certificate:							
Locked	CAPsMAN Common Name:							



#### **Configurando el Radius - Pasos**

🔏 Quick Set	Radiu	ş			
I CAPSMAN	4	New Radius Server			Find
🔚 Interfaces	#	General Status		ОК	et 🗸
🧘 Wireless		Service:	login	Cancel	
🍃 🍔 Bridge			hotspot vireless	Apply	
📑 PPP			dhcp ipsec		
🛫 Switch		Called ID:	<b></b>	Disable	
°t¦e Mesh		Domain:	<b>~</b>	Comment	
🛐 IP 🗅		Address:	10.99.1.200	Сору	
🖉 MPLS 🛛 🗅		Forest	****	Remove	
🌌 Routing 💦 🗅		becrec:		Decet Status	
🎲 System 🗈		Authentication Port:	1812	Reset Status	
👳 Queues		Accounting Port:	1813		
📄 Files		Timeout:	300 ms		
📄 Log	0 item	1			
🥵 Radius	_		Accounting Backup		
🄀 Tools 🛛 🗅	_	Realm:	▼		
🔚 New Terminal		Src. Address:	10.99.1.254		
🔜 MetaROUTER					
b Partition	_				
🗋 Make Supout.rif					





#### **Resultado Final**

CR 🚾 🕥 🕥 🛕 😧 🕕 🛈 📶 100% 🛢 5:57 AM
LAB_Wifi
Certificado de Autoridad de Certificación
(no especificados)
Identidad
lab.local\user1
Identidad anónima
Contraseña
Mostrar contraseña
Mostrar opciones avanzadas
CANCELAR CONECTAR
_

rorks

#### CLARO CR 📾 🖾 🕓 🕑 🕕 🖄 💎 📶 100% 🛢 5:57 AM

←	Wi-Fi						
AJUSTES DE LA ZONA ACTIVA WI-FI AT&T							
Conectar automáticamente Conectarse automáticamente a una punto de acceso Wi-Fi AT&T disponible							
REDES WI-FI							
	LAB_Wifi Conectado						
•	Villas6						
	00 La Vaca Lula						
	HUAWEI-E5573-79C5						
	Linksys14125						
		BUSCAR					
	$\triangleleft$ O						



# **PREGUNTAS?**

#### lucas@2n.do







