

# 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

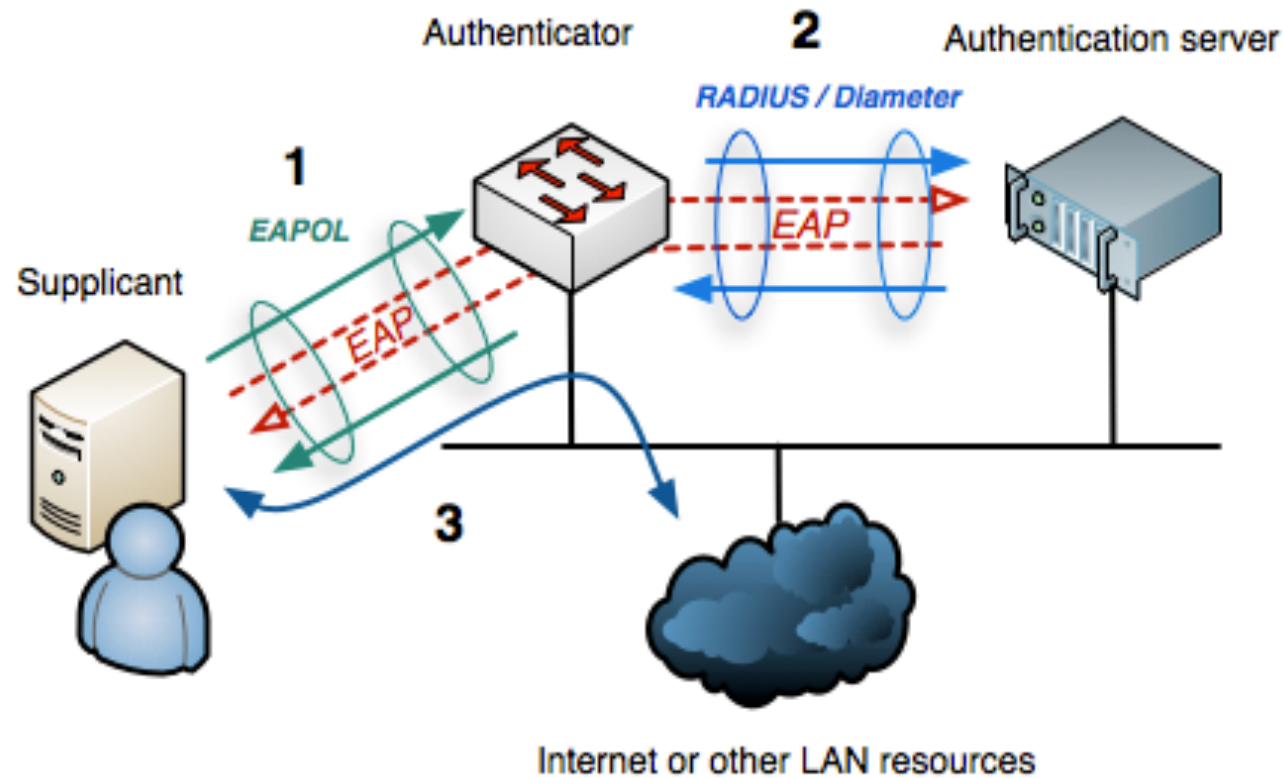
- ❖ Tendremos un control real sobre los usuario que se conectarán
- ❖ Si la clave de un usuario se ve comprometida, es fácil de realizar el cambio
- ❖ Si el usuario sale de empresa, simplemente en borrar o deshabilitar el usuario



# 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

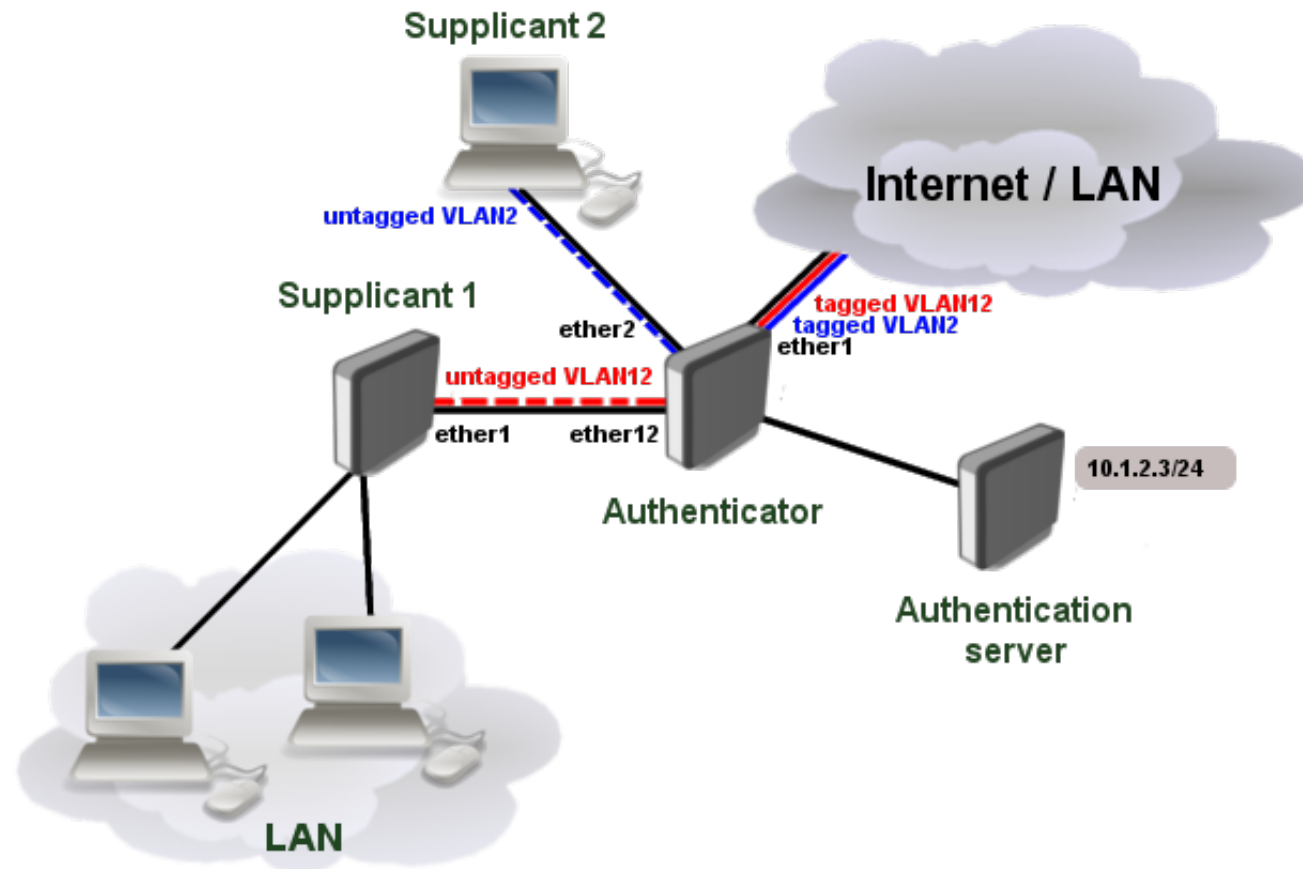
**EAP over LAN (EAPOL):** Transporta la comunicación entre el suplicante y el autenticador

**Remote Authentication 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

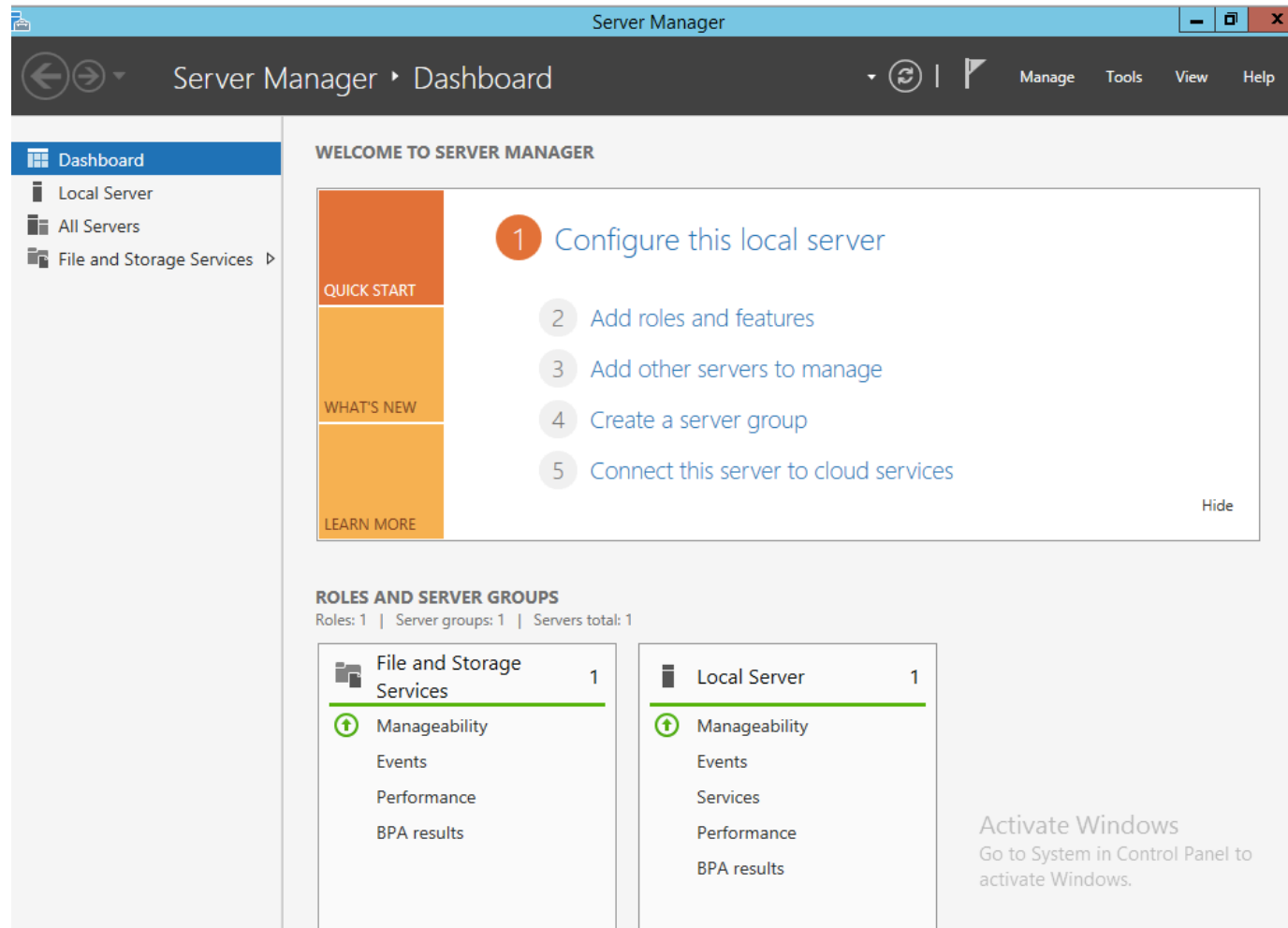
# Dot1x



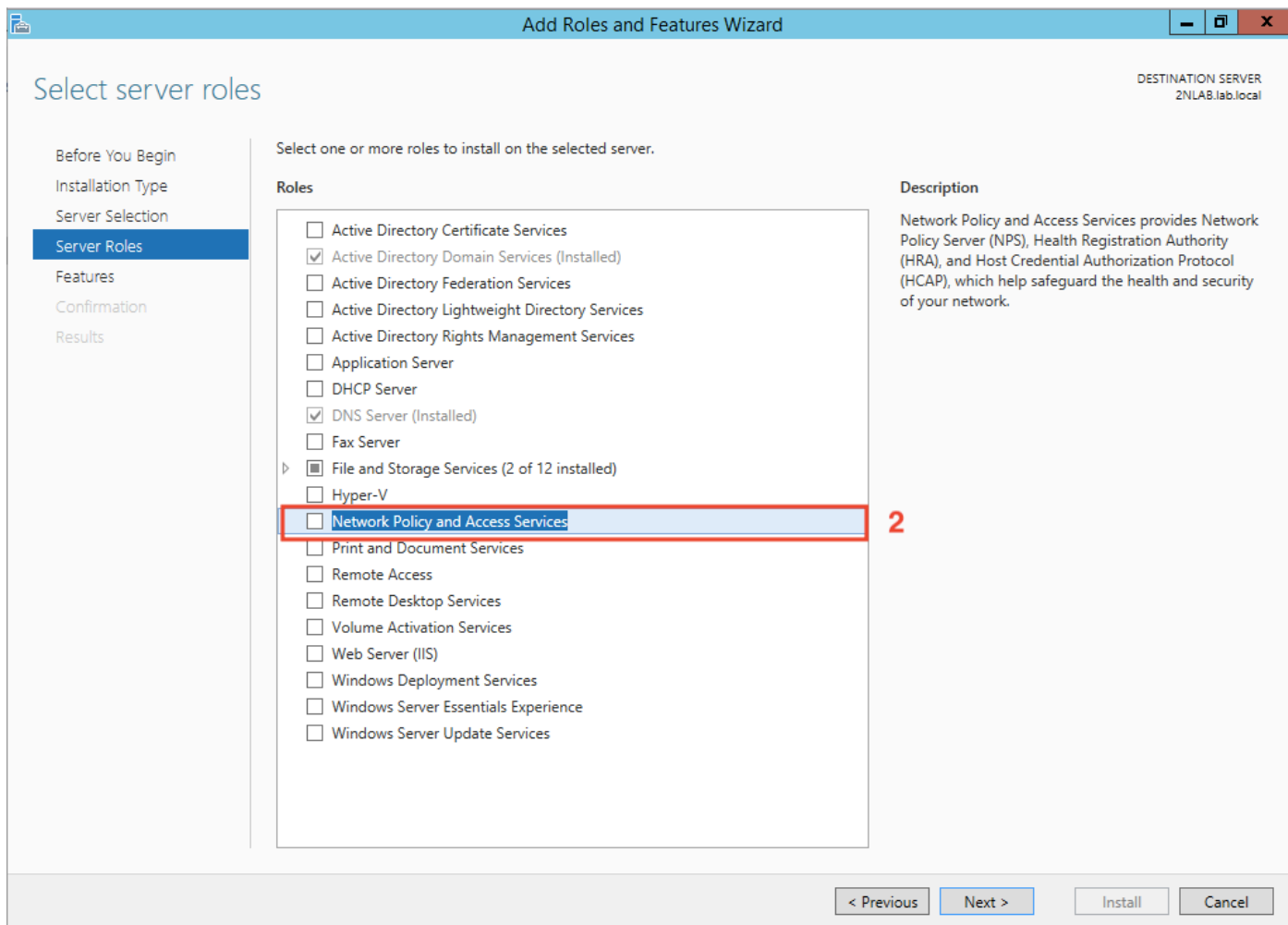
# Prerrequisitos

- ❖ 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

# Configurando Windows Server NPS - Pasos

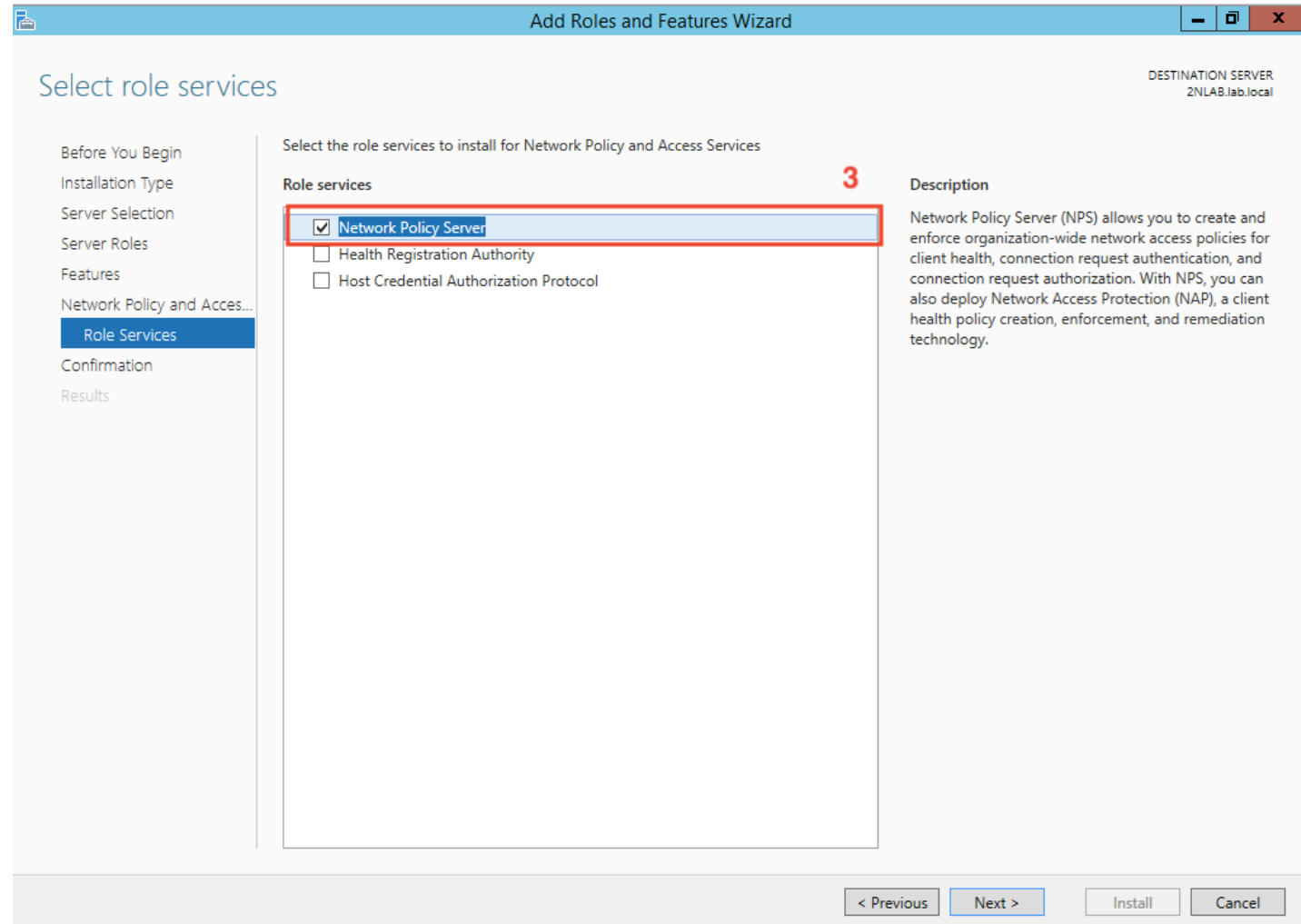


# Configurando Windows Server NPS - Pasos

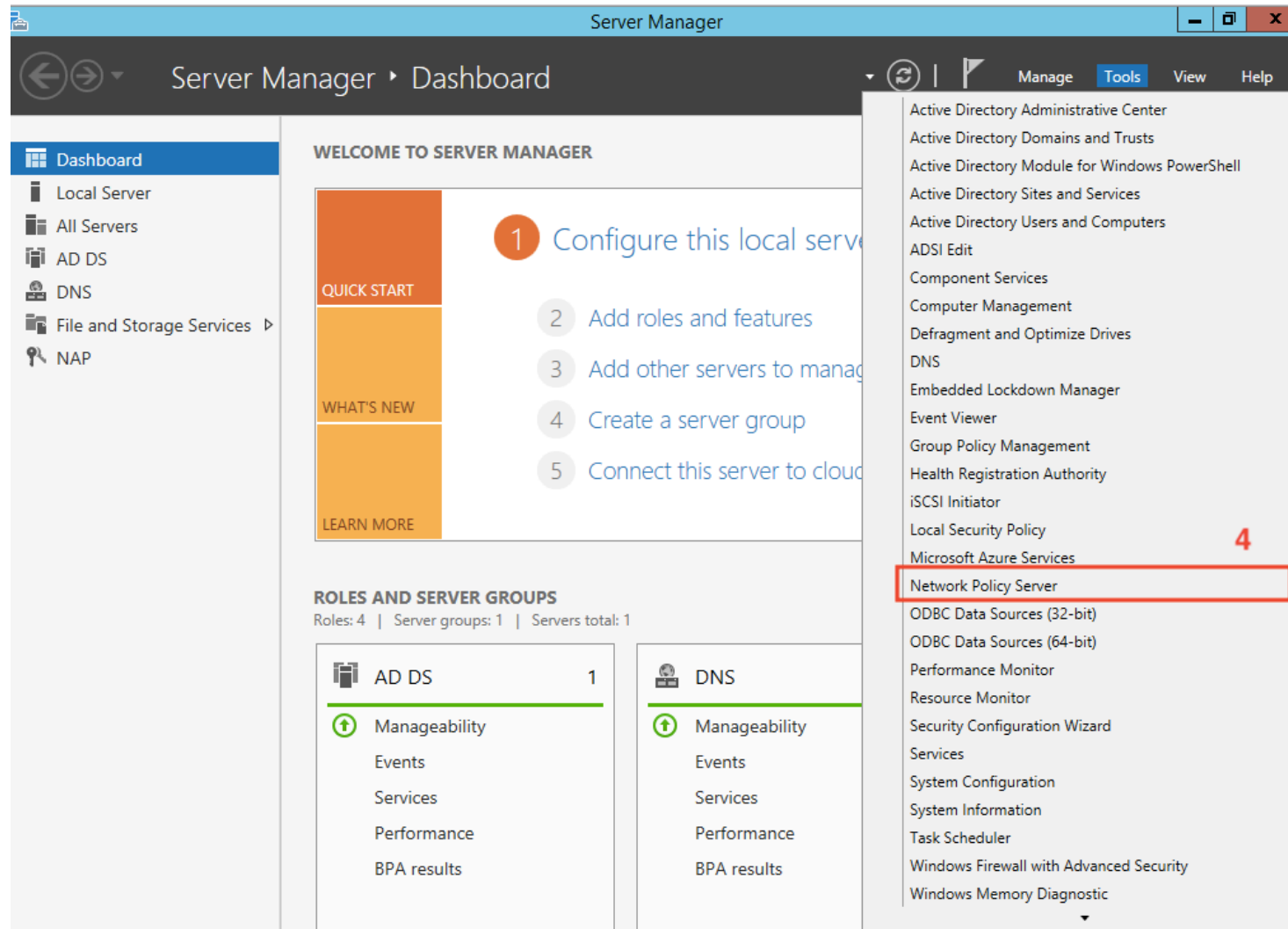




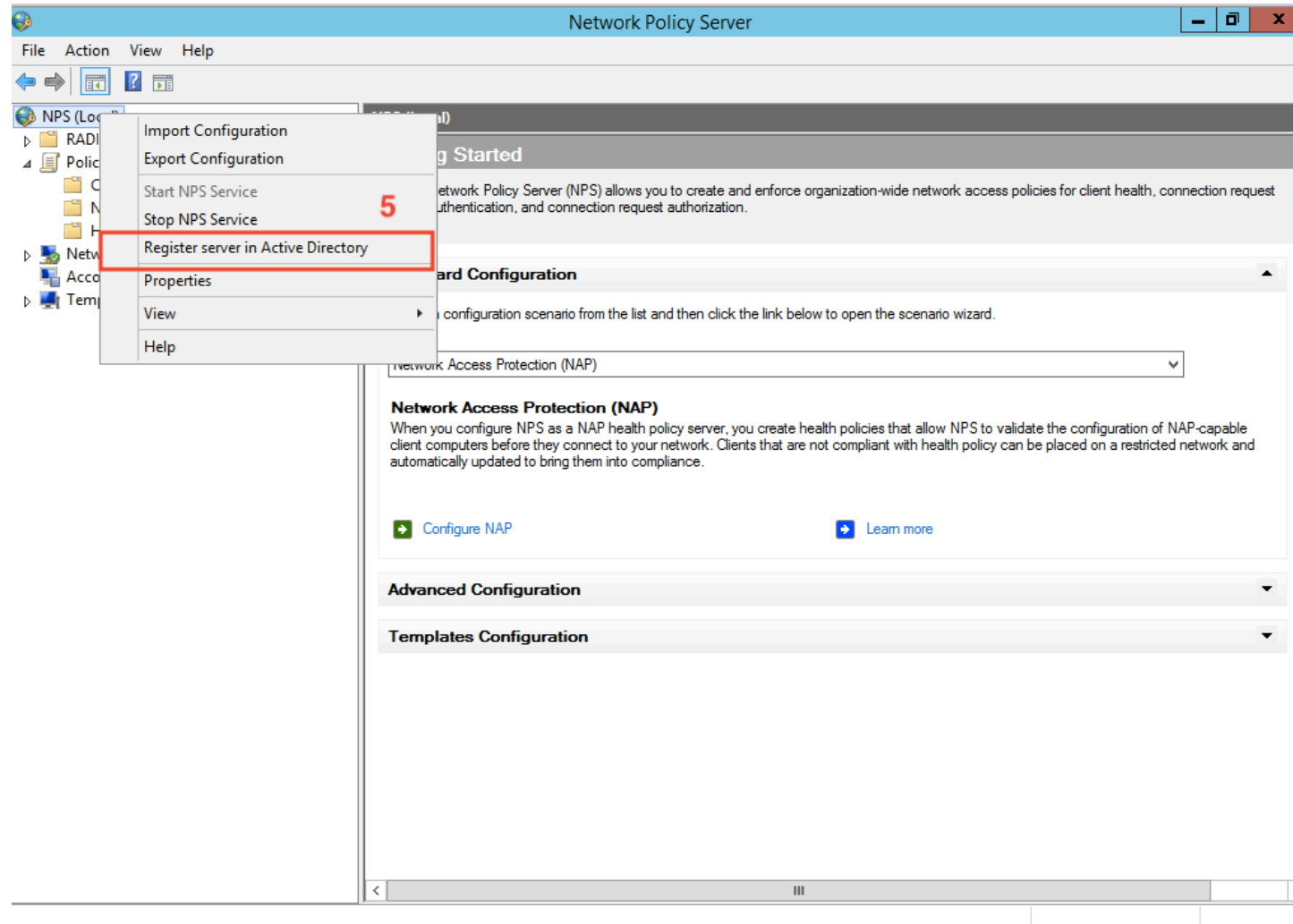
# Configurando Windows Server NPS - Pasos



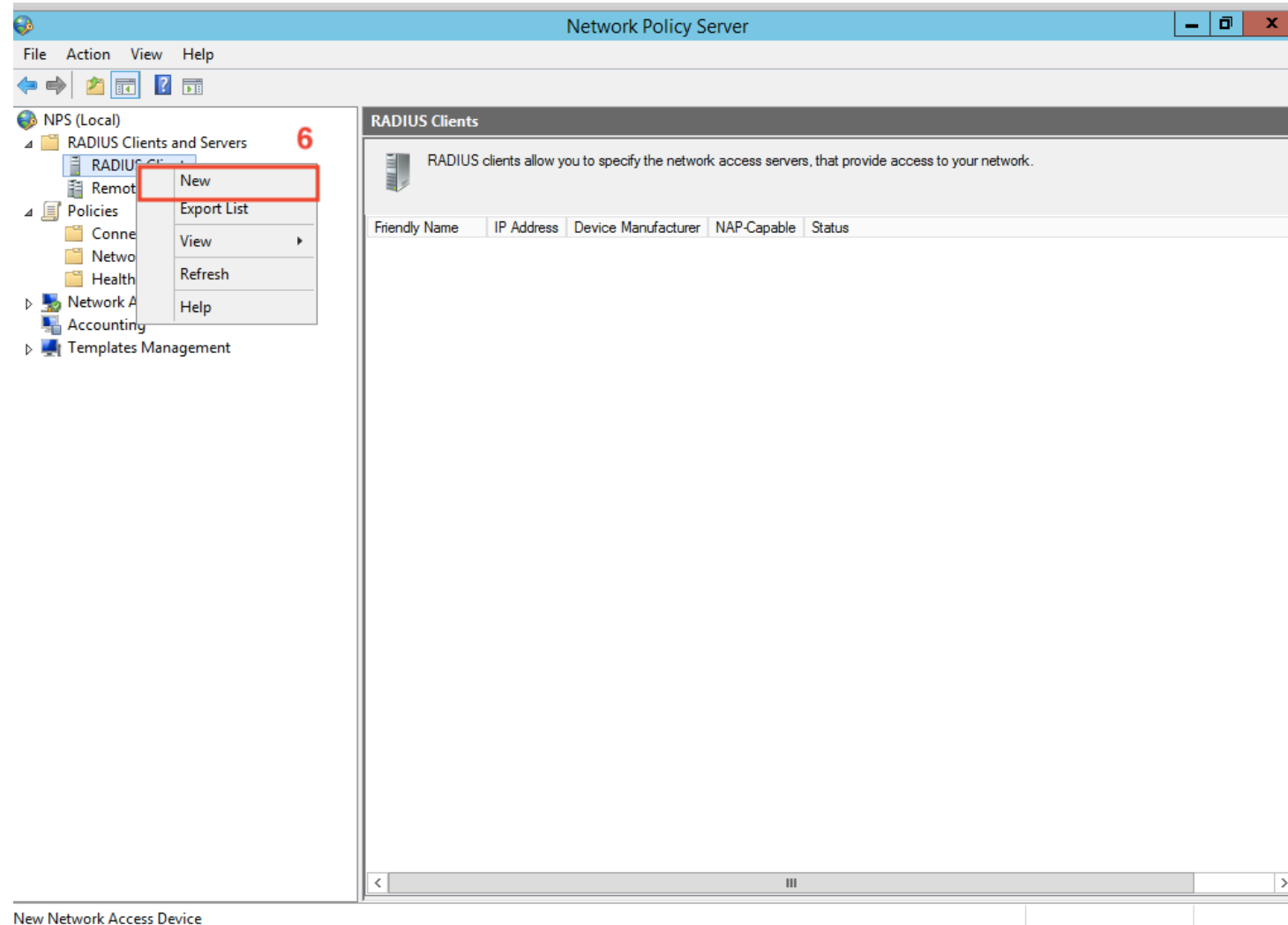
# Configurando Windows Server NPS - Pasos



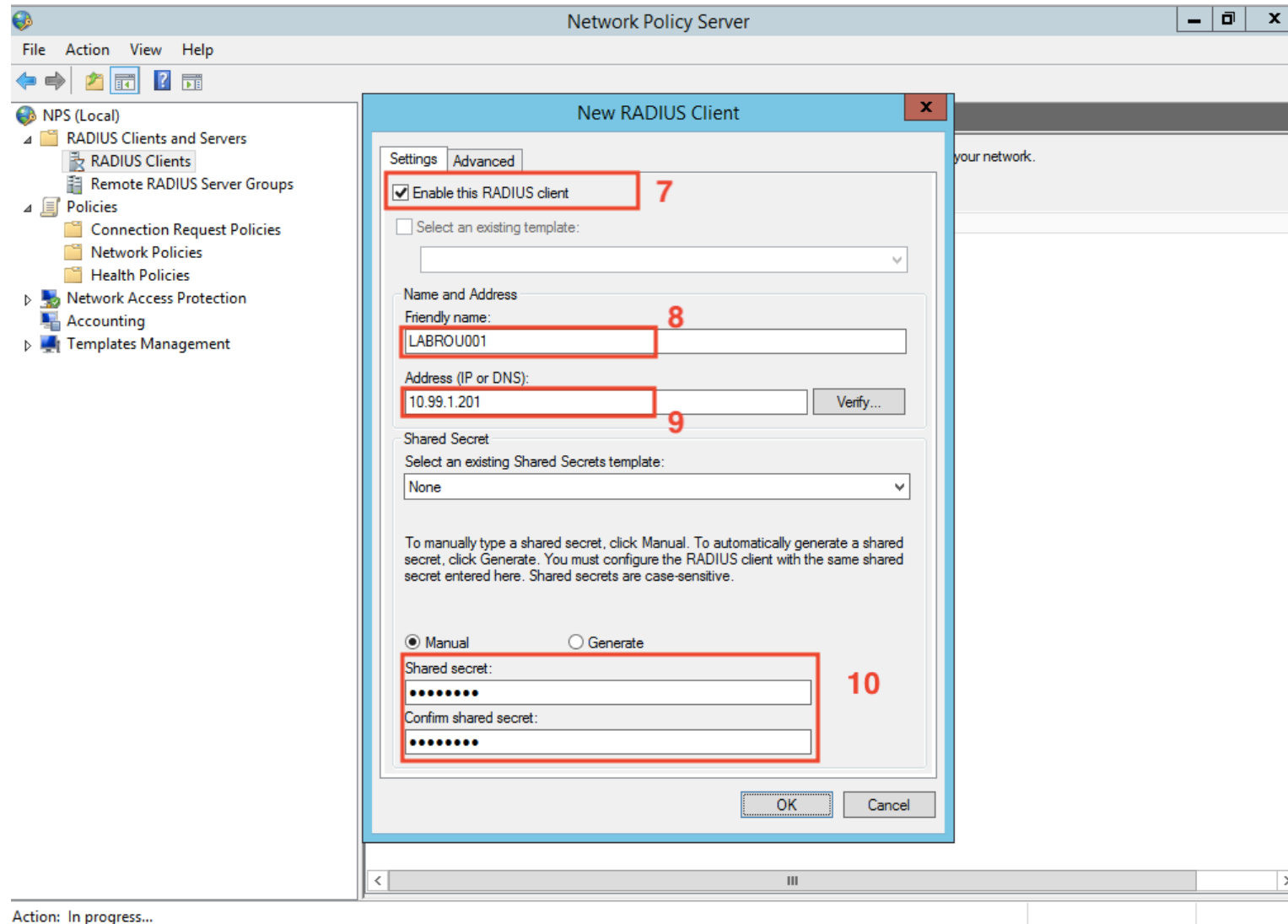
# Configurando Windows Server NPS - Pasos



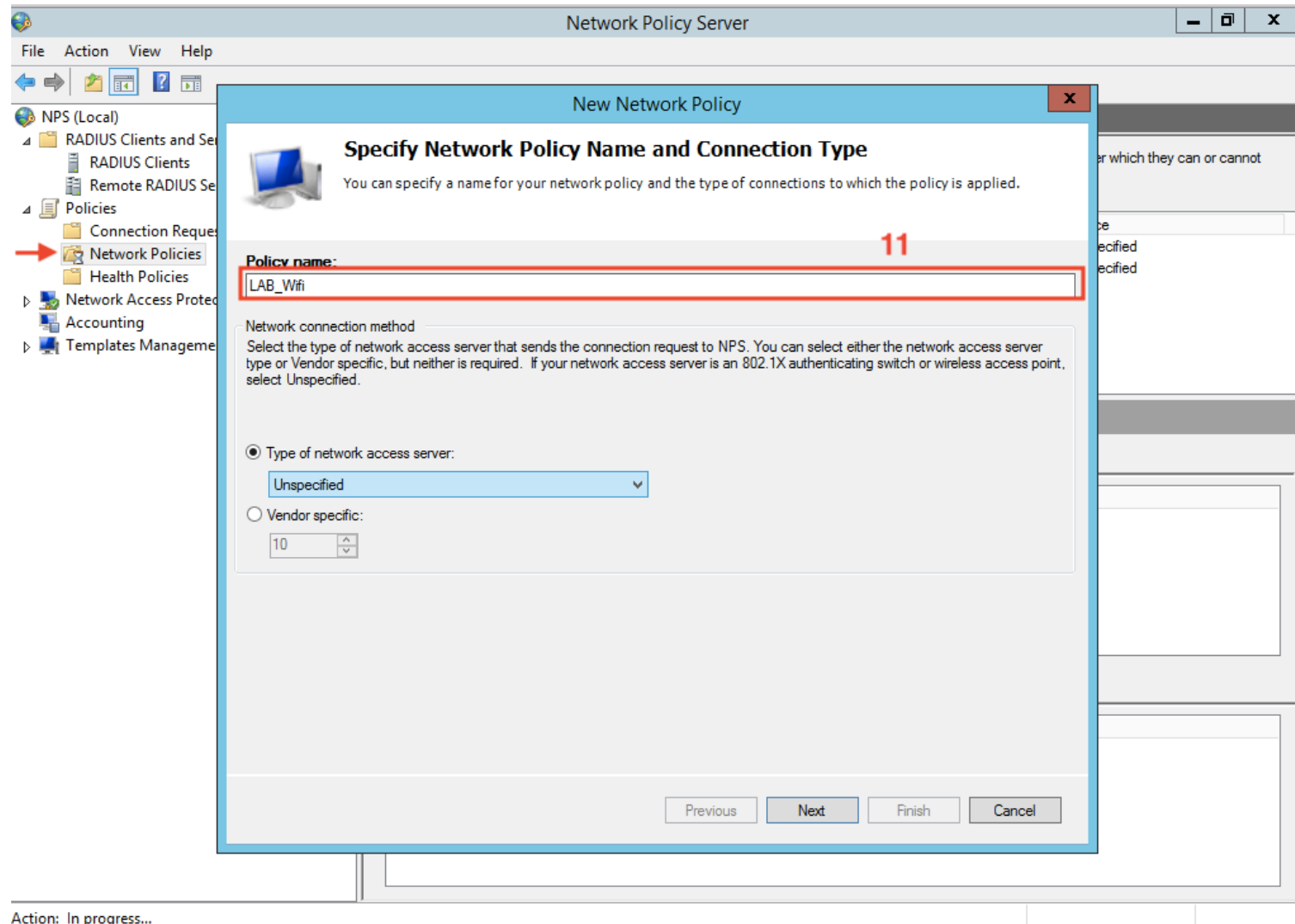
# Configurando Windows Server NPS - Pasos



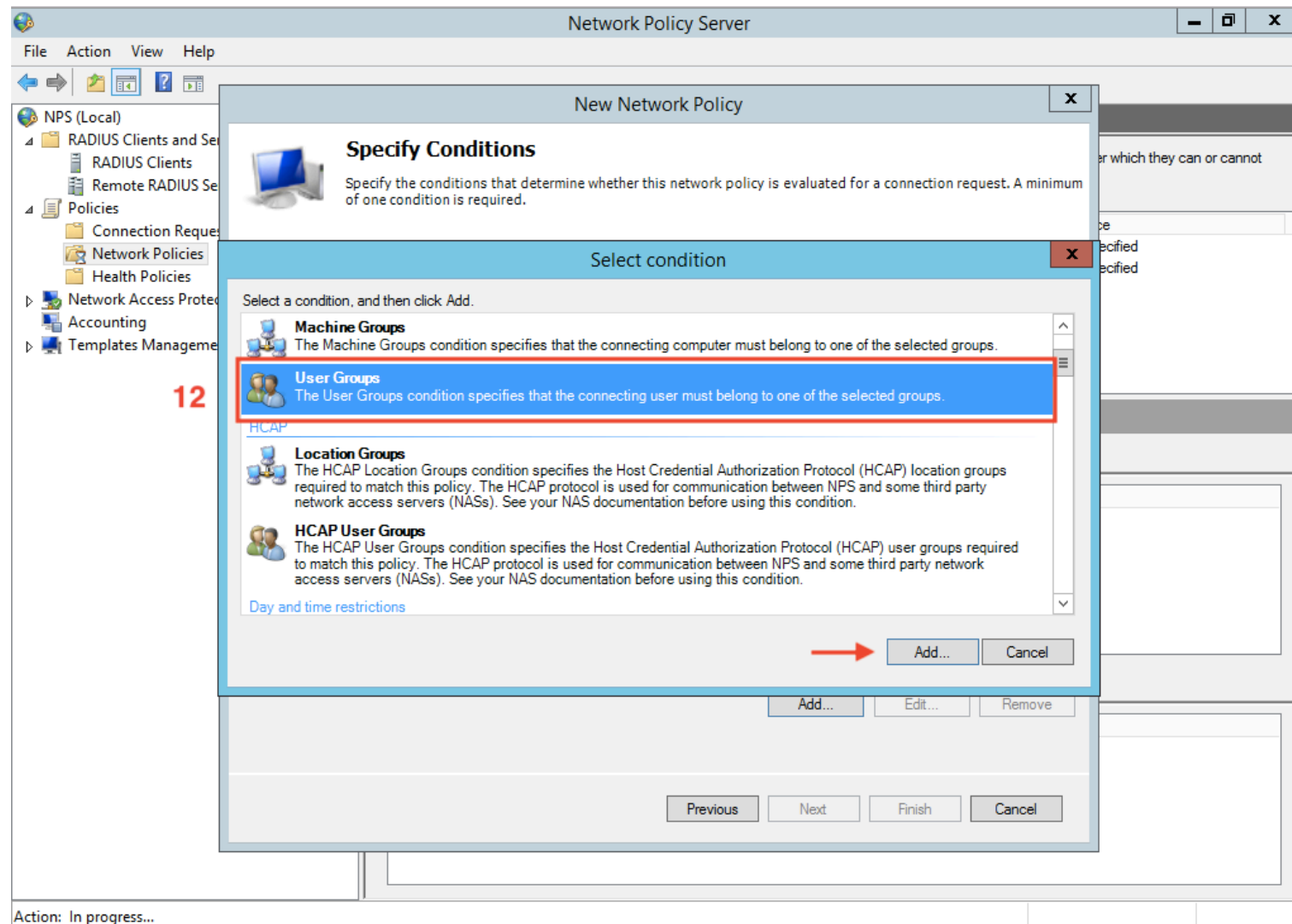
# Configurando Windows Server NPS - Pasos



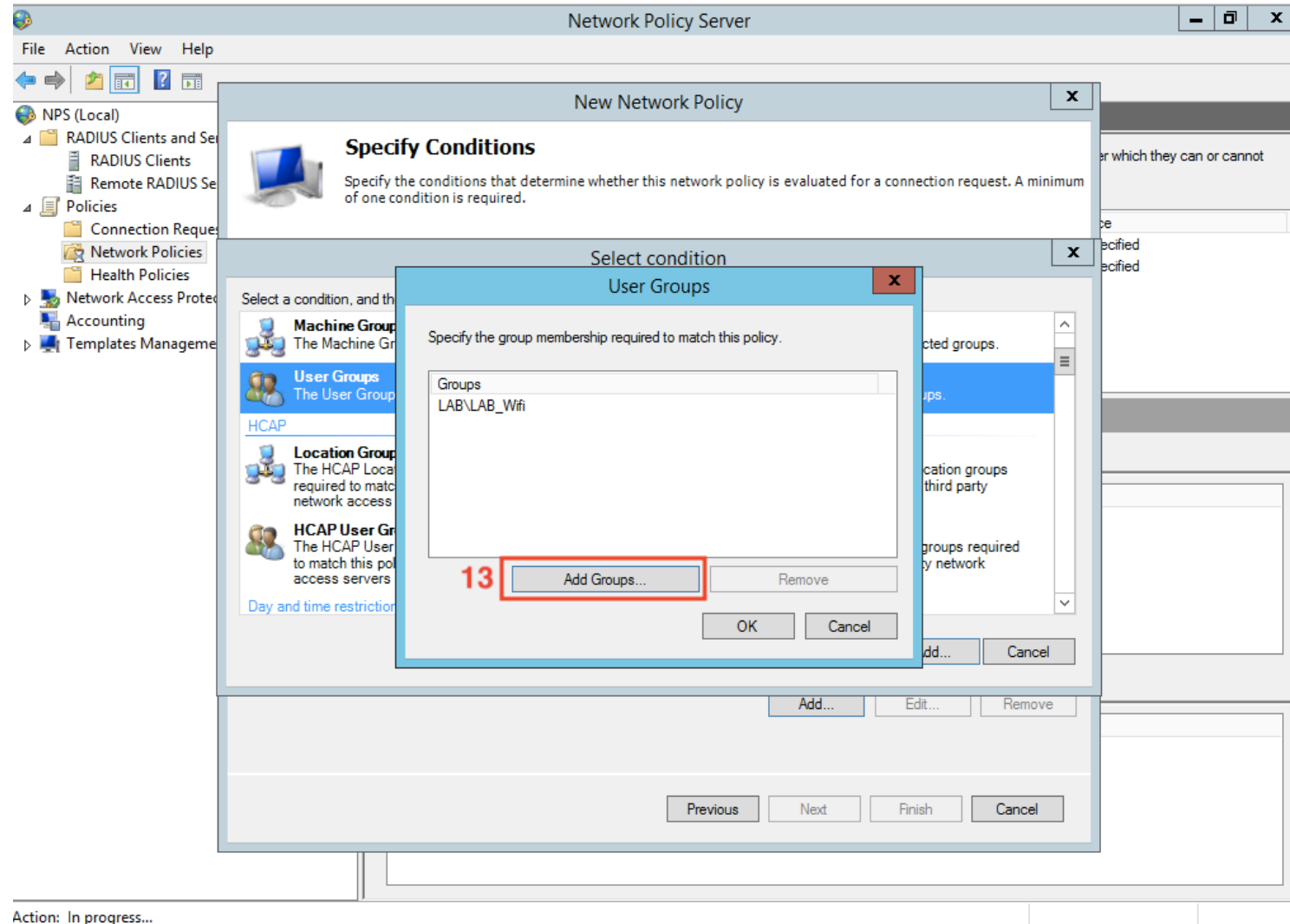
# Configurando Windows Server NPS - Pasos



# Configurando Windows Server NPS - Pasos

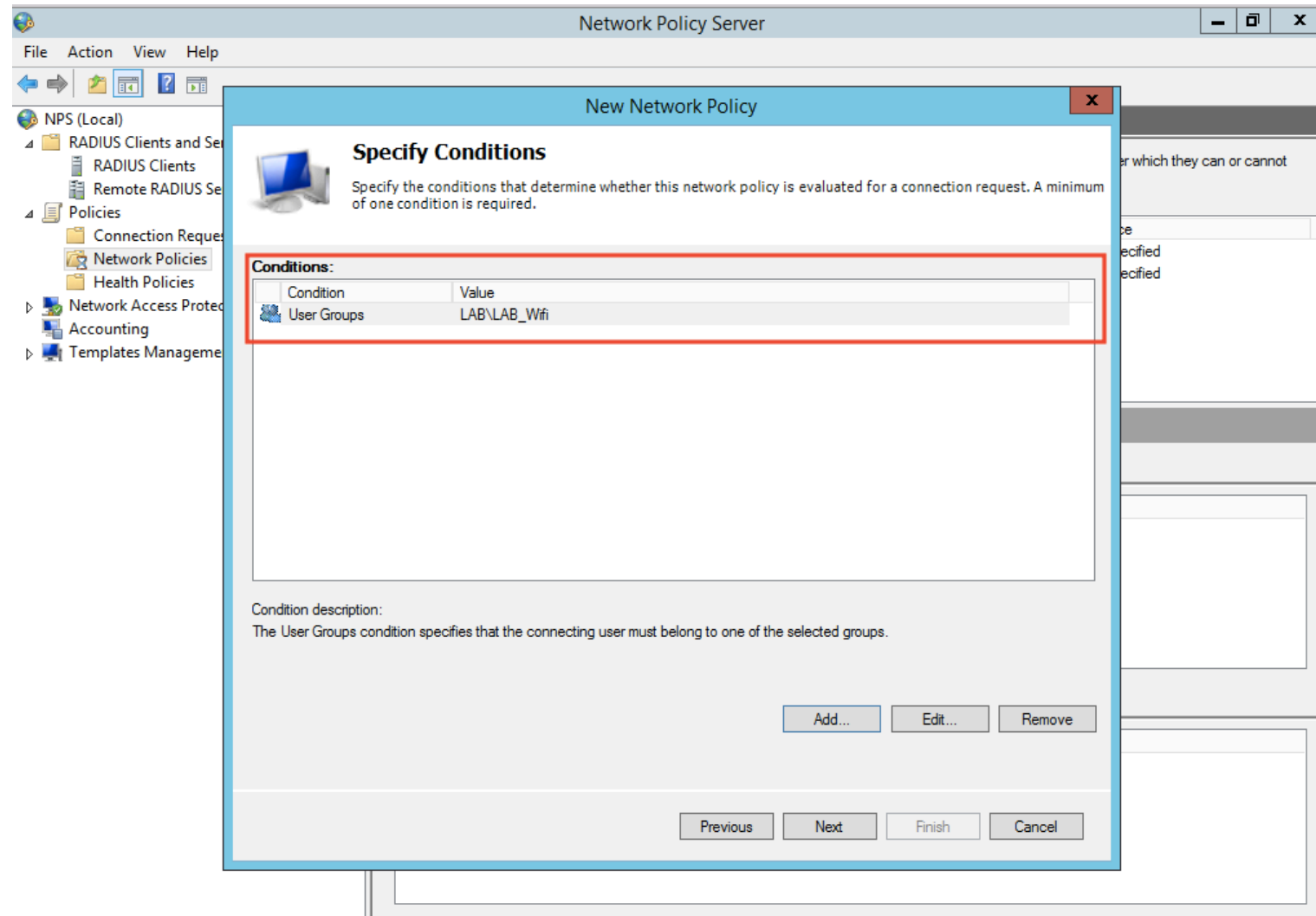


# Configurando Windows Server NPS - Pasos

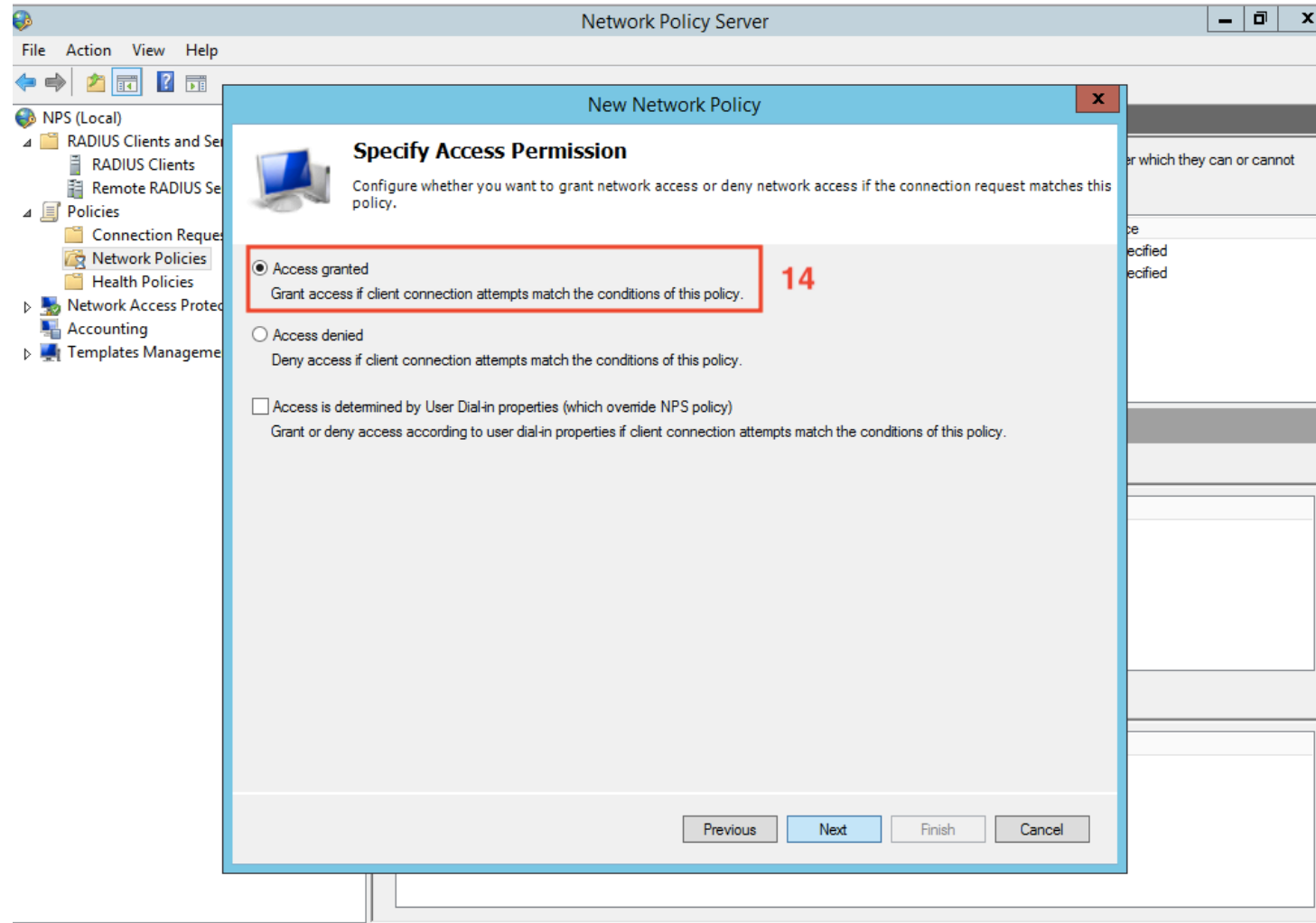




# Configurando Windows Server NPS - Pasos

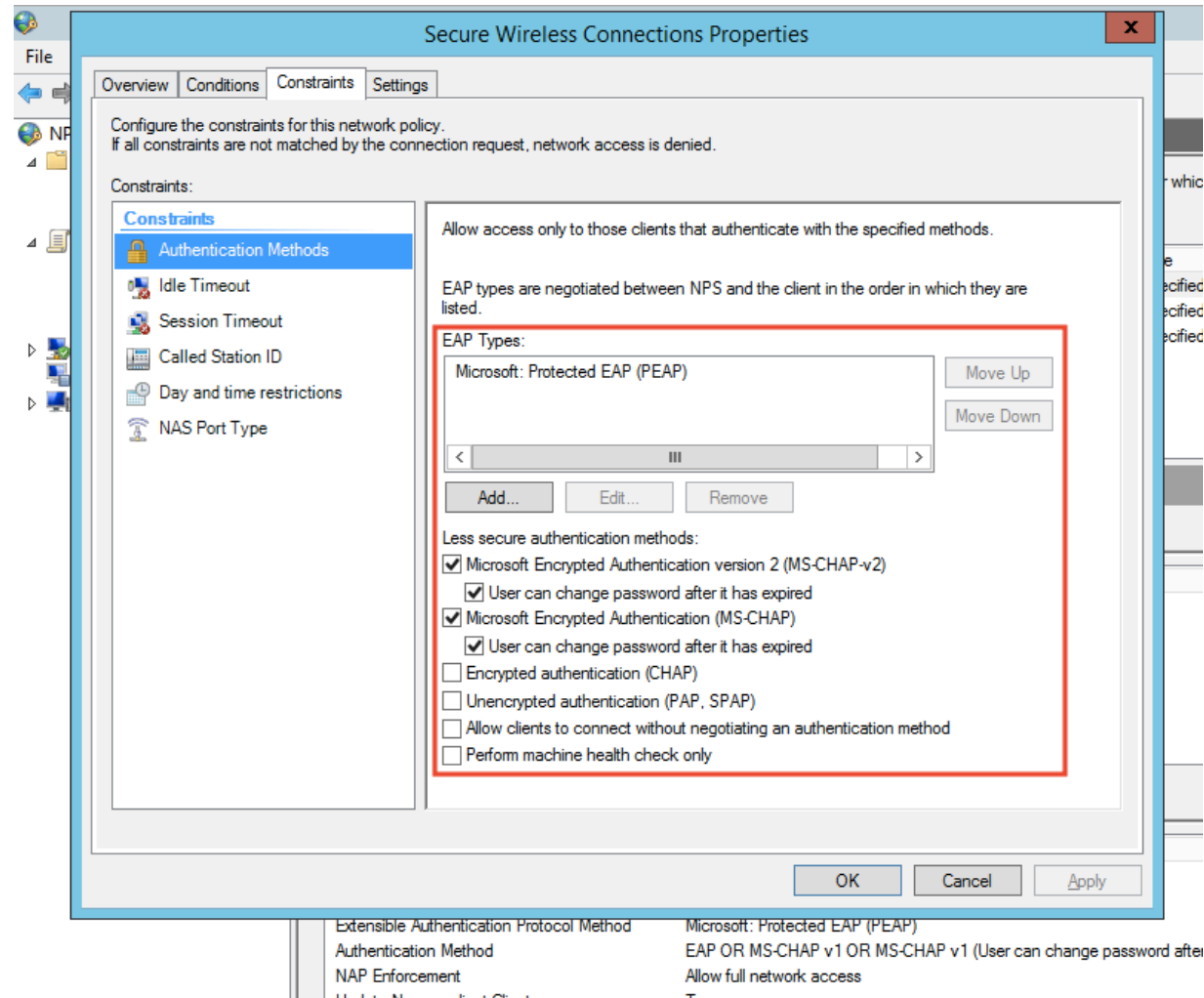


# Configurando Windows Server NPS - Pasos

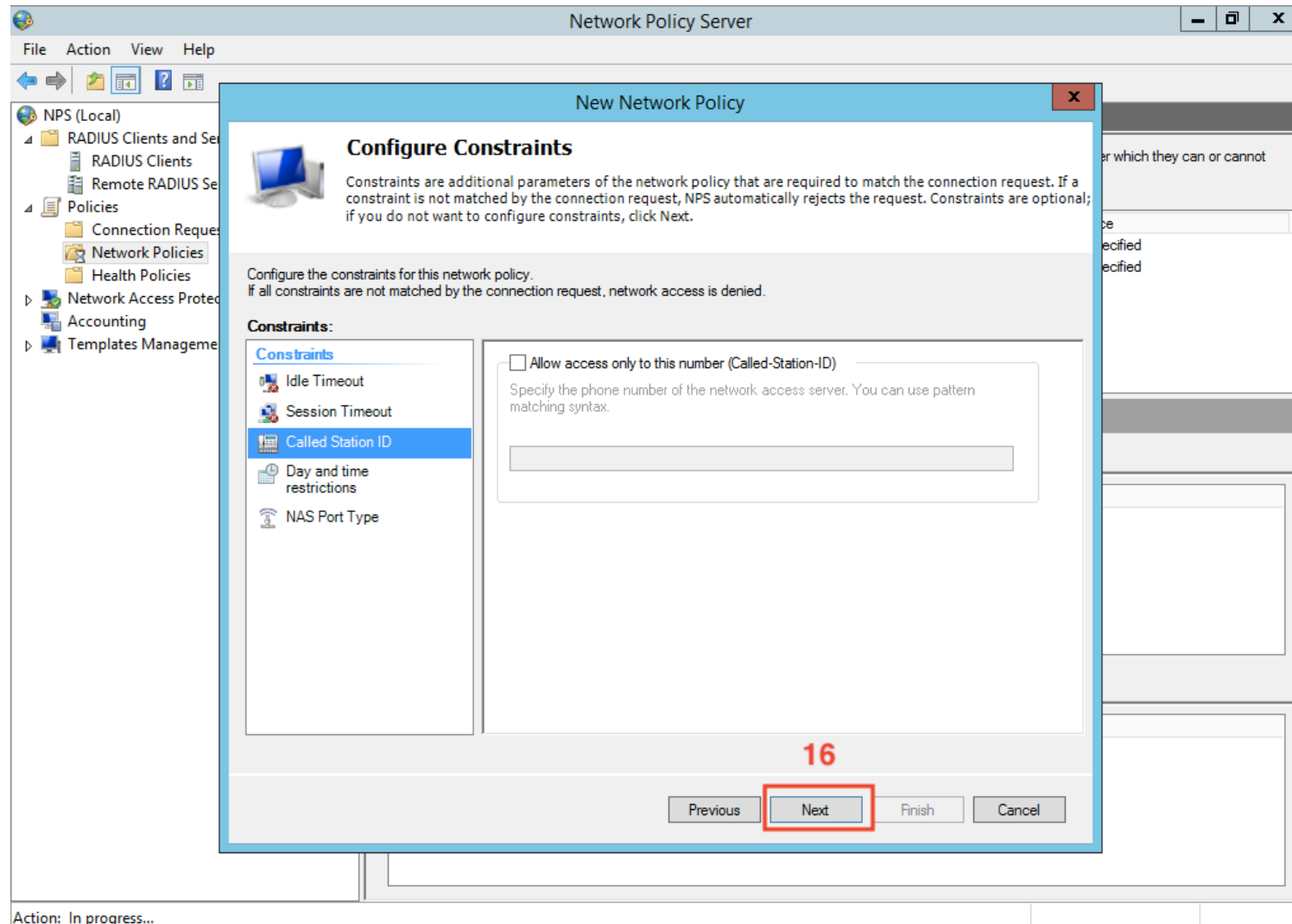


Action: In progress...

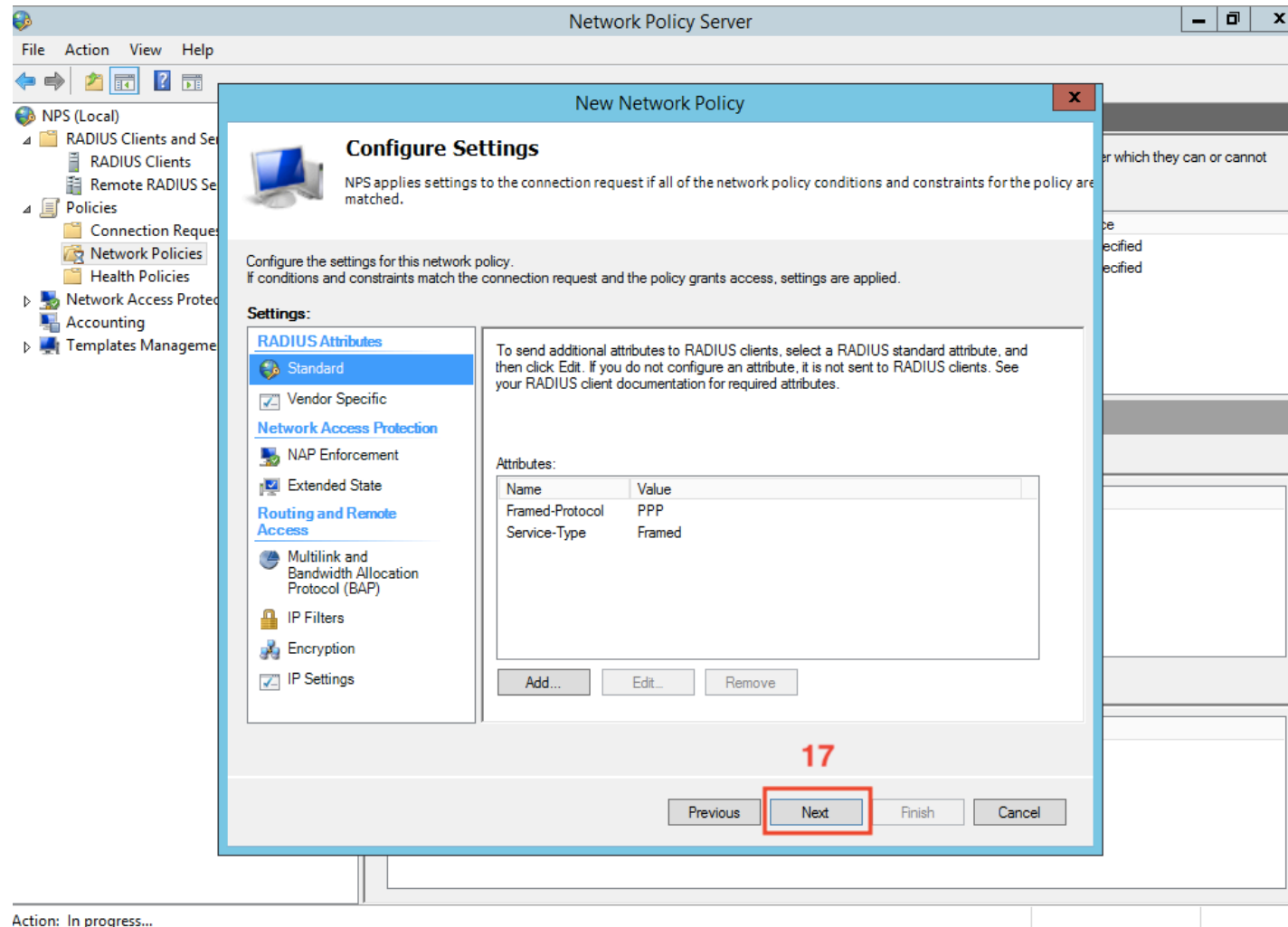
# Configurando Windows Server NPS - Pasos



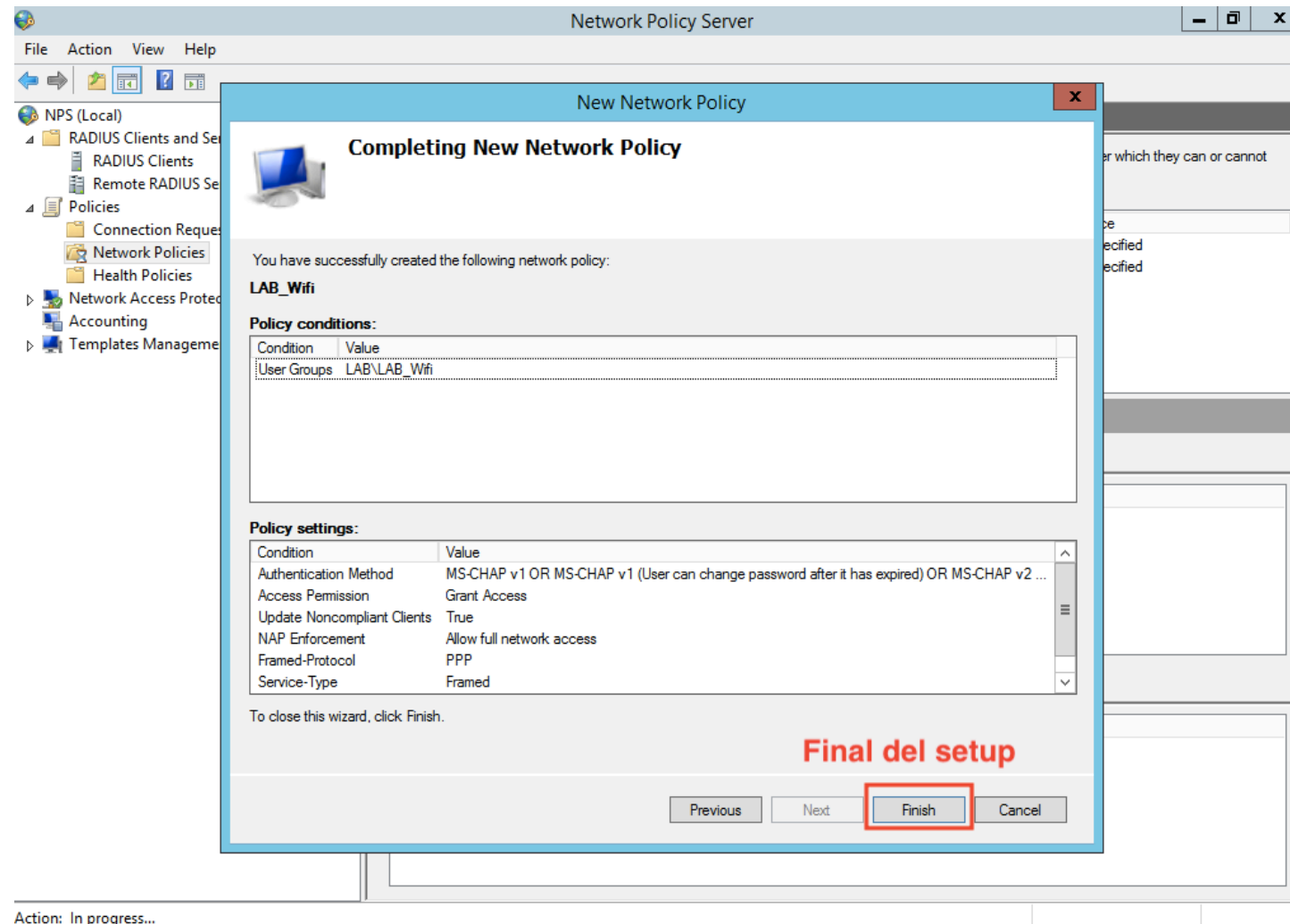
# Configurando Windows Server NPS - Pasos



# Configurando Windows Server NPS - Pasos



# Configurando Windows Server NPS - Pasos



# 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.

# Configurando el CAPsMAN - Pasos

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

+ - [Icons] Reselect Channel Manager AAA

|     | Name       | Type          | MTU  | Actual MTU | L2 MTU | Tx    | Rx    | Tx Packet (p/s) |
|-----|------------|---------------|------|------------|--------|-------|-------|-----------------|
| SMP | MikroTik 1 | CAP Interface | 1500 | 1500       | 1600   | 0 bps | 0 bps | 0 bps           |

CAPs Manager

☒ Enabled

Certificate: [Dropdown]

CA Certificate: [Dropdown]

☐ Require Peer Certificate

Generated Certificate: [Text]

Generated CA Certificate: [Text]

Package Path: [Text]

Upgrade Policy: none [Dropdown]

OK Cancel Apply Interfaces



# Configurando el CAPsMAN - Pasos

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

+ - [Folder Icon] [Filter Icon]

| Name    | Authentication T... | Encryption | Group Encryption | Group Key Update | Passphrase | EAP Methods |
|---------|---------------------|------------|------------------|------------------|------------|-------------|
| LAB_Sec | WPA2 EAP            | aes ccm    |                  |                  |            | passthrough |

CAPs Security Configuration <LAB\_Sec>

Name: LAB\_Sec

Authentication Type: ☐ WPA PSK ☐ WPA2 PSK ☐ WPA EAP ☒ WPA2 EAP ▲

Encryption: ☒ aes ccm ☐ tkip ▲

Group Encryption: ▼

Group Key Update: ▼

Passphrase: ▼

EAP Methods: passthrough ▼ ▲

EAP Radius Accounting: ☒

OK Cancel Apply Comment Copy Remove

# Configurando el CAPsMAN - Pasos

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates

+ - [icon] [icon]

| Name | Bridge | Local For... | Client To... | VLAN Mode | VLAN ID |
|------|--------|--------------|--------------|-----------|---------|
|------|--------|--------------|--------------|-----------|---------|

New CAPs Datapath Configuration

Name: datapath\_LAB

MTU: [dropdown]

L2 MTU: [dropdown]

ARP: [dropdown]

Bridge: bridgeLAB

Bridge Cost: [dropdown]

Bridge Horizon: [dropdown]

Local Forwarding: [dropdown]

Client To Client Forwarding: [dropdown]

VLAN Mode: [dropdown]

VLAN ID: [dropdown]

Interface List: [dropdown]

OK Cancel Apply Comment Copy Remove

# Configurando el CAPsMAN - Pasos

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

+ - [Icon] [Icon]

| Name | SSID | Hide SSID | Load Bal... | Country | Channel | Frequency | Band | Rate |
|------|------|-----------|-------------|---------|---------|-----------|------|------|
|      |      |           |             |         |         |           |      |      |

CAPs Configuration <cfg\_Lab>

Wireless Channel Rates Datapath Security

Name: cfg\_Lab

Mode: ap

SSID: LAB\_Wifi

Hide SSID: [Field]

Load Balancing Group: [Field]

Distance: [Field]

Hw. Retries: [Field]

Hw. Protection Mode: [Field]

OK Cancel Apply Comment Copy Remove

# Configurando el CAPsMAN - Pasos

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

+ - [icon] [icon]

| Name | SSID | Hide SSID | Load Bal... | Country | Channel | Frequency | Band | Rate |
|------|------|-----------|-------------|---------|---------|-----------|------|------|
|      |      |           |             |         |         |           |      |      |

CAPs Configuration <cfg\_Lab>

Wireless Channel Rates Datapath Security

Datapath: datapath\_LAB

MTU: [input]  
L2 MTU: [input]  
ARP: [input]  
Bridge: [input]  
Bridge Cost: [input]  
Bridge Horizon: [input]

OK  
Cancel  
Apply  
Comment  
Copy  
Remove

# Configurando el CAPsMAN - Pasos

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

+ - [Icon] [Icon]

| Name | SSID | Hide SSID | Load Bal... | Country | Channel | Frequency | Band | Rate |
|------|------|-----------|-------------|---------|---------|-----------|------|------|
|------|------|-----------|-------------|---------|---------|-----------|------|------|

CAPs Configuration <cfg\_Lab>

Wireless Channel Rates Datapath Security

Security: LAB\_Sec

Authentication Type: [Dropdown]

Encryption: [Dropdown]

Group Encryption: [Dropdown]

Group Key Update: [Dropdown]

Passphrase: [Dropdown]

EAP Methods: [Dropdown]

EAP Radius Accounting: [Dropdown]

OK Cancel Apply Comment Copy Remove

# Configurando el CAPsMAN - Pasos

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

+ - ✓ ✕ 📄 🔍

| # | Radio MAC | Identity Reg... | Common Na... | Action | Master Configura... | Slave Configuration |
|---|-----------|-----------------|--------------|--------|---------------------|---------------------|
|---|-----------|-----------------|--------------|--------|---------------------|---------------------|

New CAPs Provisioning

Radio MAC: 00:00:00:00:00:00

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Hw. Supported Modes:

Identity Regexp:

Common Name Regexp:

IP Address Ranges:

Action: create enabled

Master Configuration: cfg\_LAB

Slave Configuration:

Name Format: identity

Name Prefix:

enabled

# Configurando el CAPs - Pasos

Wireless Tables

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Security Profiles Channels

+ - ✓ ✗ CAP WPS Client Setup Repeater Scanner Freq. Usage Alignment Wireless Sniffer Wireless Snooper Find

| Name  | Type                    | Actual MTU | Tx    | Rx    | Tx Packet (p/s) | Rx Packet (p/s) | FP Tx |
|-------|-------------------------|------------|-------|-------|-----------------|-----------------|-------|
| wlan1 | Wireless (Atheros AR... | 1500       | 0 bps | 0 bps | 0               | 0               | 0 bps |

CAP

☒ Enabled

Interfaces: wlan1

Certificate: none

Discovery Interfaces: ether1

☐ Lock To CAPsMAN

CAPsMAN Addresses: 10.99.1.254

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge: none

☐ Static Virtual

Requested Certificate:

Locked CAPsMAN Common Name:

OK Cancel Apply

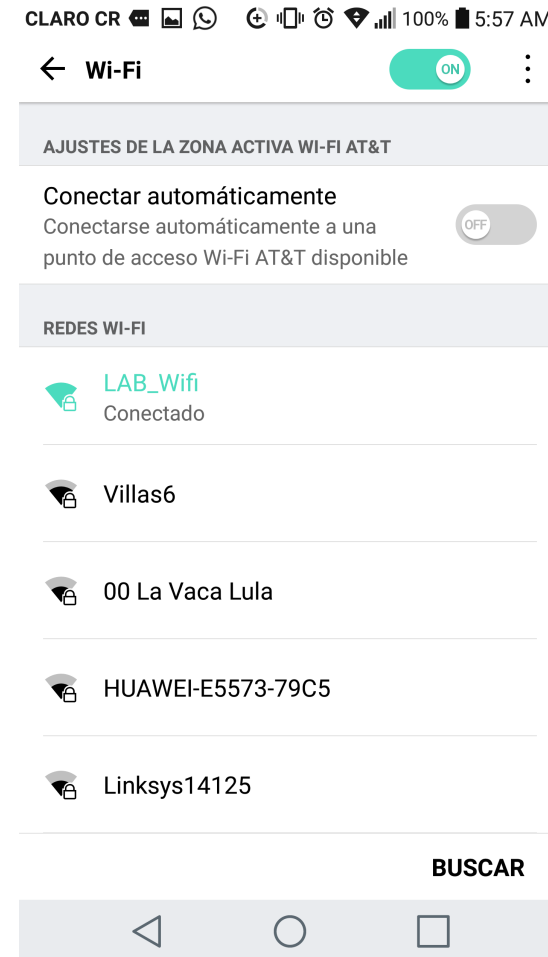
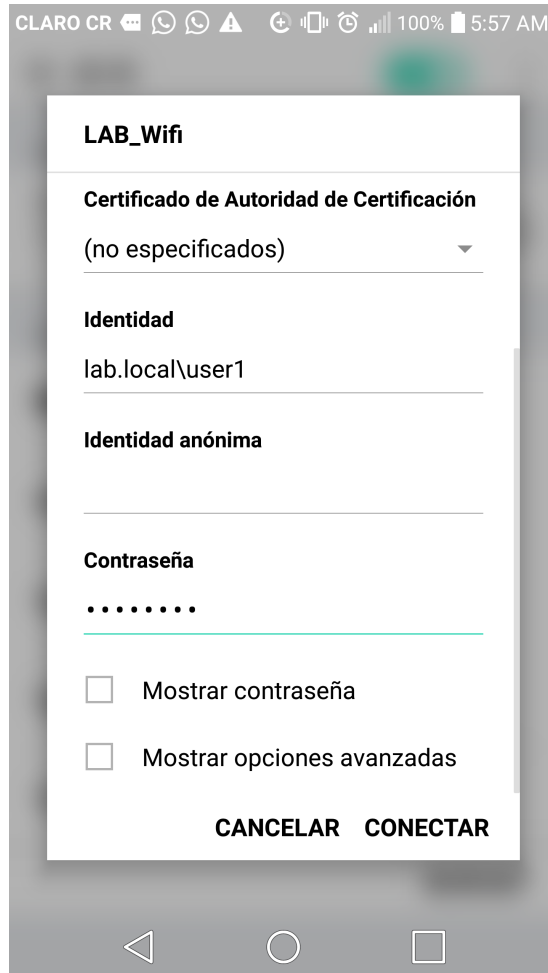
# Configurando el Radius - Pasos

The screenshot shows the 'New Radius Server' configuration window in Mikrotik WinBox. The 'General' tab is selected. The 'Service' section has 'wireless' checked. The 'Address' field is set to '10.99.1.200' and the 'Secret' field is masked with '\*\*\*\*\*'. The 'Authentication Port' is '1812' and the 'Accounting Port' is '1813'. The 'Timeout' is '300' ms. The 'Src. Address' field is set to '10.99.1.254'. The status at the bottom is 'enabled'.

| Field               | Value                                             |
|---------------------|---------------------------------------------------|
| Service             | ppp, login, hotspot, dhcp, ipsec, <b>wireless</b> |
| Called ID           |                                                   |
| Domain              |                                                   |
| Address             | 10.99.1.200                                       |
| Secret              | *****                                             |
| Authentication Port | 1812                                              |
| Accounting Port     | 1813                                              |
| Timeout             | 300 ms                                            |
| Accounting Backup   | <input type="checkbox"/>                          |
| Realm               |                                                   |
| Src. Address        | 10.99.1.254                                       |
| Status              | enabled                                           |



# Resultado Final



# PREGUNTAS?

lucas@2n.do

