

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

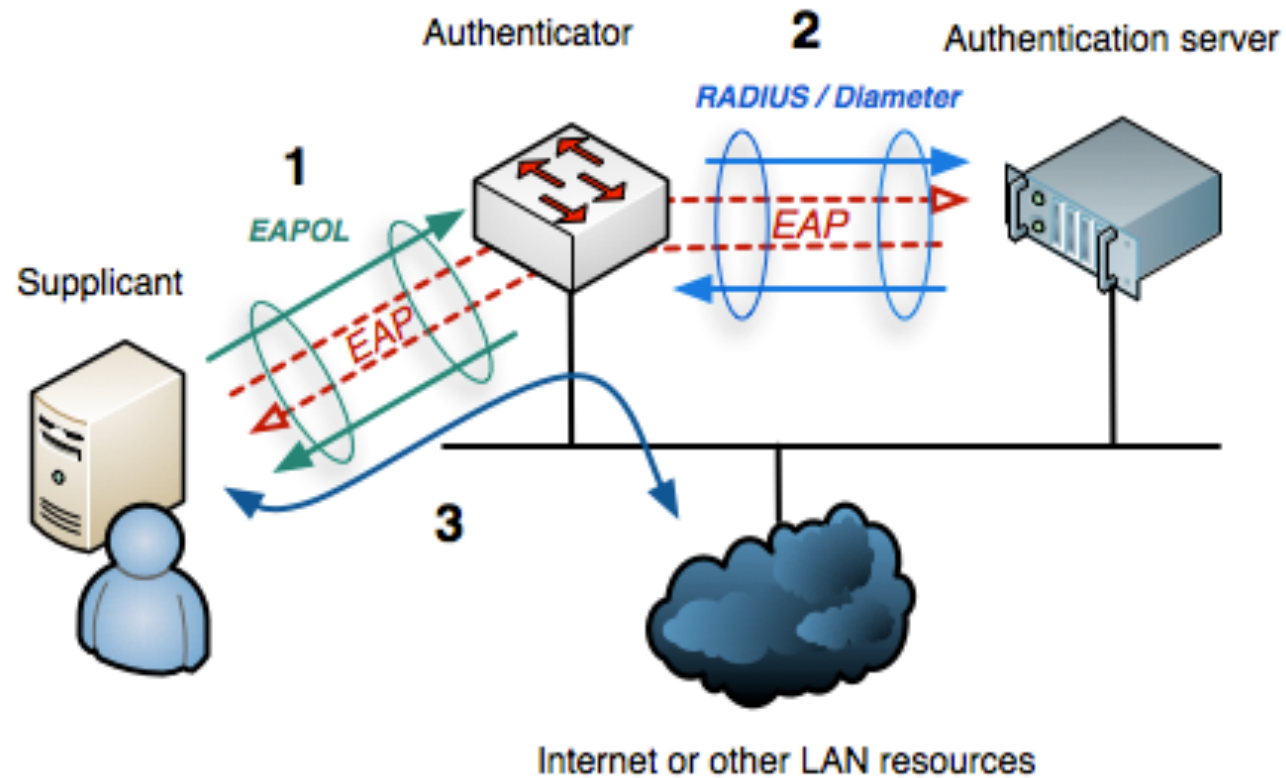
Los beneficios

- ❖ 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

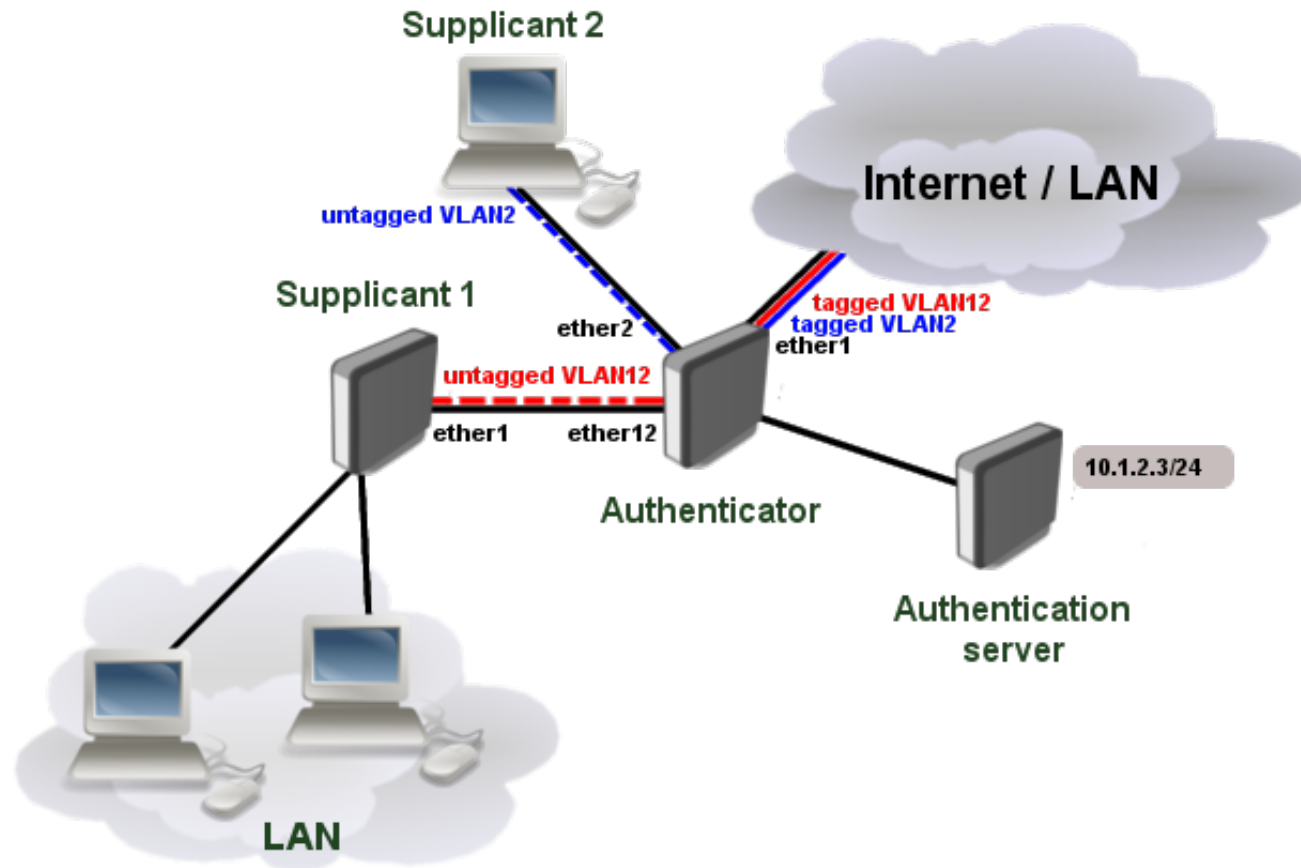
EAP over LAN (EAPOL): Transporta la comunicación entre el suplicante y el autenticador

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

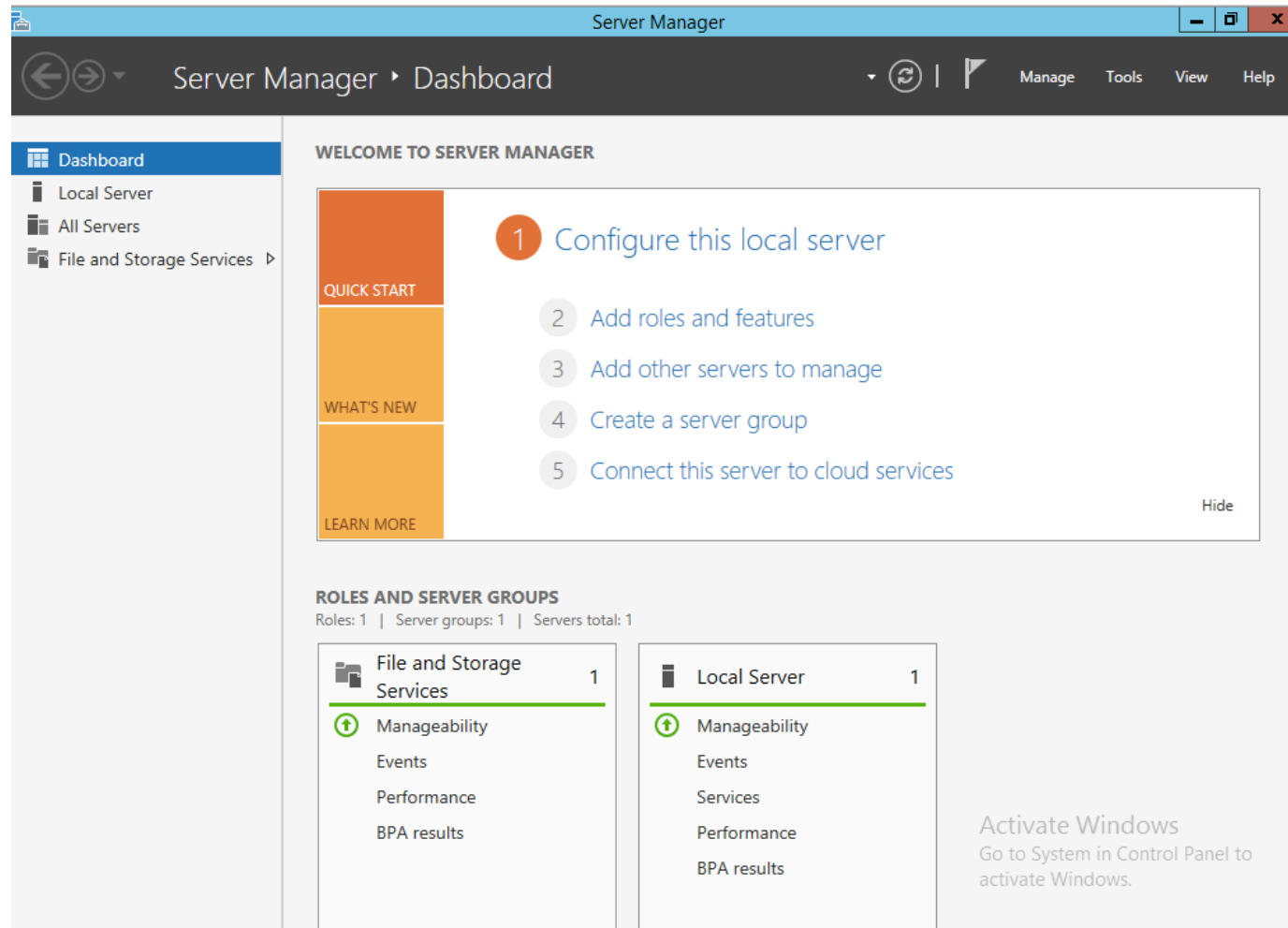
Dot1x



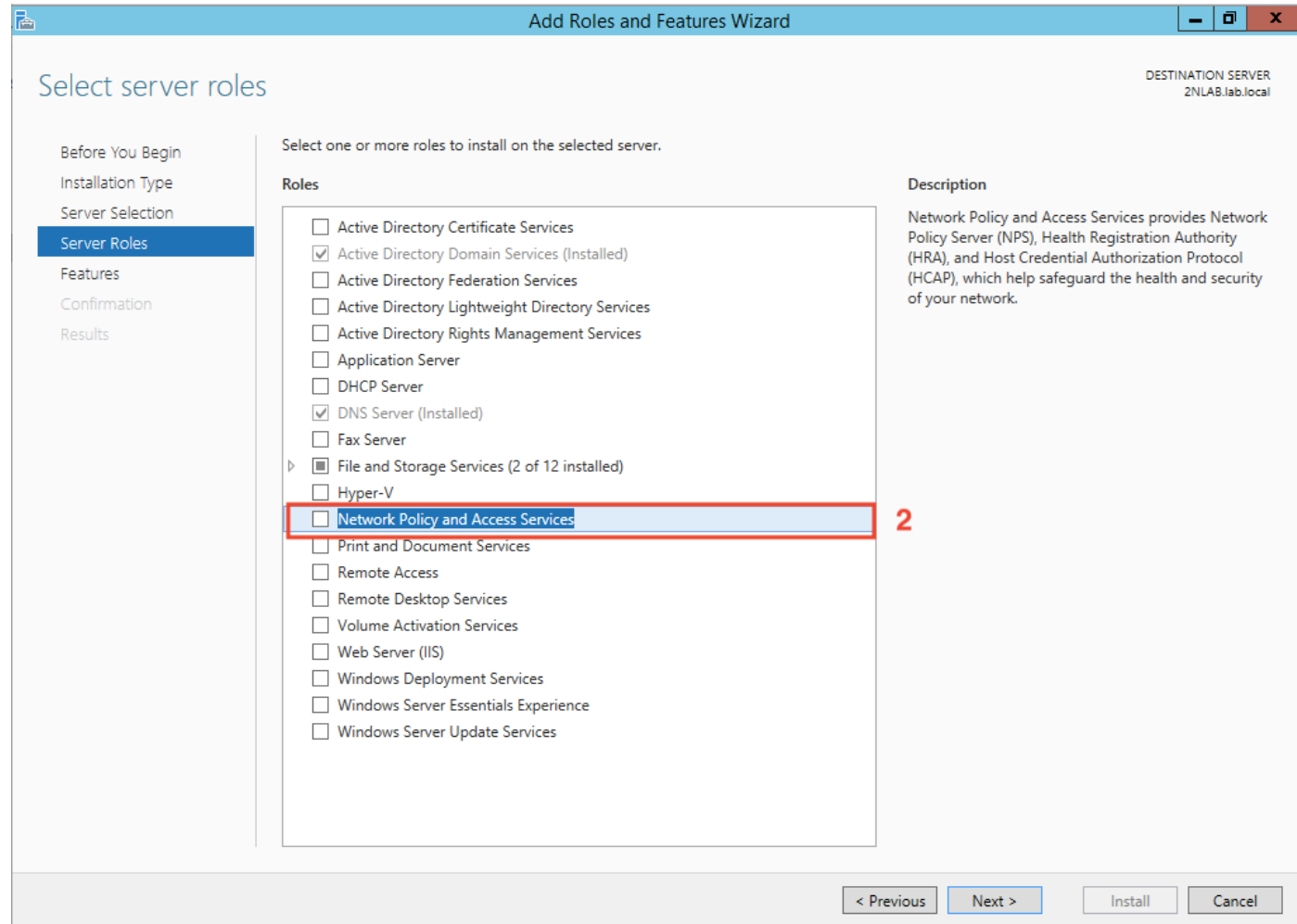
Prerrequisitos

- ❖ 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

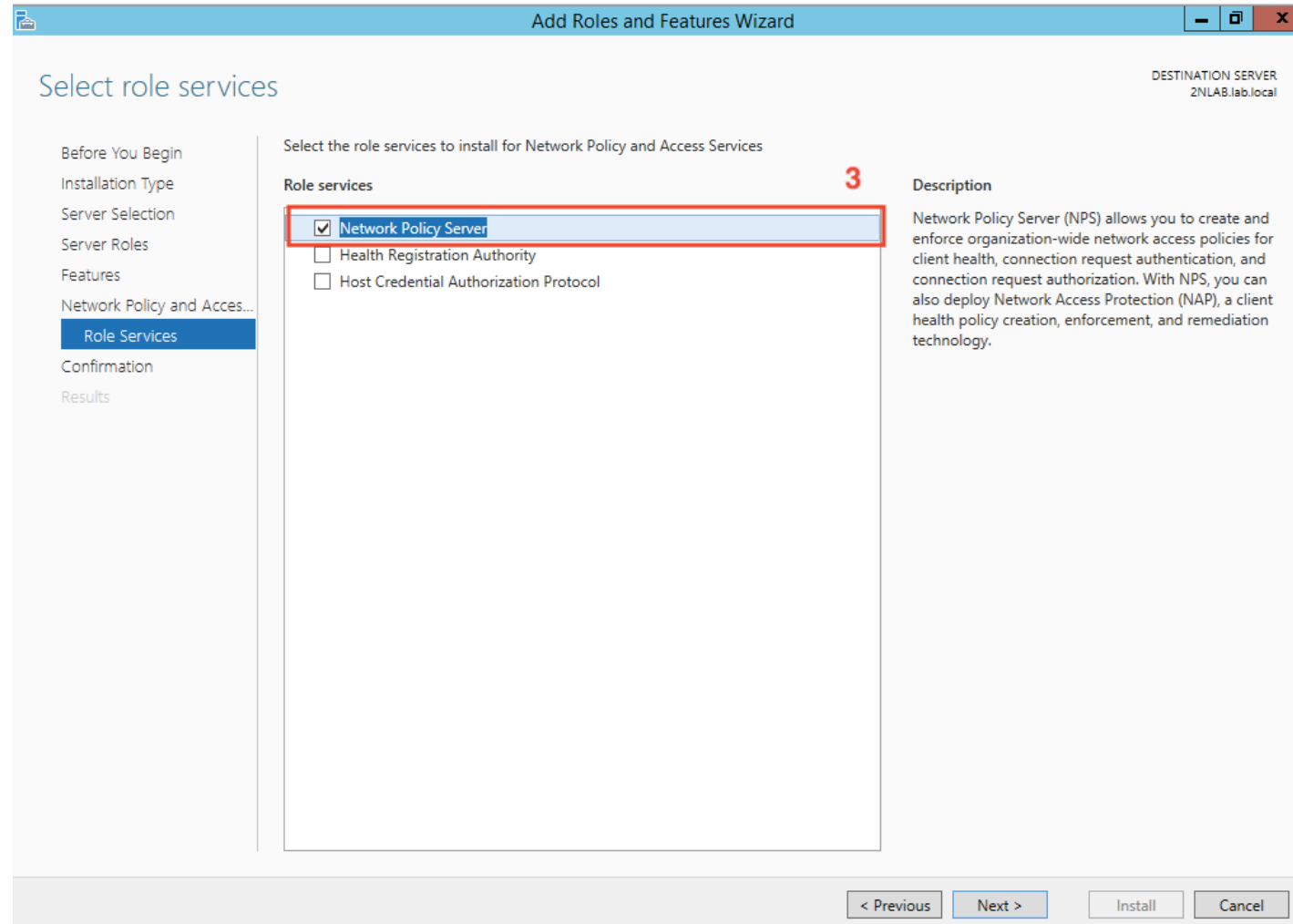
Configurando Windows Server NPS - Pasos



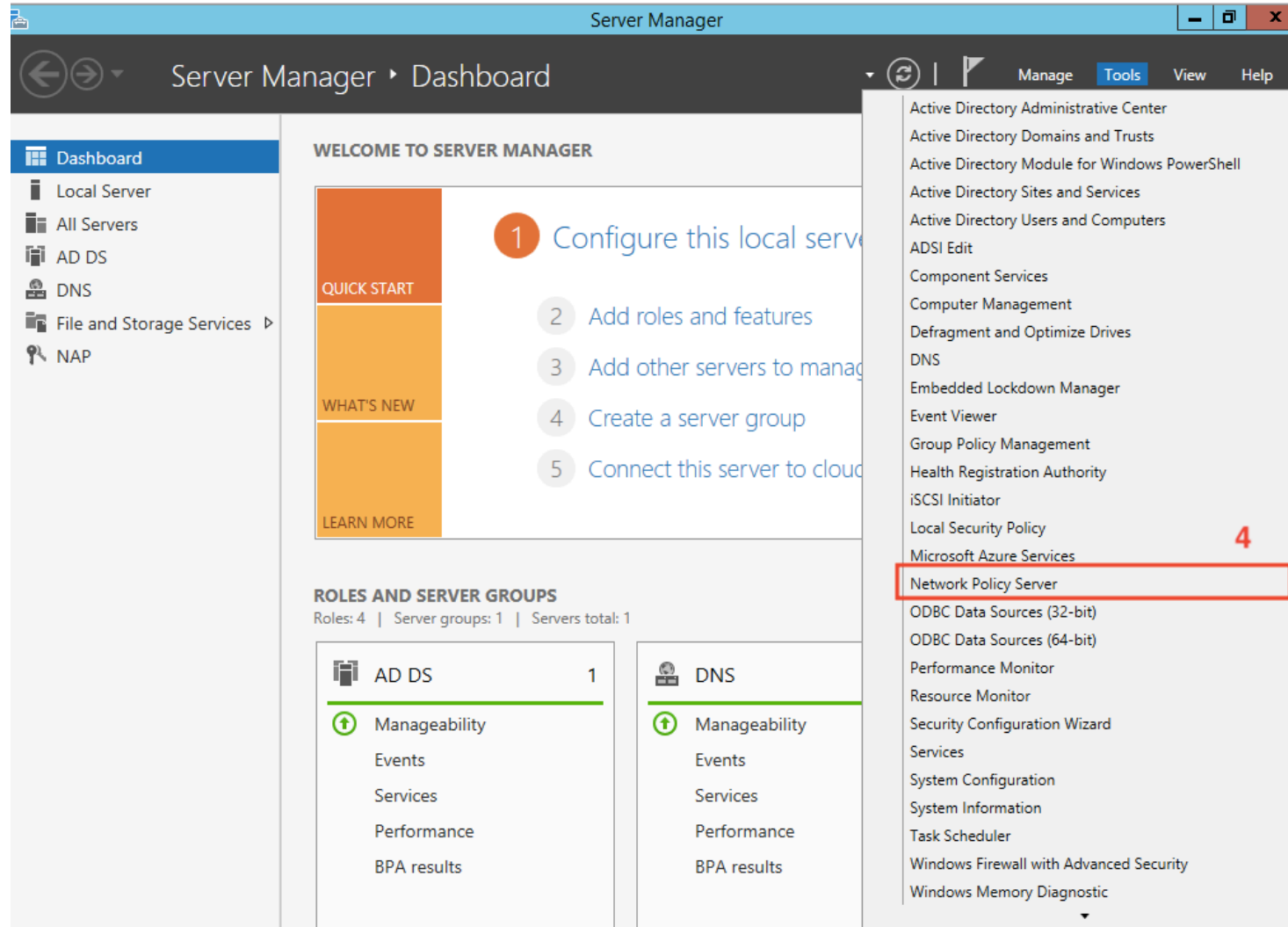
Configurando Windows Server NPS - Pasos



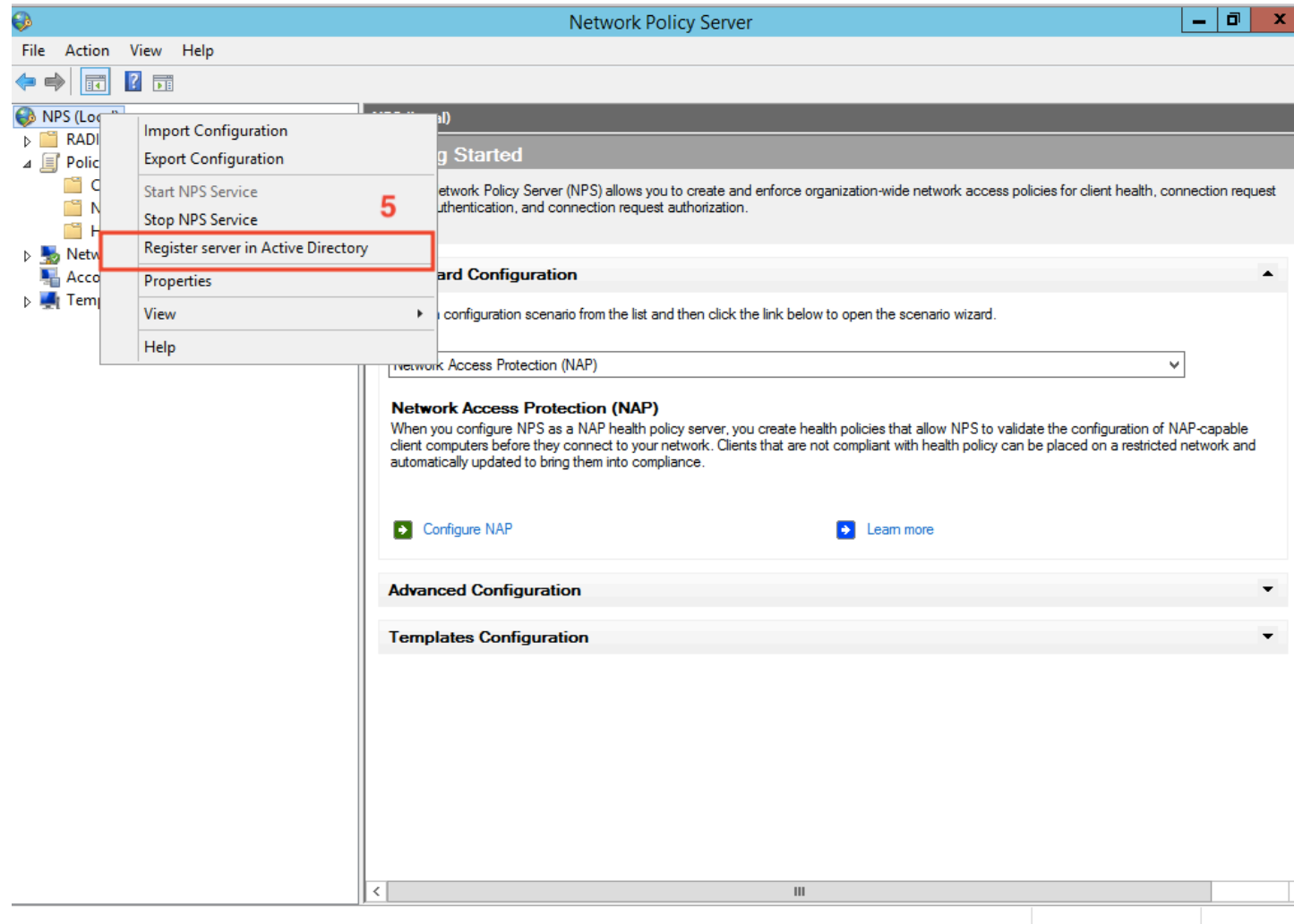
Configurando Windows Server NPS - Pasos



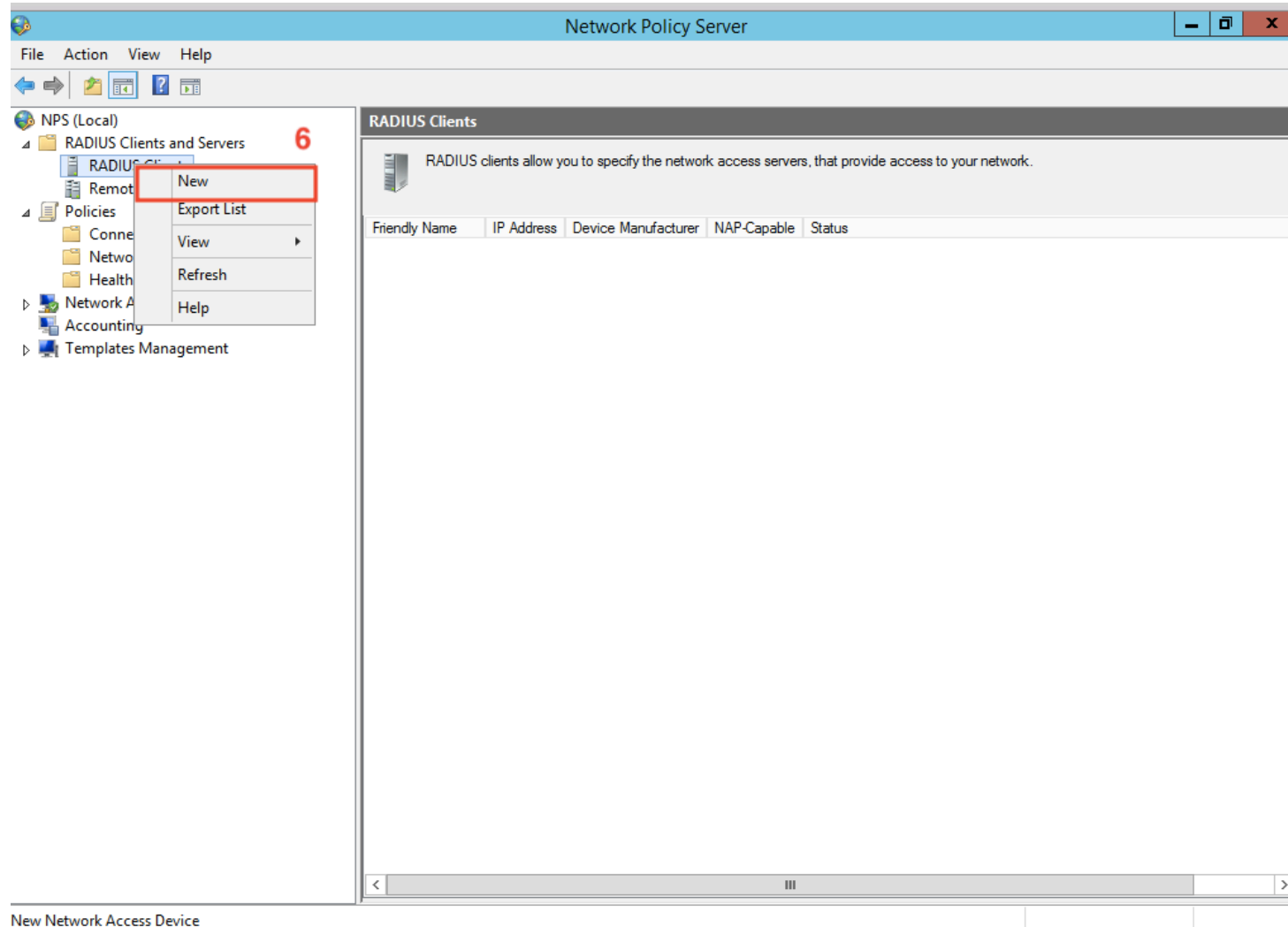
Configurando Windows Server NPS - Pasos



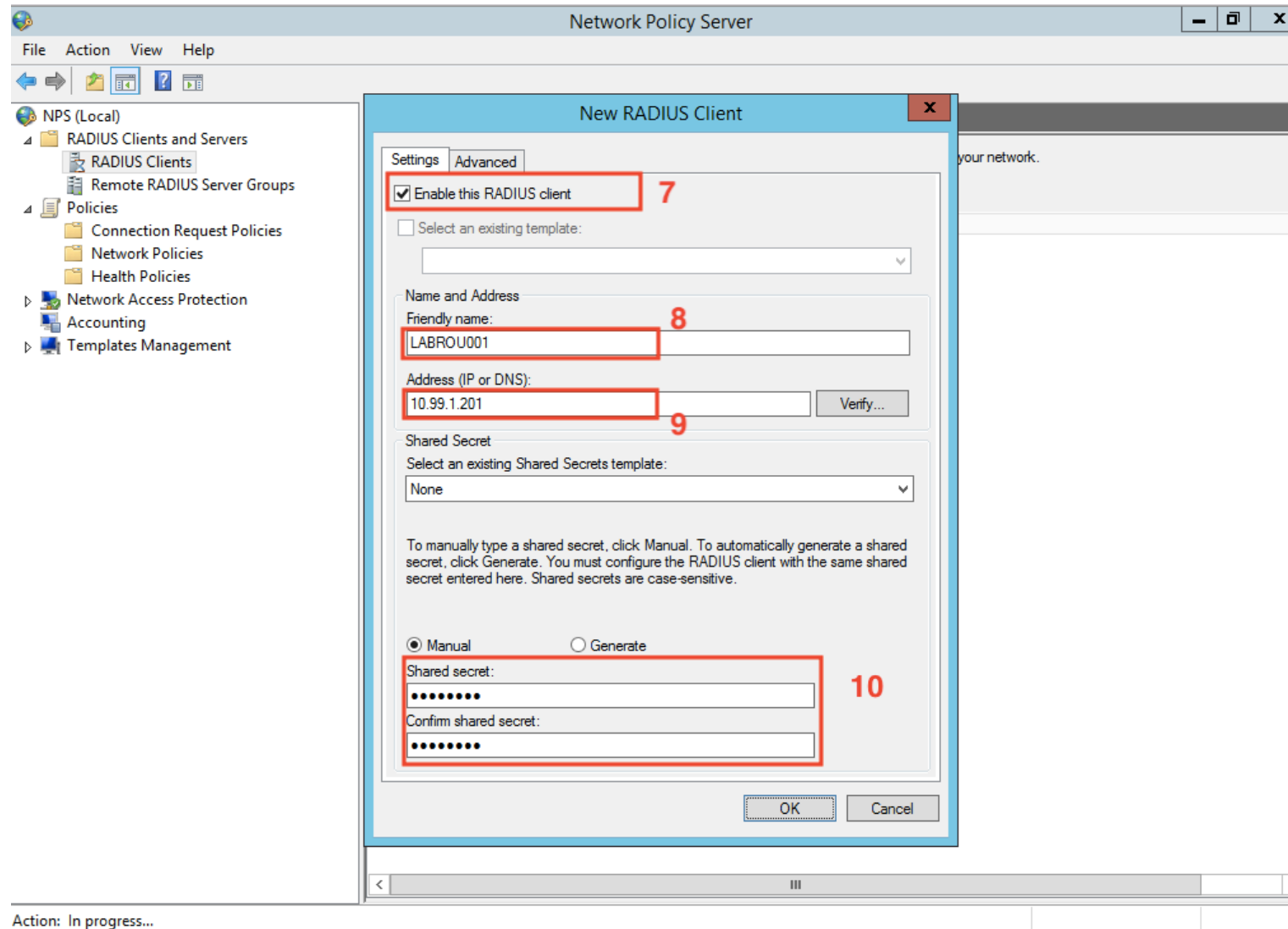
Configurando Windows Server NPS - Pasos



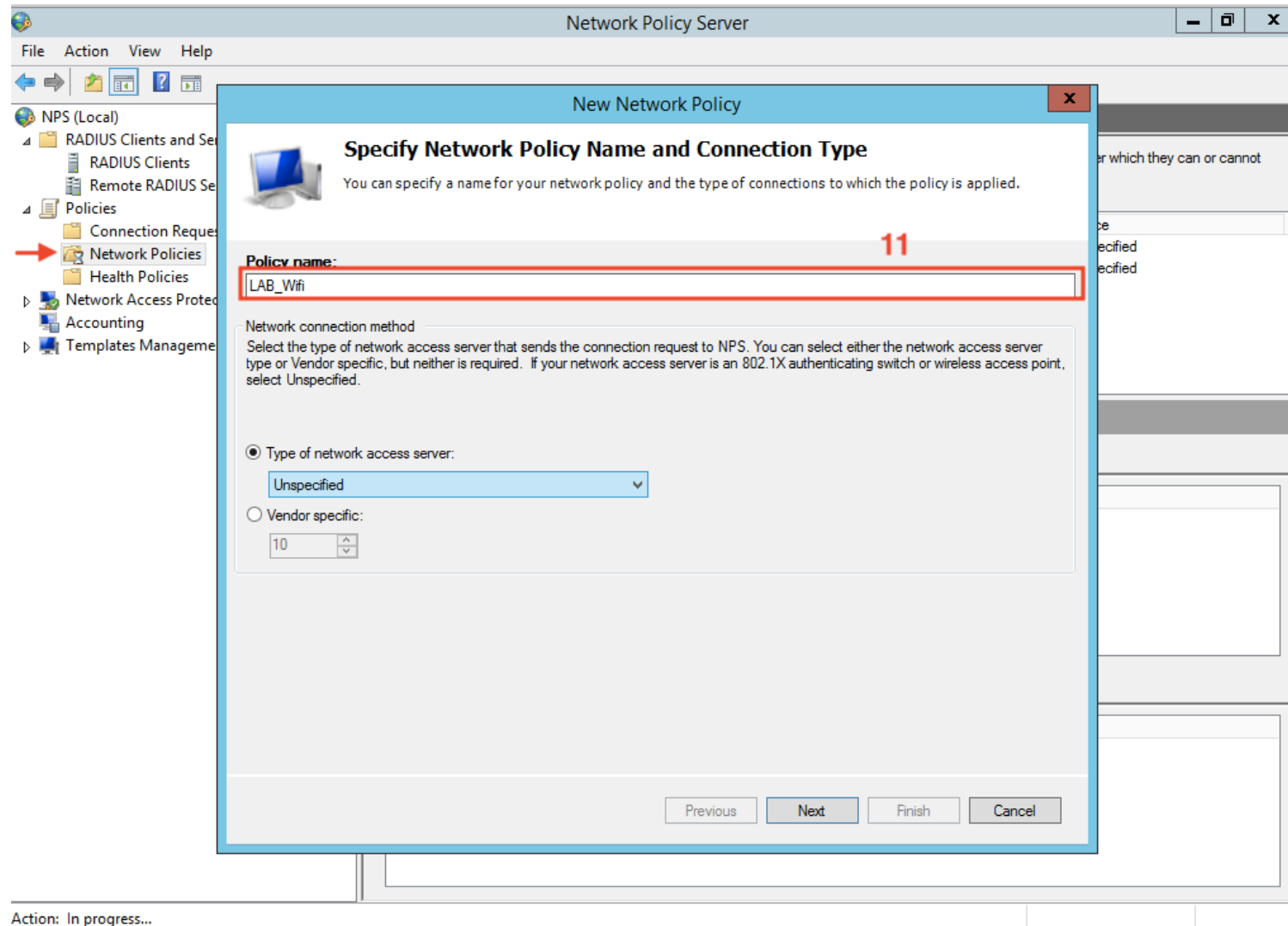
Configurando Windows Server NPS - Pasos



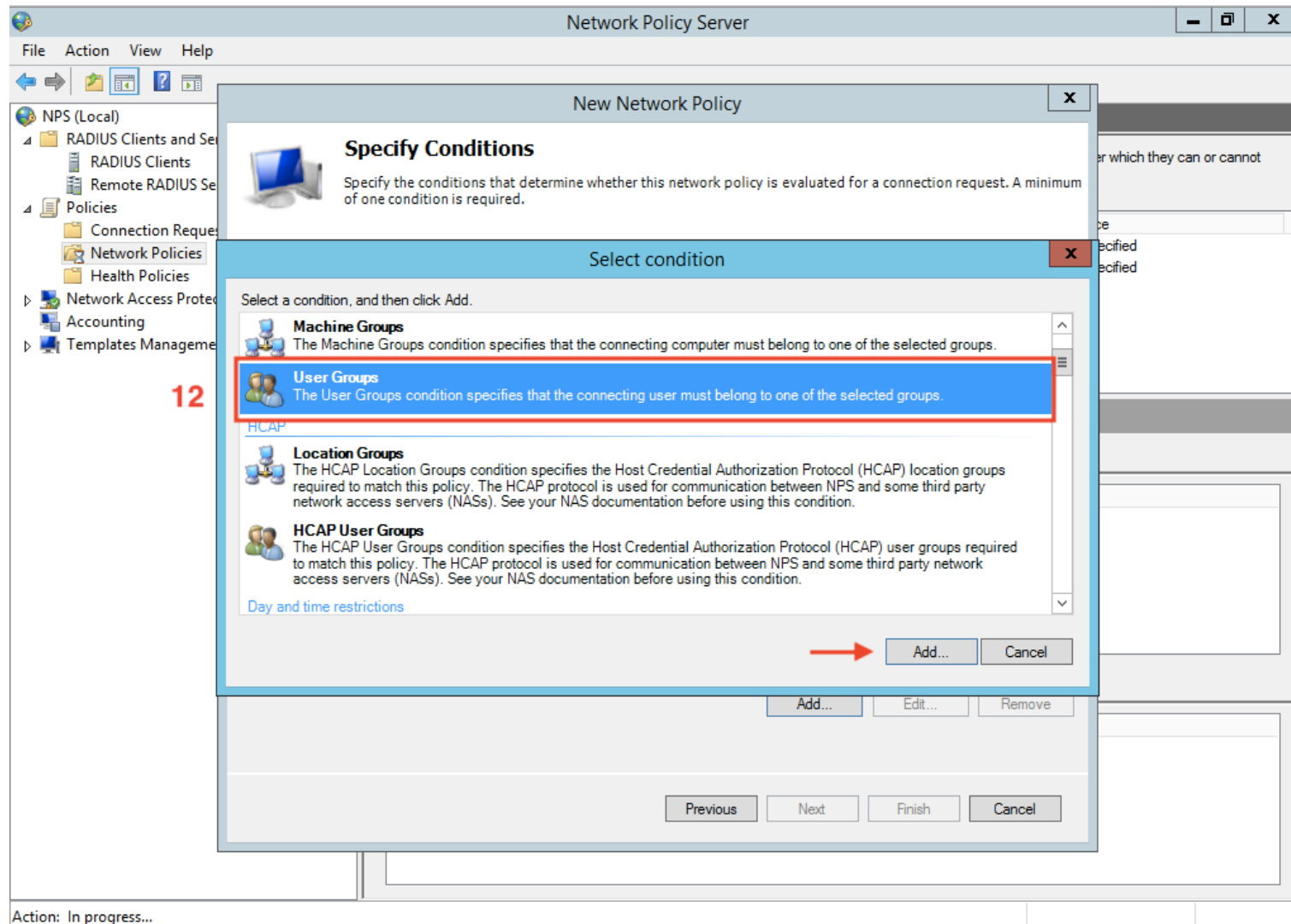
Configurando Windows Server NPS - Pasos



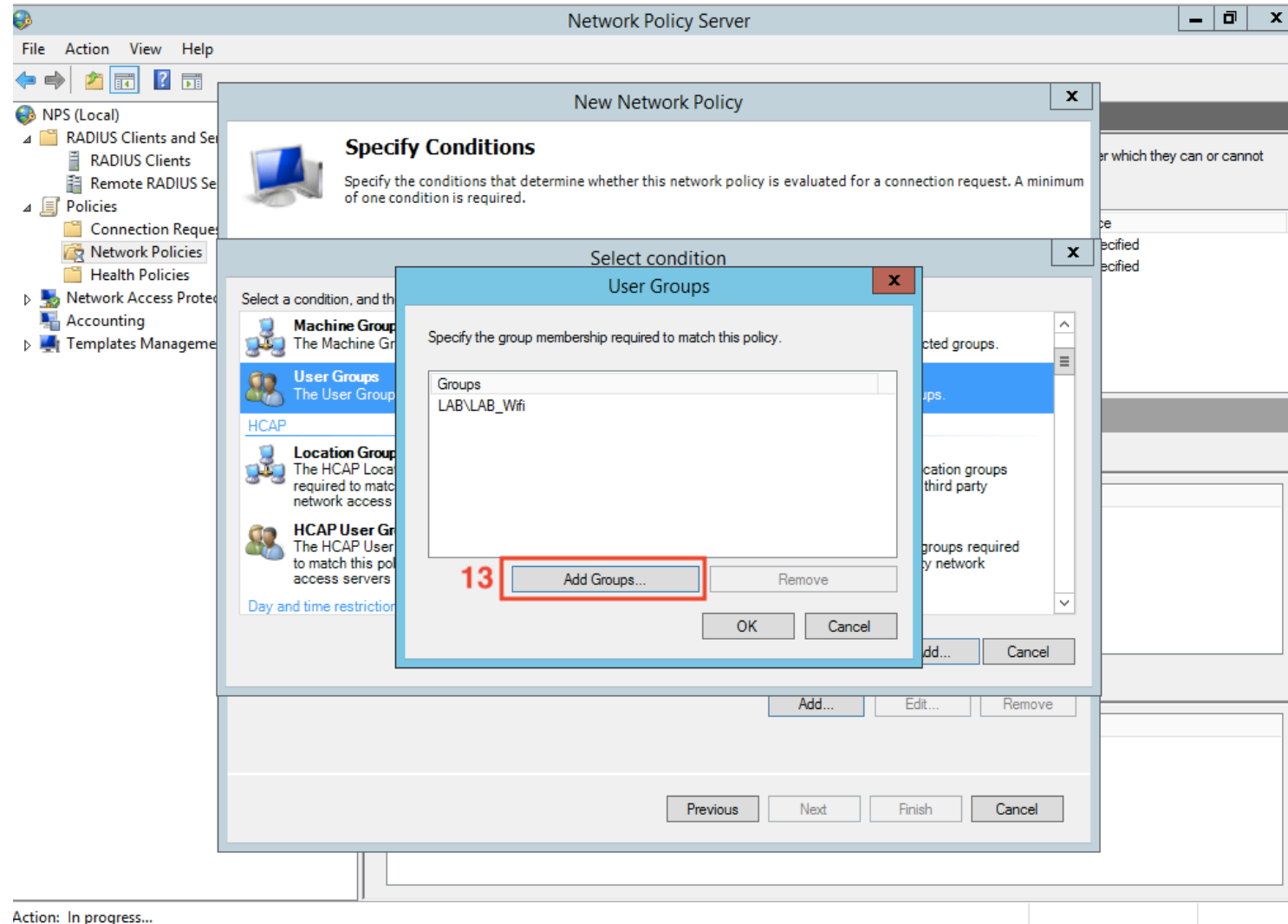
Configurando Windows Server NPS - Pasos



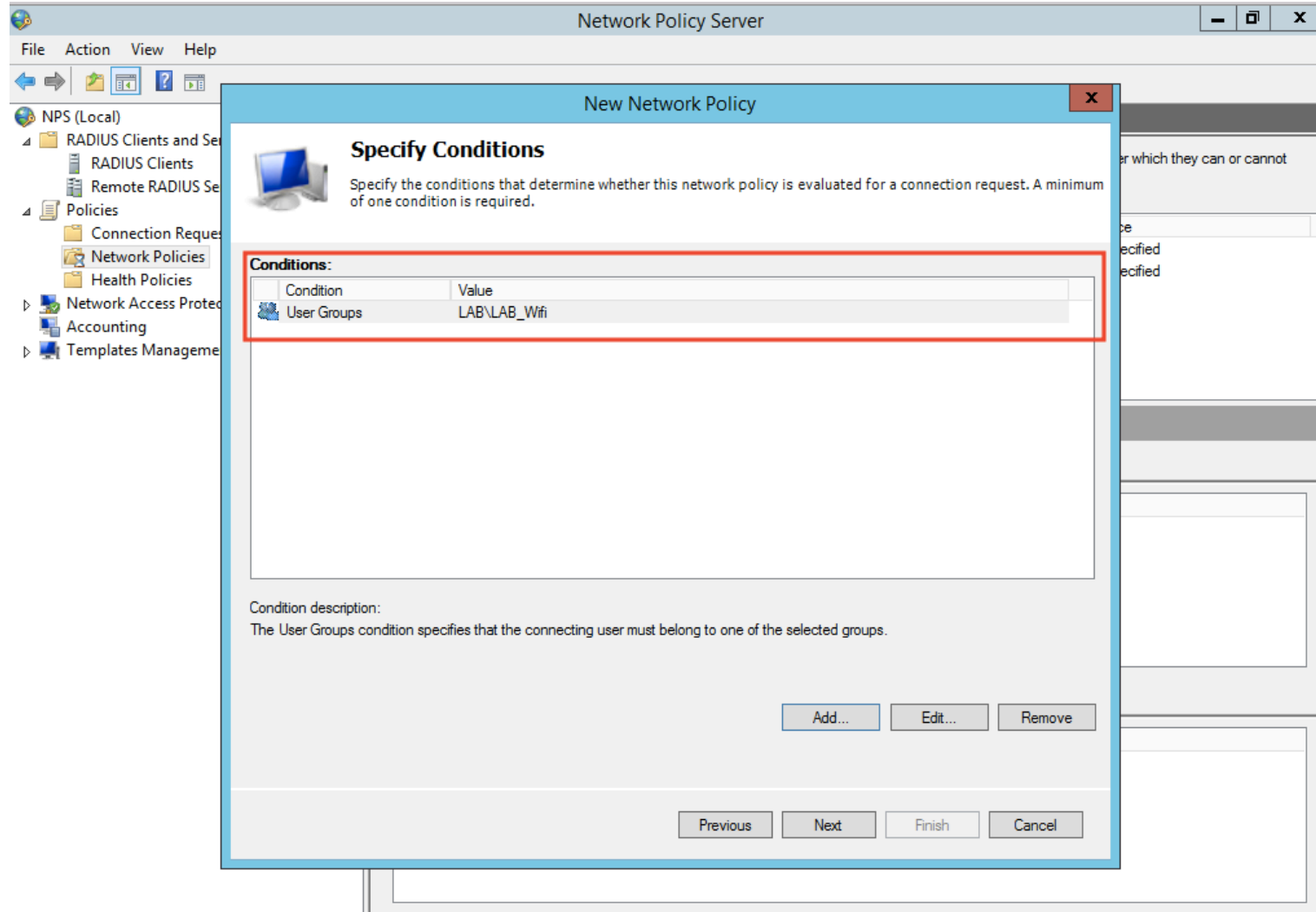
Configurando Windows Server NPS - Pasos



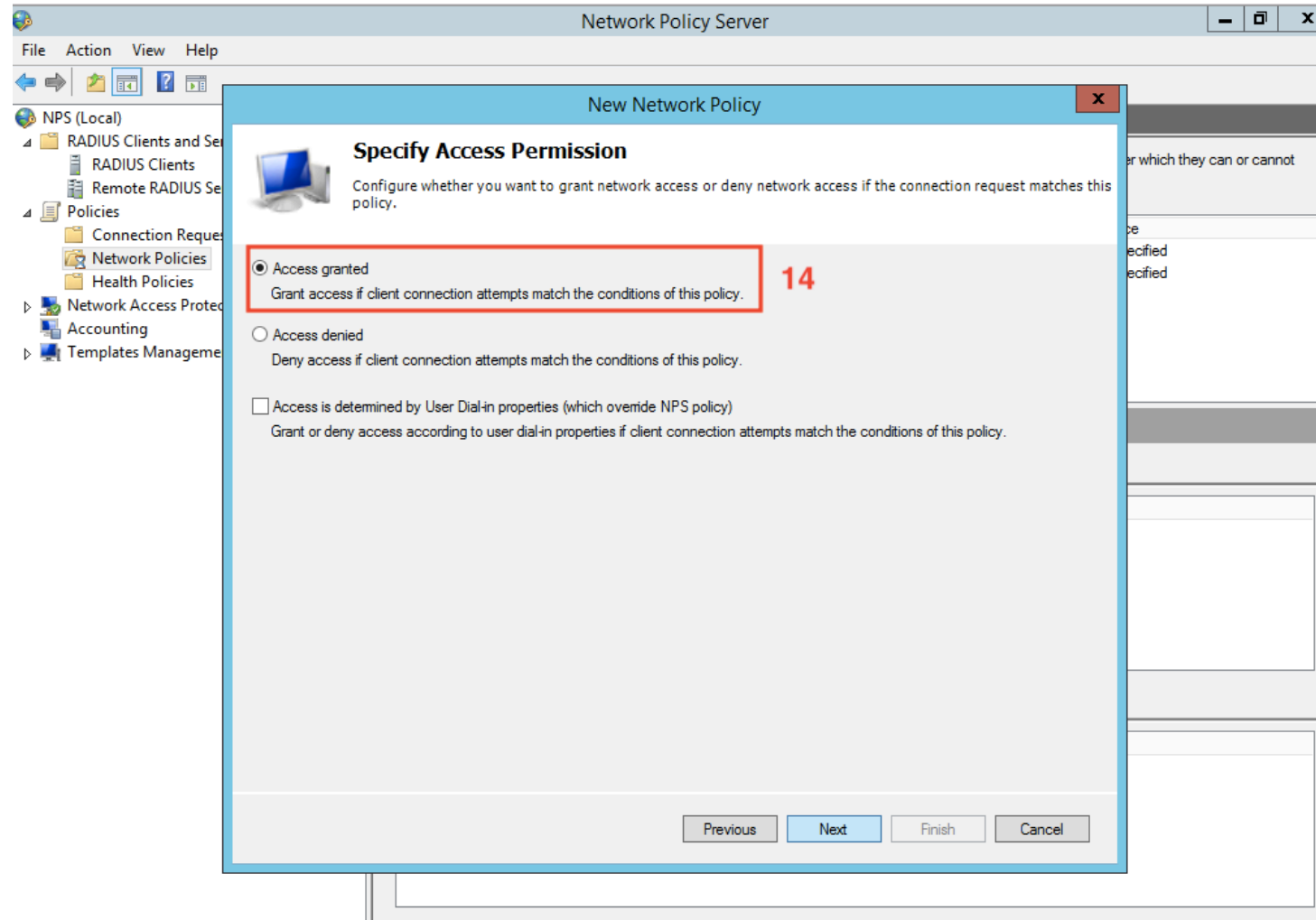
Configurando Windows Server NPS - Pasos



Configurando Windows Server NPS - Pasos

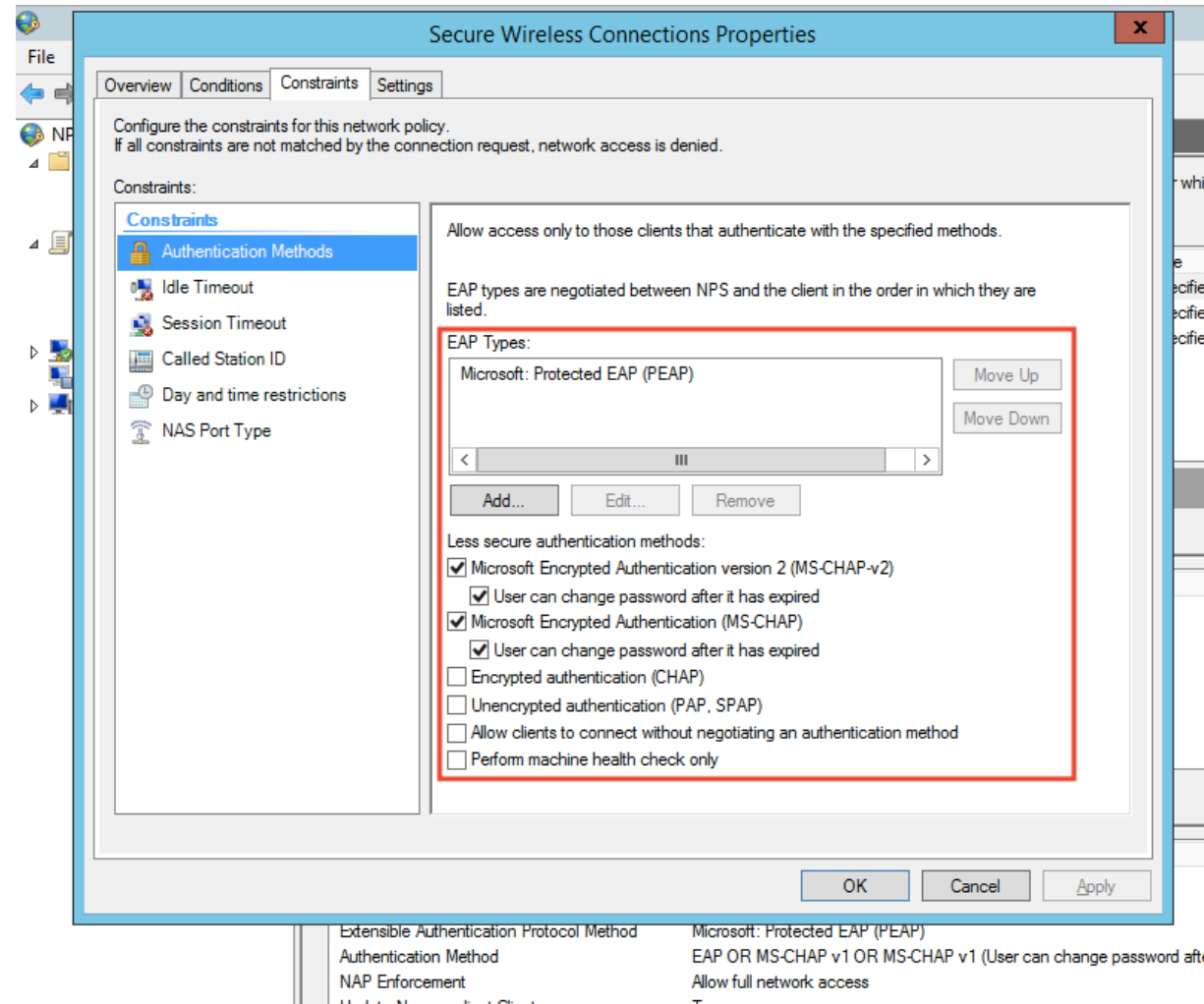


Configurando Windows Server NPS - Pasos

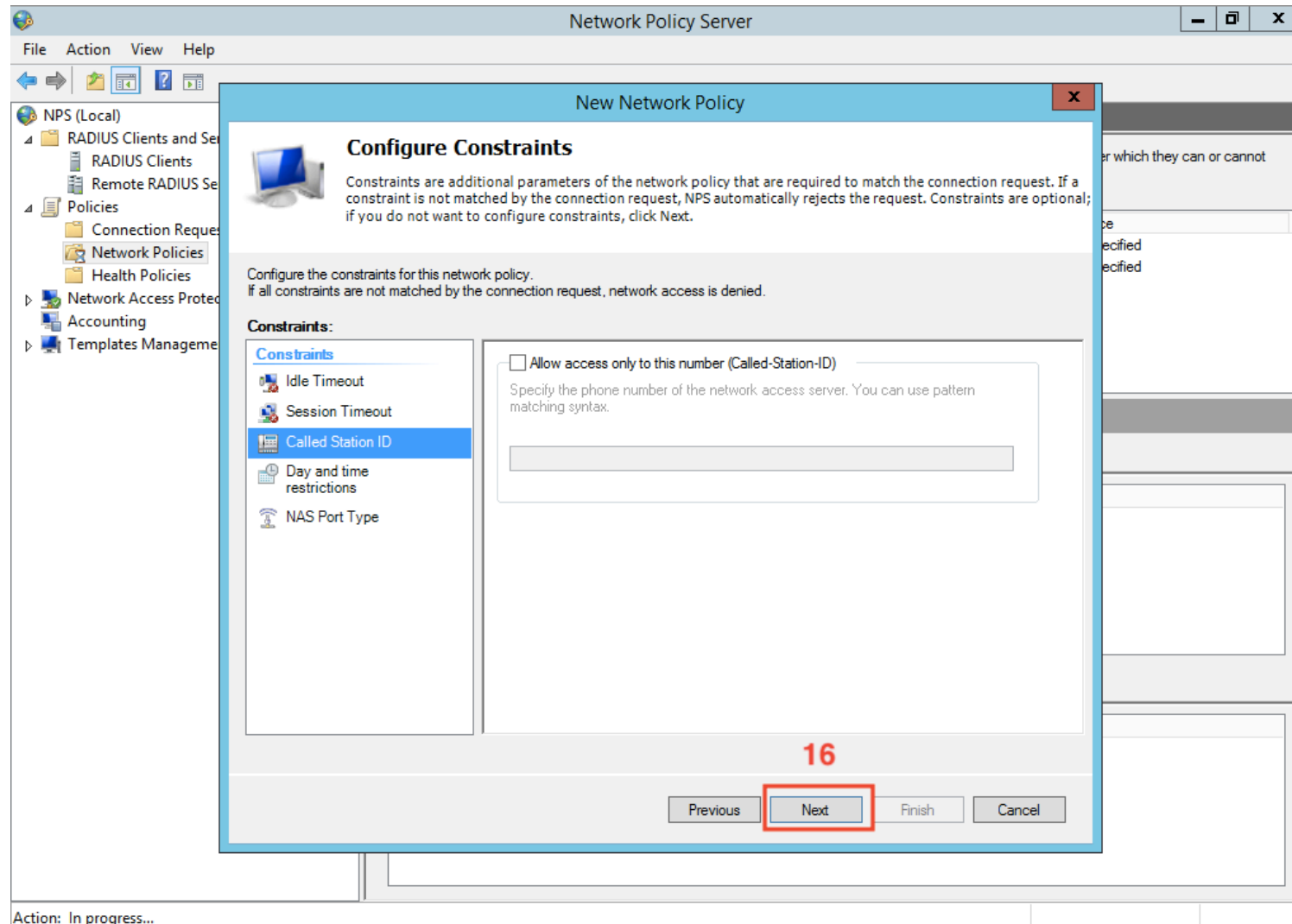


Action: In progress...

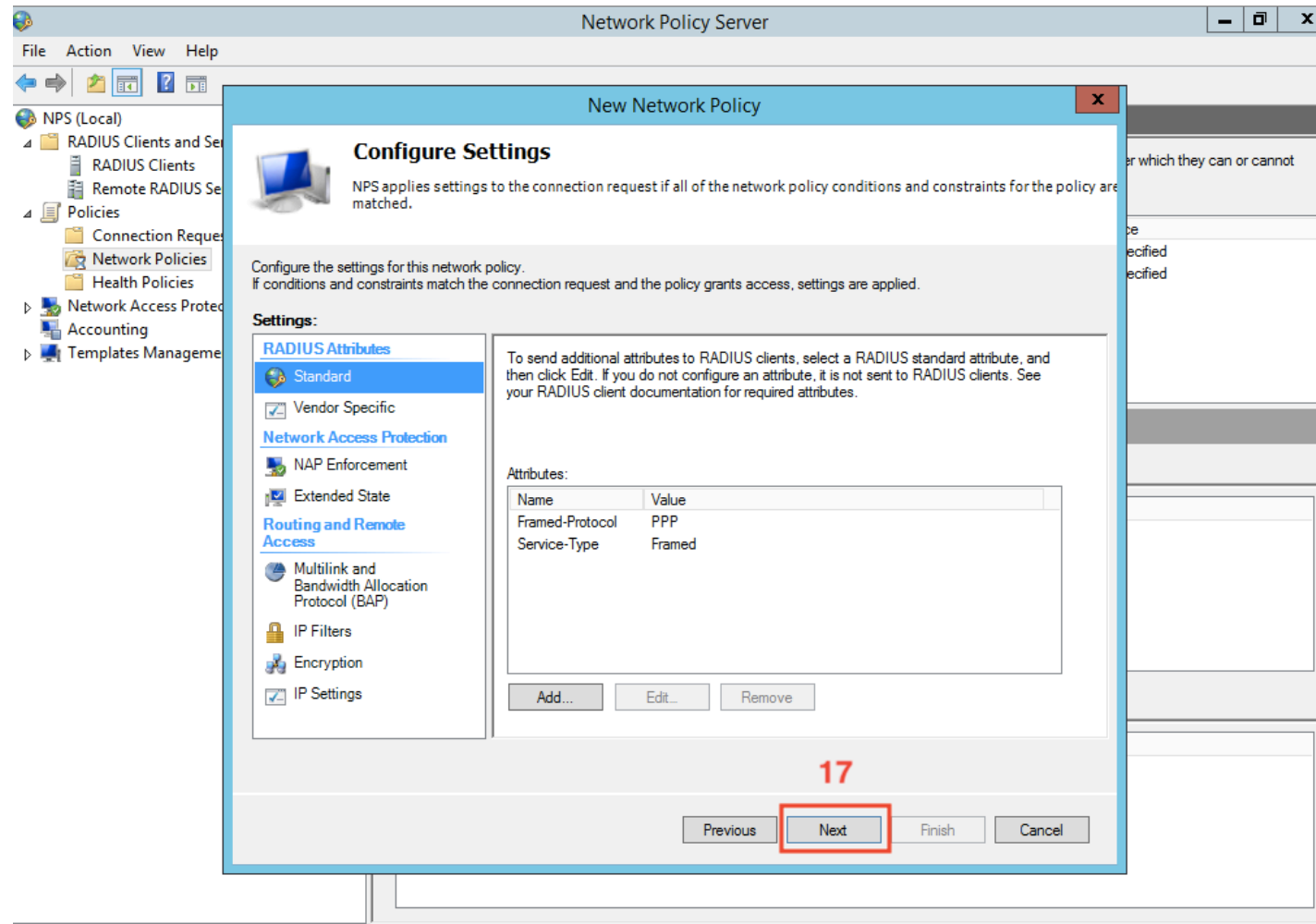
Configurando Windows Server NPS - Pasos



Configurando Windows Server NPS - Pasos

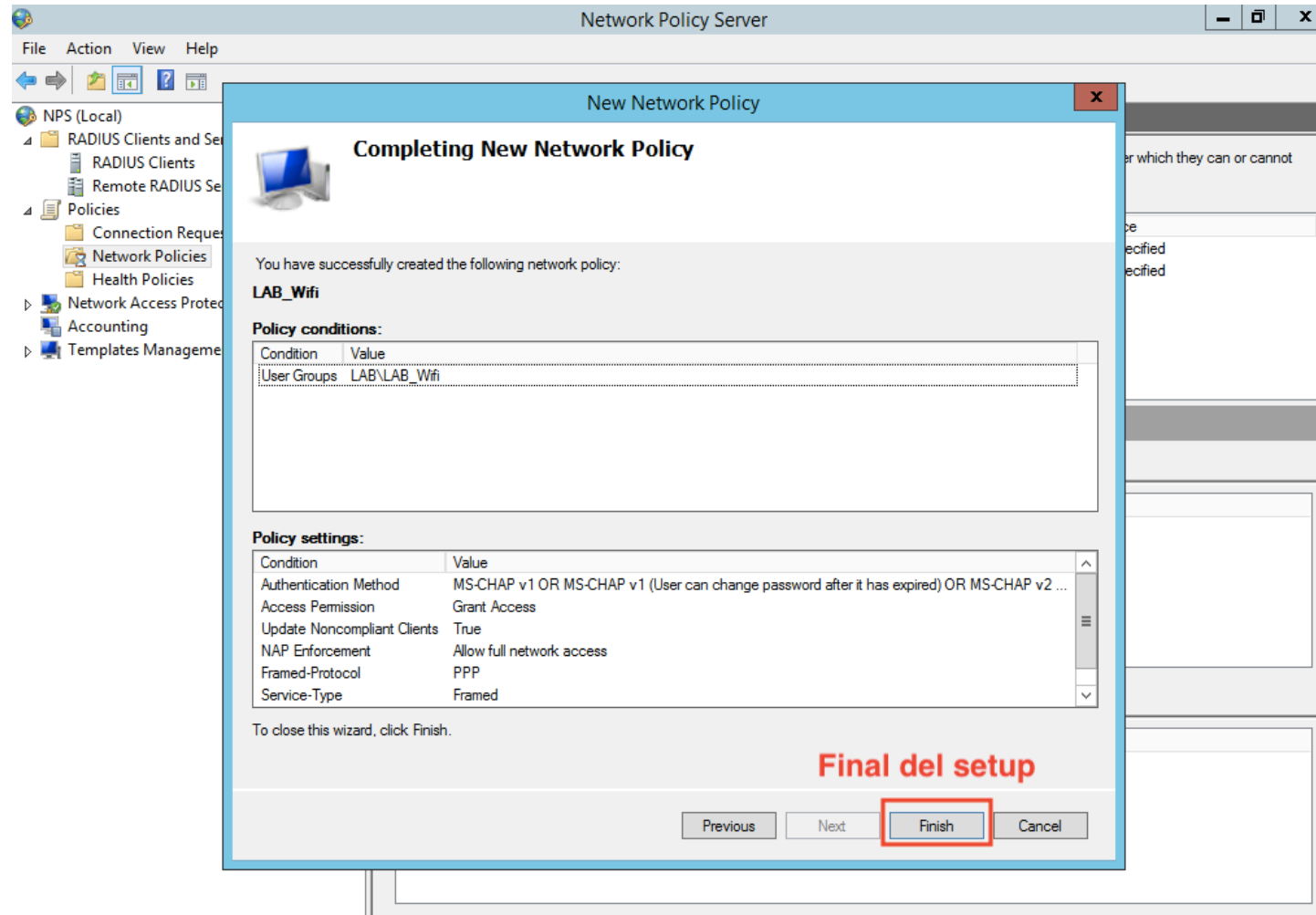


Configurando Windows Server NPS - Pasos



Action: In progress...

Configurando Windows Server NPS - Pasos



Action: In progress...

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

The screenshot shows the Mikrotik WinBox CAPsMAN configuration interface. The main window has tabs for CAP Interface, Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, Rates, Remote CAP, Radio, and Registration Table. Below the tabs are buttons for adding, removing, and checking configurations, along with 'Reselect Channel', 'Manager', and 'AAA' buttons. A table displays the configuration for a CAP interface named 'MikroTik-1'.

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

A 'CAPs Manager' dialog box is open, showing the following configuration options:

- Enabled
- Certificate: [Dropdown]
- CA Certificate: [Dropdown]
- Require Peer Certificate
- Generated Certificate: [Text Field]
- Generated CA Certificate: [Text Field]
- Package Path: [Text Field]
- Upgrade Policy: none [Dropdown]

Buttons for OK, Cancel, Apply, and Interfaces are also visible.

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

The screenshot shows the Mikrotik CAPsMAN configuration interface. The 'Datapaths' tab is selected. A dialog box titled 'New CAPs Datapath Configuration' is open, showing the following fields:

- Name:
- MTU:
- L2 MTU:
- ARP:
- Bridge:
- Bridge Cost:
- Bridge Horizon:
- Local Forwarding:
- Client To Client Forwarding:
- VLAN Mode:
- VLAN ID:
- Interface List:

Buttons on the right side of the dialog include: OK, Cancel, Apply, Comment, Copy, and Remove.

Configurando el CAPsMAN - Pasos

The screenshot shows the Mikrotik WinBox CAPsMAN configuration interface. The main window has tabs for CAP Interface, Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, Rates, Remote CAP, Radio, and Registration Table. A configuration window titled 'CAPs Configuration <cfg_Lab>' is open, showing the following fields:

Name	SSID	Hide SSID	Load Bal...	Country	Channel	Frequency	Band	Rate
cfg_Lab	LAB_Wifi							

The configuration window also includes tabs for Wireless, Channel, Rates, Datapath, and Security. The 'Name' field is set to 'cfg_Lab', the 'Mode' is set to 'ap', and the 'SSID' is set to 'LAB_Wifi'. Other fields like 'Hide SSID', 'Load Balancing Group', 'Distance', 'Hw. Retries', and 'Hw. Protection Mode' are currently empty. The window has 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove' buttons.

Configurando el CAPsMAN - Pasos

The screenshot shows the Mikrotik WinBox CAPsMAN configuration interface. The main window has tabs for CAP Interface, Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, Rates, Remote CAP, Radio, and Registration Table. A modal window titled 'CAPs Configuration <cfg_Lab>' is open, showing tabs for Wireless, Channel, Rates, Datapath, and Security. The 'Datapath' dropdown menu is highlighted with a red box and set to 'datapath_LAB'. Below this, there are input fields for MTU, L2 MTU, ARP, Bridge, Bridge Cost, and Bridge Horizon. On the right side of the modal, there are buttons for OK, Cancel, Apply, Comment, Copy, and Remove.

Configurando el CAPsMAN - Pasos

The screenshot shows the Mikrotik WinBox interface for configuring CAPsMAN. The main window is titled 'CAPsMAN' and has several tabs: 'CAP Interface', 'Provisioning', 'Configurations', 'Channels', 'Datapaths', 'Security Cfg.', 'Access List', 'Rates', 'Remote CAP', 'Radio', and 'Registration Table'. The 'Configurations' tab is active. Below the tabs are icons for adding (+), deleting (-), saving (floppy), and filtering (funnel). A table with columns 'Name', 'SSID', 'Hide SSID', 'Load Bal...', 'Country', 'Channel', 'Frequency', 'Band', and 'Rate' is visible. A dialog box titled 'CAPs Configuration <cfg_Lab>' is open, showing the 'Security' tab. The 'Security' dropdown menu is highlighted with a red box and contains the text 'LAB_Sec'. Other fields in the dialog include 'Authentication Type', 'Encryption', 'Group Encryption', 'Group Key Update', 'Passphrase', 'EAP Methods', and 'EAP Radius Accounting'. On the right side of the dialog are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and '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

Hw. Supported Modes: [dropdown]

Identity Regexp: [input]

Common Name Regexp: [input]

IP Address Ranges: [dropdown]

Action: create enabled

Master Configuration: cfg_LAB

Slave Configuration: [dropdown]

Name Format: identity

Name Prefix: [dropdown]

enabled

OK Cancel Apply Disable Comment Copy Remove

Configurando el CAPs - Pasos

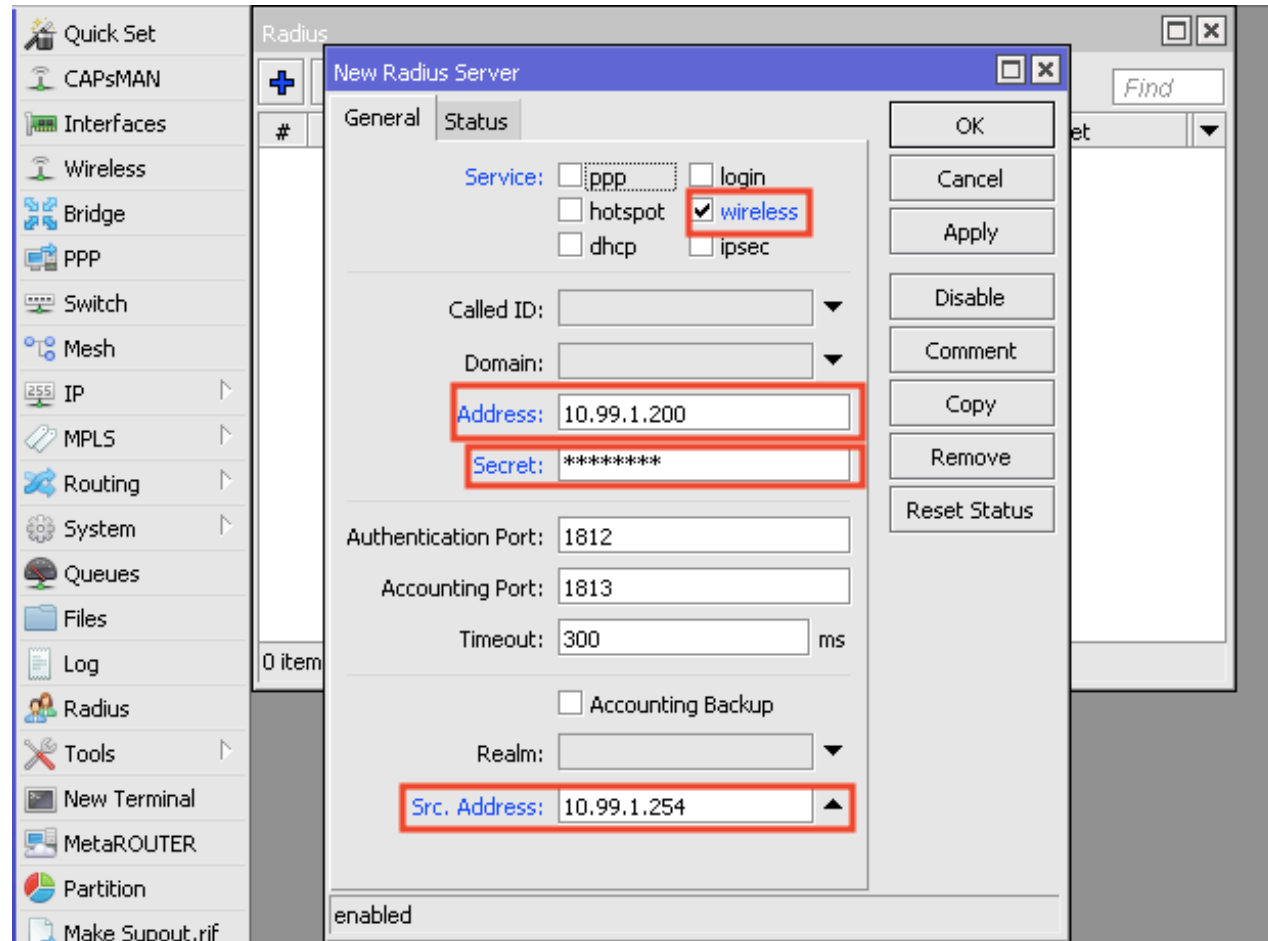
The screenshot displays the Mikrotik WinBox interface for configuring a CAP (Certificate Authentication Protocol) on a wireless interface. The 'Wireless Tables' window is open, showing a table with one entry for 'wlan1'. A 'CAP' configuration dialog box is overlaid on top, with several fields highlighted by red boxes:

- Enabled:** A checkbox that is checked.
- Interfaces:** A dropdown menu set to 'wlan1'.
- Discovery Interfaces:** A dropdown menu set to 'ether1'.
- CAPsMAN Addresses:** A dropdown menu set to '10.99.1.254'.

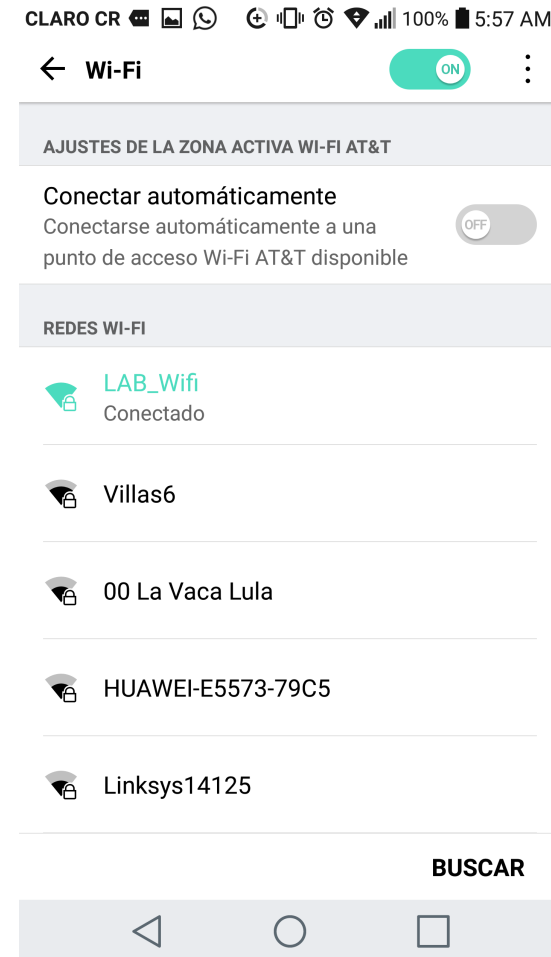
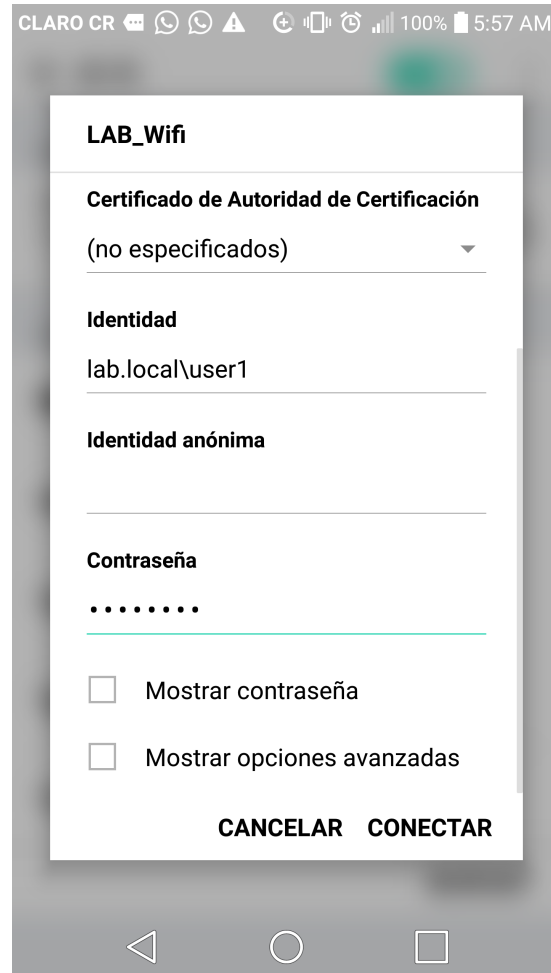
Other fields in the dialog include 'Certificate' (set to 'none'), 'Lock To CAPsMAN' (unchecked), 'CAPsMAN Names', 'CAPsMAN Certificate Common Names', 'Bridge' (set to 'none'), 'Static Virtual' (unchecked), 'Requested Certificate', and 'Locked CAPsMAN Common Name'.

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

Configurando el Radius - Pasos



Resultado Final



PREGUNTAS?

lucas@2n.do

