



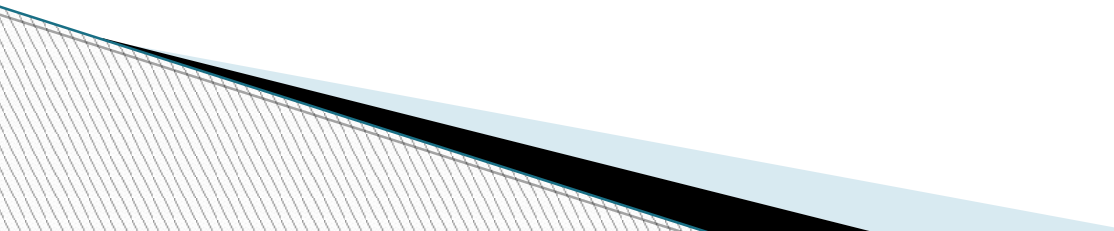
Konfigurasi MikroTIK di Sekolah Saya

Oleh Asep Jalaludin

Biodata

- ▶ Asep Jalaludin
- ▶ Pengajar Mapel Produktif TKJ dan Staf TI
- ▶ Trainer Mikrotik Academy dan Oracle Academy

SMK Bintang Nusantara School

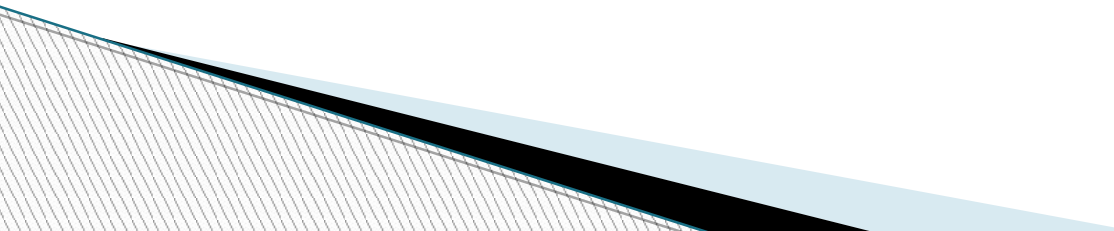
- ▶ Mulai beroperasi sejak Juli 2011
 - ▶ Berlokasi di Sepatan, Kab. Tangerang, Banten
 - ▶ Memiliki 5 Jurusan (Teknik Komputer dan Jaringan, Multimedia, Keperawatan, Farmasi , Akuntansi)
 - ▶ Jumlah siswa 123 orang (per TP 2015/2016)
 - ▶ Oktober 2014, Menjadi Mikrotik Academy
 - ▶ Agustus 2014, Menjadi Cisco Academy
 - ▶ 2014, Menjadi Oracle Academy
- 

Materi

- ▶ Konfigurasi dasar mikrotik sampai terkoneksi internet
- ▶ Bandwidth management terintegrasi dengan hotspot
- ▶ Integrasi dengan radius server dari win server 2012
- ▶ Blokir website terjadwal
- ▶ Force DHCP
- ▶ Force DNS
- ▶ Pengamanan menggunakan port knocking



Konfigurasi internet

- ▶ Set nama interface
 - ▶ Set DHCP client
 - ▶ Set IP address
 - ▶ Set DNS
 - ▶ Set route (jika tidak menggunakan DHCP client)
 - ▶ Set NAT (jika tidak menggunakan hotspot)
 - ▶ Set DHCP server (jika tidak menggunakan hotspot)
- 

Set interface name

The screenshot illustrates the steps to configure an interface name in Mikrotik WinBox. The interface list on the left shows several Ethernet interfaces, with 'ether1-internet' selected. The configuration window for this interface is open, showing the 'General' tab. The 'Name' field is highlighted, and the 'OK' button is circled.

1 Interfaces

2 ether1-internet

3 ether1-internet

4 OK

Interface	Ethernet	EoIP Tunnel
+	-	✓
Name	Type	
ether1-internet	Ethernet	
ether2-local	Ethernet	
ether3	Ethernet	
ether4	Ethernet	
ether5	Ethernet	
wlan1	Wireless	

Interface <ether1-internet>

General | Ethernet | Overall Stats | Rx Stats | Tx Stats | ...

Name: ether1-internet

Type: Ethernet

MTU: 1500

L2 MTU: 1598

Max L2 MTU: 4074

MAC Address: D4:CA:6D:E0:30:70

ARP: enabled

Master Port: none

Bandwidth (Rx/Tx): unlimited / unlimited

Switch: switch1

OK

Cancel

Apply

Disable

Comment

Torch

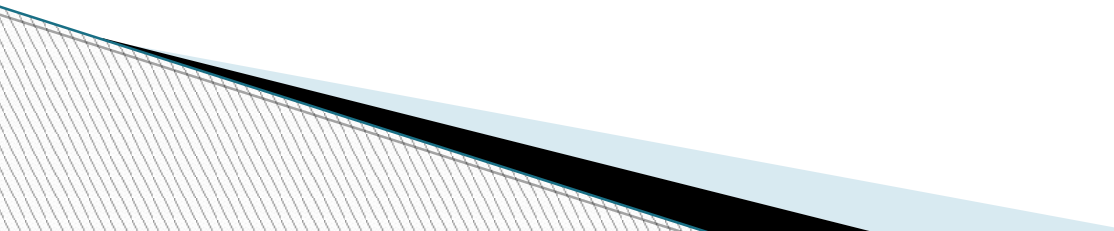
Cable Test

Blink

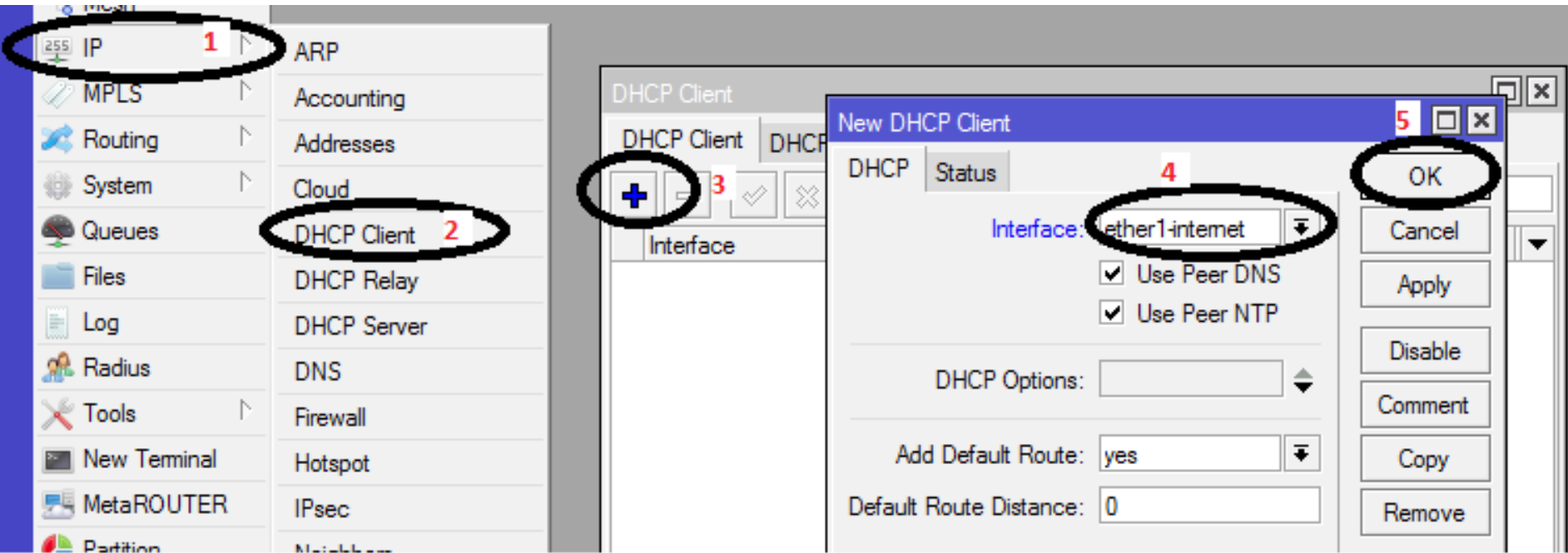
Reset MAC Address

Reset Counters

Set interface name

- ▶ /interface ethernet
 - ▶ Set name=ether1-internet
number=0
 - ▶ Set name=ether2-lokal
number=1
- 

Set DHCP client



Set DHCP client

- ▶ `/ip dhcp-client`
- ▶ `add interface=ether1 -internet`

Set IP address

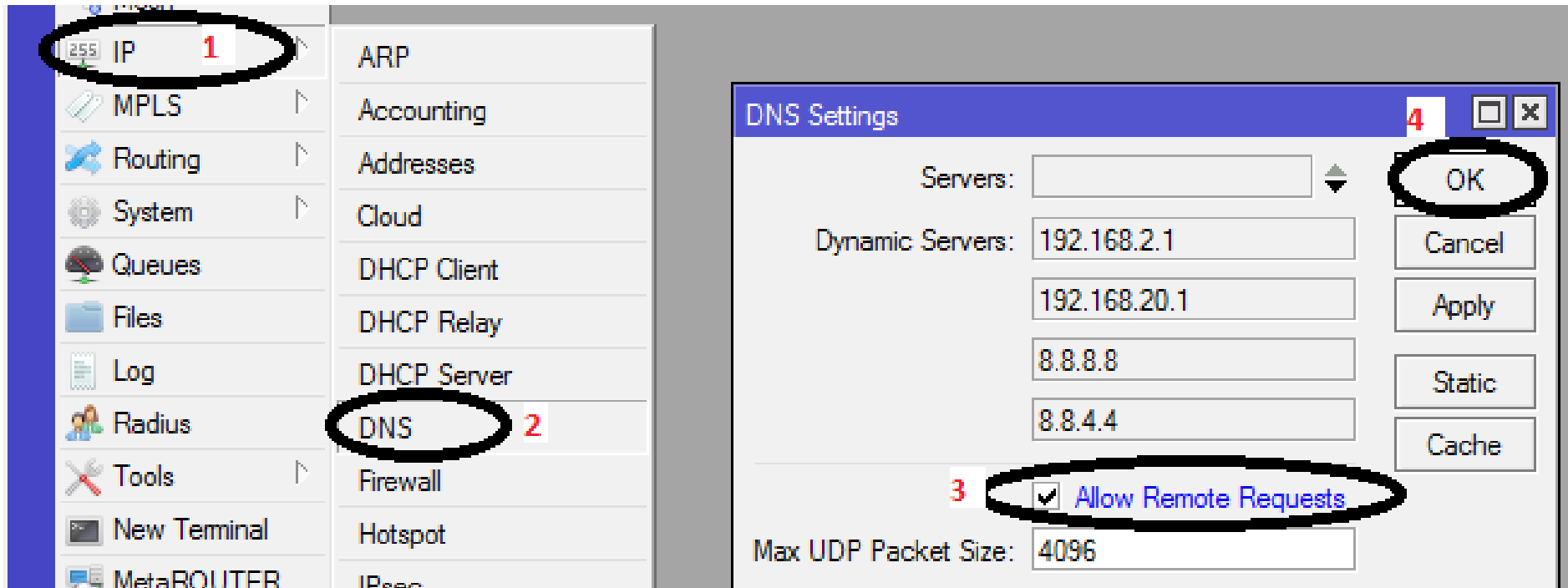
The screenshot illustrates the steps to set an IP address in Mikrotik WinBox:

1. Select **IP** in the left sidebar.
2. Select **Addresses** in the main menu.
3. Click the **+** icon in the **Address List** dialog to add a new address.
4. The **New Address** dialog appears.
5. Select the **Interface** (ether2/lokal) from the dropdown menu.
6. Click the **OK** button to confirm the address configuration.

Set IP address

- ▶ `/ip address`
- ▶ `add address=192.168.2.1 /23`
`interface=ether2-lokal`

Set DNS



Set DNS

- ▶ /ip dns
- ▶ Set servers=8.8.8.8,8.8.4.4
- ▶ set allow-remote-requests=yes

Set Route

The screenshot displays a network configuration application with a sidebar menu on the left. The 'IP' option is circled in red and labeled with a red '1'. The 'Routes' option is also circled in red and labeled with a red '2'. The 'Route List' table is visible, showing a list of routes. A red '+' button is circled in red and labeled with a red '3'. The 'New Route' dialog box is open, showing the 'General' tab. The 'Gateway' field is circled in red and labeled with a red '4', and the 'OK' button is circled in red and labeled with a red '5'.

Route List

	Routes	Next hops	Rules	VRF
3	Dst. Address	/	Gateway	
	DAS	▶ 0.0.0.0/0	192.168.2	
	DAC	▶ 192.168.2.0/23	ether1-int	
	DAC	▶ 192.168.4.0/23	ether2-lok	

New Route

General Attributes

Dst. Address: 0.0.0.0/0

4 Gateway: 0.0.0.0

Check Gateway:

Type: unicast

Distance:

Scope: 30

Target Scope: 10

OK Cancel Apply Disable Comment Copy Remove

Set Route

- ▶ `/ip route`
- ▶ `add gateway=192.168.20.1`

Set NAT

This screenshot shows the Mikrotik WinBox interface with several components highlighted for setting up NAT:

- 1**: The **IP** menu item in the left sidebar is circled.
- 2**: The **Firewall** sub-menu under the IP menu is circled.
- 3**: The **NAT** tab in the Firewall configuration window is circled.
- 4**: The **+** button to add a new rule is circled.
- 5**: The **Chain** dropdown menu in the 'New NAT Rule' dialog is circled, showing 'srcnat' selected.
- 6**: The **Out. Interface** dropdown menu in the 'New NAT Rule' dialog is circled, showing 'ether1-internet' selected.
- 7**: The **Action** tab in the 'New NAT Rule' dialog is circled.

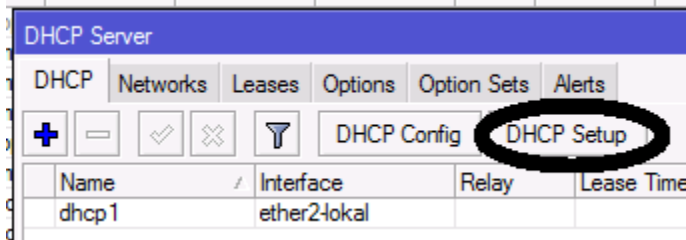
This is a close-up of the 'New NAT Rule' dialog, specifically the **Action** tab. The following elements are highlighted:

- 8**: The **Action** dropdown menu is circled, showing 'masquerade' selected.
- 9**: The **OK** button is circled.

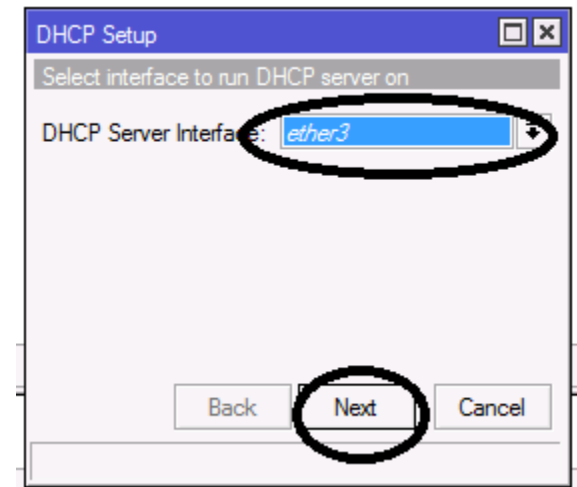
Set NAT

- ▶ `/ip firewall nat`
- ▶ `add action=masquerade chain=srcnat out-interface=ether1-internet`

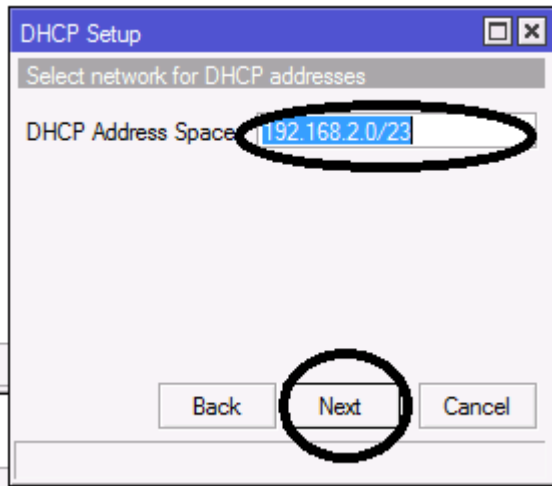
Set DHCP-Server (1)



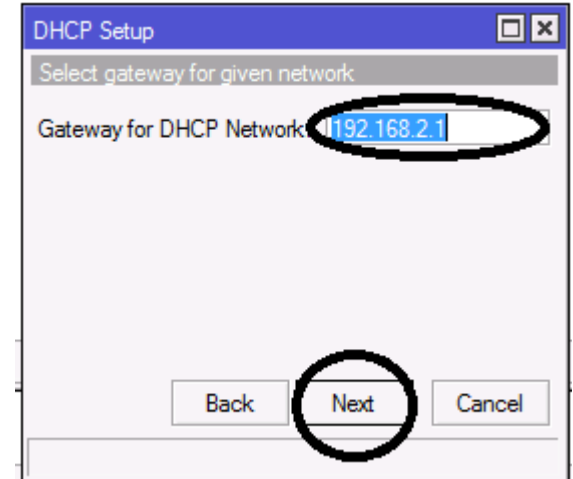
Tahap 1



Tahap 2

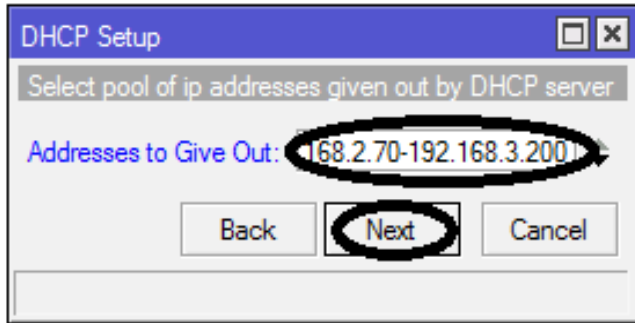


Tahap 3

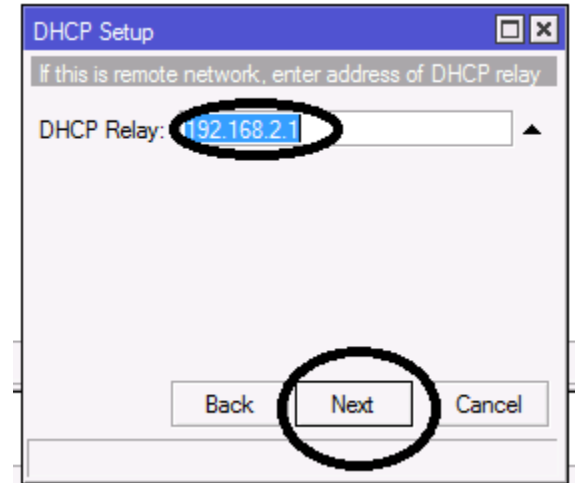


Tahap 4

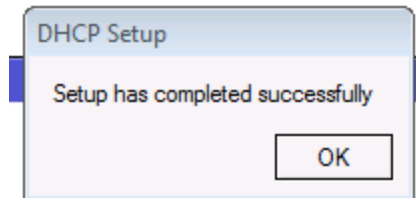
Set DHCP-Server (2)



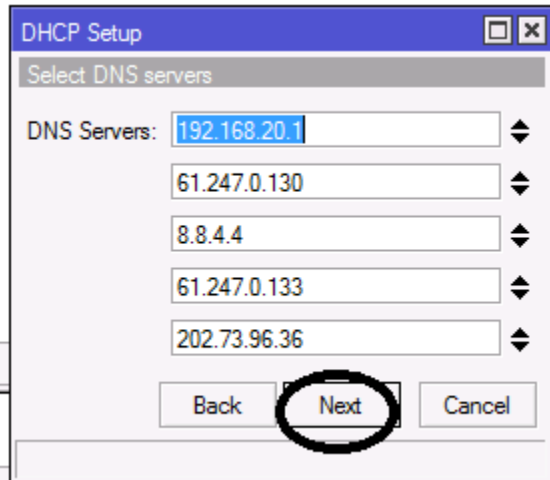
Tahap 5



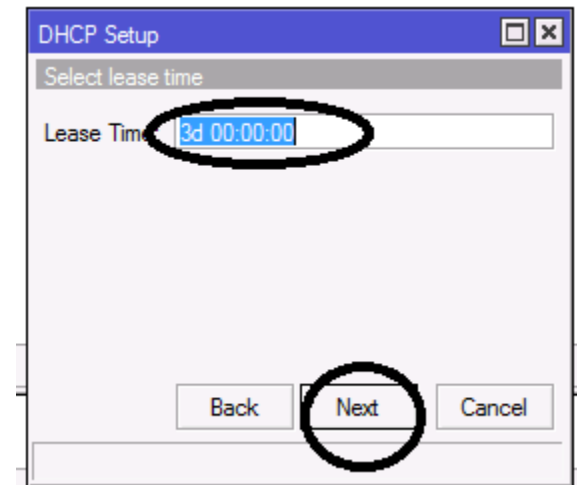
Tahap 6



Tahap 9

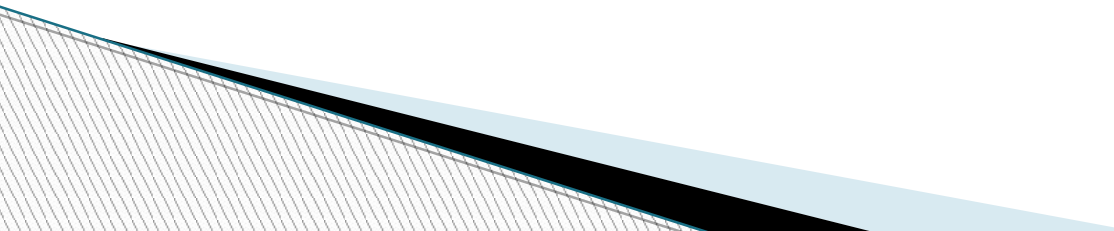


Tahap 7



Tahap 8

Set DHCP-Server (1)

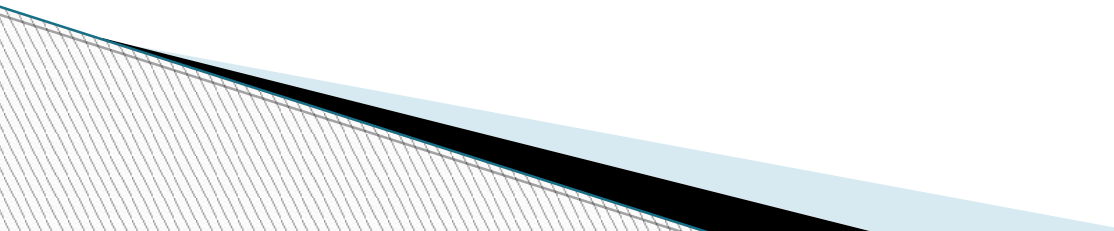
- ▶ `/ip dhcp-server setup`
 - ▶ Select interface to run DHCP server on
 - ▶ dhcp server interface: ether2-lokal
 - ▶ Select network for DHCP addresses
 - ▶ dhcp address space: 192.168.2.0/23
 - ▶ Select gateway for given network
- 

Set DHCP-Server (2)

- ▶ gateway for dhcp network: 192.168.2.1
- ▶ Select pool of ip addresses given out by DHCP server
- ▶ addresses to give out: 192.168.2.70–192.168.3.200
- ▶ Select DNS servers
- ▶ dns servers: 192.168.2.1,192.168.20.1
- ▶ Select lease time
- ▶ lease time: 3d



Hotspot dan QoS

- ▶ Setup Hotspot
 - ▶ Set IP Binding
 - ▶ Set Walled Garden
 - ▶ Set Hotspot User Profile untuk manajemen bandwidth
 - ▶ Tampilan simple queues setelah terpasang Hotspot
 - ▶ Tampilan NAT setelah terpasang Hotspot
- 

Set Hotspot (1)

The image shows the Mikrotik WinBox interface for configuring a Hotspot. The process is annotated with numbers 1 through 9:

- 1**: In the left sidebar, the **IP** menu item is circled.
- 2**: In the left sidebar, the **Hotspot** menu item is circled.
- 3**: In the main window, the **Hotspot Setup** button is circled.
- 4**: In the **Hotspot Setup** dialog, the **HotSpot Interface** dropdown menu is circled, showing **ether2-0/24**.
- 5**: In the **Hotspot Setup** dialog, the **Next** button is circled.
- 6**: In the **Hotspot Setup** dialog, the **Local Address of Network** text box is circled, showing **192.168.2.1/23**.
- 7**: In the **Hotspot Setup** dialog, the **Next** button is circled.
- 8**: In the **Hotspot Setup** dialog, the **Address Pool of Network** text box is circled, showing **2.70-192.168.3.200**.
- 9**: In the **Hotspot Setup** dialog, the **Next** button is circled.

Set Hotspot (2)

Hotspot Setup

Select hotspot SSL certificate 10

Select Certificate: none

Back 11 Next Cancel

Hotspot Setup

Select SMTP server 12

IP Address of SMTP Server: 0.0.0.0

Back 13 Next Cancel

Hotspot Setup

Setup DNS configuration

DNS Servers:

Back 14 Next Cancel

Hotspot Setup

DNS name of local hotspot server

DNS Name:

Back 15 Next Cancel

Hotspot Setup

Create local HotSpot user

Name of Local HotSpot User: admin 16

Password for the User: admin

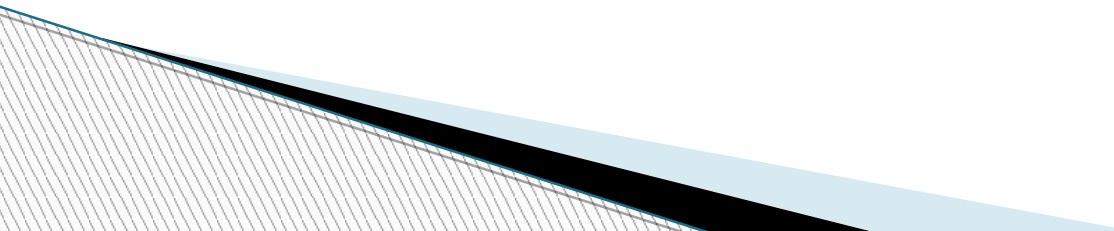
Back 17 Next Cancel

Hotspot Setup

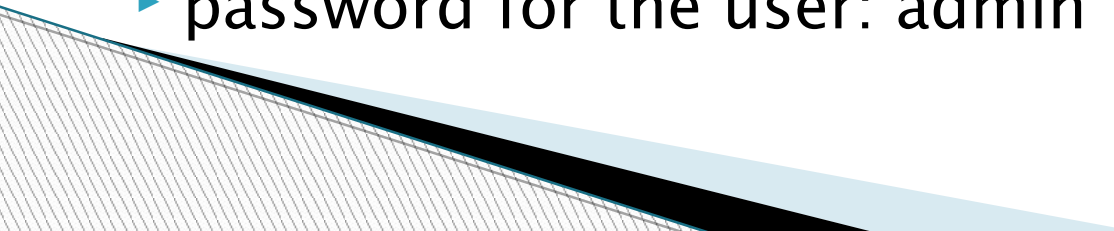
Setup has completed successfully 18

OK

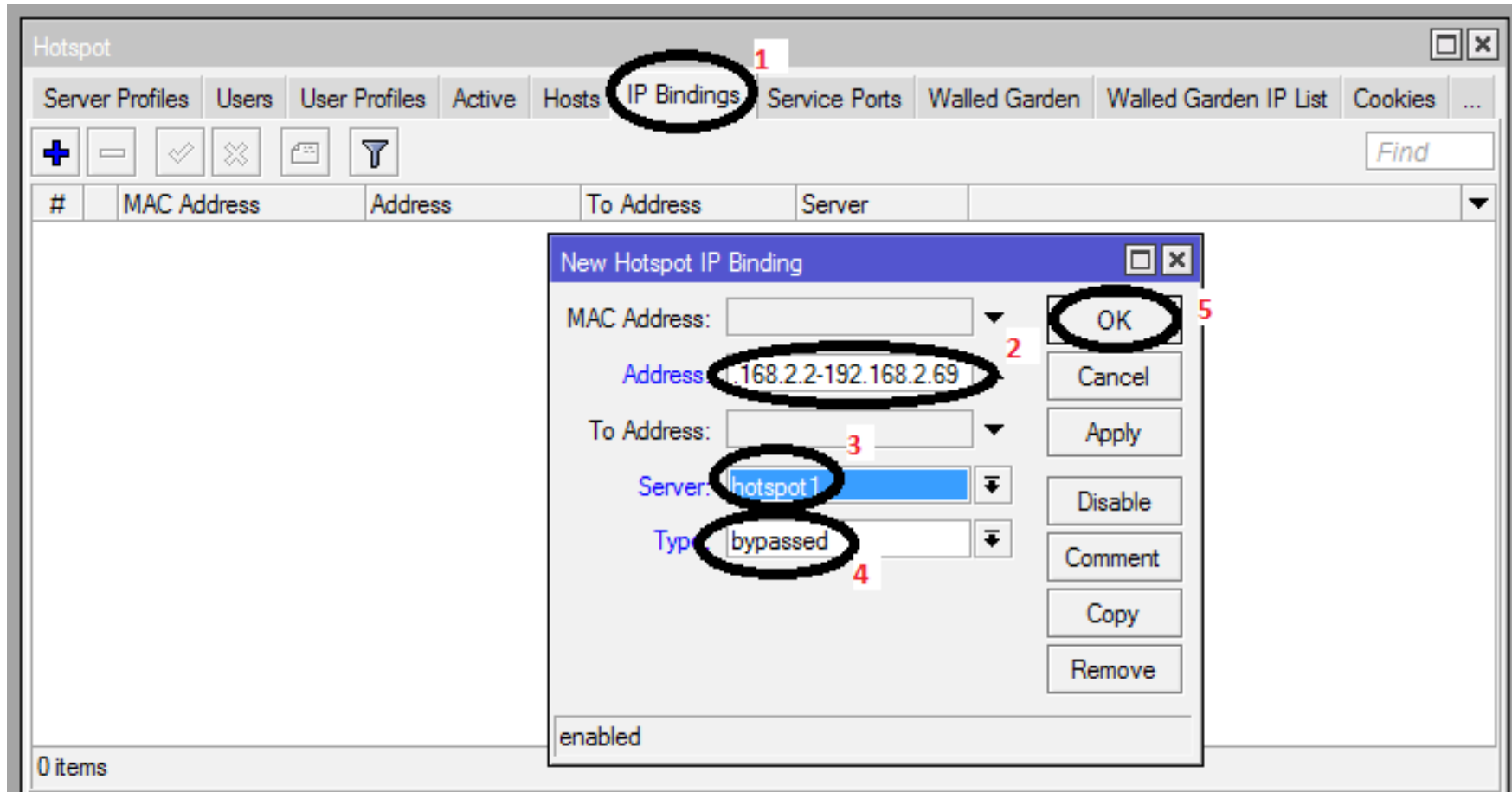
Set Hotspot (1)

- ▶ /ip hotspot setup
 - ▶ Select interface to run HotSpot on
 - ▶ hotspot interface: ether2-lokal
 - ▶ Set HotSpot address for interface
 - ▶ local address of network: 192.168.2.1 /23
 - ▶ masquerade network: yes
 - ▶ Set pool for HotSpot addresses
 - ▶ address pool of network: 192.168.2.70–192.168.3.200
- 

Set Hotspot (2)

- ▶ Select hotspot SSL certificate
 - ▶ select certificate: none
 - ▶ Select SMTP server
 - ▶ ip address of smtp server: 0.0.0.0
 - ▶ Setup DNS configuration
 - ▶ dns servers:
 - ▶ DNS name of local hotspot server
 - ▶ dns name:
 - ▶ Create local hotspot user
 - ▶ name of local hotspot user: admin
 - ▶ password for the user: admin
- 

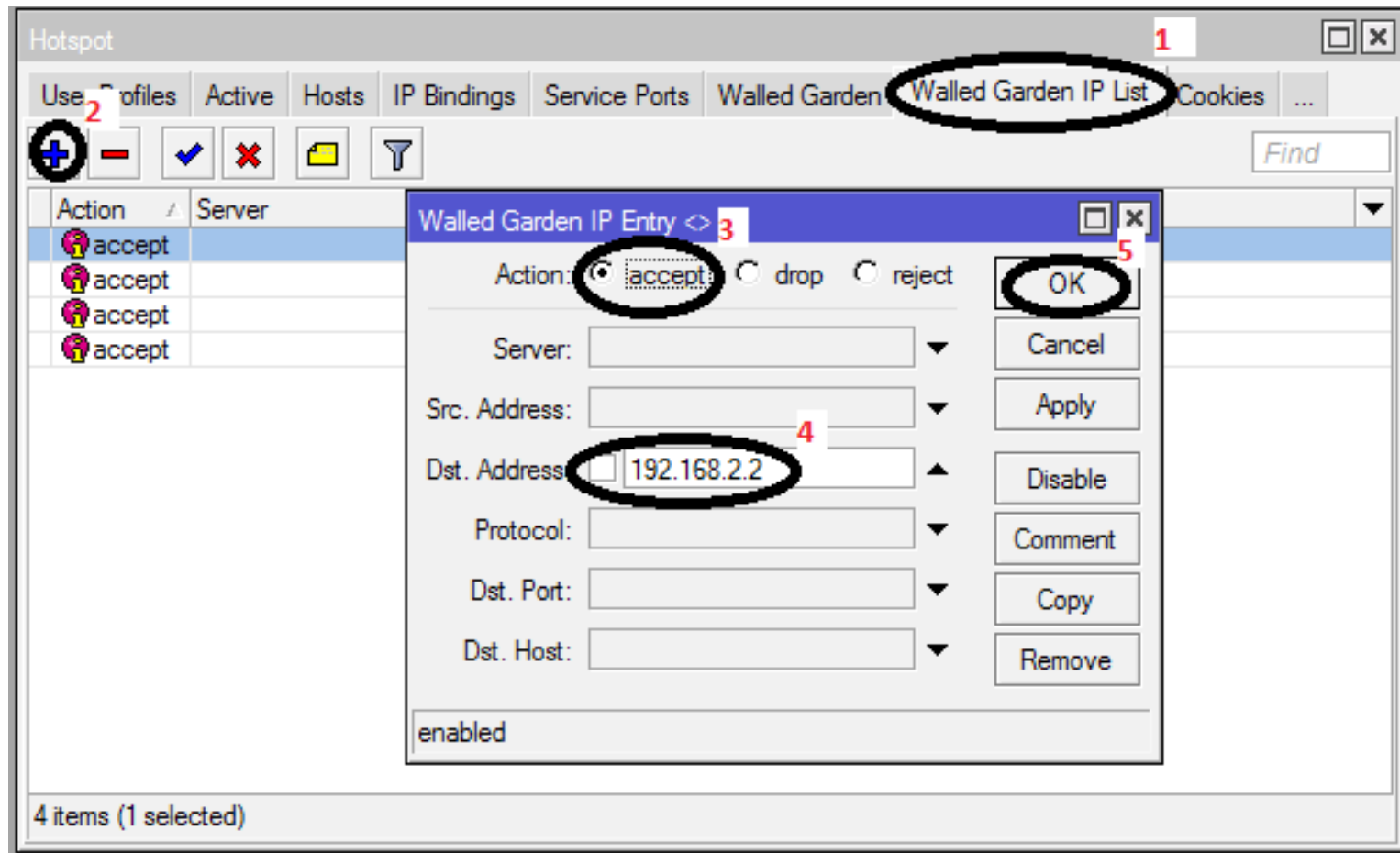
Set IP binding Hotspot



Set IP binding Hotspot

- ▶ `/ip hotspot ip-binding add
address=192.168.2.2-192.168.2.69
server=hotspot1 type=bypassed`

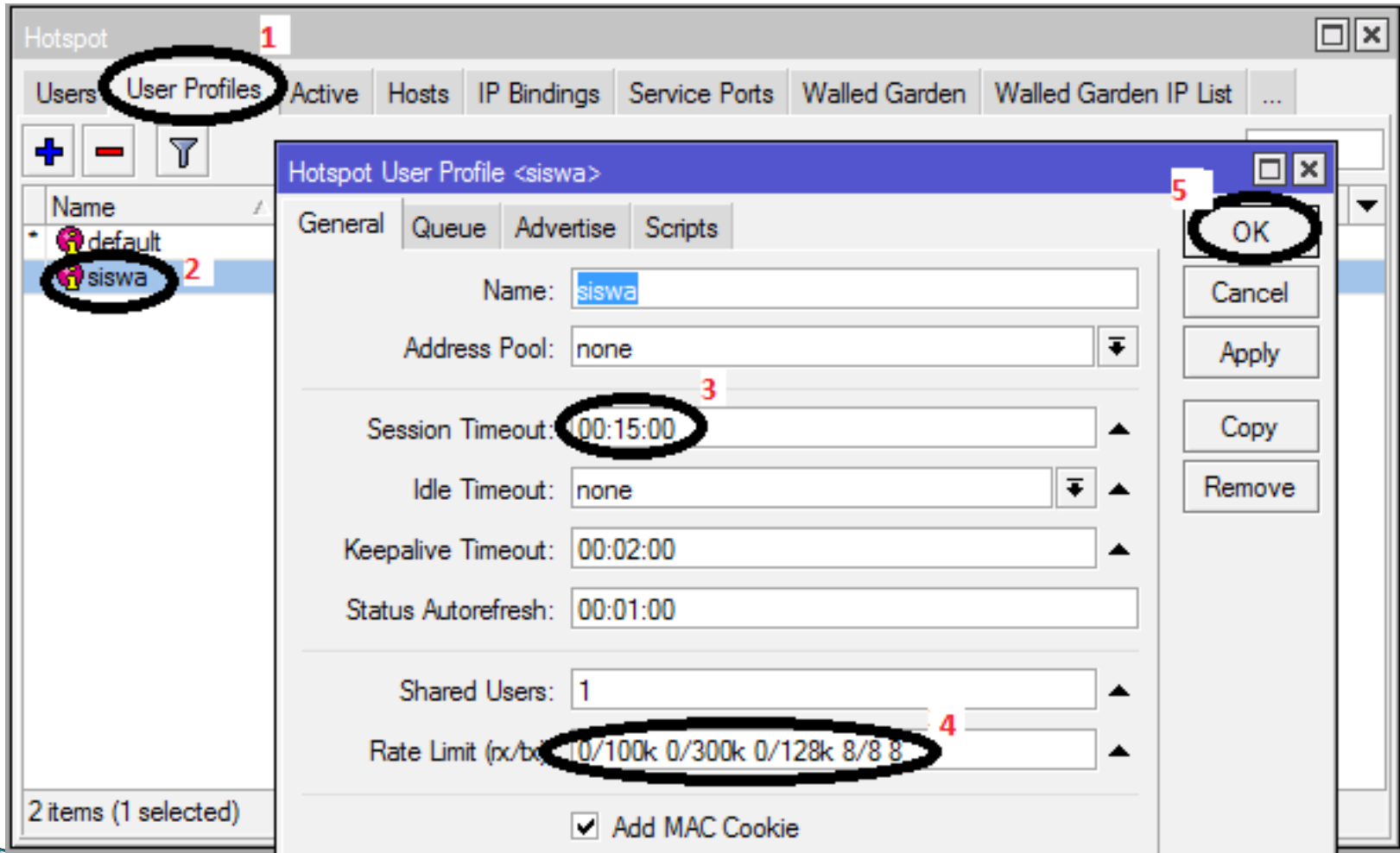
Set Walled Garden Hotspot



Set Walled Garden Hotspot

- ▶ `/ip hotspot walled-garden ip
add action=accept
disabled=no dst-
address=192.168.2.2`

Set Hotspot User Profile untuk manajemen bandwidth



Set Hotspot User Profile untuk manajemen bandwidth

- ▶ `/ip hotspot user profile add name=siswa
rate-limit="0/100k 0/300k 0/128k 8/8 8"
session-timeout=15m transparent-
proxy=yes`

Tampilan simple queues setelah terpasang Hotspot

Queue List						
Simple Queues Interface Queues Queue Tree Queue Types						
+ - ✓ ✗ ☰ ⌵ ↺ Reset Counters ∞ Reset All Counters						
#		Name	Target	Upload Max Limit	Download Max Limit	Packet Marks
14	D	<hotspot-mm2013-agipirfanm...	192.168.2.208	unlimited	100k	
15	D	<hotspot-tkj2015-karluki>	192.168.3.83	unlimited	100k	
16	D	<hotspot-kp2013-santaclarita>	192.168.2.232	unlimited	100k	
17	D	<hotspot-tkj2015-trisnapriant...	192.168.3.134	unlimited	100k	
18	D	<hotspot-tkj2015-tiocakka>	192.168.3.80	unlimited	100k	
19	D	<hotspot-kp2015-nisamaulan...	192.168.2.196	unlimited	100k	
20	D	<hotspot-kp2014-destiyanak...	192.168.2.141	unlimited	100k	
21	D	<hotspot-mm2013-nuryrahma...	192.168.2.214	unlimited	100k	
22	D	<hotspot-kp2013-rimamonica>	192.168.3.51	unlimited	100k	
23	D	<hotspot-ak2015-yusniati>	192.168.2.225	unlimited	100k	
24	D	<hotspot-tkj2015-fadhilahafri...	192.168.3.78	unlimited	100k	
25	D	<hotspot-mm2015-avikadwia...	192.168.3.192	unlimited	100k	
26	D	<hotspot-fm2015-chantikaca...	192.168.2.204	unlimited	100k	
27	D	<hotspot-mm2013-ridhohadis...	192.168.2.215	unlimited	100k	
28	D	<hotspot-tkj2015-muhamadfa...	192.168.3.82	unlimited	100k	
29	D	hs-<hotspot1>	ether2-lokal	unlimited	unlimited	
30 items		0 B queued		0 packets queued		

Simple Queue <<hotspot-tkj2015-muhamadfaozi>>



General

Advanced

Statistics

Traffic

Total

...

Name: <hotspot-tkj2015-muhamadfaozi>

Target: 192.168.3.82

Dst.:

Target Upload

Target Download

Max Limit: unlimited

100k

--▲-- Burst

Burst Limit: unlimited

300k

Burst Threshold: unlimited

128k

Burst Time: 8

8

--▼-- Time

OK

Copy

Remove

Reset Counters

Reset All Counters

Torch

unlimited
packets queued

Simple Queue <<hotspot-kp2015-umimawadah>>



General

Advanced

Statistics

Traffic

Total

...

Packet Marks:

Target Upload

Target Download

Limit At: unlimited

100k

Priority: 8

8

Queue Type: default-small

default-small

Parent: none

OK

Copy

Remove

Reset Counters

Reset All Counters

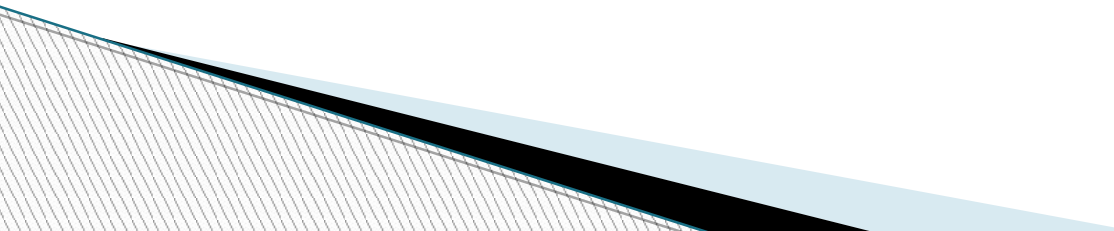
Torch

Tampilan NAT setelah terpasang Hotspot

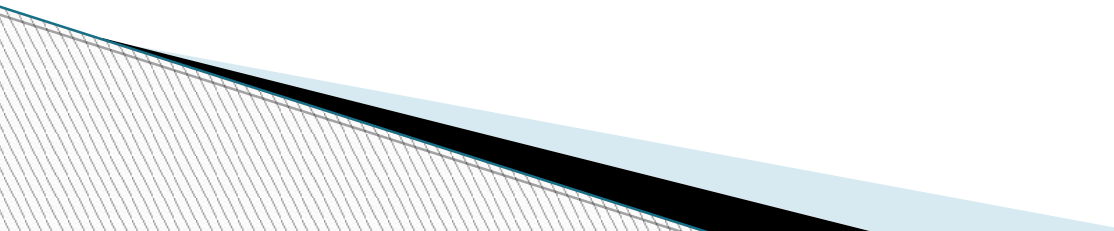
Firewall												
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols												
+ - [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon]												
Reset Counters 00 Reset All Counters Find all												
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets	
0	D [icon] jump	dstnat								0 B	0	
1	D [icon] jump	hotspot								0 B	0	
2	D [icon] [icon] redir...	hotspot			17 (u...		53			0 B	0	
3	D [icon] [icon] redir...	hotspot			6 (tcp)		53			0 B	0	
4	D [icon] [icon] redir...	hotspot			6 (tcp)		80			0 B	0	
5	D [icon] [icon] redir...	hotspot			6 (tcp)		443			0 B	0	
6	D [icon] jump	hotspot			6 (tcp)					0 B	0	
7	D [icon] jump	hotspot			6 (tcp)					0 B	0	
8	D [icon] [icon] redir...	hs-unauth			6 (tcp)		80			0 B	0	
9	D [icon] [icon] redir...	hs-unauth			6 (tcp)		3128			0 B	0	
10	D [icon] [icon] redir...	hs-unauth			6 (tcp)		8080			0 B	0	
11	D [icon] [icon] redir...	hs-unauth			6 (tcp)		443			0 B	0	
12	D [icon] jump	hs-unauth			6 (tcp)		25			0 B	0	
13	D [icon] [icon] redir...	hs-auth			6 (tcp)					0 B	0	
14	D [icon] jump	hs-auth			6 (tcp)		25			0 B	0	
::: place rules here												
15	X pas...	unused-hs...								0 B	0	
::: masquerade hotspot network												
16	[icon] [icon] mas...	srcnat	192.168.4....							133 B	1	



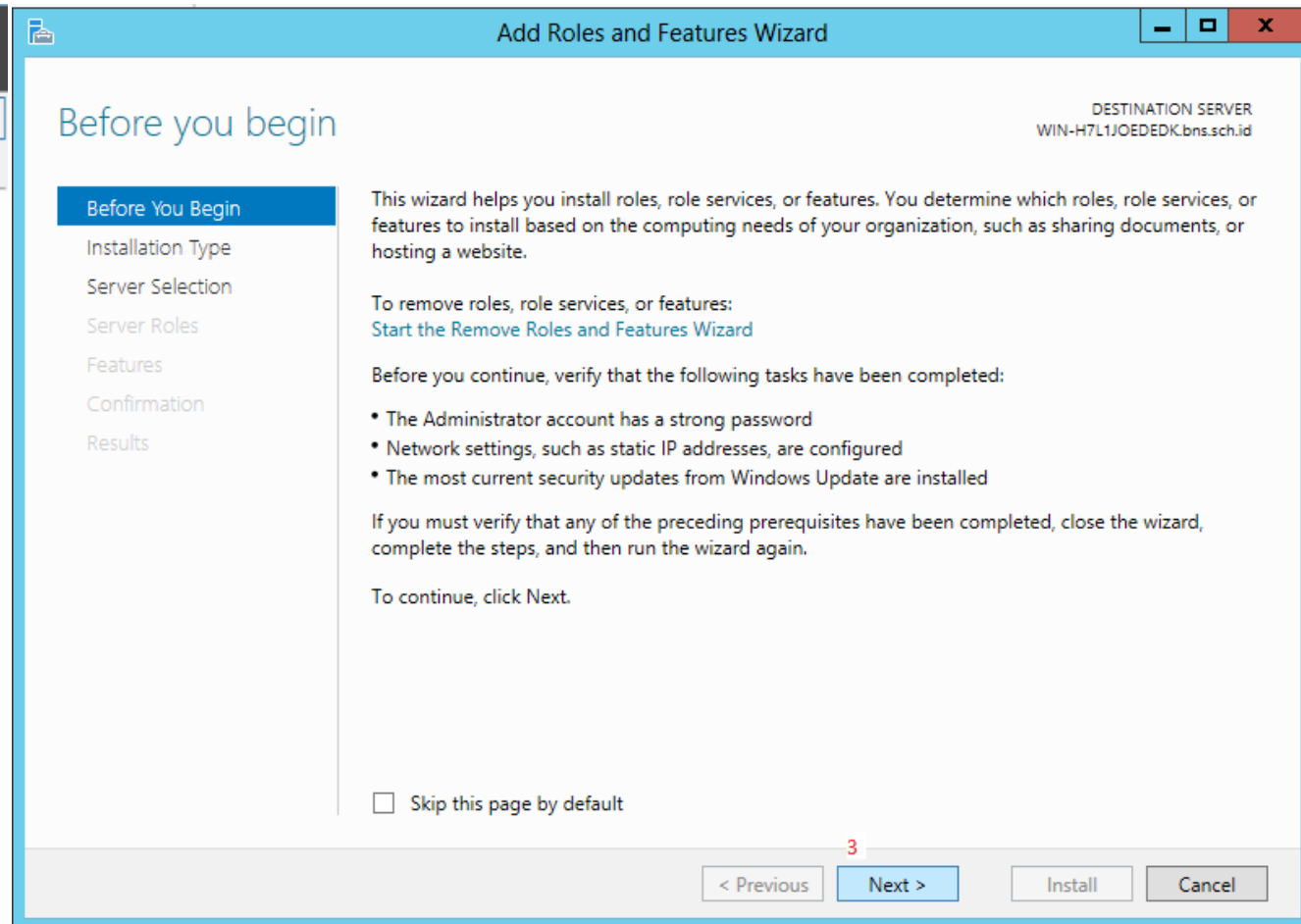
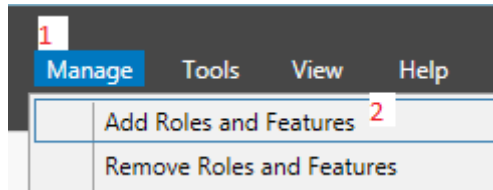
Integrasi dengan radius server dari win server 2012

- ▶ Persiapan
 - ▶ Instal NPAS (Network Policy and Access Services)
 - ▶ Konfigurasi NPAS
 - ▶ Konfigurasi Password Container
 - ▶ Set Radius di Mikrotik
 - ▶ Info tambahan integrasi radius server
- 

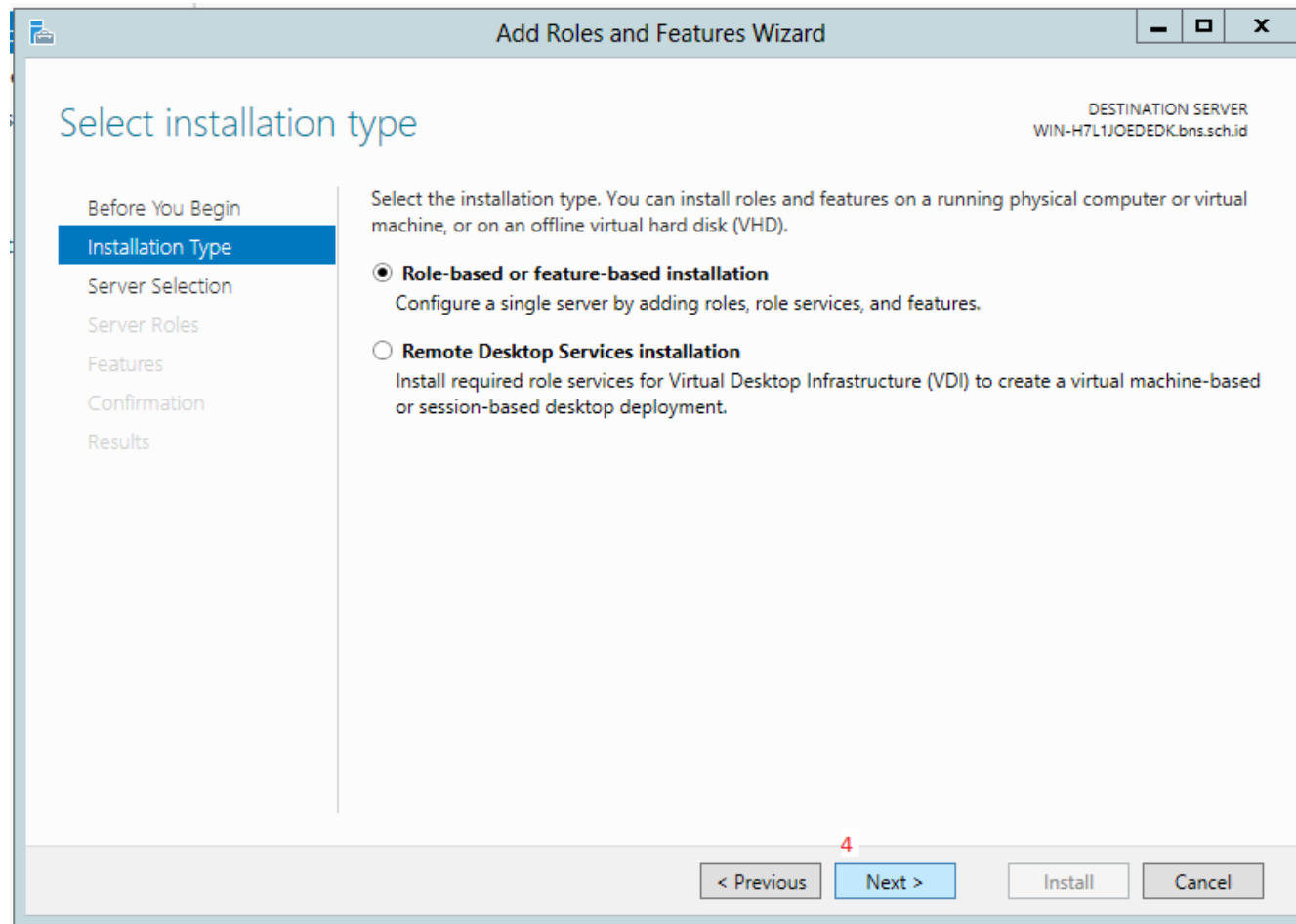
Persiapan

- ▶ Pastikan sudah terinstal DNS server
 - ▶ Pastikan sudah terinstal Active Directory
 - ▶ Pastikan sudah di promote Active Directory-nya
 - ▶ Pastikan sudah ada grup untuk user-user hotspot
 - ▶ Pastikan ada user di grup untuk hotspot
 - ▶ Pastikan IP server radius sudah ada di Binding dan ada di Walled Garden-nya hotspot
- 

Instal NPAS



Instal NPAS



Instal NPAS

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar reads 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. In the top right corner, it says 'DESTINATION SERVER WIN-H7L1JOEDEDK.bns.sch.id'. On the left, a navigation pane lists: 'Before You Begin', 'Installation Type', 'Server Selection' (highlighted), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the instruction 'Select a server or a virtual hard disk on which to install roles and features.' with two radio buttons: 'Select a server from the server pool' (selected) and 'Select a virtual hard disk'. Below this is a 'Server Pool' section with a 'Filter:' text box and a table. The table has columns 'Name', 'IP Address', and 'Operating System'. One row is visible and highlighted: 'WIN-H7L1JOEDEDK.bns....', '192.168.1.102', and 'Microsoft Windows Server 2012 Datacenter'. Below the table, it says '1 Computer(s) found' and a paragraph: 'This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.' At the bottom, there are buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A small red '5' is positioned above the 'Next >' button.

DESTINATION SERVER
WIN-H7L1JOEDEDK.bns.sch.id

Select destination server

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool
☐ Select a virtual hard disk

Server Pool

Filter:

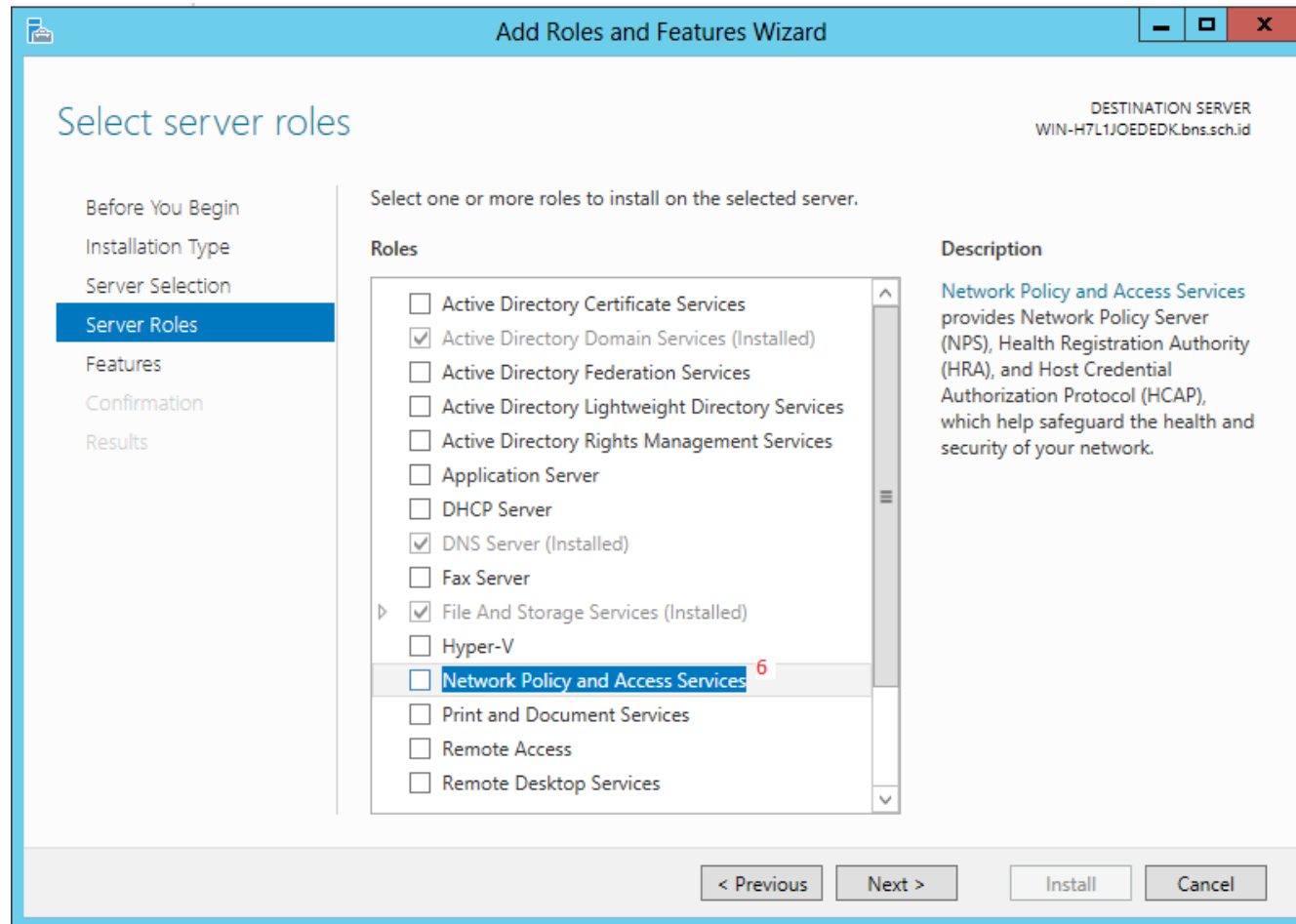
Name	IP Address	Operating System
WIN-H7L1JOEDEDK.bns....	192.168.1.102	Microsoft Windows Server 2012 Datacenter

1 Computer(s) found

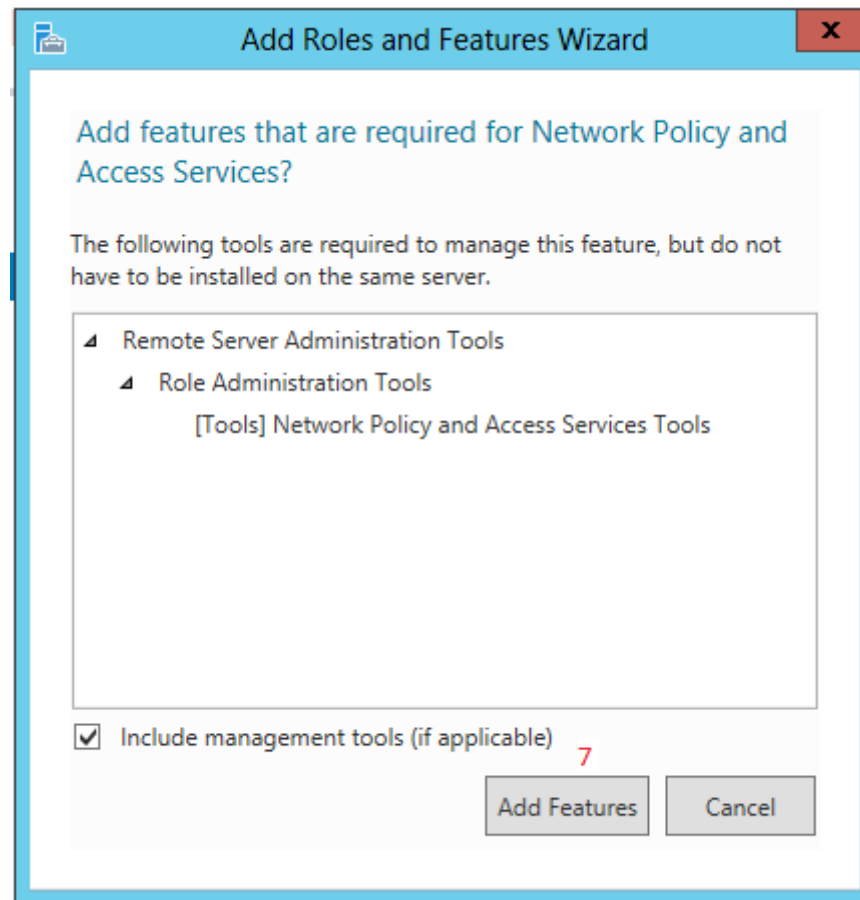
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous 5 Next > Install Cancel

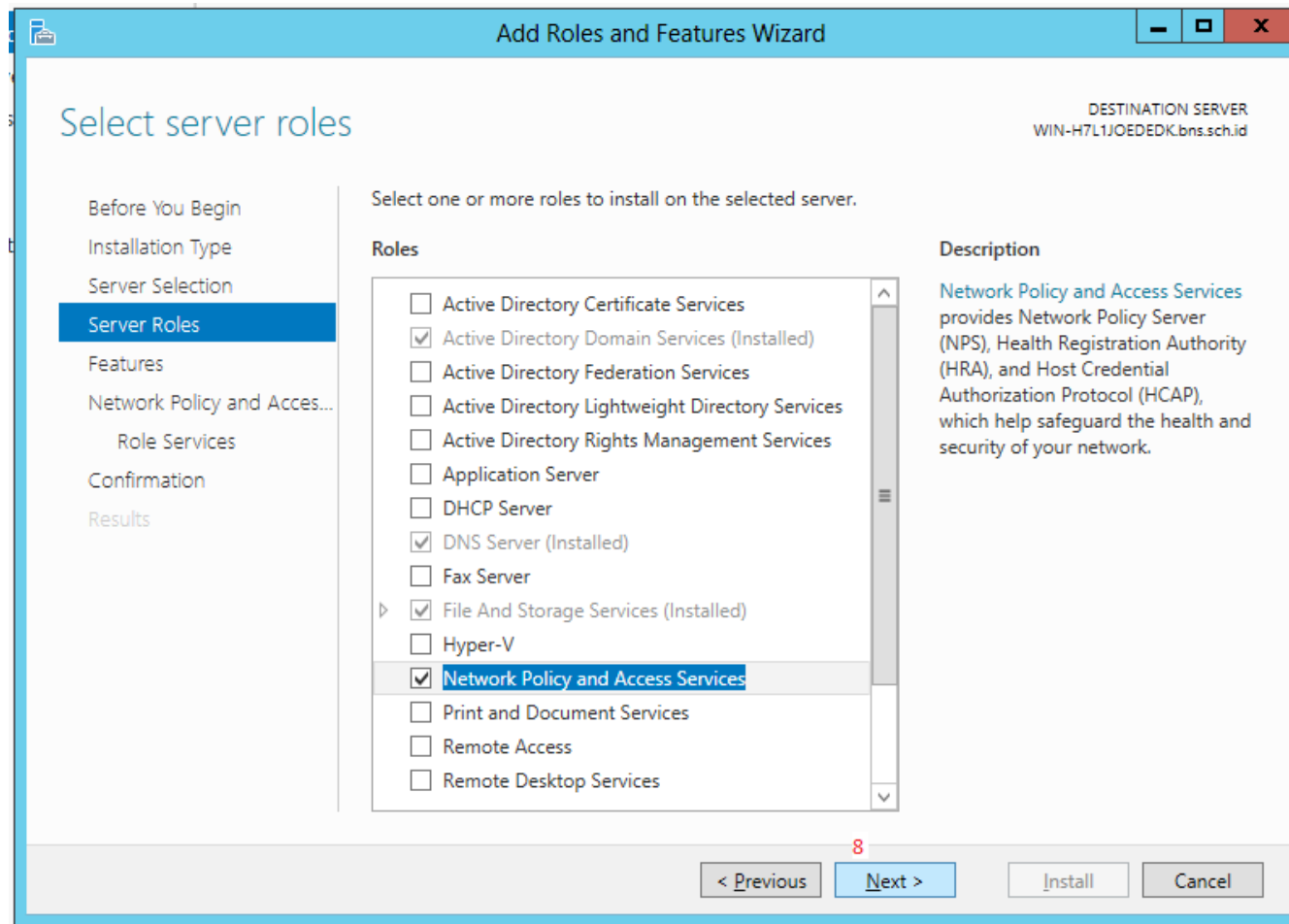
Instal NPAS



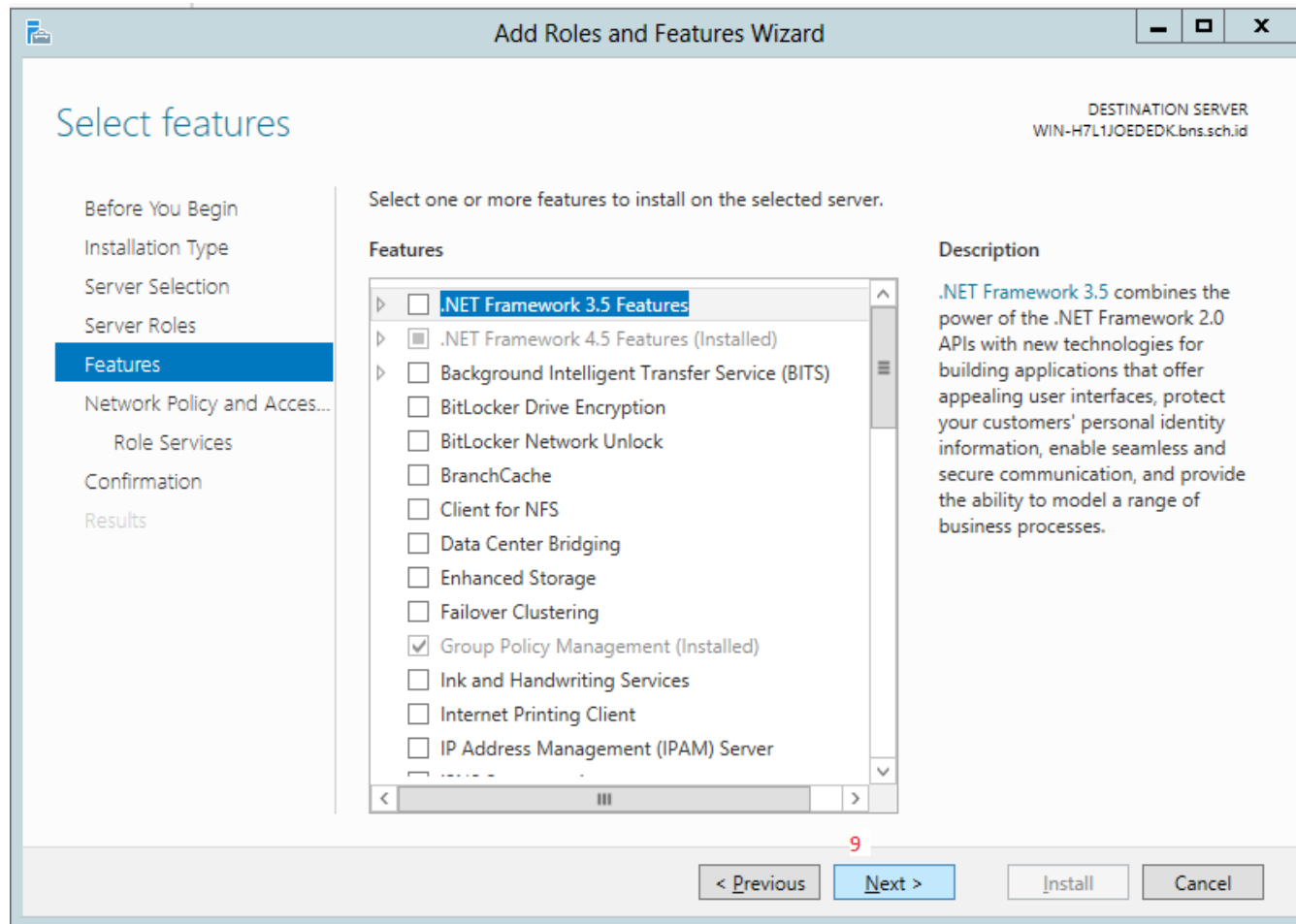
Instal NPAS



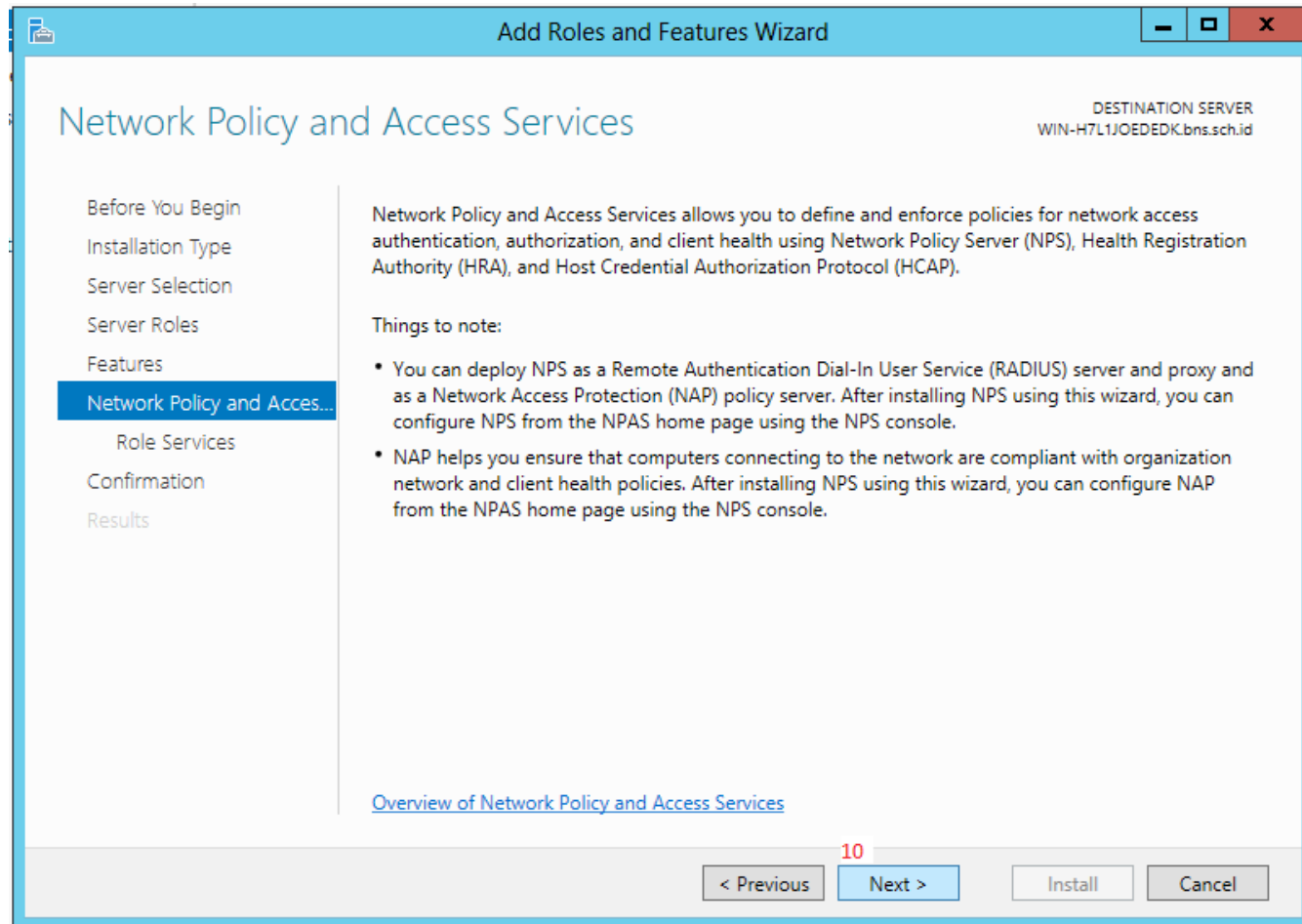
Instal NPAS



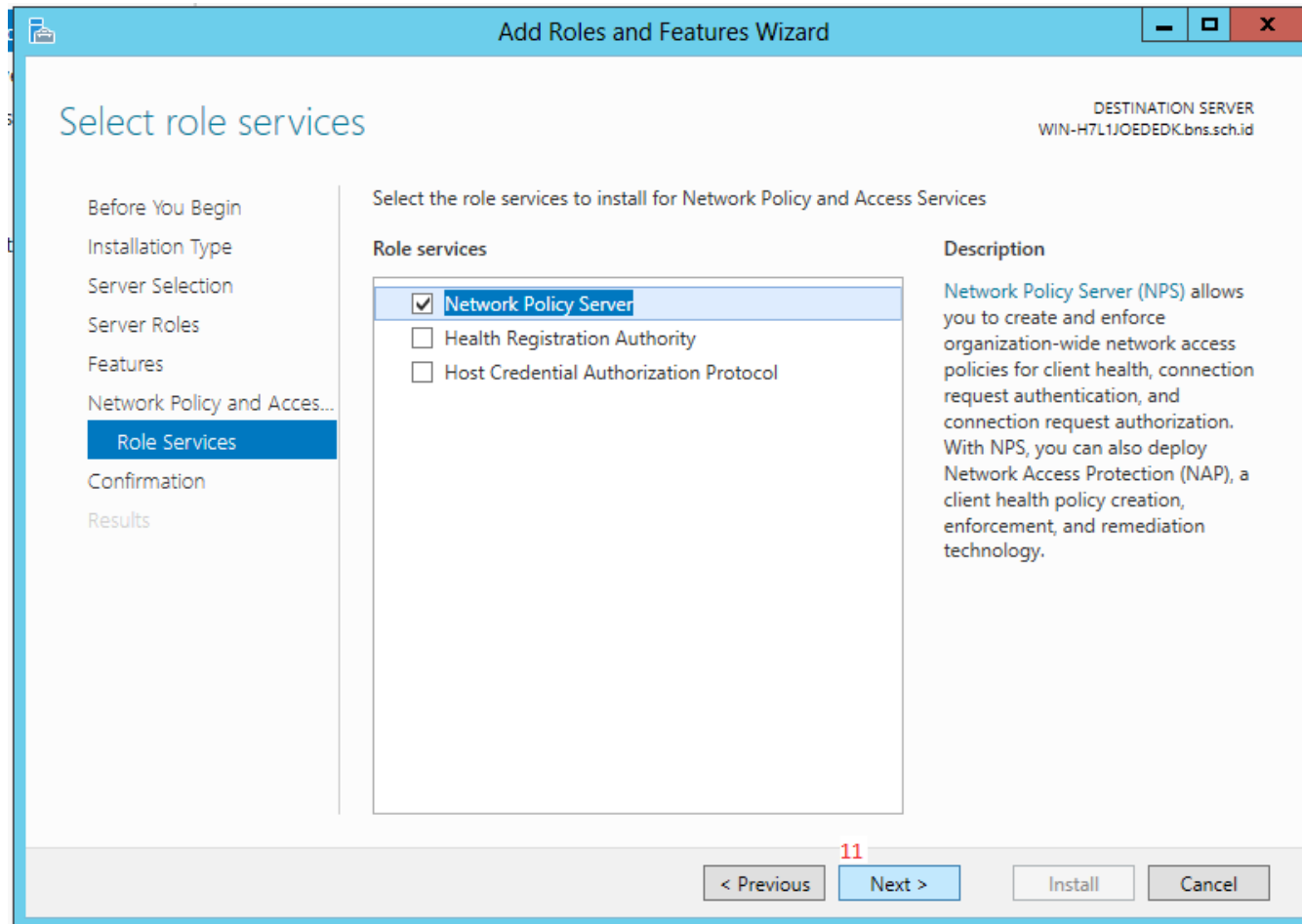
Instal NPAS



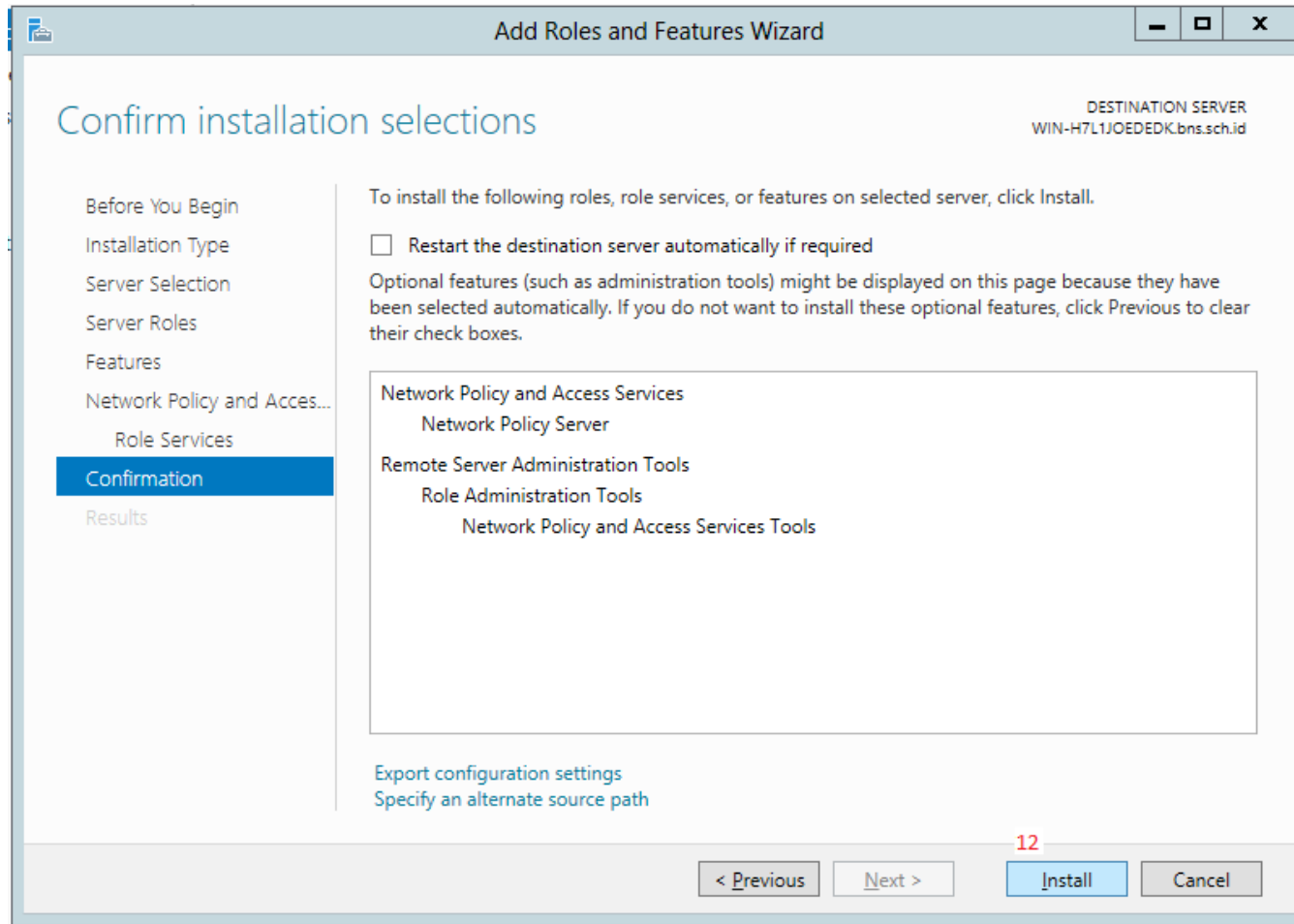
Instal NPAS



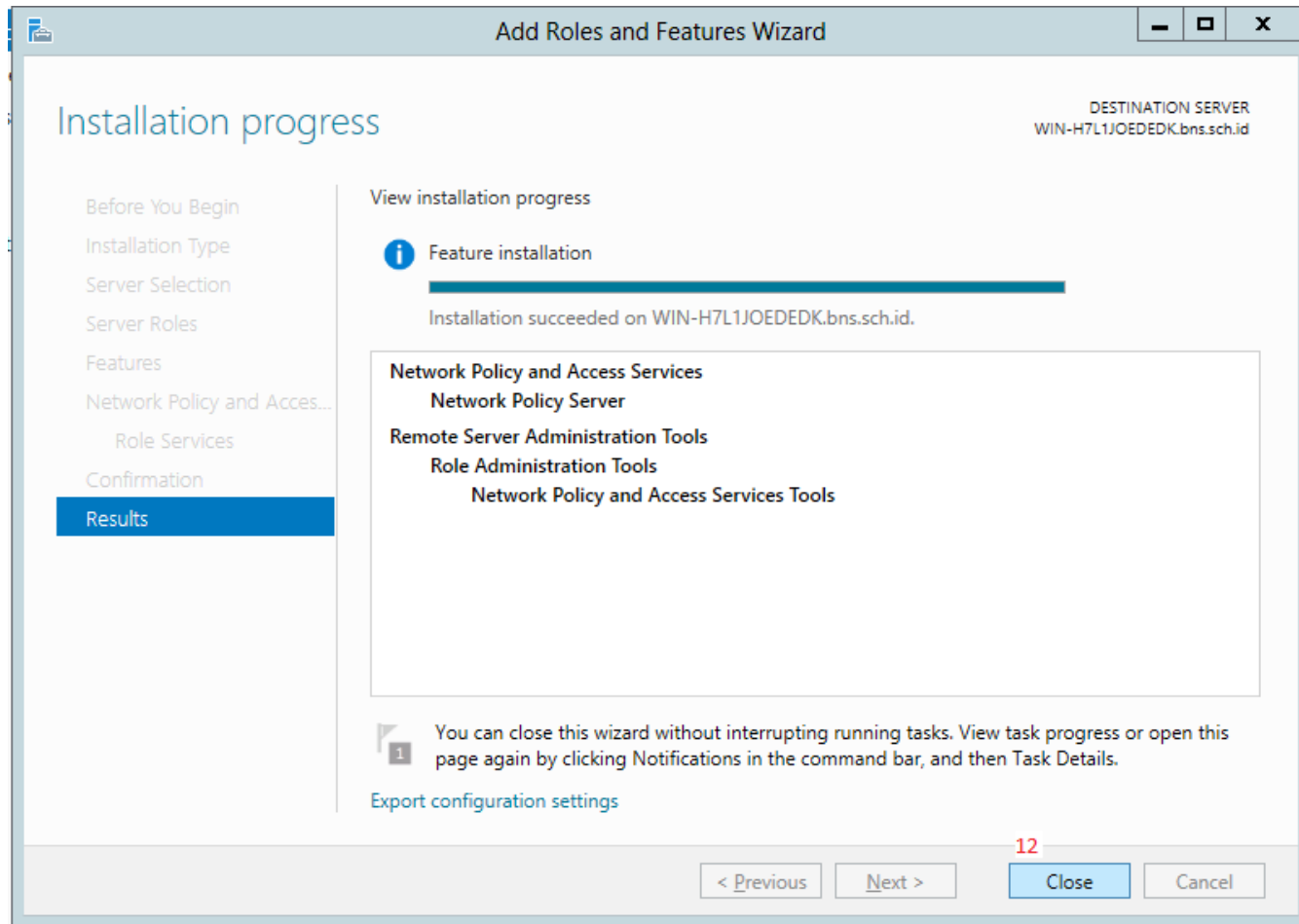
Instal NPAS



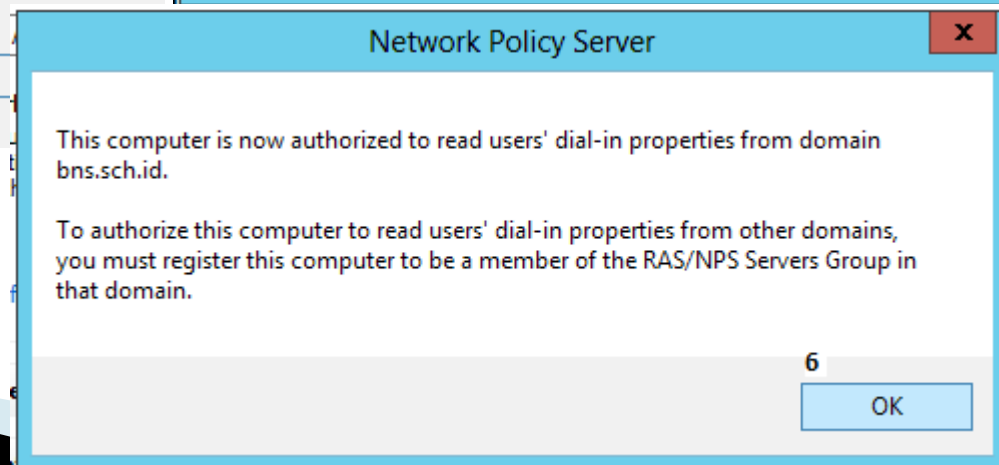
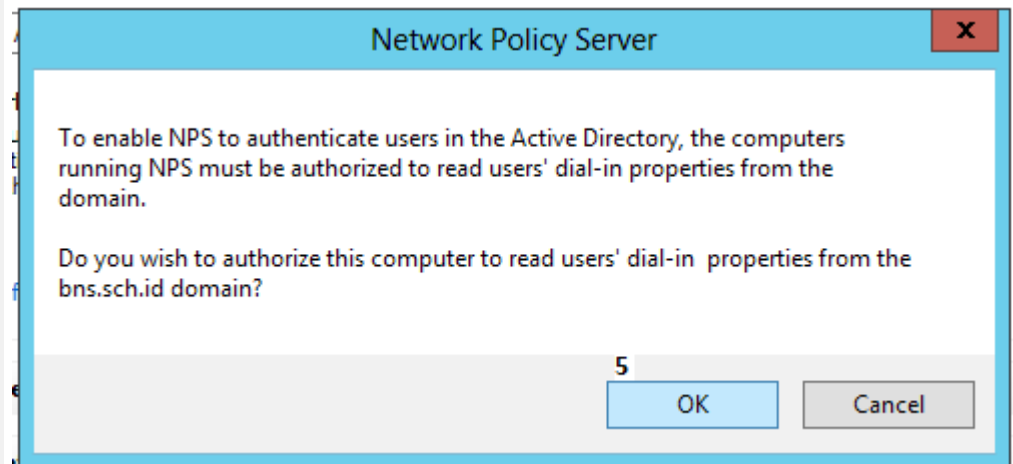
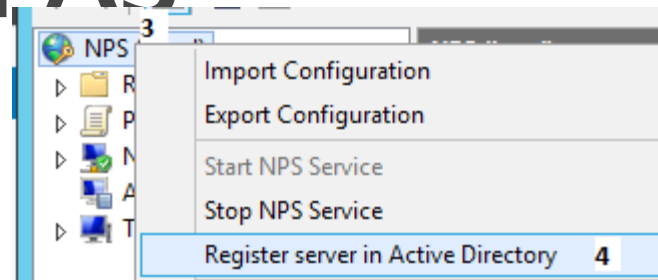
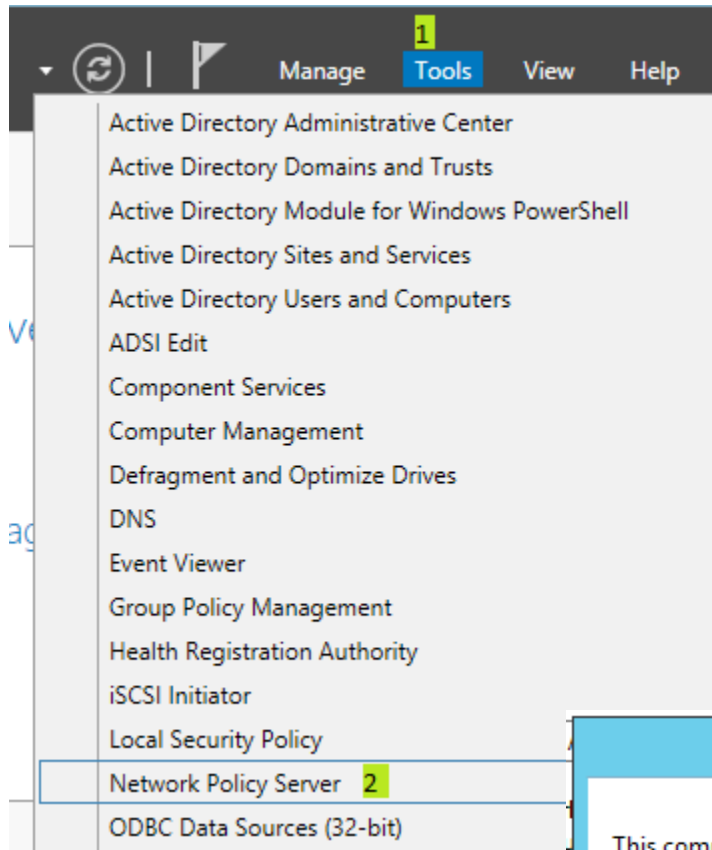
Instal NPAS



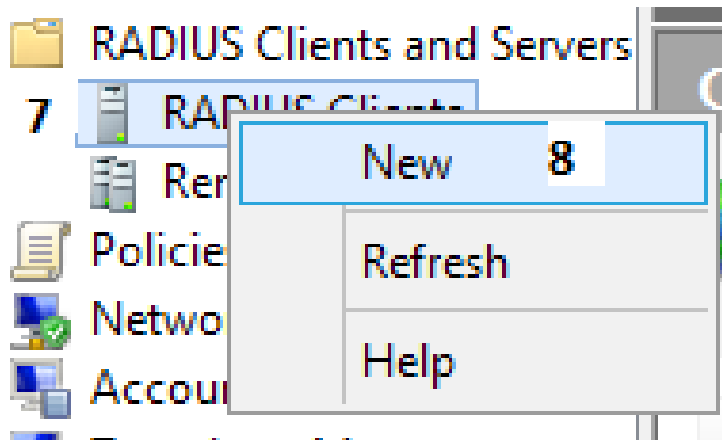
Instal NPAS



Konfigurasi NPAS



Konfigurasi NPAS



mikrotik Properties X

Settings **Advanced**

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:
 9

Address (IP or DNS):
 10 Verify...

Shared Secret

Select an existing Shared Secrets template:

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

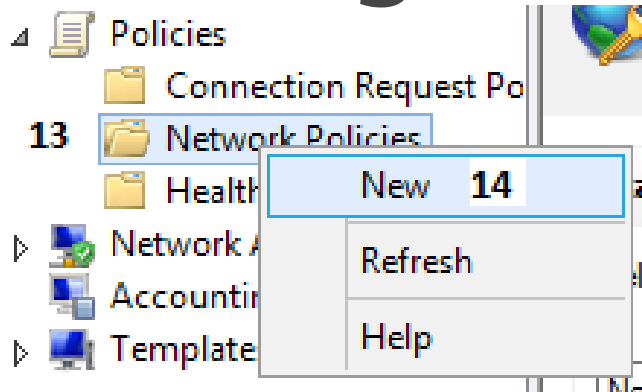
☒ Manual ☐ Generate

Shared secret:
 11

Confirm shared secret:
 11

12 OK Cancel Apply

Konfigurasi NPAS



New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

hotspot 15

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server:

Unspecified

☐ Vendor specific:

10

16

Previous Next Finish Cancel

Konfigurasi NPAS

New Network Policy



Specify Conditions
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
-----------	-------

Condition description:

17

Add...

Edit...

Remove

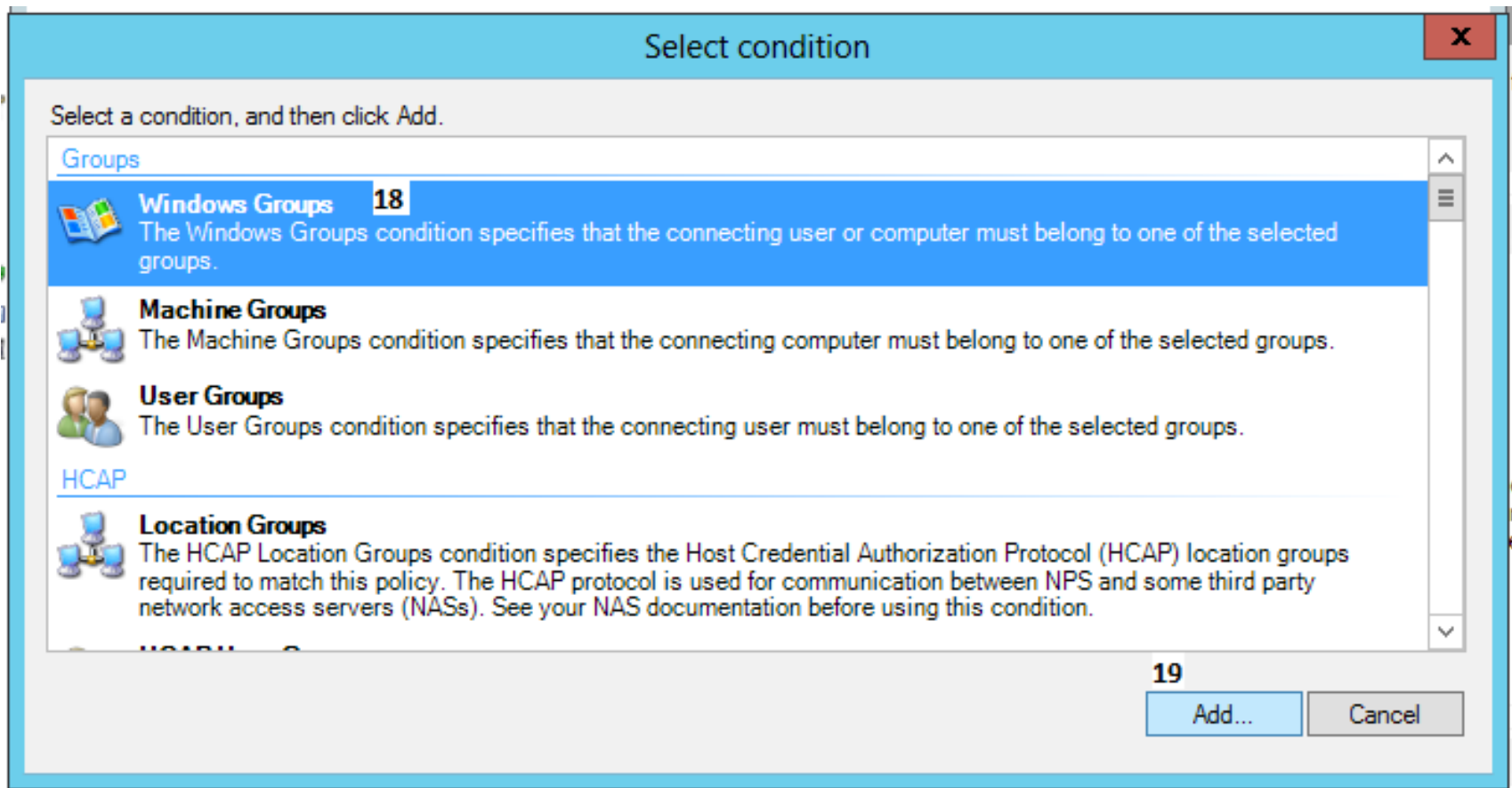
Previous

Next

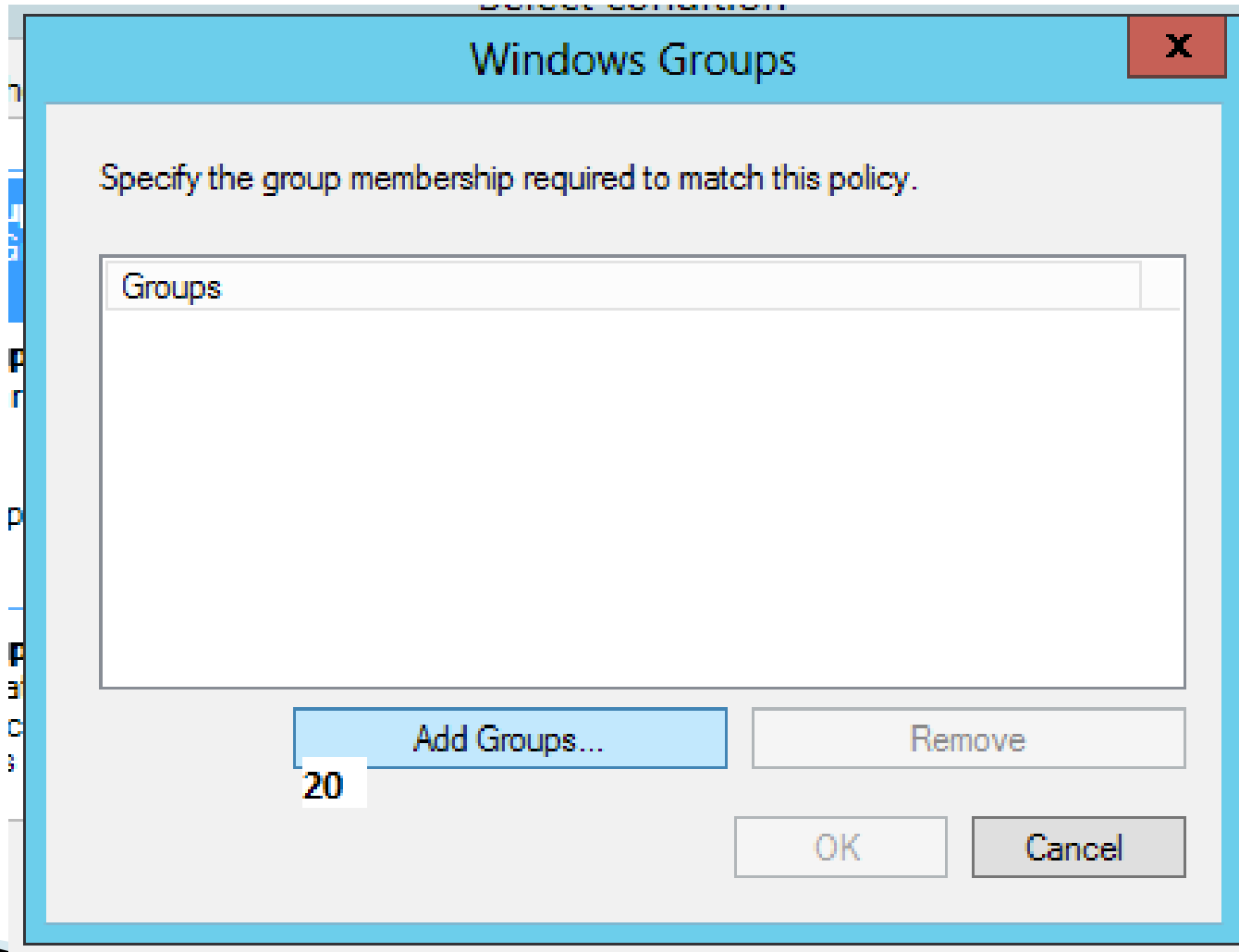
Finish

Cancel

Konfigurasi NPAS



Konfigurasi NPAS



Konfigurasi NPAS

The image shows a 'Select Group' dialog box with a light blue title bar and standard Windows window controls (help, close). The dialog contains three main sections for configuration. The first section, 'Select this object type:', has a text box with 'Group' and a button 'Object Types...'. The second section, 'From this location:', has a text box with 'bns.sch.id' and a button 'Locations...'. The third section, 'Enter the object name to select (examples):', has a large text box containing 'siswa' followed by '21' (highlighted in yellow) and a button 'Check Names'. At the bottom, there are three buttons: 'Advanced...', '22' (highlighted in yellow), and 'OK', followed by a 'Cancel' button.

Select Group

Select this object type:

Group

Object Types...

From this location:

bns.sch.id

Locations...

Enter the object name to select (examples):

siswa 21

Check Names

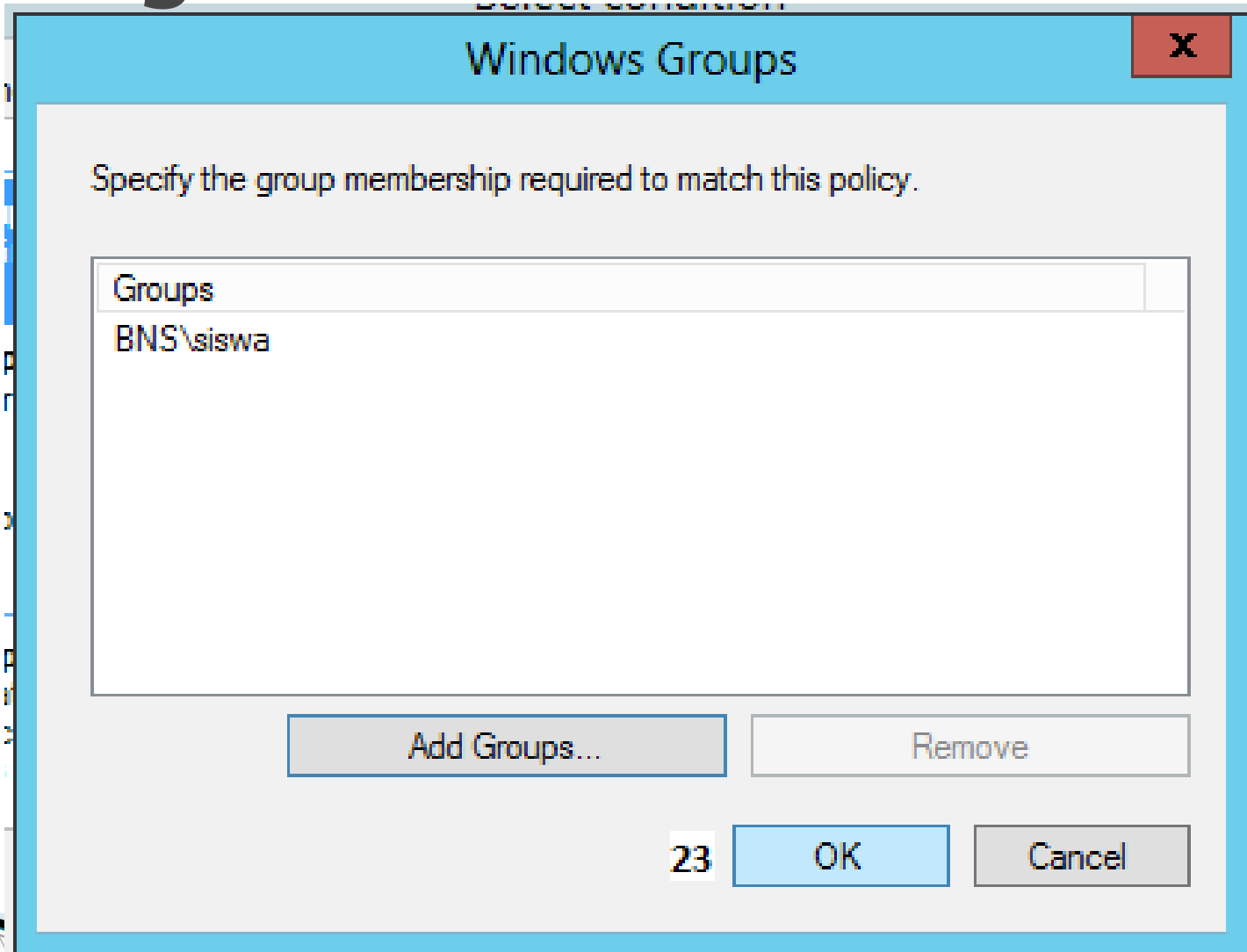
Advanced...

22

OK

Cancel

Konfigurasi NPAS



Konfigurasi NPAS

New Network Policy



Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
 Windows Groups	BNS\siswa

Condition description:

The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Add...

Edit...

Remove

24

Previous

Next

Finish

Cancel

Konfigurasi NPAS

New Network Policy ✕

 **Specify Access Permission**

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

☒ Access granted
Grant access if client connection attempts match the conditions of this policy.

☐ Access denied
Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

25

Previous Next Finish Cancel

Konfigurasi NPAS

New Network Policy



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up

Move Down

Add...

Edit...

Remove

Less secure authentication methods:

☒ 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

☒ Encrypted authentication (CHAP) 26

☒ Unencrypted authentication (PAP, SPAP) 27

☐ Allow clients to connect without negotiating an authentication method.

☐ Perform machine health check only

28

Previous

Next

Finish

Cancel

Konfigurasi NPAS

Connection Request Policy



You selected one or more insecure authentication methods. To ensure that each protocol is correctly configured for the remote access, policy, and domain levels, follow the step-by-step procedures in Help.

View the corresponding Help topic?

29

Yes

No

Konfigurasi NPAS

New Network Policy



Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints

 Idle Timeout

 Session Timeout

 Called Station ID

 Day and time restrictions

 NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

^

v

30

Previous

Next

Finish

Cancel

Konfigurasi NPAS

New Network Policy



Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

- ☒ Standard
- ☐ Vendor Specific

Network Access Protection

- ☐ NAP Enforcement
- ☒ Extended State

Routing and Remote Access

- ☐ Multilink and Bandwidth Allocation Protocol (BAP)
- ☐ IP Filters
- ☐ Encryption
- ☒ IP Settings

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

33

Konfigurasi NPAS

New Network Policy



Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes**
 - ☒ Standard
 - ☒ Vendor Specific
- Network Access Protection**
 - ☒ NAP Enforcement
 - ☒ Extended State
- Routing and Remote Access**
 - ☒ Multilink and Bandwidth Allocation Protocol (BAP)
 - ☒ IP Filters
 - ☒ Encryption
 - ☒ IP Settings

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
------	-------

34

Konfigurasi NPAS

New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

hotspot

Policy conditions:

Condition	Value
Windows Groups	BNS\siswa

Policy settings:

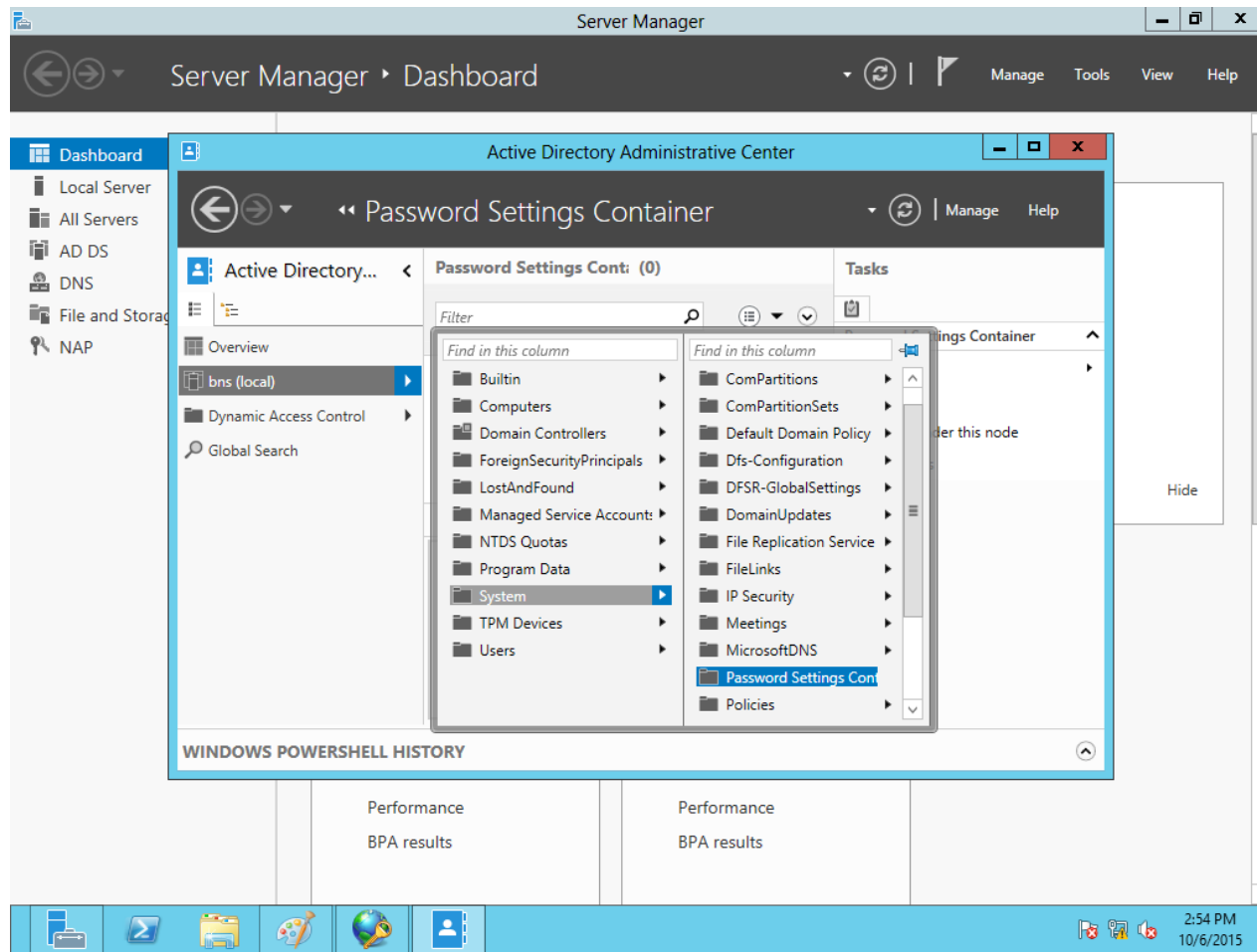
Condition	Value
Authentication Method	Unencrypted authentication (PAP, SPAP) OR Encryption authentication (CHAP) OR MS-CHAP v1 ...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Ignore User Dial-In Properties	False
Extended State	<Blank>

To close this wizard, click Finish.

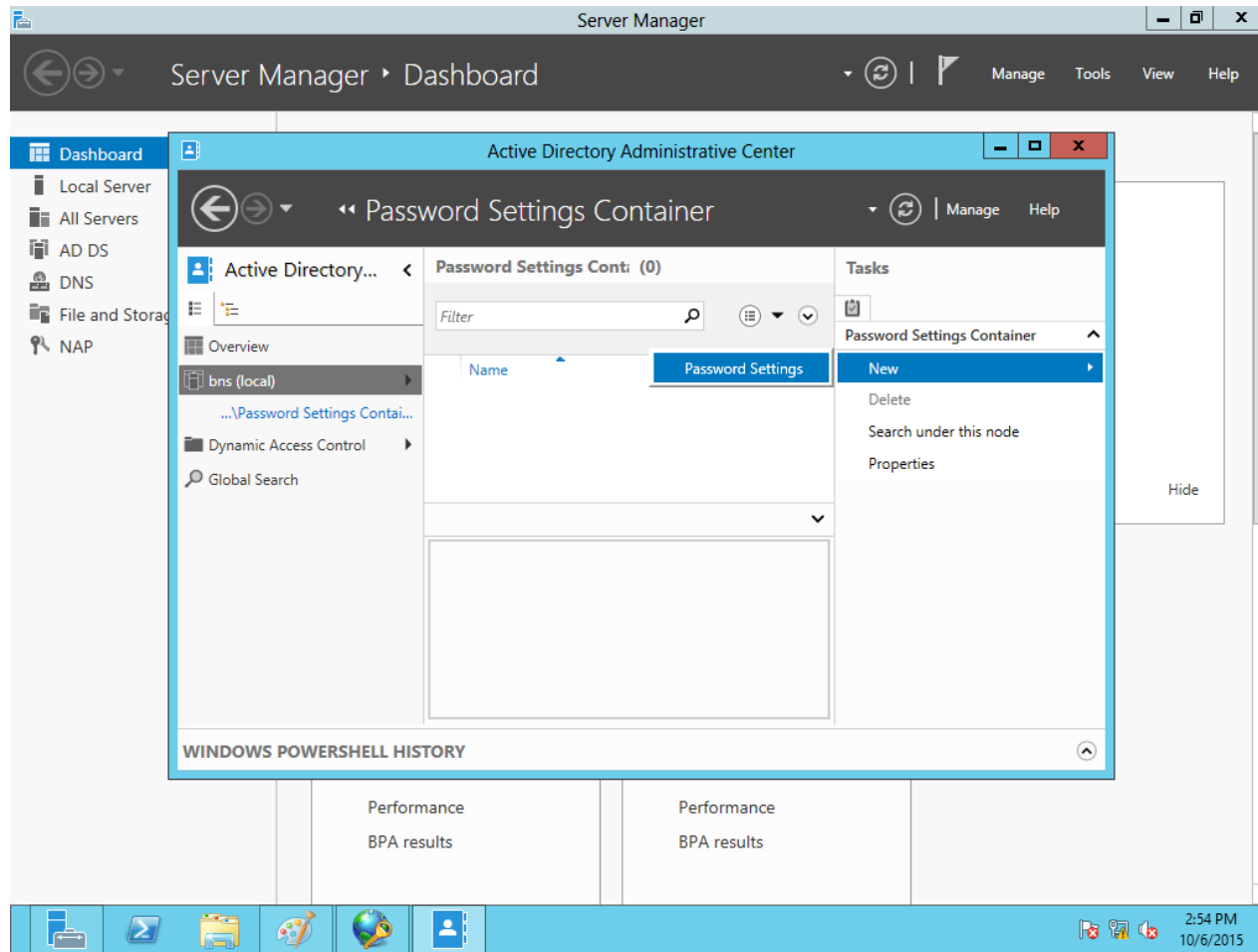
35

Previous Next Finish Cancel

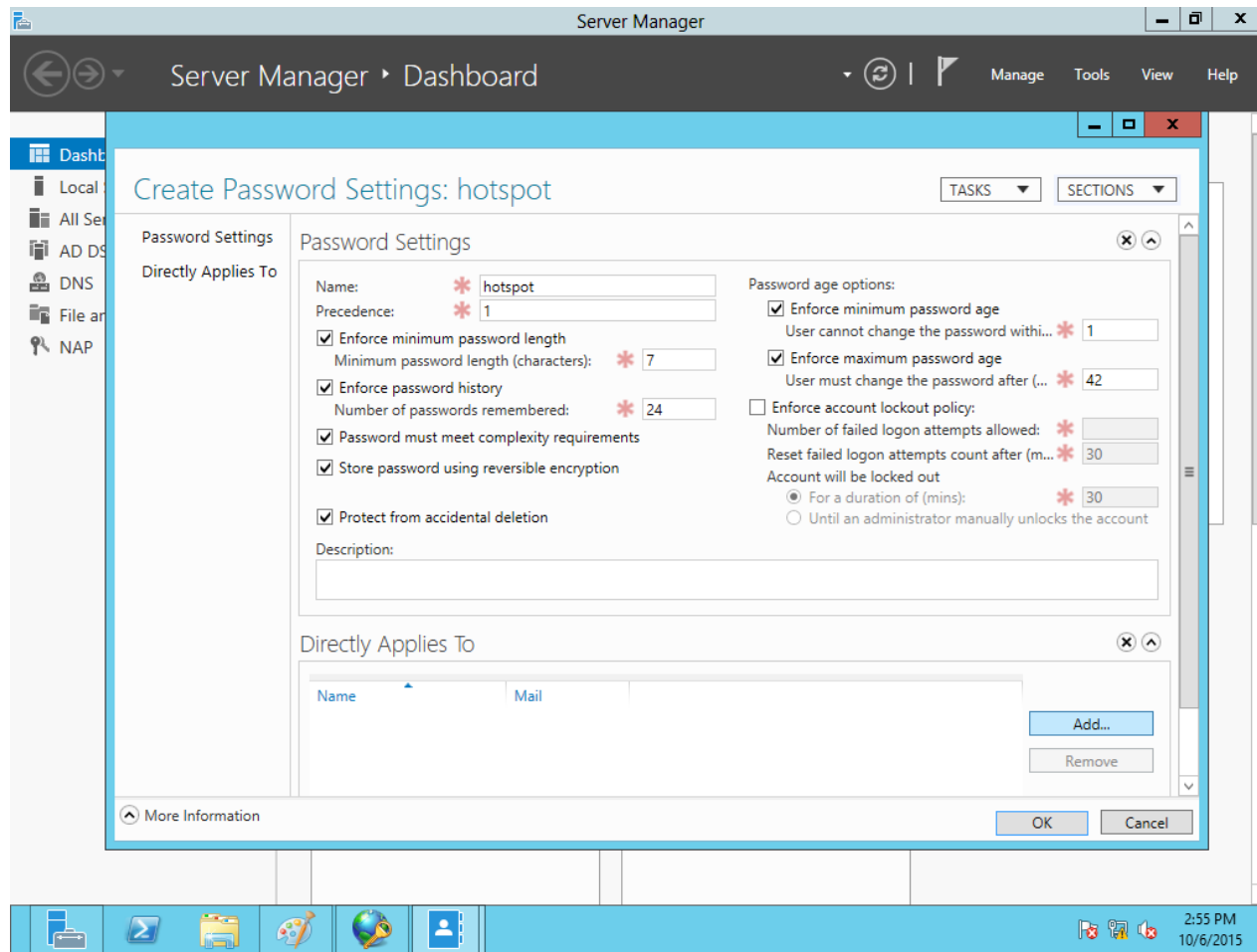
Konfigurasi Password Container



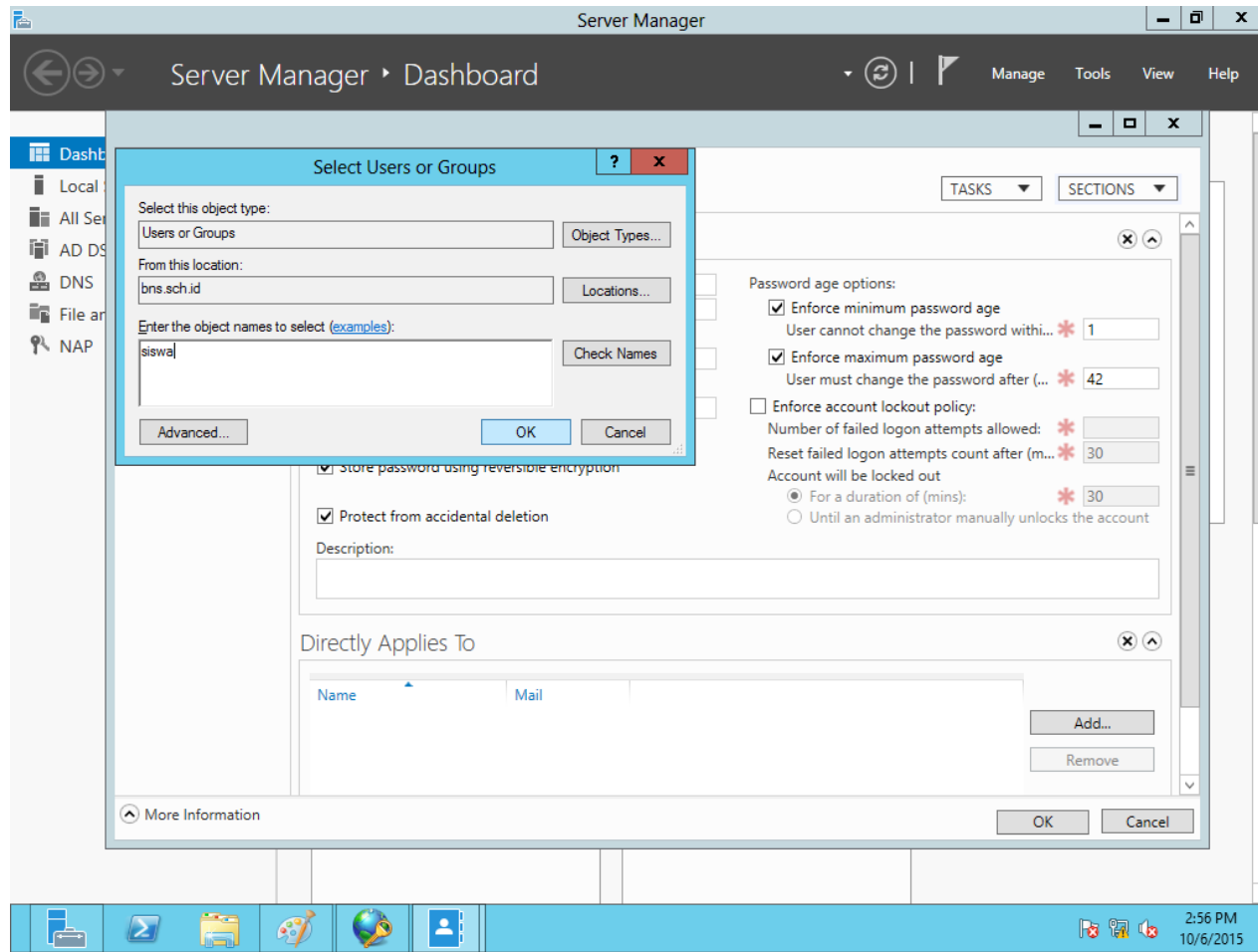
Konfigurasi Password Container



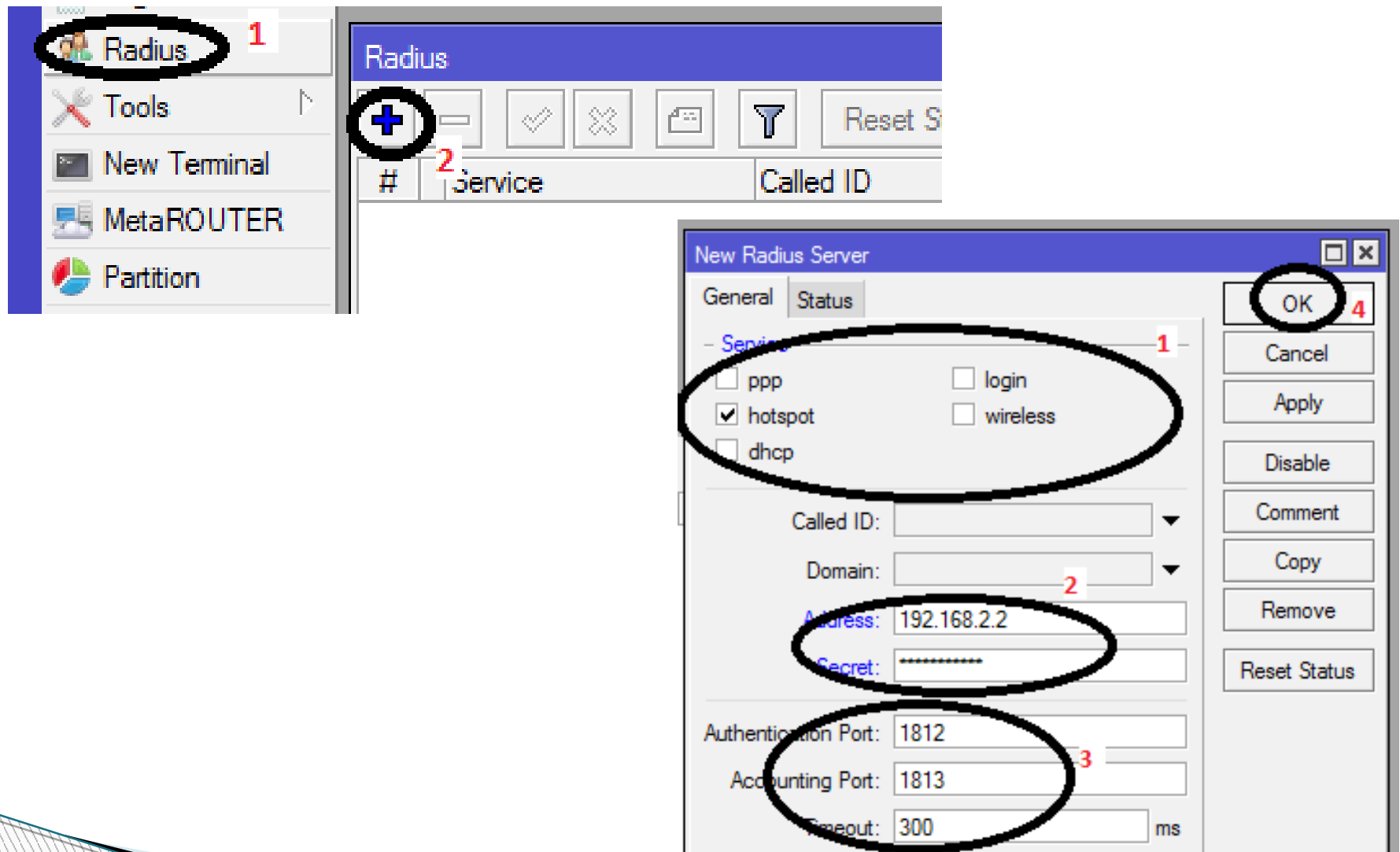
Konfigurasi Password Container



Konfigurasi Password Container



Set Radius di MikroTik (1)



The image shows the MikroTik WinBox interface for configuring a Radius server. The 'Radius' menu is highlighted with a red '1'. The '+' button in the toolbar is highlighted with a red '2'. The 'New Radius Server' dialog box is open, showing the 'General' tab. The 'Service' section has 'hotspot' selected (marked with a red '1'). The 'Address' field is set to '192.168.2.2' (marked with a red '2'). The 'Authentication Port' (1812) and 'Accounting Port' (1813) fields are circled with a red '3'. The 'OK' button is circled with a red '4'.

Radius 1

Tools

New Terminal

MetaROUTER

Partition

Radius

Service

Called ID

New Radius Server

General Status

Service

☐ ppp

☒ hotspot

☐ dhcp

☐ login

☐ wireless

Called ID:

Domain:

Address: 192.168.2.2

Secret:

Authentication Port: 1812

Accounting Port: 1813

Timeout: 300 ms

OK 4

Cancel

Apply

Disable

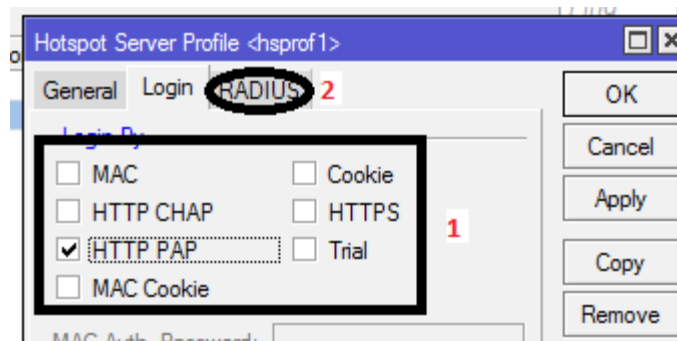
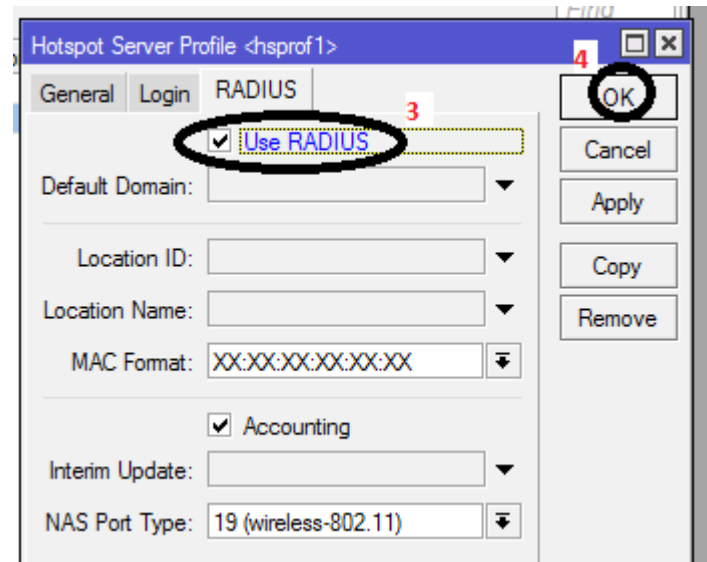
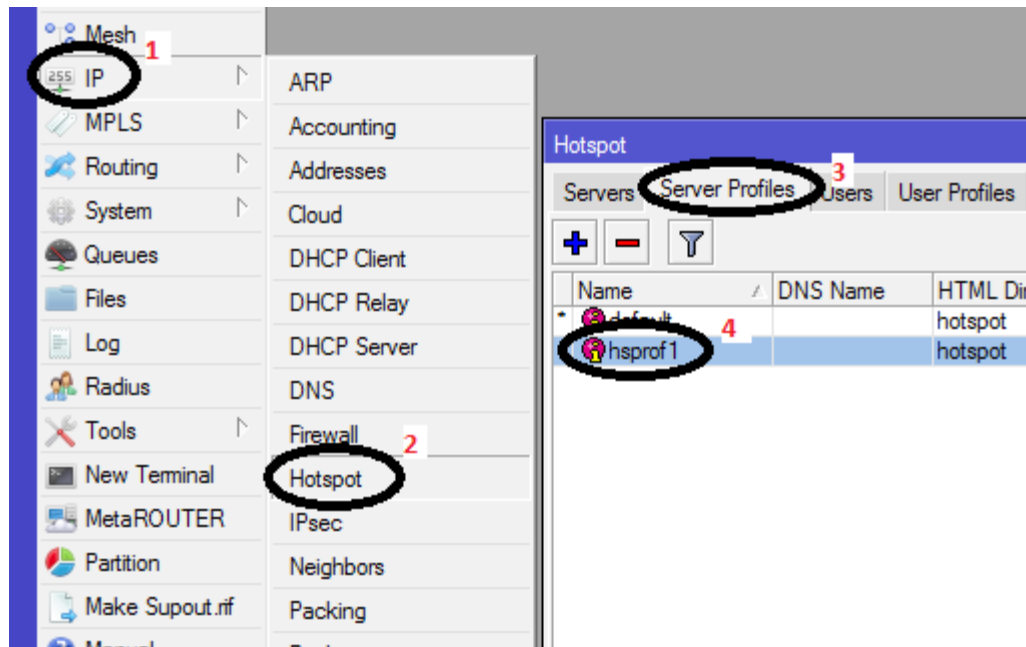
Comment

Copy

Remove

Reset Status

Set Radius di Mikrotik (2)



Info tambahan integrasi radius server

- ▶ password container dapat menjadi standar pengaturan password grup atau user
- ▶ Bandwidth manajemen di hotspot tetap berfungsi meskipun user berasal dari radius nya win2012



Blokir web terjadwal (1)

SET NTP CLIENT

- ▶ `/system ntp client`
- ▶ `set enabled=yes primary-ntp=119.82.243.189
secondary-ntp=203.114.224.252`

SET FIREWALL

- ▶ `/ip firewall filter`
- ▶ `add action=drop chain=forward comment=blok
content=facebook.com`
- ▶ `out-interface=ether1-internet src-
address=192.168.2.70-192.168.3.200`

Blokir web terjadwal (2)

SET SCRIPT

- ▶ add name=**allow**
policy=read,write,policy,test,sniff
source="/ip firewall filter set [/ip firewall
filter find comment="**blok**"] disabled=yes"
- ▶ add name=**denied**
policy=read,write,policy,test,sniff
source="/ip firewall filter set [/ip firewall
filter find comment="blok"] disabled=no"

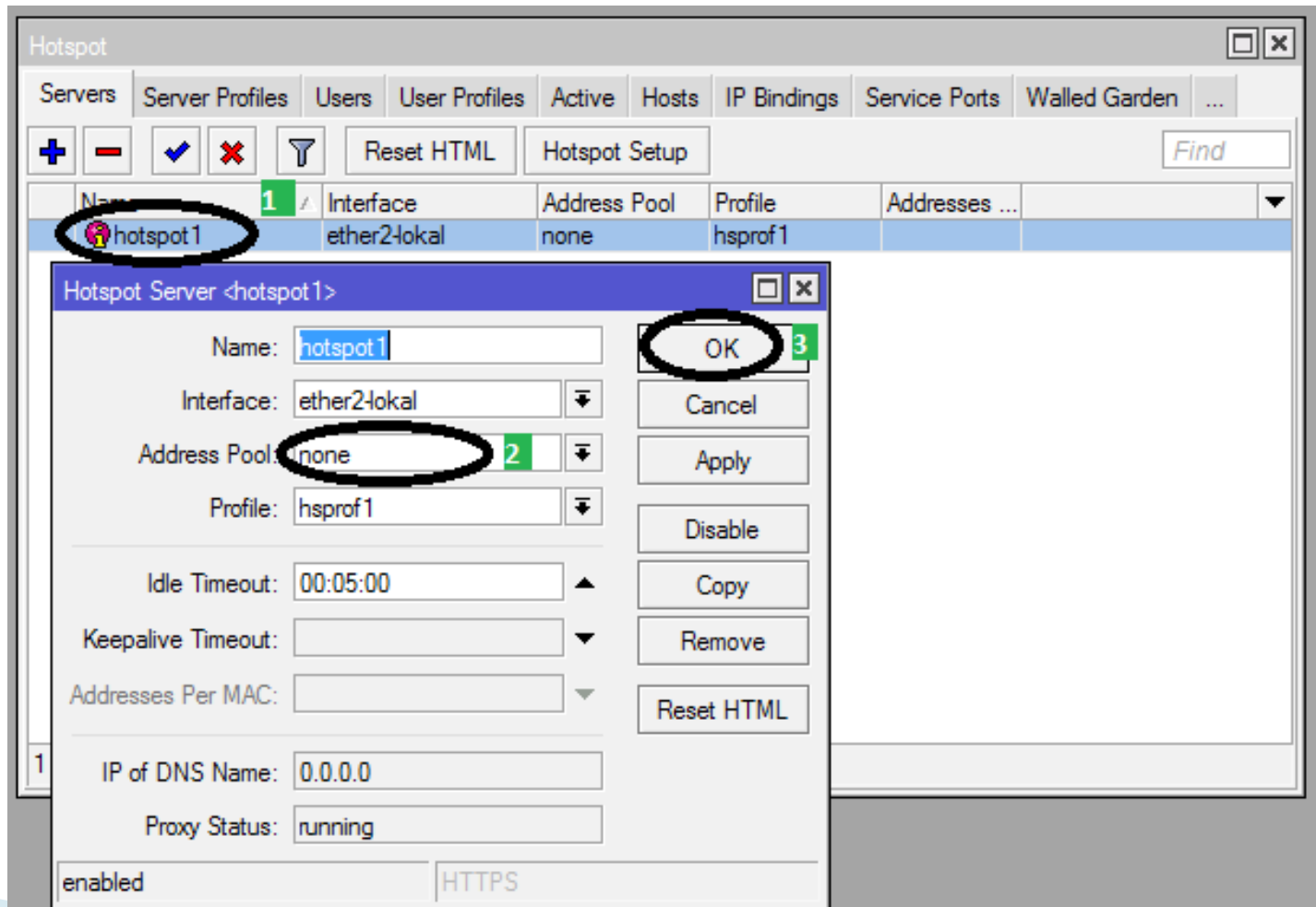
Blokir web terjadwal (3)

SET SCHEDULER

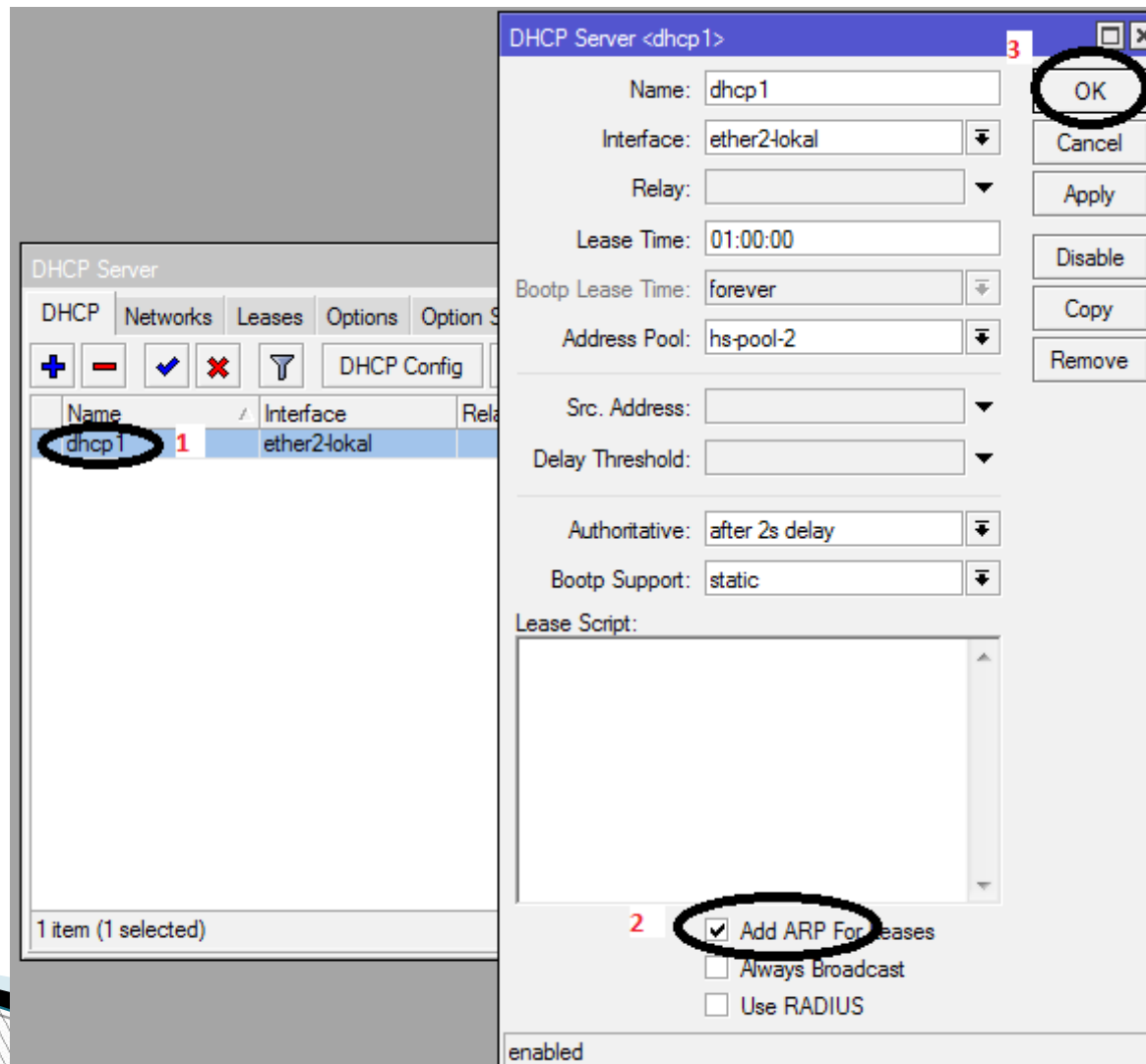
- ▶ /system scheduler
- ▶ add interval=1 d name=07.00 on-event=denied
policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive
start-date=sep/17/2015 start-time=07:00:00
- ▶ add interval=1 d name=12.00 on-event=allow
policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive
start-date=sep/17/2015 start-time=12:00:00
- ▶ add interval=1 d name=13.00 on-event=denied
policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive
start-date=sep/17/2015 start-time=13:00:00
- ▶ add interval=1 d name=15.45 on-event=allow
policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive
start-date=sep/17/2015 start-time=15:45:00



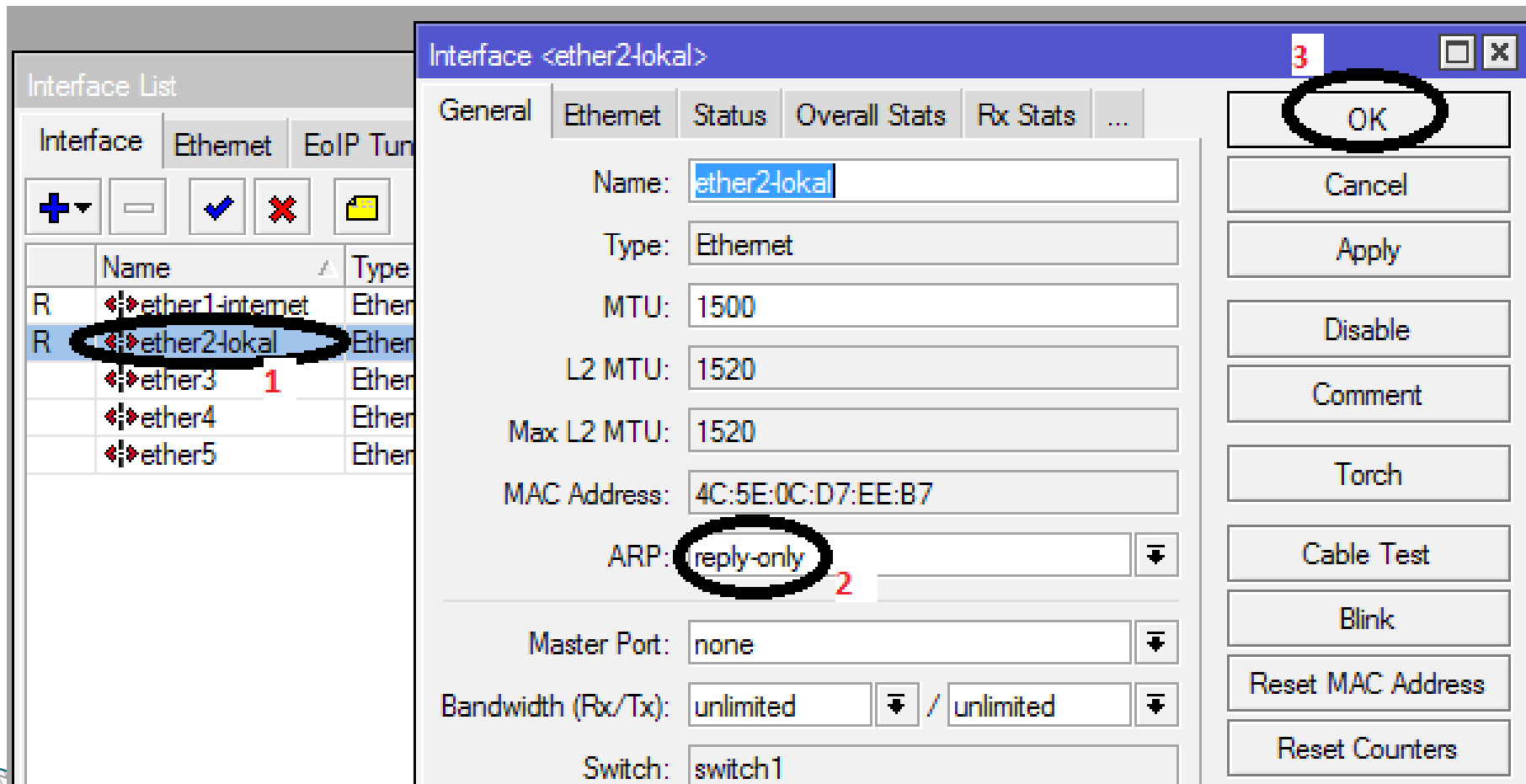
Force DHCP (1)



Force DHCP (2)



Force DHCP (3)

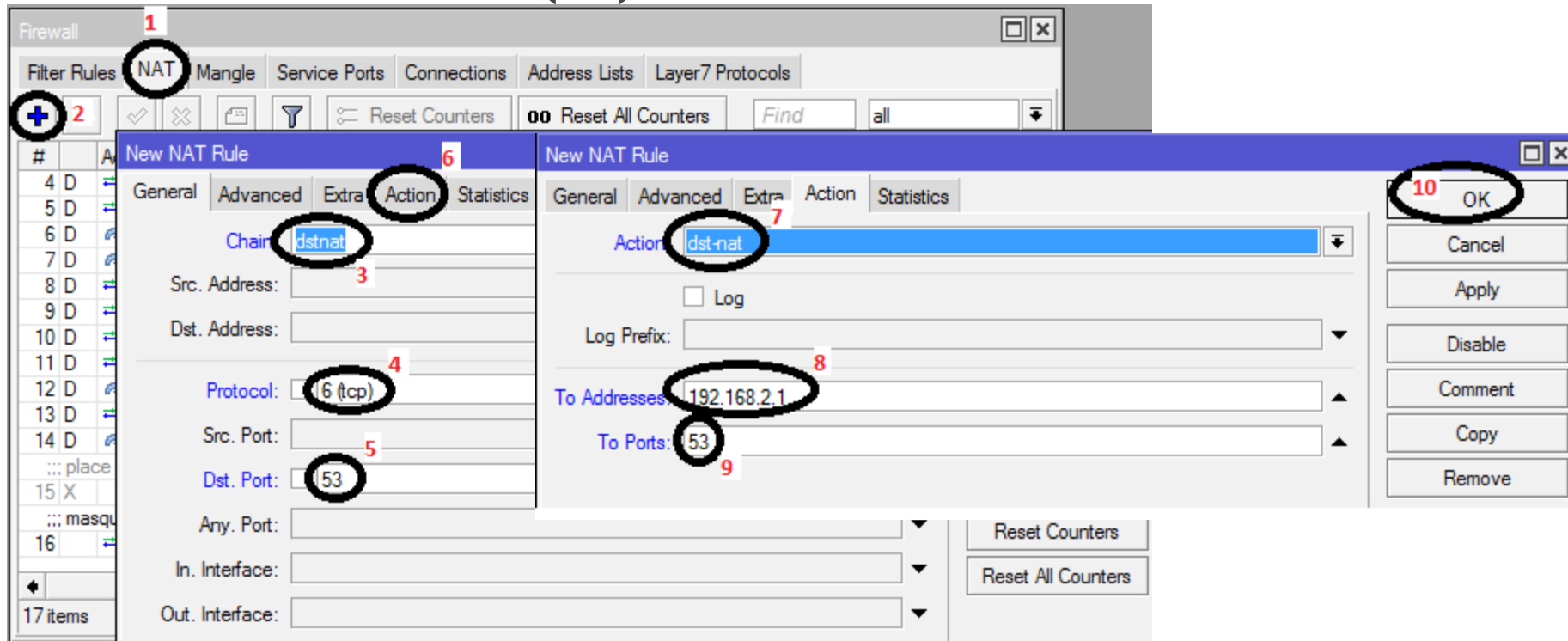


Force DHCP

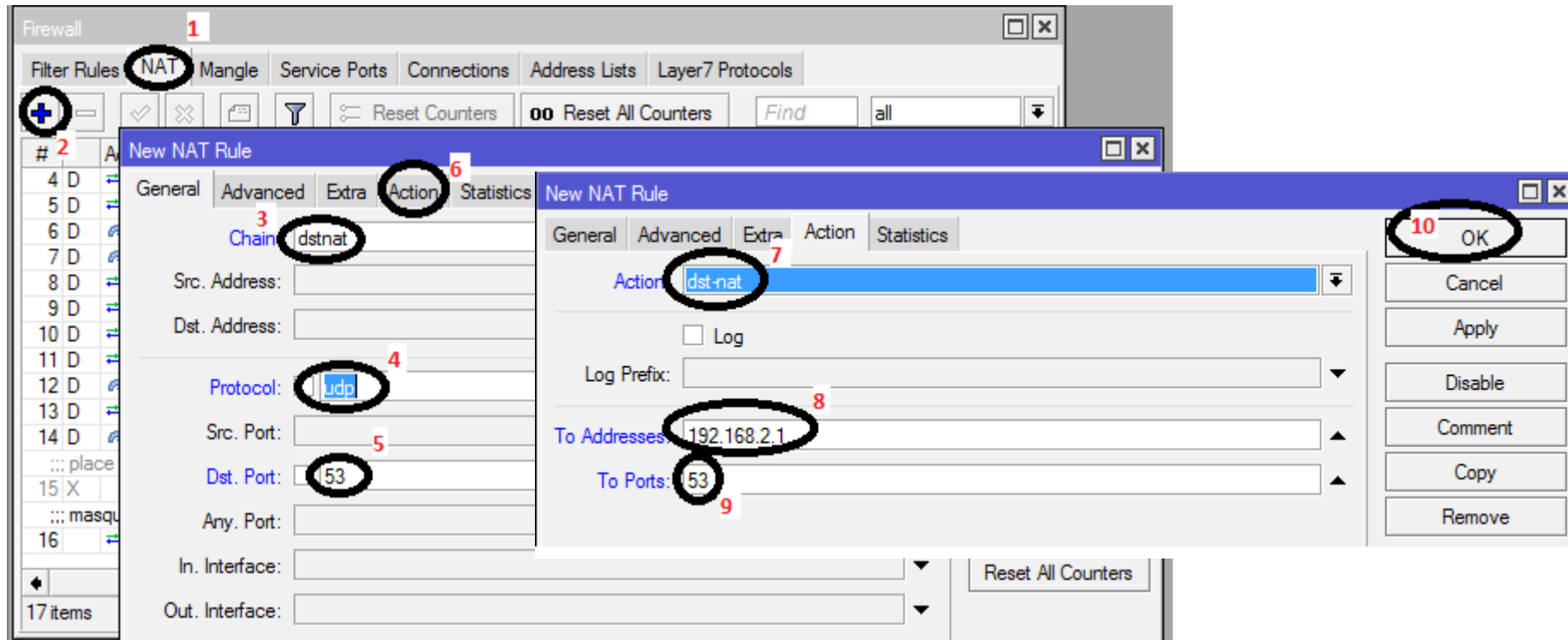
- ▶ `/ip hotspot set hotspot1 address-pool=none`
- ▶ `/ip dhcp-server set add-arp=yes
numbers=dhcp1`
- ▶ `/interface ethernet set ether2-lokal
arp=reply-only`



Force DNS (1)



Force DNS (2)



Force DNS

- ▶ `/ip firewall nat`
- ▶ `add chain=dstnat protocol=tcp dst-port=53
action=dst-nat to-addresses=192.168.2.1
to-ports=53`
- ▶ `add chain=dstnat protocol=udp dst-port=53
action=dst-nat to-addresses=192.168.2.1
to-ports=53`



Port knocking (1)

The screenshot shows the Mikrotik WinBox interface. On the left sidebar, the 'IP' menu is circled (1) and the 'Firewall' option is circled (2). The main window displays the 'Firewall' configuration page, with the 'Filter Rules' tab selected (3). A '+' icon is circled (4). Below, a table lists the existing filter rules:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port
0	D jump	forward				
1	D jump	forward				
2	D jump	input				
3	D drop	input			6 (tcp)	6
4	D jump	hs-input				
5	D acc...	hs-input			17 (u...	6
6	D acc...	hs-input			6 (tcp)	6
7	D jump	hs-input				
8	D reject	hs-unauth			6 (tcp)	
9	D reject	hs-unauth				
10	D reject	hs-unauth-to				

The 'New Firewall Rule' dialog box is shown with the 'General' tab selected (1). The 'Chain' is set to 'input' (2). The 'Protocol' is set to '6 (tcp)' (3). The 'Src. Port' is empty (4). The 'Dst. Port' is set to '123' (5).

The 'Firewall Rule <123>' dialog box is shown with the 'Action' tab selected (6). The 'Action' is set to 'add src to address list' (7). The 'Log' checkbox is unchecked. The 'Log Prefix' is empty. The 'Address List' is set to 'boleh' (8). The 'Timeout' is set to '00:01:00' (9). The 'OK' button is circled (10).

Port knocking (2)

The image shows the Mikrotik WinBox interface with several components highlighted by red circles and numbers 1 through 7, indicating the steps for configuring port knocking.

Step 1: The left sidebar menu is shown with 'IP' selected.

Step 2: The 'Firewall' option is selected in the left sidebar menu.

Step 3: The 'Filter Rules' tab is selected in the top toolbar.

Step 4: The 'Add' button (a blue circle with a plus sign) is clicked to create a new rule.

Step 5: The 'New Firewall Rule' dialog box is open, and the 'General' tab is selected.

Step 6: The 'Chain' dropdown is set to 'input'.

Step 7: The 'Action' dropdown is set to 'drop'.

Step 8: The 'Log' checkbox is checked.

Step 9: The 'Log Prefix' field is set to 'boleh'.

Step 10: The 'OK' button is clicked to save the rule.

Step 11: The 'New Firewall Rule' dialog box is open, and the 'Action' tab is selected.

Step 12: The 'Log' checkbox is checked.

Step 13: The 'Log Prefix' field is set to 'boleh'.

Step 14: The 'OK' button is clicked to save the rule.

Step 15: The 'New Firewall Rule' dialog box is open, and the 'General' tab is selected.

Step 16: The 'Chain' dropdown is set to 'input'.

Step 17: The 'Action' dropdown is set to 'drop'.

Step 18: The 'Log' checkbox is checked.

Step 19: The 'Log Prefix' field is set to 'boleh'.

Step 20: The 'OK' button is clicked to save the rule.

Step 21: The 'New Firewall Rule' dialog box is open, and the 'General' tab is selected.

Step 22: The 'Chain' dropdown is set to 'input'.

Step 23: The 'Action' dropdown is set to 'drop'.

Step 24: The 'Log' checkbox is checked.

Step 25: The 'Log Prefix' field is set to 'boleh'.

Step 26: The 'OK' button is clicked to save the rule.

Step 27: The 'New Firewall Rule' dialog box is open, and the 'General' tab is selected.

Step 28: The 'Chain' dropdown is set to 'input'.

Step 29: The 'Action' dropdown is set to 'drop'.

Step 30: The 'Log' checkbox is checked.

Step 31: The 'Log Prefix' field is set to 'boleh'.

Step 32: The 'OK' button is clicked to save the rule.

Step 33: The 'New Firewall Rule' dialog box is open, and the 'General' tab is selected.

Step 34: The 'Chain' dropdown is set to 'input'.

Step 35: The 'Action' dropdown is set to 'drop'.

Step 36: The 'Log' checkbox is checked.

Step 37: The 'Log Prefix' field is set to 'boleh'.

Step 38: The 'OK' button is clicked to save the rule.

Step 39: The 'New Firewall Rule' dialog box is open, and the 'General' tab is selected.

Step 40: The 'Chain' dropdown is set to 'input'.

Step 41: The 'Action' dropdown is set to 'drop'.

Step 42: The 'Log' checkbox is checked.

Step 43: The 'Log Prefix' field is set to 'boleh'.

Step 44: The 'OK' button is clicked to save the rule.

Step 45: The 'New Firewall Rule' dialog box is open, and the 'General' tab is selected.

Step 46: The 'Chain' dropdown is set to 'input'.

Step 47: The 'Action' dropdown is set to 'drop'.

Step 48: The 'Log' checkbox is checked.

Step 49: The 'Log Prefix' field is set to 'boleh'.

Step 50: The 'OK' button is clicked to save the rule.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port
0	D	jump	forward			
1	D	jump	forward			
2	D	jump	input			
3	D	drop	input		6 (tcp)	
4	D	jump	hs-input			
5	D	acc...	hs-input		17 (u...	
6	D	acc...	hs-input		6 (tcp)	
7	D	jump	hs-input			
8	D	reject	hs-auth		6 (tcp)	

Port knocking

- ▶ `/ip firewall filter`
- ▶ `add chain=input protocol=tcp dst-port=1 2 3
action=add-src-to-address-list address-
list=boleh address-list-timeout=10m`
- ▶ `add chain=input src-address-list=!boleh
action=drop`



1. ID-networkers, Mas Dedi khususnya (training gratis untuk guru SMK)
2. Pak Ziad Sobri (proses menjadi mikrotik academy)
3. Mas Supono (Materi mikrotiknya)
4. www.forummikrotik.com (materi mikrotiknya)
5. Wiki.mikrotik.com (panduannya)
6. SMK Bintang Nusantara School, (menyediakan tempat dan perangkat untuk latihan)



TERIMA KASIH