اونيۏرسيتي مليسيا ڤهڠ
UNIVERSITI MALAYSIA PAHANG

BCN3043
NETWORK SERVICE ADMIN

LECTURER NAME: DR NOORHUZAIMI @ KARIMAH BINTI MOHD NOOR

PROJECT TITLE: NETWORK POLICY SERVER

SUBMISSION DATE: 16 JUNE 2023

GROUP MEMBERS:

NAME	MATRIC ID	SECTION	PHOTO
NISHANTI A/P VENGADRAJ	CA20047	02B	
MOHD AENNAZ BIN ABD AZIZ	CA20073	02B	
MUHAMMAD IRFAN BIN ROSLI	CA21089	01A	
MUHAMMAD AFFIQ BIN MUHAMMAD ASRI	CA21064	01A	
MUHAMMAD NUR AIMAN BIN ALI	CA21062	01A	

Table of Content

1.0 INTRODUCTION

1.1 INTRODUCTION TO NETWORK POLICY SERVER

The Network Policy Server (NPS), developed by Microsoft, is a powerful network access control server that provides a centralized platform for managing network authentication, authorization, and accounting (AAA) policies. NPS offers a flexible and scalable solution for controlling network access based on predefined policies, enhancing the overall security and efficiency of an organization's network infrastructure.

NPS provides network managers with a wide range of tools and features that enable them to impose granular access controls. It enables the development of network rules that describe the conditions under which people, devices, or organizations have access to network resources. These rules can take into account a number of characteristics, including user identification, group membership, time of day, and network location, allowing administrators to adjust access rights to individual needs.

NPS also provides extensive auditing and accounting capabilities, enabling organizations to monitor and manage network access activities. This capability is crucial in preserving regulatory compliance and aiding forensic investigation in the case of a security incident.

1.2 SUMMARIZE

This report aims to provide an overview of Network Policy Server (NPS) and its server services. It begins with an introduction to NPS, highlighting its role as a centralized authentication, authorization, and accounting (AAA) infrastructure for network access.

The detailed explanation of each assigned server service will include:

1. Detail about the Service:
   This section will provide an in-depth description of the assigned service, including its purpose, functionality, and key features.

2. The Importance of the Service:
   The significance and benefits of the service will be highlighted, discussing how it contributes to network security, access control, and compliance.

3. Working Mechanism (Supported with Figures):
   To enhance understanding, the working mechanism of the service will be explained using visual aids such as figures and diagrams. These visuals will help illustrate the flow and processes involved in the service.

4. Examples of Scenarios:
   Real-world scenarios will be presented to demonstrate the practical application of the assigned service in different network environments. This will showcase how organizations can utilize the service to meet their specific needs.

5. Advantages and Disadvantages:
   A balanced analysis of the service will be provided, discussing its advantages and disadvantages. This will enable readers to understand the potential benefits and limitations of implementing the service.

6. Citations and References:
   To ensure accuracy and credibility, all information and sources used in the report will be properly cited and referenced following the APA format. A list of references will be included at the end of the report.

1.3 TASK DISTRIBUTION

Subtopic	**Contribution**
- Introduction - Summarize - Task Distribution	- Aennaz
- Details of NPS	- Affiq
- Importance of NPS	- Affiq
- How it works	- Irfan
- Example of NPS Scenario	- Irfan
- Advantages & Disadvantages	- Nishanti
- Step by Step Configuration/Coding	- Aennaz - Nishanti
- Conclusion	- Aiman
- In-Text Citations & References	- Aiman - Nishanti
- Report Format & Rubric	- Aennaz - Nishanti
- Hard Copy Report	- Aiman

2.0 CONCEPT OF NETWORK POLICY SERVER

2.1 DETAILS OF NETWORK POLICY SERVER

Network Policy Service (NPS) is a centralized system or service that allows for the enforcement and maintenance of network policies inside a computer network. It is an operating system component that offers a framework for managing and enforcing network access controls. It is also typically used in Microsoft Active Directory systems to regulate network resource access and guarantee policy compliance. A Network Policy Service's primary objective is to govern and manage network access based on established policies. These policies can establish the rules and circumstances for granting or rejecting network resource access, as well as the level of access allowed to various individuals or groups.

One of the many NPS applications is network access control. Organizations may use NPS to restrict and manage network access based on specified policies. It guarantees that only authorized users and devices may access network resources. Next is authentication. NPS supports various authentication methods and verifies the identity of users or devices before granting network access. It ensures that only authenticated users can connect to the network and helps prevent unauthorized access. Then there's logging and auditing. NPS has logging and accounting features, which allow it to record network access activity for auditing reasons. It provides logs and reports that may be used to monitor resource utilization, track user activity, and investigate security problems.

2.2 IMPORTANCE OF NETWORK POLICY SERVER

Network Policy Server typically used in Microsoft Active Directory systems to regulate access to network resources and ensure policy compliance. There are several important Network policy servers such as authentication, authentication in Network Policy Server (NPS) refers to the process of confirming the identity of a person or device seeking to join a network or use network resources. Organizations may use NPS to authenticate people and devices seeking to connect to the network. It accepts a variety of authentication mechanisms, including username/password, digital certificates, smart cards, and others. NPS guarantees that only authorized persons or devices have access to network resources by authenticating network users.

The following step is authorization. The process of providing or refusing access to network resources based on rights, characteristics, and network access policies set by authenticated users is referred to as authorization in Network Policy Server (NPS). After a user's identification has been validated, NPS decides what activities the person is permitted to conduct and what network resources they may access. NPS allows network managers to set access policies that describe which individuals or groups are authorized to access certain network resources, such as servers, apps, or shared files. These policies, which can be based on user factors such as group membership, user roles, or custom attributes, ensure that only authorized users have access to sensitive information or can conduct certain tasks.

Network Access regulate (NAC) is another significant network policy server. It is a security tool used to enforce policies and regulate network access. It guarantees that only authorized and conforming devices are allowed to connect to the network, while banning or restricting access to unauthorized or non-compliant devices. The Network Policy Server (NPS) role in Microsoft Windows Server provides a policy-based network access control solution.

Furthermore, logging and auditing are vital in NPS. Network Policy Server (NPS) logging and auditing are critical components for monitoring and maintaining a network's security and operational integrity. Administrators may track and evaluate events related to authentication, authorization, and accounting procedures using NPS's rich logging features. These logs can be utilized for troubleshooting, compliance auditing, security analysis, and report generation.

2.3 HOW IT WORKS?

An organization has used a Network Policy Server (NPS) to develop a secure Wi-Fi access control system. For the Wi-Fi network, the NPS server serves as the primary authentication and authorization authority. An employee must input their username and password while utilizing a device that was provided by the employer to access the network. This data is transmitted by the Wi-Fi access point to the NPS server for validation like in figure 0.1. The NPS server compares the employee's credentials to the user database of the company and assesses authorization policies such as group membership or device type. The NPS server authorizes access if the credentials are legitimate and the employee satisfies the permission requirements, enabling the employee's device to join safely to the Wi-Fi network.

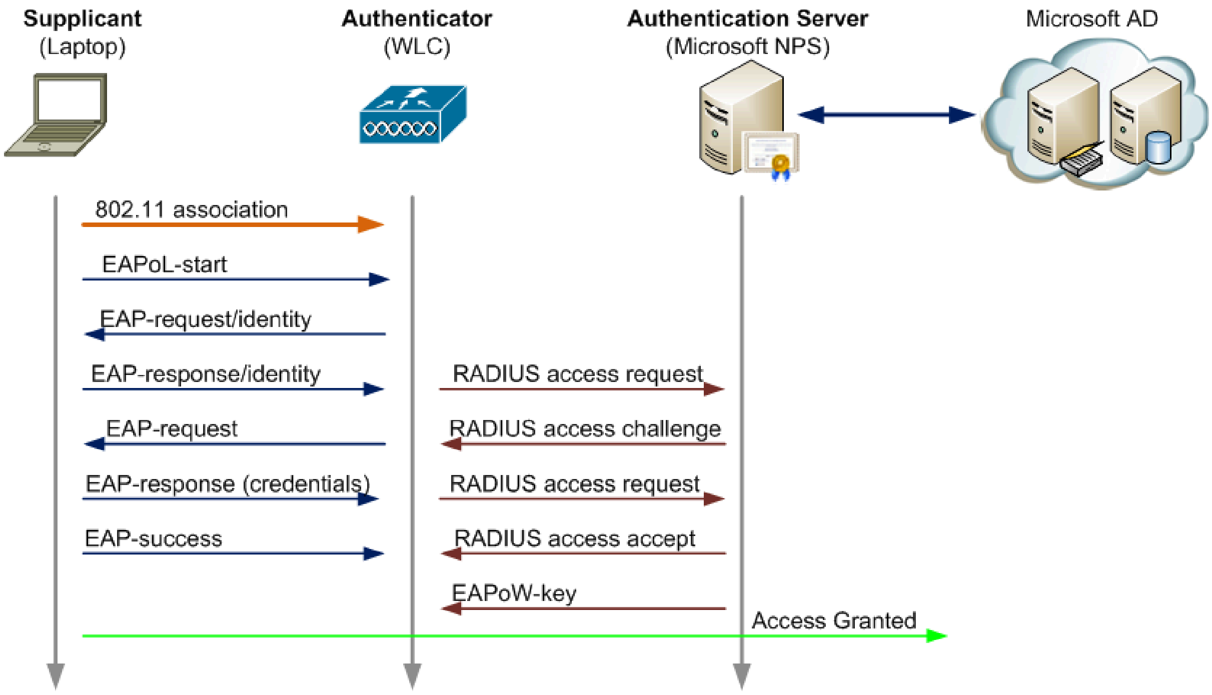


Figure 0.1

Similar to that, temporary credentials are given to visitors who want to join the Wi-Fi network. The access point sends the data to the NPS server once the guest inputs these credentials on the Wi-Fi login screen. The NPS server checks the authorization policies particular to guest access and validates the guest's credentials. It might impose limitations like limiting access to only the internet and disabling access to internal resources. The NPS server allows restricted access to the guest's device if their credentials are legitimate and they satisfy the authorization requirements, allowing them to connect to the Wi-Fi network with the specified limitations.

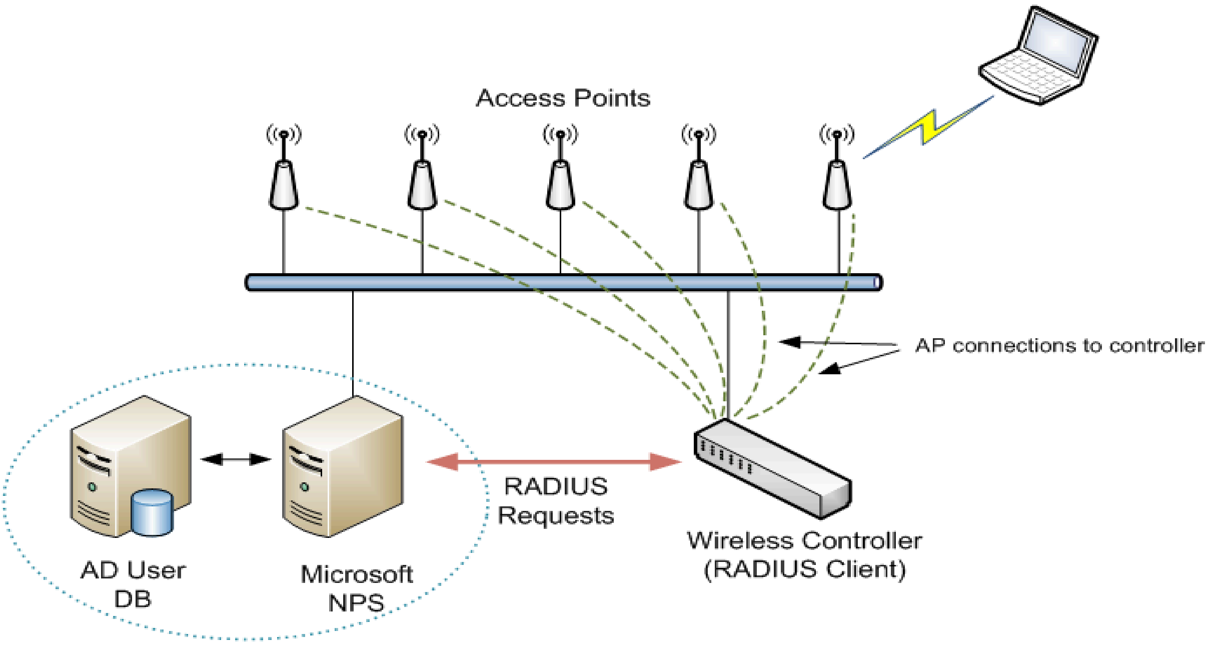


Figure 0.2

In this case, the company can make sure that only authorized users, such as employees with legitimate credentials, are able to connect to the Wi-Fi network by using NPS. It offers a secure and controlled Wi-Fi environment by enabling centralized control and enforcement of access regulations. Additionally, the organization is able to distinguish between various user classes, such as employees and visitors, and implement tailored access limits as necessary thanks to the use of NPS.

2.4 EXAMPLE OF NETWORK POLICY SERVER SCENARIO

You can specify who is allowed to join the network and the situations under which they can or cannot connect using network policy, which are conditions of requirements, constraints, and settings. Therefore there are several scenarios that ornament the example of a network policy server are being used.

Scenario 1: An organization is aware of how crucial it is to protect the security of its wireless network while carefully controlling access. The company will handle this by installing a Network Policy Server (NPS), which functions as a RADIUS server for dial-in users requiring remote authentication. When a user tries to join the wireless network, the NPS assumes responsibility for confirming their credentials, including their login and password. The NPS then evaluates the user's request for access to the wireless network in light of the organization's established network policies before approving or rejecting it. By guaranteeing that only authorized users with valid credentials can connect to the wireless network, this technique increases the organization's overall security measures.

Scenario 2 : A company takes proactive measures to provide remote workers' secure access to the internal network. To authenticate and authorize VPN connections, they set up a Network Policy Server (NPS) that serves as a Remote Authentication Dial-In User Service (RADIUS) server. The NPS takes on the duty of confirming user credentials, and carefully assessing whether they belong to the specified network policies. These regulations may specify membership in specified groups or adherence to certain security standards. The NPS effectively controls VPN access by subjecting user credentials to these policy checks and only allowing access to those who meet the required requirements. As a result, the business makes sure that its distant employees may access the internal network safely, improving network security as well as protecting sensitive data.

Scenario 3 : Guests can access a guest network at a hotel or café. They set up an NPS as a RADIUS server to control visitor access and authentication. The NPS requests a valid access code or payment information when a visitor wants to connect to the network. Following authentication, the NPS imposes rules on guest users, such as time limits, bandwidth restrictions, and content filtering

2.5 ADVANTAGES AND DISADVANTAGES

The Network Policy Server (NPS) provides several benefits to organizations. The first advantage is centralized policy management, which allows administrators to establish and implement network policies from a single place. This simplifies management and ensures consistent policy enforcement across the company's network. Because of NPS's seamless interaction with Microsoft Active Directory, existing user and group accounts may be used for authentication. Organizations can utilize this connectivity to implement policies based on user IDs and simplify user management.

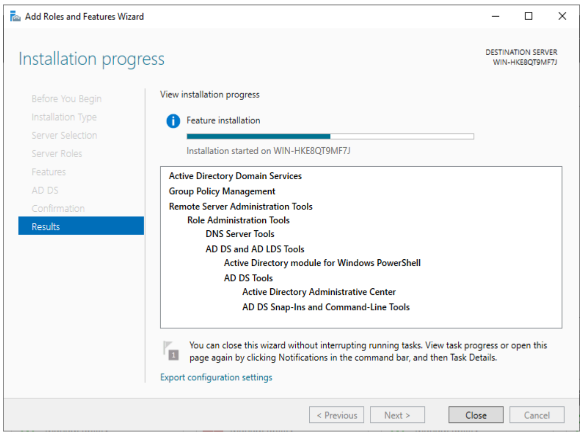
Furthermore, NPS supports a range of authentication mechanisms, including 802.1X, RADIUS, and PEAP, allowing customers to choose the optimal one for their network architecture and security requirements. Furthermore, NPS enables granular access control, which allows administrators to establish rules based on a range of parameters such as user identification, device type, time of day, and so on.

Despite its advantages, NPS has certain disadvantages to consider. To begin, it is primarily intended for use in Windows Server settings, which limits its compatibility with other operating systems. Organizations that use a mixed operating system environment may need to look into alternate alternatives. Furthermore, establishing and configuring NPS may be difficult, necessitating knowledge and skill in network security and policy management.

3.0 STEP BY STEP CONFIGURATION/CODING

3.1 FIGURE WITH CAPTION

Setting Up Required Feature for Network Policy Server



Installation progress

DESTINATION SERVER
WIN-HKE8QT9MF7J

View installation progress

Feature installation

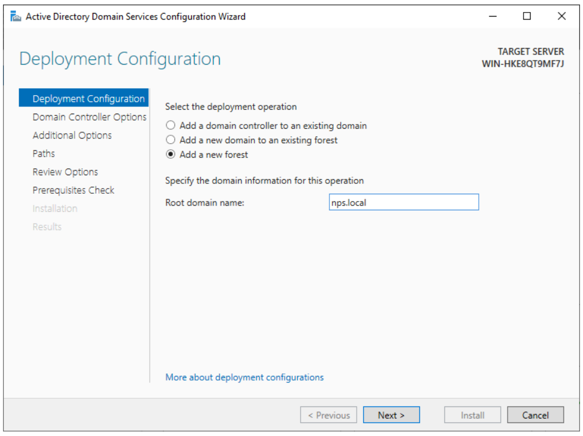
Installation started on WIN-HKE8QT9MF7J

Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
    Role Administration Tools
        DNS Server Tools
        AD DS and AD LDS Tools
            Active Directory module for Windows PowerShell
            AD DS Tools
                Active Directory Administrative Center
                AD DS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Figure 1.0: ADDS & DNS Feature



Deployment Configuration

TARGET SERVER
WIN-HKE8QT9MF7J

Select the deployment operation

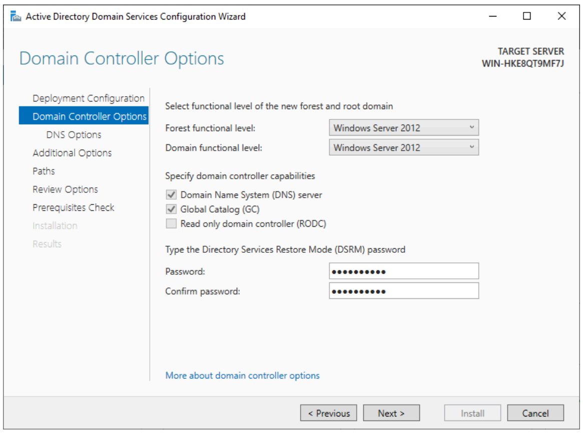
○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: nps.local

More about deployment configurations

Figure 1.1: Specify Root Domain Name



Domain Controller Options

TARGET SERVER
WIN-HKE8QT9MF7J

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012
Domain functional level: Windows Server 2012

Specify domain controller capabilities

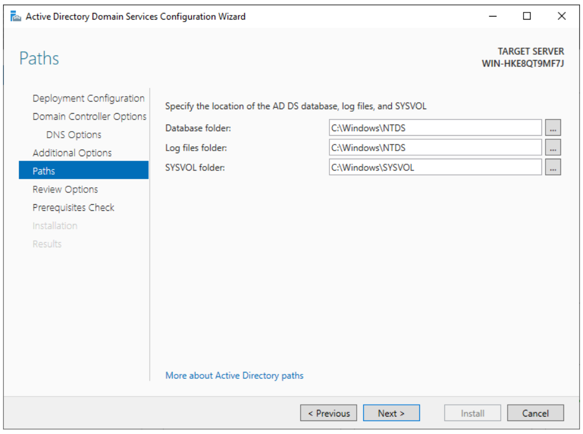
☑ Domain Name System (DNS) server
☑ Global Catalog (GC)
□ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●●
Confirm password: ●●●●●●●●●●

More about domain controller options

Figure 1.2: Set Password



Paths

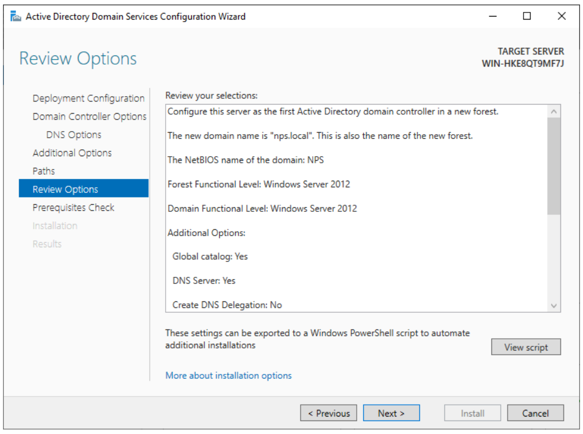
TARGET SERVER
WIN-HKE8QT9MF7J

Specify the location of the AD DS database, log files, and SYSVOL

Database folder: C:\Windows\NTDS
Log files folder: C:\Windows\NTDS
SYSVOL folder: C:\Windows\SYSVOL

More about Active Directory paths

Figure 1.3: Specify Path



Review Options

TARGET SERVER
WIN-HKE8QT9MF7J

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "nps.local". This is also the name of the new forest.

The NetBIOS name of the domain: NPS

Forest Functional Level: Windows Server 2012

Domain Functional Level: Windows Server 2012

Additional Options:

Global catalog: Yes

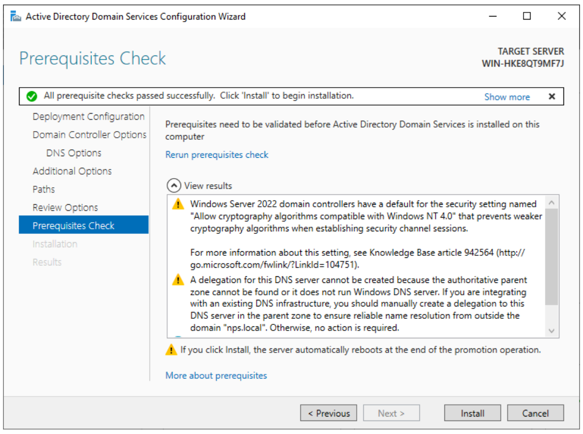
DNS Server: Yes

Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations

More about installation options

Figure 1.4: Review Selection



Prerequisites Check

TARGET SERVER
WIN-HKE8QT9MF7J

All prerequisite checks passed successfully. Click 'Install' to begin installation.

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

Rerun prerequisites check

Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

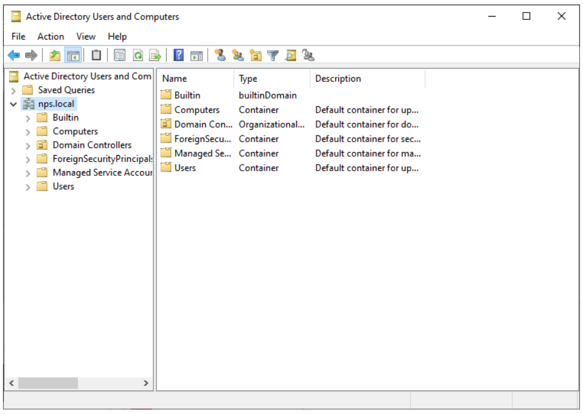
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "nps.local". Otherwise, no action is required.

If you click Install, the server automatically reboots at the end of the promotion operation.

More about prerequisites

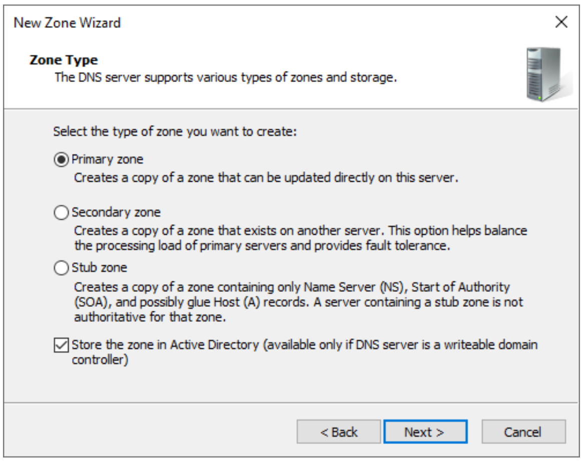
Figure 1.5: Prerequisites Check Feature

Active Directory



Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...

Figure 1.6: Set New Zone



Zone Type

The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

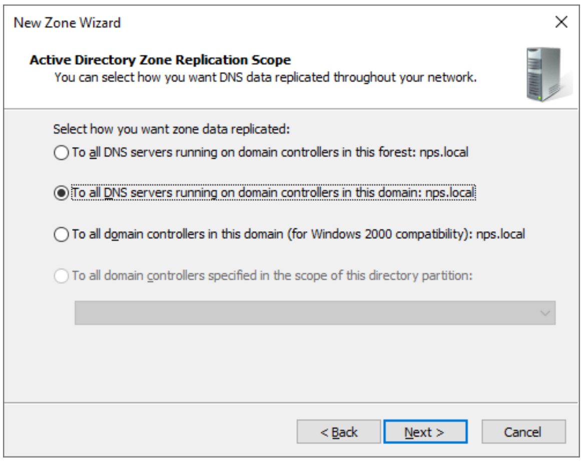
● Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☑ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

Figure 1.7: Select type of zone and storage



Active Directory Zone Replication Scope

You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

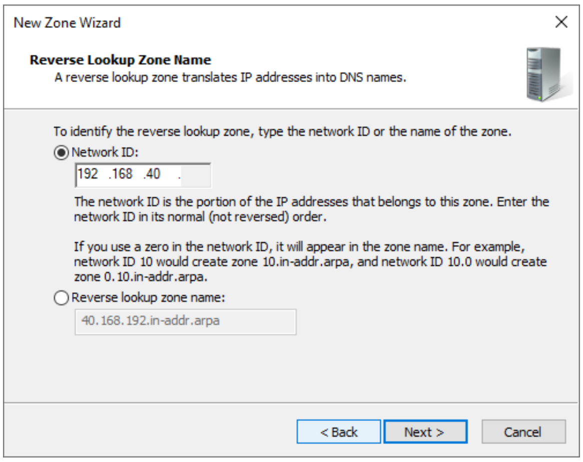
○ To all DNS servers running on domain controllers in this forest: nps.local

● To all DNS servers running on domain controllers in this domain: nps.local

○ To all domain controllers in this domain (for Windows 2000 compatibility): nps.local

○ To all domain controllers specified in the scope of this directory partition:

Figure 1.8: Set Replication Scope



Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

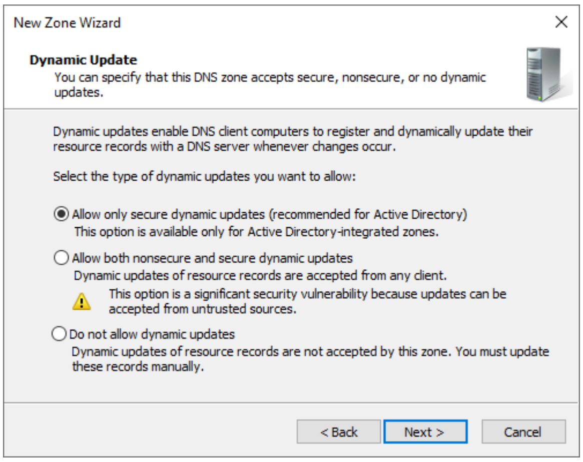
● Network ID:
192 .168 .40 .

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

○ Reverse lookup zone name:
40.168.192.in-addr.arpa

Figure 1.9: Set Reverse lookup zone



Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

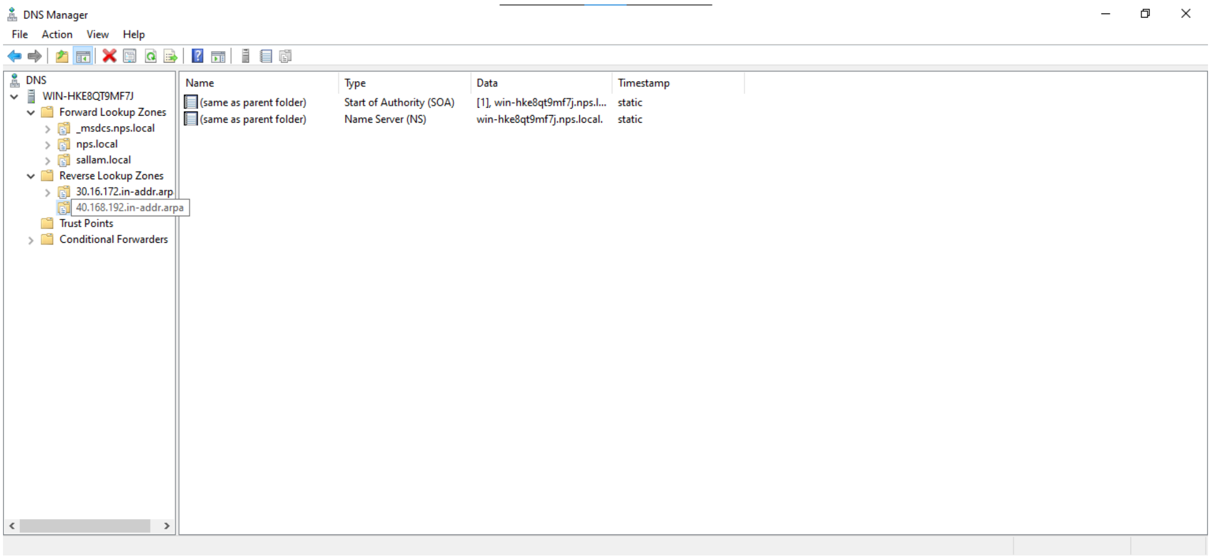
Select the type of dynamic updates you want to allow:

● Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

○ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
⚠ This option is a significant security vulnerability because updates can be accepted from untrusted sources.

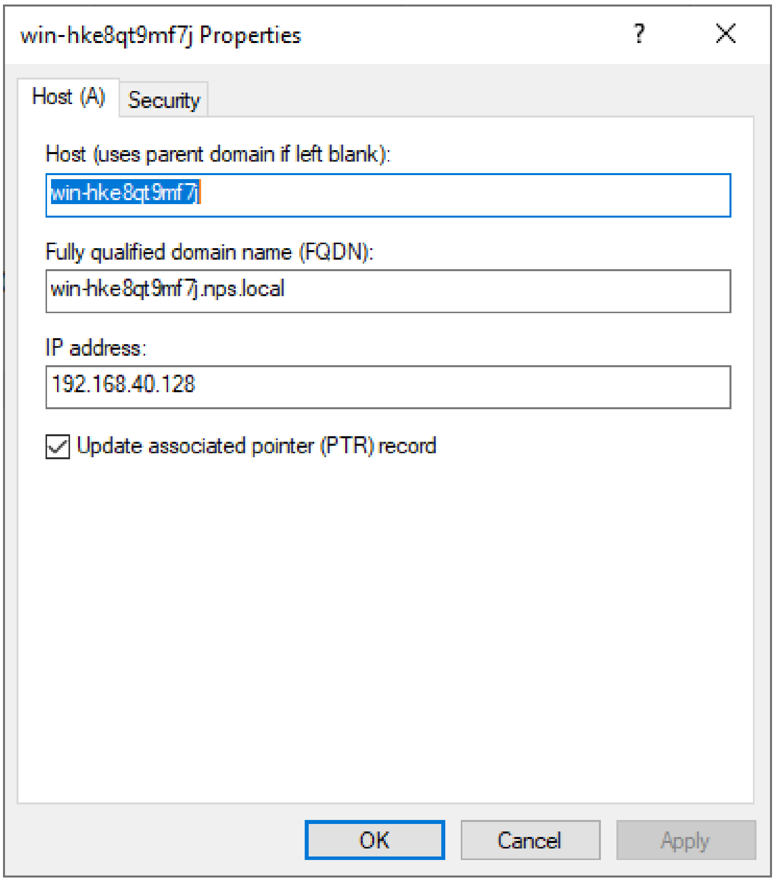
○ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

Figure 2.0: Specify DNS Updates



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[1], win-hke8qt9mf7j.nps.l...	static
(same as parent folder)	Name Server (NS)	win-hke8qt9mf7j.nps.local.	static

Figure 2.1: Reverse Lookup Zone IP Created



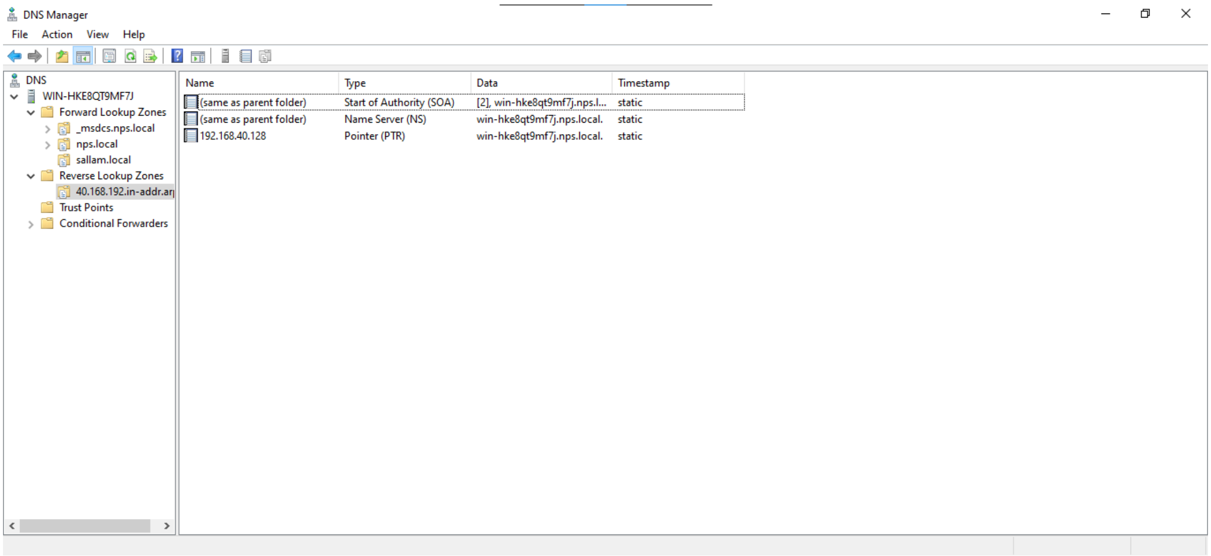
Host (uses parent domain if left blank): win-hke8qt9mf7j

Fully qualified domain name (FQDN): win-hke8qt9mf7j.nps.local

IP address: 192.168.40.128

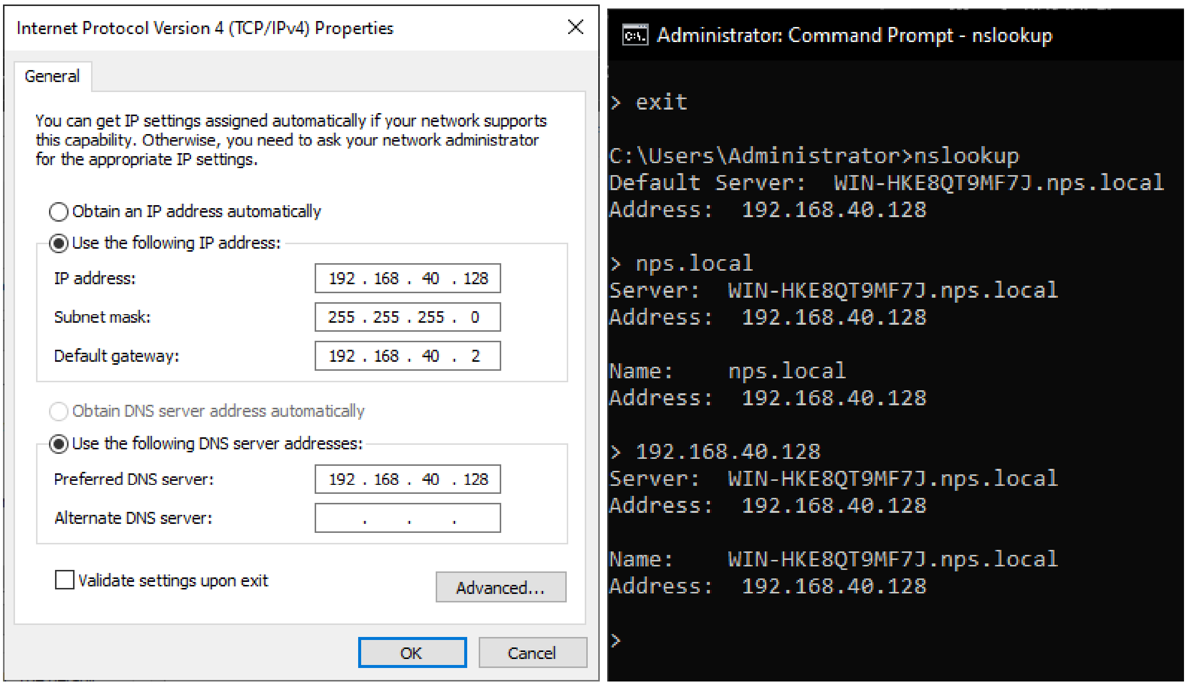
☑ Update associated pointer (PTR) record

Figure 2.2: Server Properties



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[2], win-hke8qt9mf7j.nps.l...	static
(same as parent folder)	Name Server (NS)	win-hke8qt9mf7j.nps.local.	static
192.168.40.128	Pointer (PTR)	win-hke8qt9mf7j.nps.local.	static

Figure 2.3: New Pointer Created



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 40 . 128

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 40 . 2

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 40 . 128

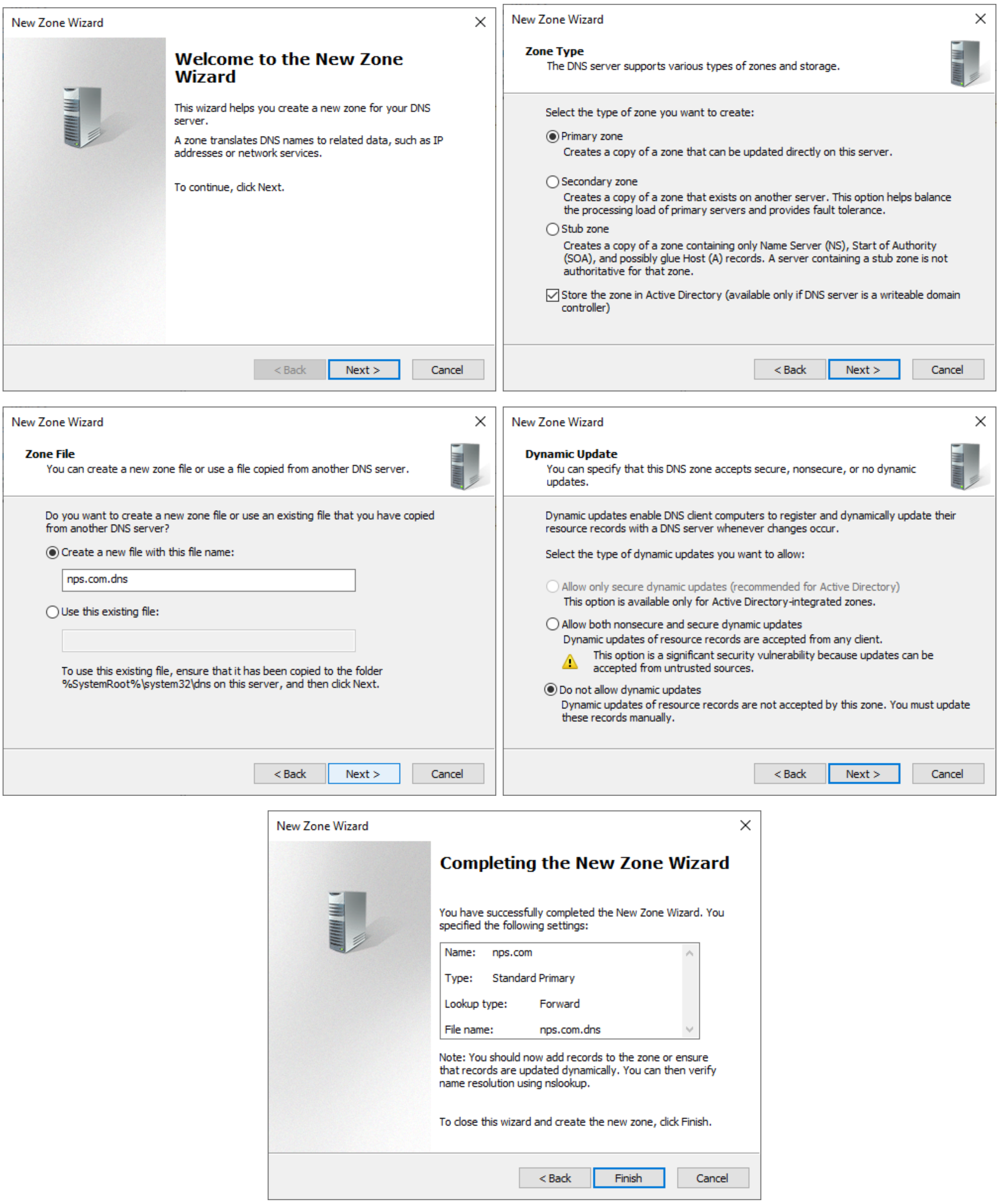
Alternate DNS server: . . .

□ Validate settings upon exit

```
> exit

C:\Users\Administrator>nslookup
Default Server:  WIN-HKE8QT9MF7J.nps.local
Address:  192.168.40.128

> nps.local
Server:  WIN-HKE8QT9MF7J.nps.local
Address:  192.168.40.128

Name:    nps.local
Address:  192.168.40.128

> 192.168.40.128
Server:  WIN-HKE8QT9MF7J.nps.local
Address:  192.168.40.128

Name:    WIN-HKE8QT9MF7J.nps.local
Address:  192.168.40.128

>
```

Figure 2.4: Setting Up IPv4 for Active Directory

Domain Name System (DNS)



New Zone Wizard

Welcome to the New Zone Wizard

This wizard helps you create a new zone for your DNS server.

A zone translates DNS names to related data, such as IP addresses or network services.

To continue, click Next.

New Zone Wizard

Zone Type
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

● Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☑ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

New Zone Wizard

Zone File
You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

● Create a new file with this file name:
nps.com.dns

○ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

New Zone Wizard

Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

○ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

○ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
⚠ This option is a significant security vulnerability because updates can be accepted from untrusted sources.

● Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

New Zone Wizard

Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

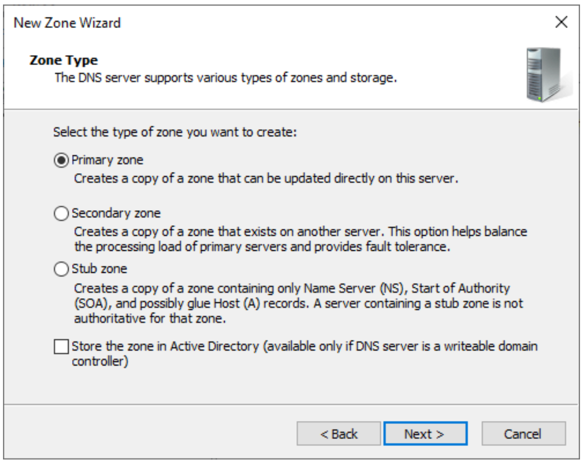
Name: nps.com
Type: Standard Primary
Lookup type: Forward
File name: nps.com.dns

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

Figure 2.6: Setting Up Standard Primary DNS

Reverse Lookup Zone



Zone Type
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

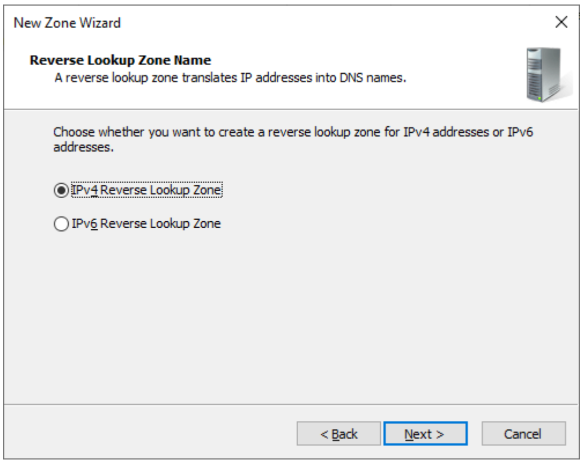
● Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

□ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

Figure 2.7: Setup New zone



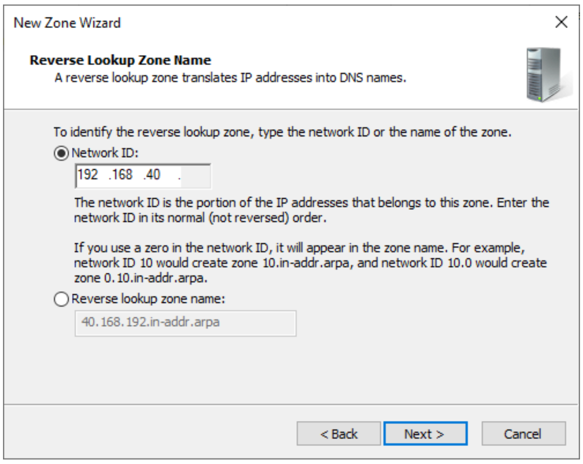
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

● IPv4 Reverse Lookup Zone

○ IPv6 Reverse Lookup Zone

Figure 2.8: Choose IPv4 Lookup Zone



Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

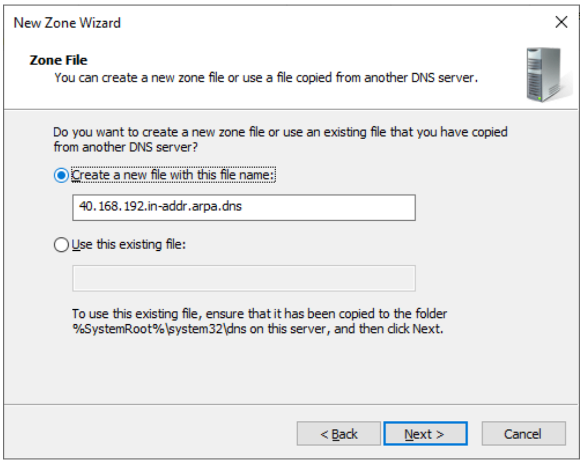
● Network ID:
192 .168 .40 .

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

○ Reverse lookup zone name:
40.168.192.in-addr.arpa

Figure 2.9: Set 3 Octet Network ID



Zone File
You can create a new zone file or use a file copied from another DNS server.

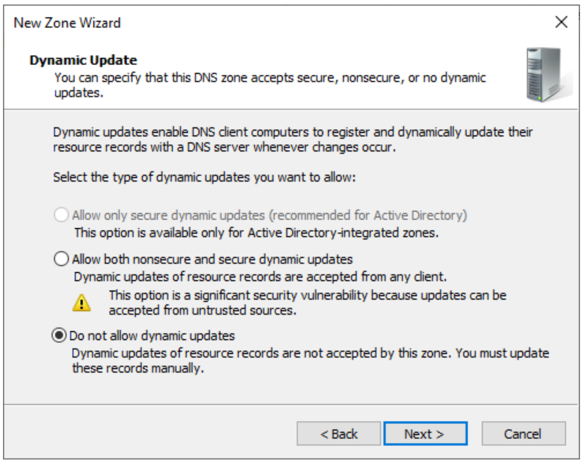
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

● Create a new file with this file name:
40.168.192.in-addr.arpa.dns

○ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

Figure 3.0: Set File Name



Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

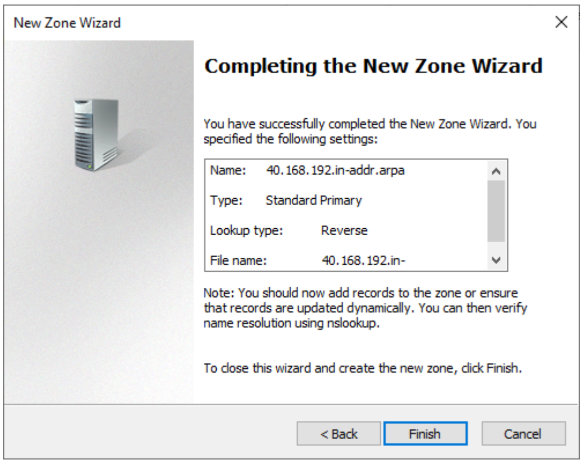
Select the type of dynamic updates you want to allow:

○ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

○ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
⚠ This option is a significant security vulnerability because updates can be accepted from untrusted sources.

● Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

Figure 3.1: Don't Allow Dynamic Update



Completing the New Zone Wizard

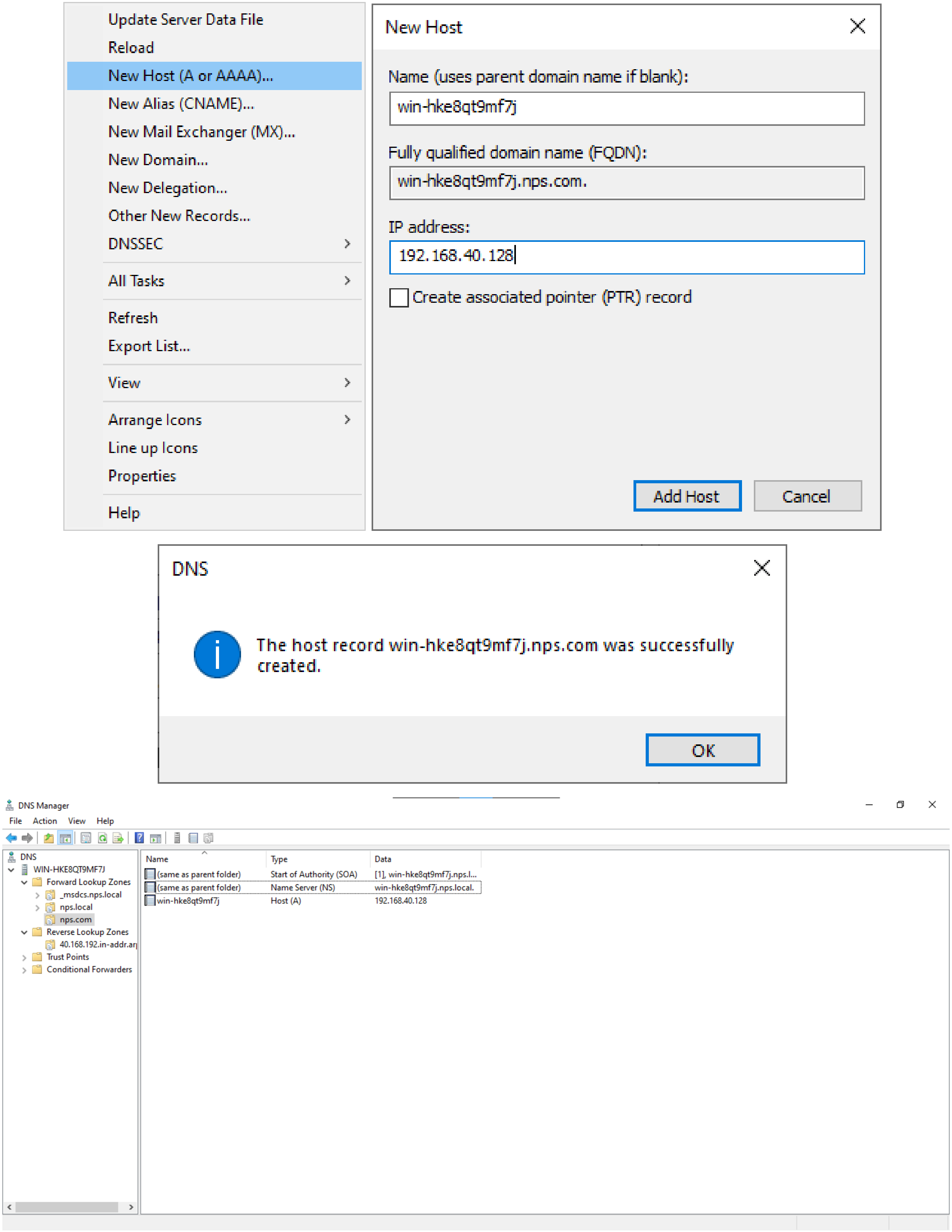
You have successfully completed the New Zone Wizard. You specified the following settings:

Name: 40.168.192.in-addr.arpa
Type: Standard Primary
Lookup type: Reverse
File name: 40.168.192.in-

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

Figure 3.2: Finish the setup



New Host

Name (uses parent domain name if blank):
win-hke8qt9mf7j

Fully qualified domain name (FQDN):
win-hke8qt9mf7j.nps.com.

IP address:
192.168.40.128

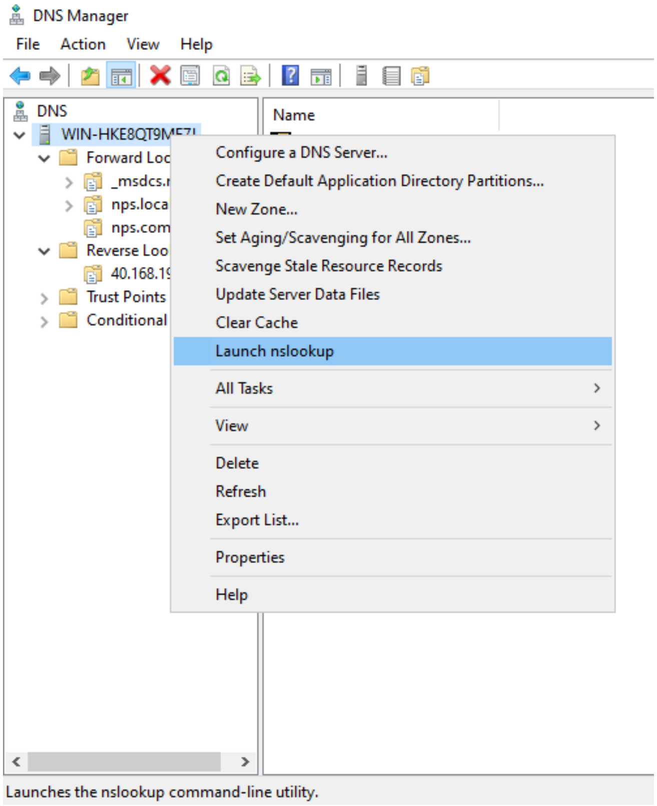
□ Create associated pointer (PTR) record

DNS

The host record win-hke8qt9mf7j.nps.com was successfully created.

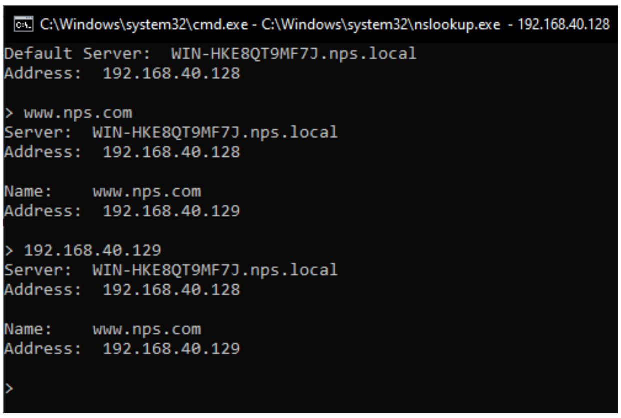
Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], win-hke8qt9mf7j.nps.l...
(same as parent folder)	Name Server (NS)	win-hke8qt9mf7j.nps.local.
win-hke8qt9mf7j	Host (A)	192.168.40.128

Figure 3.3: New Host for Forward Lookup Zone



Launches the nslookup command-line utility.

Figure 3.4: Start nslookup command

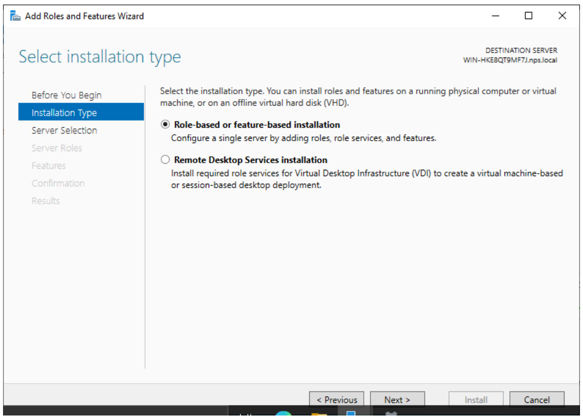

C:\Windows\system32\cmd.exe - C:\Windows\system32\nslookup.exe - 192.168.40.128

```
Default Server:  WIN-HKE8QT9MF7J.nps.local
Address:  192.168.40.128

> www.nps.com
Server:  WIN-HKE8QT9MF7J.nps.local
Address:  192.168.40.128

Name:    www.nps.com
Address:  192.168.40.129

> 192.168.40.129
Server:  WIN-HKE8QT9MF7J.nps.local
Address:  192.168.40.128

Name:    www.nps.com
Address:  192.168.40.129

>
```

Figure 3.5: Result on nslookup command

Network Policy Server

Installing Network Policy Server (NPS) Feature



Select installation type

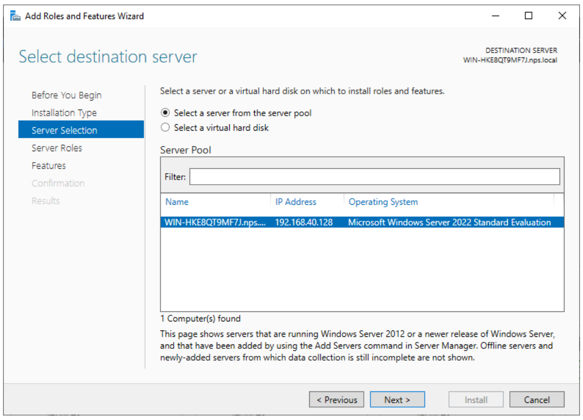
DESTINATION SERVER
WIN-HKE8QT9MF7J.nps.local

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Figure 3.6: Select Installation Type



Select destination server

DESTINATION SERVER
WIN-HKE8QT9MF7J.nps.local

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

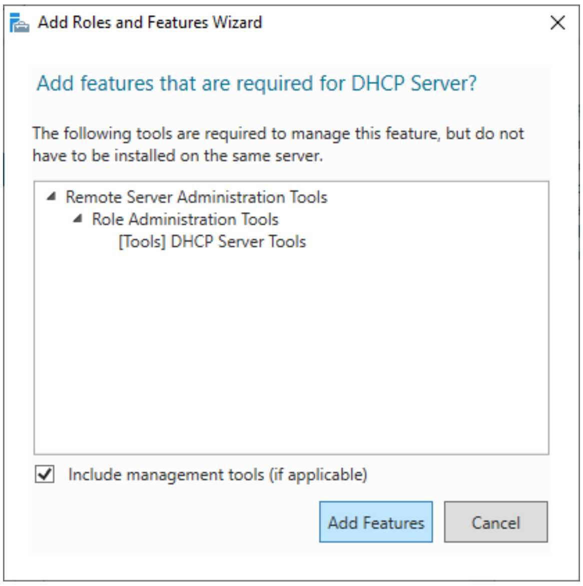
Filter:

Name	IP Address	Operating System
WIN-HKE8QT9MF7J.nps....	192.168.40.128	Microsoft Windows Server 2022 Standard Evaluation

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, 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.

Figure 3.7: Select Destination Server



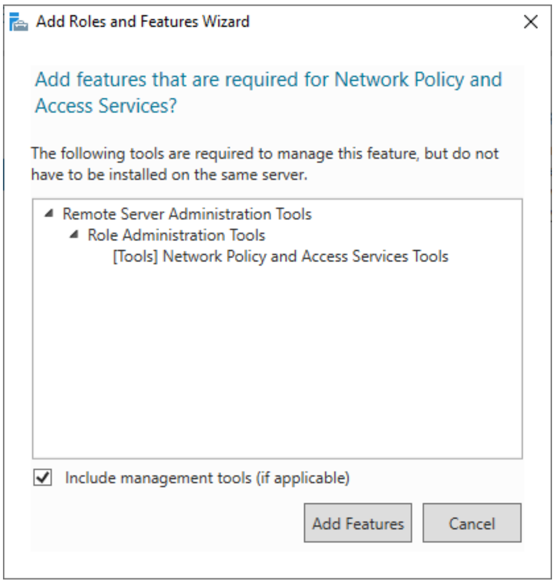
Add features that are required for DHCP Server?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] DHCP Server Tools

☑ Include management tools (if applicable)

Figure 3.8: Add Feature



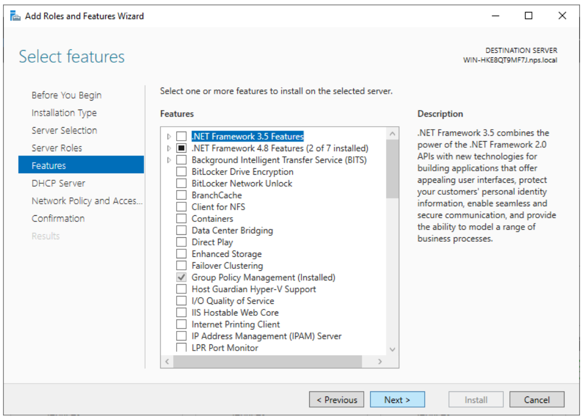
Add features that are required for Network Policy and Access Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] Network Policy and Access Services Tools

☑ Include management tools (if applicable)

Figure 3.9: Add Feature



Select features

DESTINATION SERVER
WIN-HKE8QT9MF7J.nps.local

Select one or more features to install on the selected server.

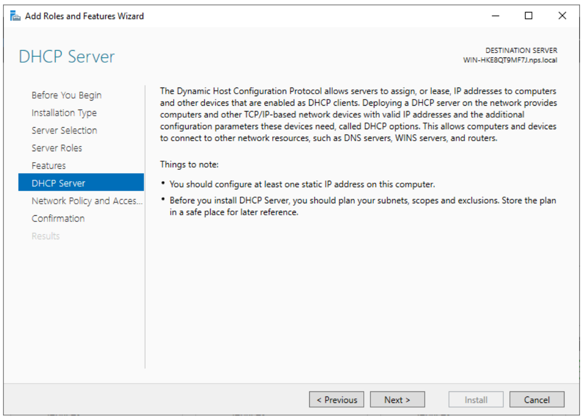
Features

- ☐ .NET Framework 3.5 Features
- ■ .NET Framework 4.8 Features (2 of 7 installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Containers
- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☑ Group Policy Management (Installed)
- ☐ Host Guardian Hyper-V Support
- ☐ I/O Quality of Service
- ☐ IIS Hostable Web Core
- ☐ Internet Printing Client
- ☐ IP Address Management (IPAM) Server
- ☐ LPR Port Monitor

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Figure 4.0: Additional Feature



DHCP Server

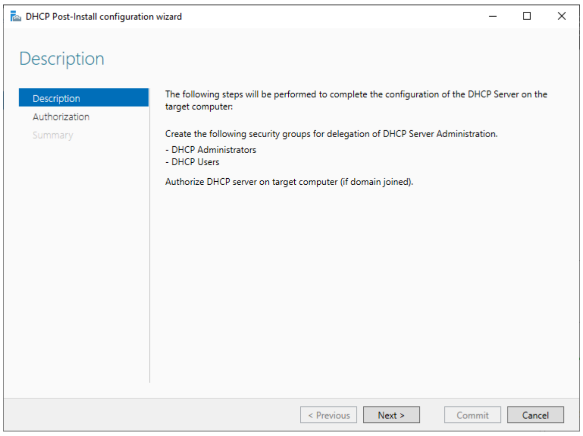
DESTINATION SERVER
WIN-HKE8QT9MF7J.nps.local

The Dynamic Host Configuration Protocol allows servers to assign, or lease, IP addresses to computers and other devices that are enabled as DHCP clients. Deploying a DHCP server on the network provides computers and other TCP/IP-based network devices with valid IP addresses and the additional configuration parameters these devices need, called DHCP options. This allows computers and devices to connect to other network resources, such as DNS servers, WINS servers, and routers.

Things to note:

- You should configure at least one static IP address on this computer.
- Before you install DHCP Server, you should plan your subnets, scopes and exclusions. Store the plan in a safe place for later reference.

Figure 4.1: Install

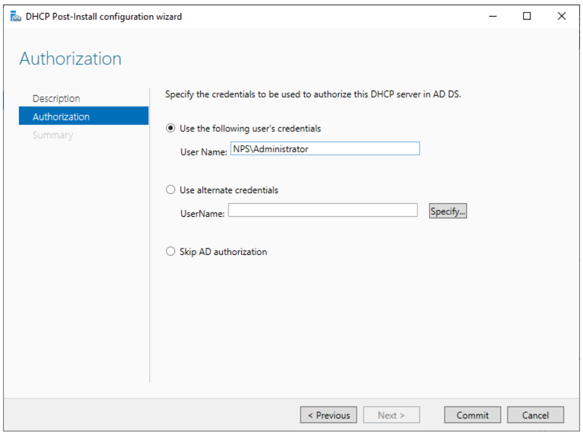


The following steps will be performed to complete the configuration of the DHCP Server on the target computer:

Create the following security groups for delegation of DHCP Server Administration.
- DHCP Administrators
- DHCP Users

Authorize DHCP server on target computer (if domain joined).

Figure 4.2: Setup DHCP Configuration



Specify the credentials to be used to authorize this DHCP server in AD DS.

● Use the following user's credentials

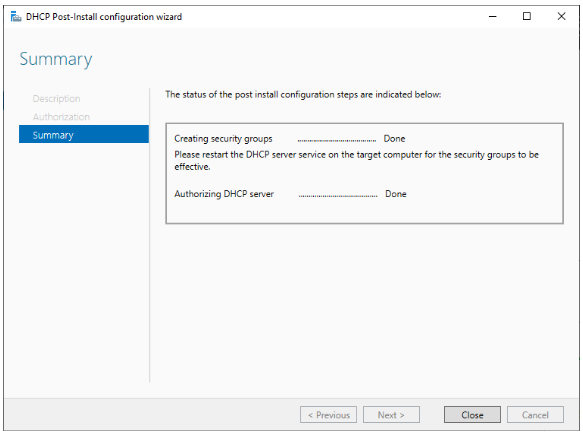
User Name: NPS\Administrator

○ Use alternate credentials

UserName:

○ Skip AD authorization

Figure 4.3: Setup Authorization Config



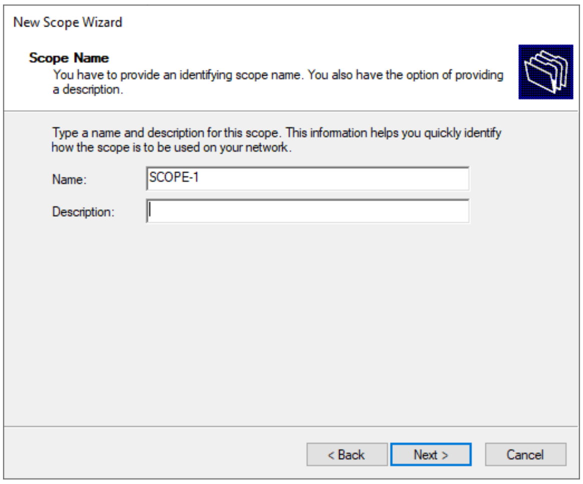
The status of the post install configuration steps are indicated below:

Creating security groups .... Done
Please restart the DHCP server service on the target computer for the security groups to be effective.

Authorizing DHCP server .... Done

Figure 4.4: DHCP Summary Config

Dynamic Host Configuration Protocol (DHCP)


New Scope Wizard

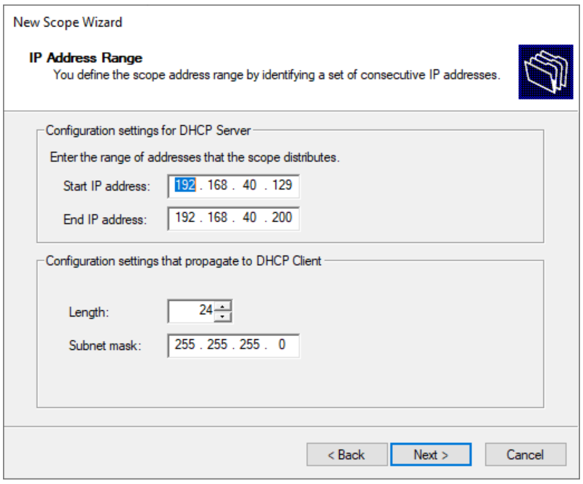
Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: SCOPE-1

Description:

Figure 4.5: New Scope


New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 40 . 129

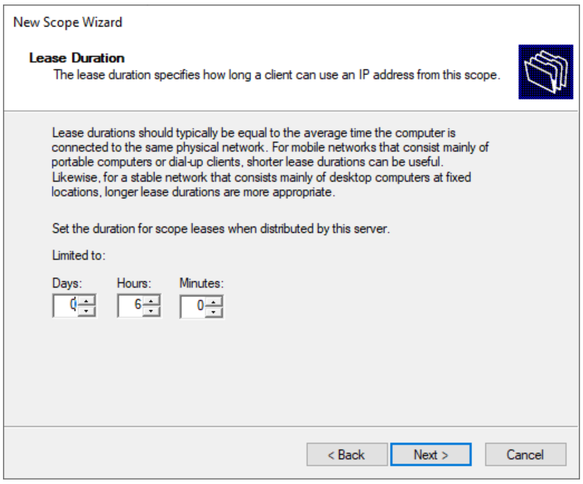
End IP address: 192 . 168 . 40 . 200

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

Figure 4.6: Set IP Range


New Scope Wizard

Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.

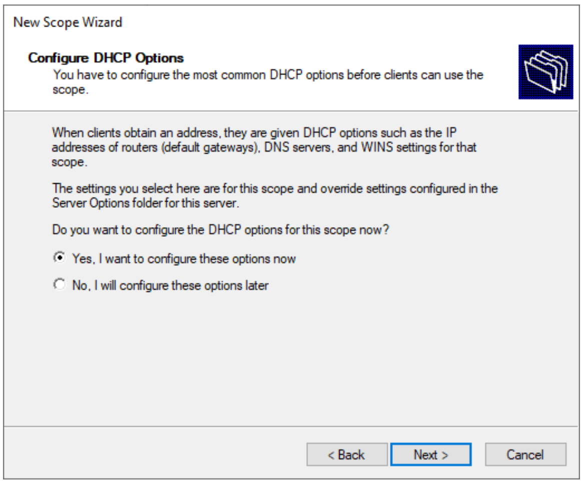
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: 0 Hours: 6 Minutes: 0

Figure 4.7: Set Lease Duration


New Scope Wizard

Configure DHCP Options
You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

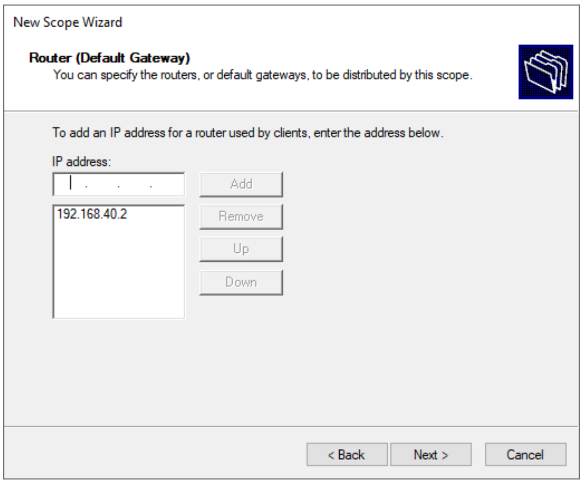
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

● Yes, I want to configure these options now

○ No, I will configure these options later

Figure 4.8: Apply DHCP Configuration


New Scope Wizard

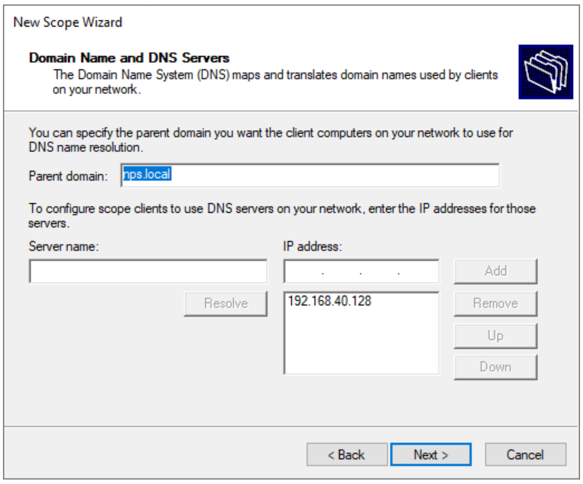
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

192.168.40.2

Figure 4.9: Add Default Gateway



New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain: nps.local

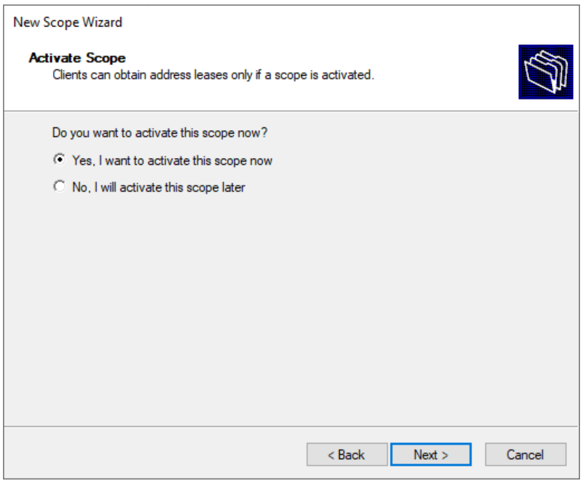
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

192.168.40.128

Figure 5.0: Set Parent Domain



New Scope Wizard

Activate Scope

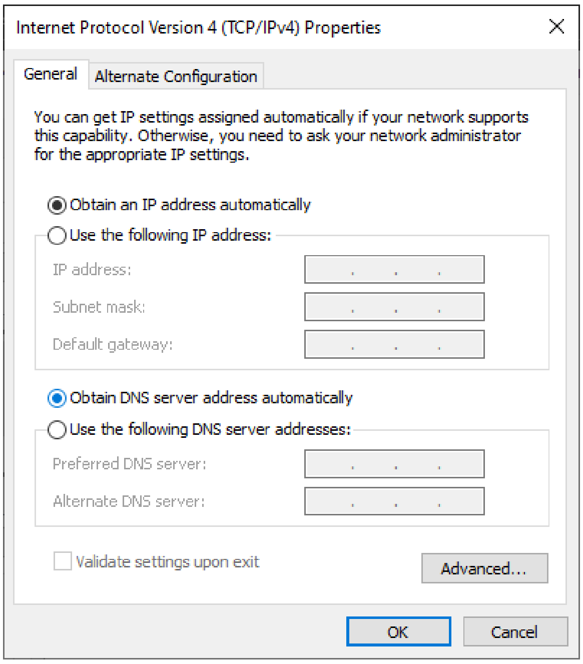
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

● Yes, I want to activate this scope now

○ No, I will activate this scope later

Figure 5.1: Activate Scope



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

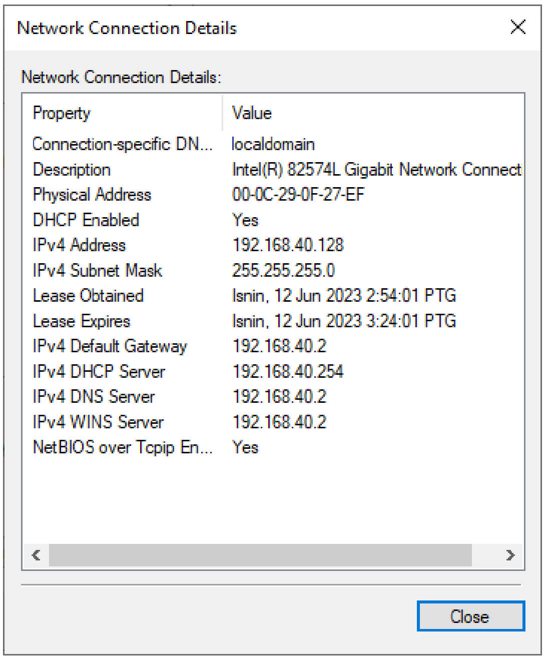
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

Figure 5.2: Set IPv4 & DNS Automatically



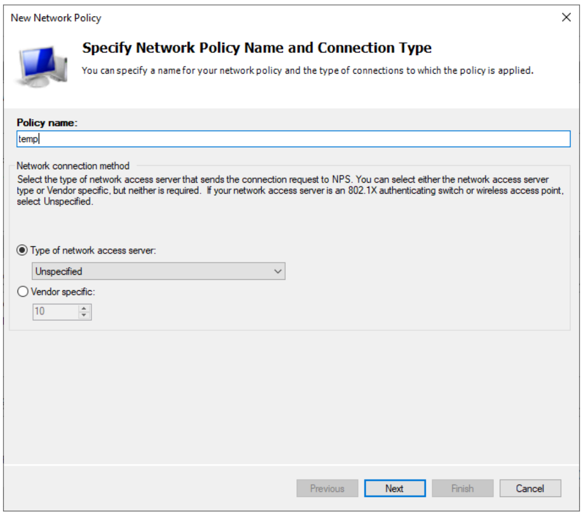
Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	localdomain
Description	Intel(R) 82574L Gigabit Network Connect
Physical Address	00-0C-29-0F-27-EF
DHCP Enabled	Yes
IPv4 Address	192.168.40.128
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Isnin, 12 Jun 2023 2:54:01 PTG
Lease Expires	Isnin, 12 Jun 2023 3:24:01 PTG
IPv4 Default Gateway	192.168.40.2
IPv4 DHCP Server	192.168.40.254
IPv4 DNS Server	192.168.40.2
IPv4 WINS Server	192.168.40.2
NetBIOS over Tcpip En...	Yes

Figure 5.3: DHCP Address Obtain

Network Policy Service (NPS)


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: temp

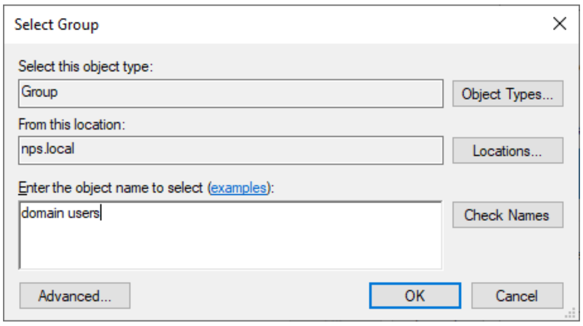
Network connection method

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

Figure 5.4: Specify Network Access Server

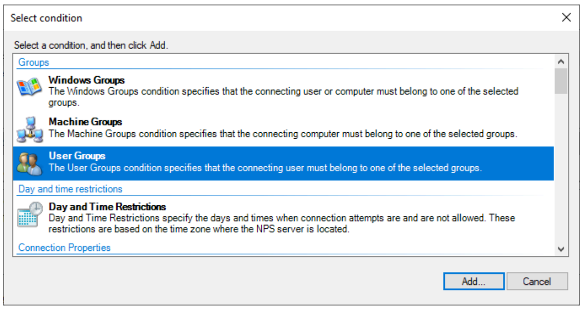

Select Group

Select this object type: Group

From this location: nps.local

Enter the object name to select (examples): domain users

Figure 5.5: Enter Object Name


Select condition

Select a condition, and then click Add.

Groups

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

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

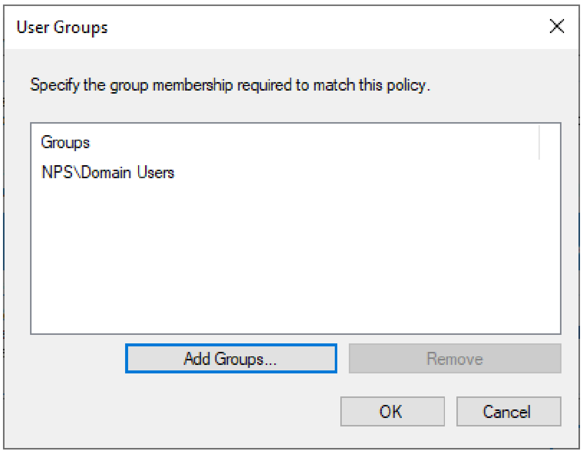
User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

Day and time restrictions

Day and Time Restrictions
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.

Connection Properties

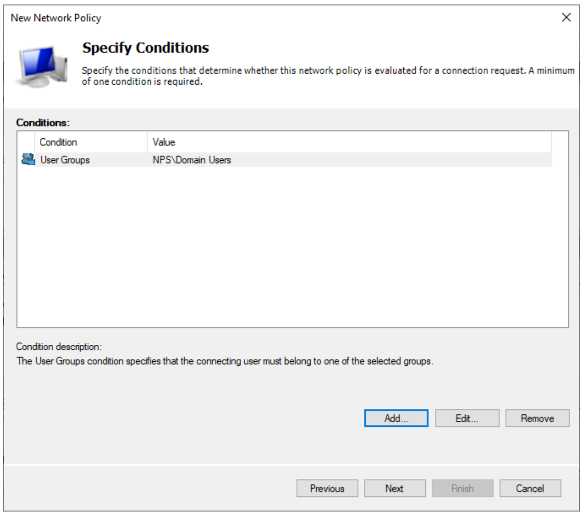
Figure 5.6: Select Condition


User Groups

Specify the group membership required to match this policy.

Groups
NPS\Domain Users

Figure 5.7: Add User Group into policy


New Network Policy

Specify Conditions

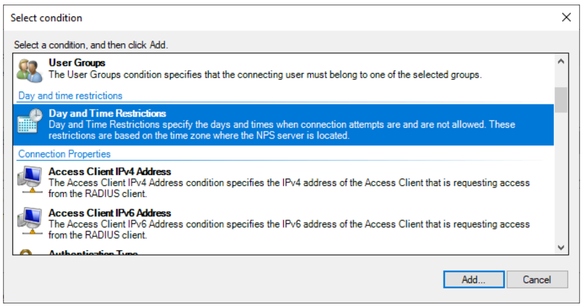
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
User Groups	NPS\Domain Users

Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

Figure 5.8: Add Condition for the NPS


Select condition

Select a condition, and then click Add.

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

Day and time restrictions

Day and Time Restrictions
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.

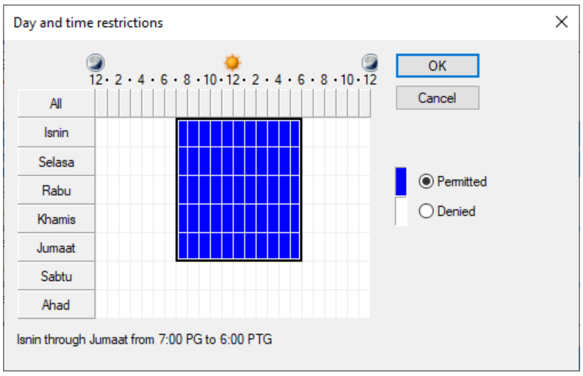
Connection Properties

Access Client IPv4 Address
The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access from the RADIUS client.

Access Client IPv6 Address
The Access Client IPv6 Address condition specifies the IPv6 address of the Access Client that is requesting access from the RADIUS client.

Authentication Type

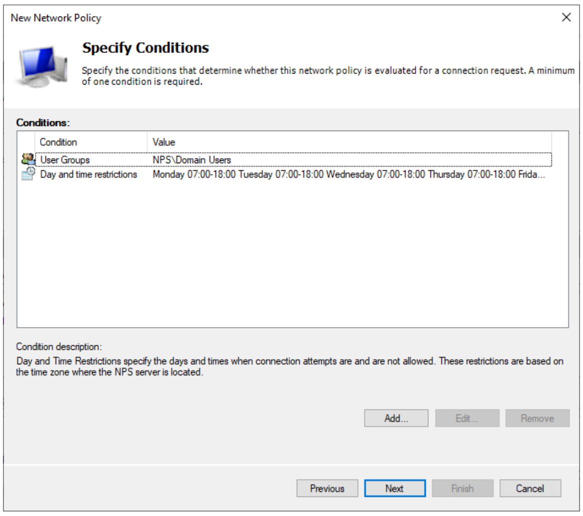
Figure 5.9: Select Condition


Day and time restrictions

● Permitted
○ Denied

Isnin through Jumaat from 7:00 PG to 6:00 PTG

Figure 6.0: Choose Day & Time Restriction


New Network Policy

Specify Conditions

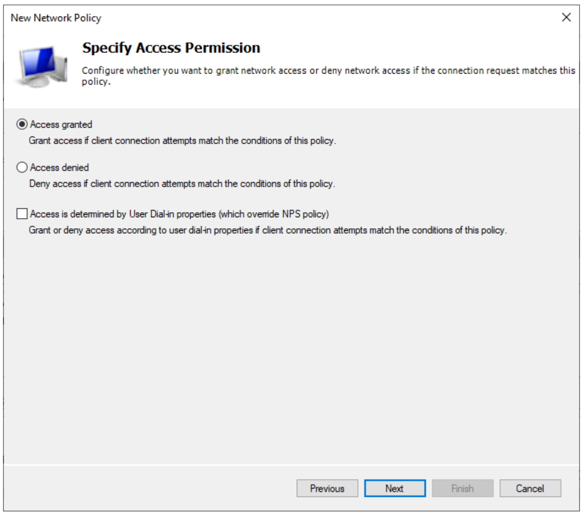
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
User Groups	NPS\Domain Users
Day and time restrictions	Monday 07:00-18:00 Tuesday 07:00-18:00 Wednesday 07:00-18:00 Thursday 07:00-18:00 Frida...

Condition description:
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.

Figure 6.1: Next


New Network Policy

Specify Access Permission

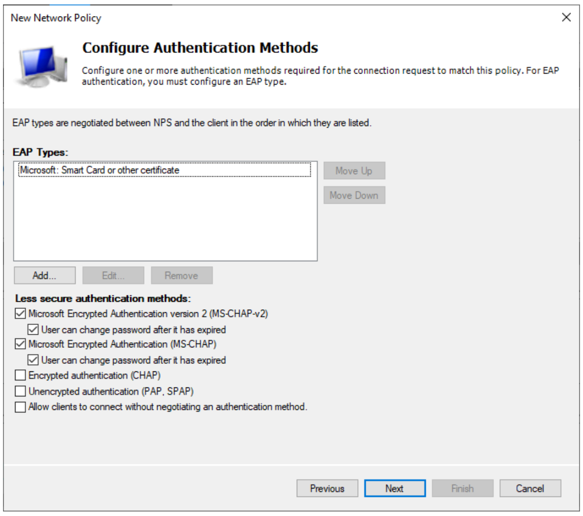
Configure whether you want to grant network access or deny network access if the connection request matches this policy.

● 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.

Figure 6.2: Specify Access Permission


New Network Policy

Configure Authentication Methods

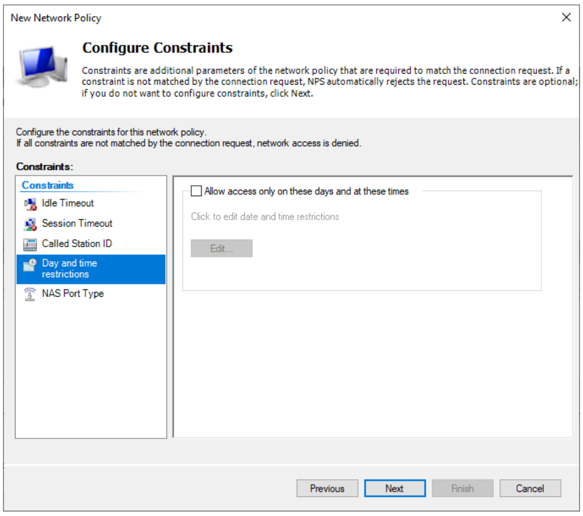
Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

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

EAP Types:
Microsoft: Smart Card or other certificate

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)
□ Unencrypted authentication (PAP, SPAP)
□ Allow clients to connect without negotiating an authentication method.

Figure 6.3: Configure Authentication Methods


New Network Policy

Configure Constraints

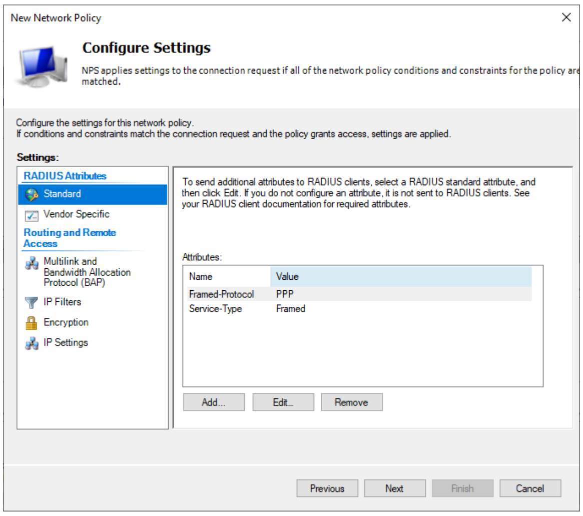
Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

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

Constraints:

□ Allow access only on these days and at these times
Click to edit date and time restrictions

Figure 6.4: Configure Constraints


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:

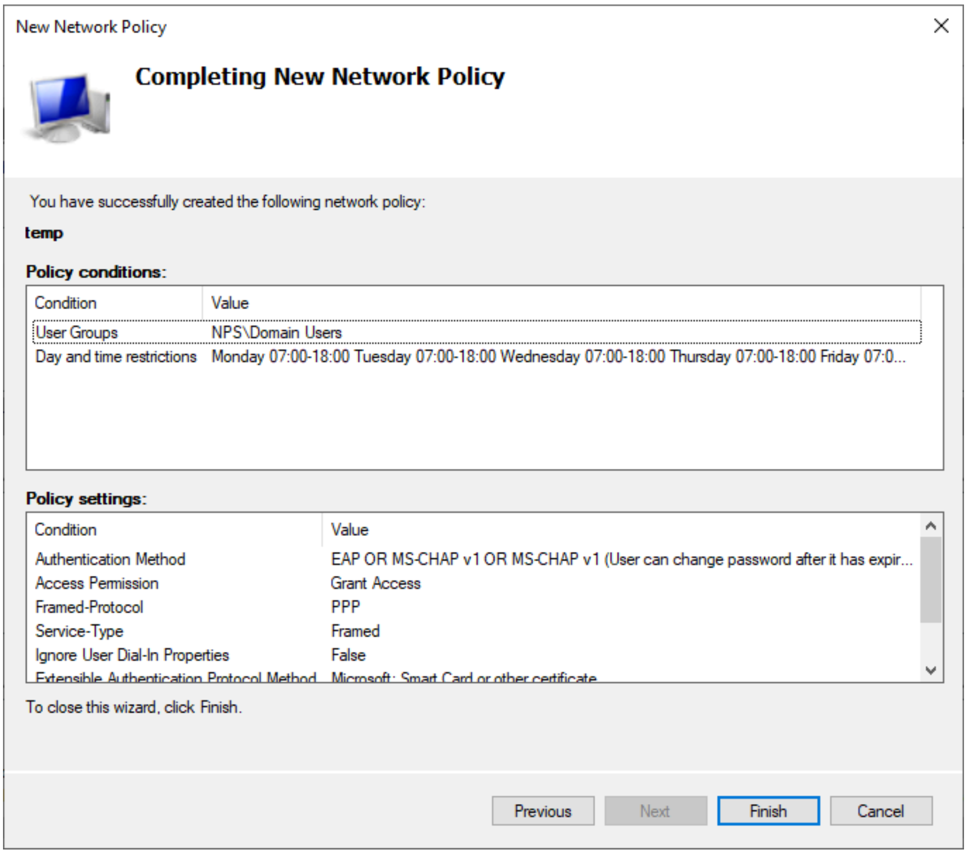
RADIUS Attributes
Standard
Vendor Specific
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings

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

Figure 6.5: Configure Settings



Completing New Network Policy

You have successfully created the following network policy:

temp

Policy conditions:

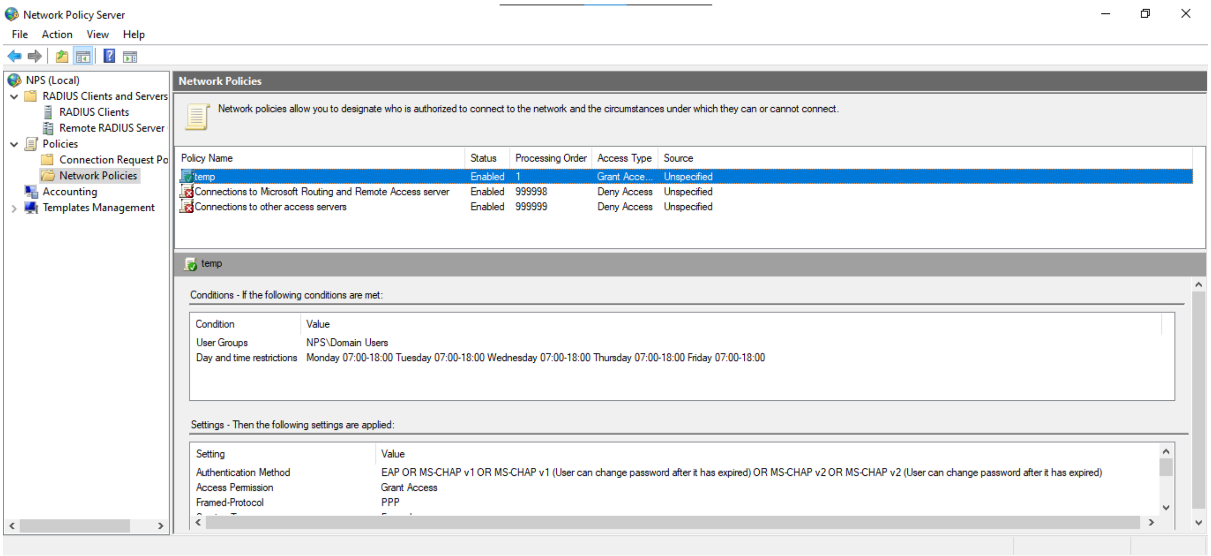
Condition	Value
User Groups	NPS\Domain Users
Day and time restrictions	Monday 07:00-18:00 Tuesday 07:00-18:00 Wednesday 07:00-18:00 Thursday 07:00-18:00 Friday 07:0...

Policy settings:

Condition	Value
Authentication Method	EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expir...
Access Permission	Grant Access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False
Extensible Authentication Protocol Method	Microsoft: Smart Card or other certificate

To close this wizard, click Finish.

Figure 6.6: Completing Network Policy Setup



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
temp	Enabled	1	Grant Acce...	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	Enabled	999999	Deny Access	Unspecified

Conditions - If the following conditions are met:

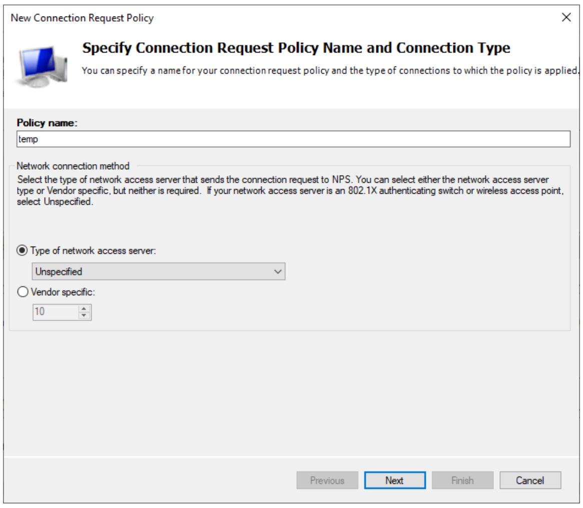
Condition	Value
User Groups	NPS\Domain Users
Day and time restrictions	Monday 07:00-18:00 Tuesday 07:00-18:00 Wednesday 07:00-18:00 Thursday 07:00-18:00 Friday 07:00-18:00

Settings - Then the following settings are applied:

Setting	Value
Authentication Method	EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 OR MS-CHAP v2 (User can change password after it has expired)
Access Permission	Grant Access
Framed-Protocol	PPP

Figure 6.7: New Policy Implemented for Network Policies

NPS: Connection Request Policy



Specify Connection Request Policy Name and Connection Type

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

Policy name: temp

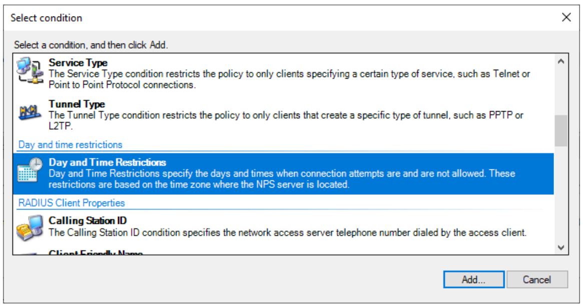
Network connection method

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

Figure 6.8: Specify Connection Request



Select a condition, and then click Add.

Service Type
The Service Type condition restricts the policy to only clients specifying a certain type of service, such as Telnet or Point to Point Protocol connections.

Tunnel Type
The Tunnel Type condition restricts the policy to only clients that create a specific type of tunnel, such as PPTP or L2TP.

Day and time restrictions

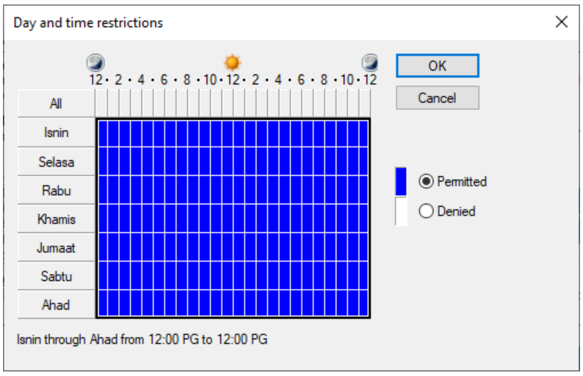
Day and Time Restrictions
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.

RADIUS Client Properties

Calling Station ID
The Calling Station ID condition specifies the network access server telephone number dialed by the access client.

Client Friendly Name

Figure 6.9: Set Condition

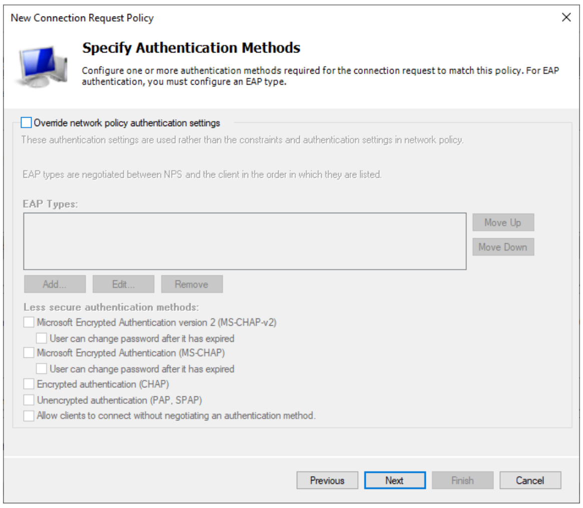


● Permitted

○ Denied

Isnin through Ahad from 12:00 PG to 12:00 PG

Figure 7.0: Set Day & Time Restriction



Specify 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.

□ Override network policy authentication settings

These authentication settings are used rather than the constraints and authentication settings in network policy.

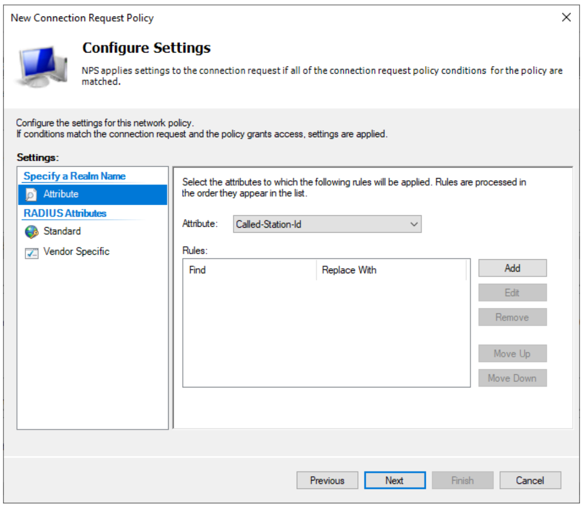
EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

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)
- □ Unencrypted authentication (PAP, SPAP)
- □ Allow clients to connect without negotiating an authentication method.

Figure 7.1: Specify Auth Methods



Configure Settings

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

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

Settings:

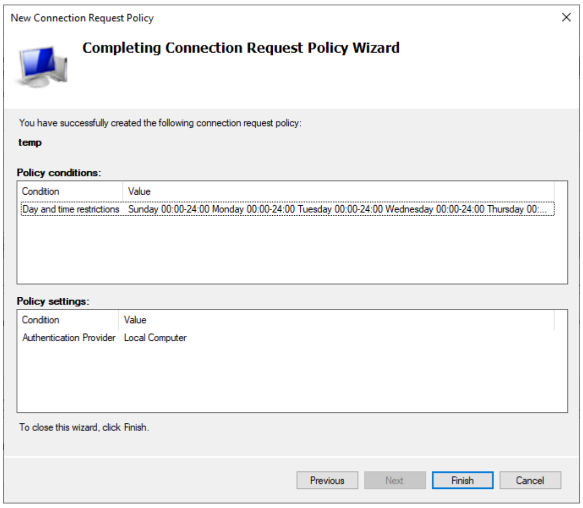
Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list.

Attribute: Called-Station-Id

Rules:

Find	Replace With

Figure 7.1: Configure Settings



Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

temp

Policy conditions:

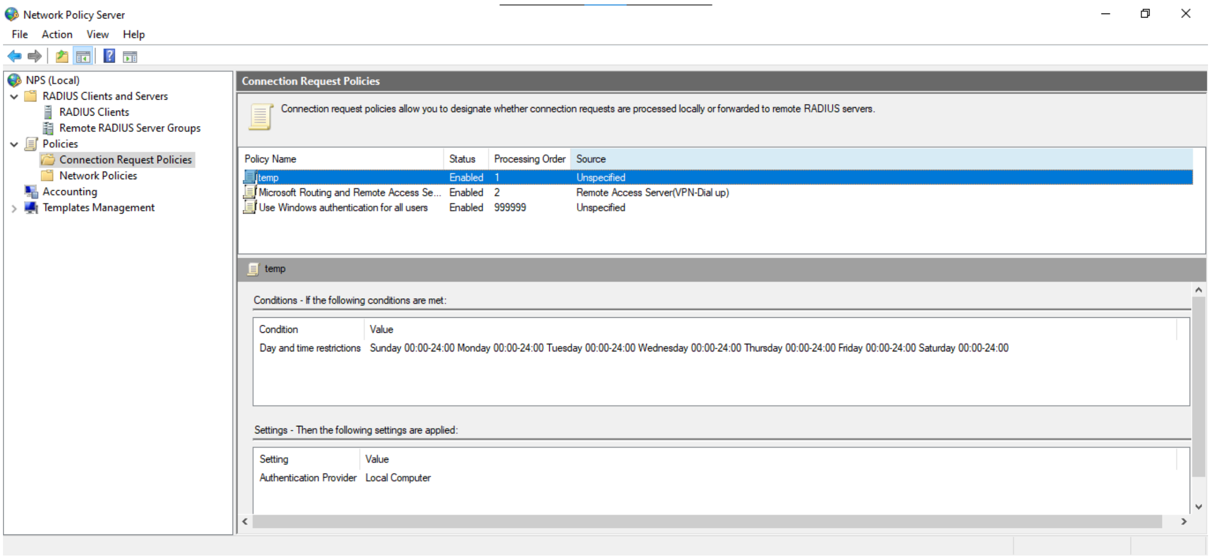
Condition	Value
Day and time restrictions	Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00 Thursday 00:...

Policy settings:

Condition	Value
Authentication Provider	Local Computer

To close this wizard, click Finish.

Figure 7.2: Complete the setup



Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

Policy Name	Status	Processing Order	Source
temp	Enabled	1	Unspecified
Microsoft Routing and Remote Access Se...	Enabled	2	Remote Access Server(VPN-Dial up)
Use Windows authentication for all users	Enabled	999999	Unspecified

Conditions - If the following conditions are met:

Condition	Value
Day and time restrictions	Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00 Thursday 00:00-24:00 Friday 00:00-24:00 Saturday 00:00-24:00

Settings - Then the following settings are applied:

Setting	Value
Authentication Provider	Local Computer

Figure 7.2: New Policy Implemented for Connection Request Policies

3.2 EXPLANATION

Network Policy Server & Active Directory

When the Network Policy Server (NPS) interacts with Active Directory (AD), it relies on the following key components and processes:

a. User and Computer Accounts: Active Directory holds information about users and computers, such as usernames, passwords, group memberships, and other features. This information is used by NPS to authenticate and authorize people and computers seeking to access network resources.

b. Authentication: NPS asks Active Directory for authentication data whenever a user or computer tries to join the network. Active Directory checks the supplied credentials against the user and computer accounts that are already saved. The authentication is successful if the credentials are accurate.

c. Authorization: Following a successful authentication, NPS queries Active Directory for authorization data. Checking the user's group memberships and related network access regulations is part of this process. Active Directory decides what degree of access the user or computer should have based on the defined policies. It might define, for instance, whether a user is permitted to connect to a certain network segment or access a particular set of resources.

d. Group Policies: Administrators may create and administer centralized security rules for users and machines inside a domain using Active Directory's Group Policy functionality. In order to enforce certain network access rules and configurations, NPS might make use of Group Policy settings. For instance, it can implement certain network settings, impose particular security protocols, or limit access to particular network resources.

Network Policy Server & Domain Name System

The Network Policy Server (NPS) and Domain Name System (DNS) are two discrete parts of a network architecture that have various functions. They can cooperate, nevertheless, to improve network performance. The description of their functions and probable interactions is as follows:

a. Network Policy Server (NPS): For network access, the Windows Server operating system's NPS component offers authentication, authorization, and accounting (AAA) services. By defining and enforcing network access policies, administrators may control who can connect to the network, what degree of access they have, and what requirements they must follow in order to access it.

b. Domain Name System (DNS): Domain name system (DNS) is a service and protocol that converts domain names (like www.example.com) into IP addresses (like 192.168.0.1). It serves as a directory service for both local and global networks, enabling users to find and access network resources by utilizing names that can be understood by humans rather than numeric IP addresses.

Although NPS and DNS have different functions, they can intersect in the following ways:

c. DNS-Based Network Access Control (DNS-NAC): NPS can make use of DNS-NAC, a function that enables network access controls to be implemented in accordance with DNS data. NPS, for instance, has the ability to control resource access based on DNS domain names. When network access must be permitted or restricted based on certain DNS-related criteria, this might be helpful.

d. DNS Dynamic Update: NPS servers can dynamically update DNS records when a client successfully authenticates or fails authentication. This integration helps keep DNS records up-to-date, allowing DNS-based services to make access decisions based on the updated authentication status.

DNS Resolution for NPS Configuration: NPS servers may rely on DNS for name resolution when configuring certain aspects. For instance, when configuring RADIUS (Remote Authentication Dial-In User Service) clients or RADIUS servers in NPS, the server names or IP addresses are often specified using domain names that are resolved by DNS.

Network Policy Server & Dynamic Host Configuration Protocol (DHCP)

The Network Policy Server (NPS) and Dynamic Host Configuration Protocol (DHCP) are two different components that serve distinct purposes in a network infrastructure. However, they can work together to enhance network management and security. Here's an explanation of their roles and potential interactions:

a. NPS: NPS is a component of the Windows Server operating system that provides authentication, authorization, and accounting (AAA) services for network access. It allows administrators to define and enforce network access policies, determine who can connect to the network, and specify conditions that must be met for access.

b. DHCP: DHCP is a network protocol that dynamically assigns IP addresses and other network configuration settings to devices on a network. It automates the process of IP address allocation, allowing devices to join the network without manual IP configuration.

NPS and DHCP can interact in the following ways:

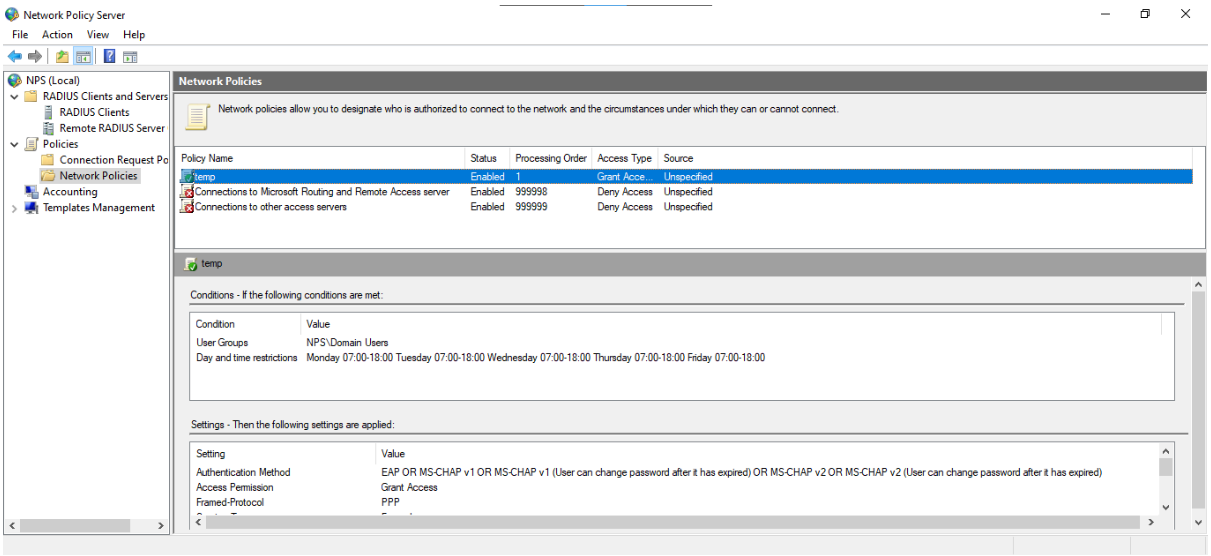
DHCP Relay Agent: NPS can act as a DHCP Relay Agent, forwarding DHCP messages between DHCP clients and DHCP servers. This is particularly useful when NPS is located in a different subnet from the DHCP server. The NPS server receives DHCP requests from clients, relays them to the DHCP server, and then forwards the DHCP responses back to the clients. This enables centralized management of DHCP services and simplifies network configuration.

a. MAC Address-Based Authentication: NPS can authenticate network access based on the MAC (Media Access Control) addresses of devices. In this scenario, NPS can utilize the DHCP snooping feature, which inspects DHCP messages to gather MAC address information. NPS can then use this information to authorize or deny access to the network based on predefined policies.

b. DHCP Option-Based Authorization: NPS can use DHCP options to authorize or restrict access to the network. DHCP options are additional parameters sent by the DHCP server to clients during the IP address assignment process. NPS can examine these options to determine whether a client is authorized to access the network or not.

c. Integration with Active Directory: Both NPS and DHCP can integrate with Active Directory (AD). NPS can use AD for user authentication and authorization, while DHCP can utilize AD to dynamically update DNS records for DHCP-assigned IP addresses.

3.1 RESULT



Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
temp	Enabled	1	Grant Acce...	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	Enabled	999999	Deny Access	Unspecified

temp

Conditions - If the following conditions are met:

Condition	Value
User Groups	NPS\Domain Users
Day and time restrictions	Monday 07:00-18:00 Tuesday 07:00-18:00 Wednesday 07:00-18:00 Thursday 07:00-18:00 Friday 07:00-18:00

Settings - Then the following settings are applied:

Setting	Value
Authentication Method	EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 OR MS-CHAP v2 (User can change password after it has expired)
Access Permission	Grant Access
Framed-Protocol	PPP

Network Policy Server (NPS), there are two types of policies that work together to control network access: Connection Request Policies and Network Policies.

1. <u>Connection Request Policies</u>
   Connection Request Policies specify the conditions under which NPS will process and handle incoming connection requests. These policies help determine whether NPS should process a connection request or ignore it.
2. <u>Network Policies</u>
   Network Policies define the rules that determine whether to grant or deny network access to clients based on specific conditions and settings. They are evaluated after the Connection Request Policy and provide more granular control over network access.

Achieving the Desired Control:
By configuring both Connection Request Policies and Network Policies, you can achieve comprehensive network access control. Connection Request Policies filter and determine which requests should be processed, while Network Policies define the specific access rules and settings for granted connections.

You may control connection requests based on fundamental criteria using Connection Request Policies as an initial filter. Then, Network Policies offer finer-grained control by enabling you to specify certain requirements, limitations, and settings for network access. You can enforce access control based on user or computer groups, authentication techniques, session limitations, encryption specifications, and other factors by carefully configuring these policies, ensuring that network resources are only accessible to authorized entities and in accordance with the desired criteria.

4.0 CONCLUSION

The Network Policy Server (NPS) is a powerful network access control server developed by Microsoft. It provides centralized management of network authentication, authorization, and accounting (AAA) policies, enhancing network security and efficiency. NPS offers granular access control based on predefined policies, taking into account user identification, group membership, time of day, and network location.

The importance of NPS lies in its ability to regulate access to network resources, authenticate users and devices, and provide logging and auditing capabilities for monitoring network access activities. It integrates seamlessly with Microsoft Active Directory, allowing for the use of existing user and group accounts for authentication and simplifying user administration.

NPS works by authorizing or denying access based on user credentials and network security policies. It communicates with users and devices using the RADIUS protocol and verifies user credentials before determining the level of authorization based on configured policies. NPS can enforce various network policies, such as restricting access to specific services or applications.

While NPS offers several advantages, such as centralized policy administration, support for multiple authentication methods, and granular access control, it also has limitations. It is primarily designed for Windows Server environments, limiting its compatibility with other operating systems. Setting up and configuring NPS can be complex and requires expertise in network security and policy management.

The report includes step-by-step configurations and coding examples for setting up NPS, Active Directory, DNS, and DHCP. These examples provide visual aids to help understand the process and ensure proper implementation.

In conclusion, the Network Policy Server (NPS) is a valuable tool for managing network access and enhancing security. It offers centralized control, authentication, authorization, and accounting capabilities, making it an essential component in network infrastructure. However, organizations should consider its compatibility limitations and complexity when implementing NPS.

REFERENCES

[1] Bonatti, P., & Olmedilla, D. (2005, June). Driving and monitoring provisional trust negotiation with metapolicies. In *Sixth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'05)* (pp. 14-23). IEEE.

[2] Hu, Z., Wang, M., Yan, X., Yin, Y., & Luo, Z. (2015, February). A comprehensive security architecture for SDN. In 2015 18th International Conference on Intelligence in Next Generation Networks (pp. 30-37). IEEE.

[3] Ponnappan, A., Yang, L., Pillai, R., & Braun, P. (2002, June). A policy based QoS management system for the IntServ/DiffServ based Internet. In Proceedings Third International Workshop on Policies for Distributed Systems and Networks (pp. 159-168). IEEE.

[4] Raymer, D., Strassner, J., Lehtihet, E., & Van der Meer, S. (2006, June). End-to-end model driven policy based network management. In *Seventh IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'06)* (pp. 4-pp). IEEE.

[5] Stone, G. N., Lundy, B., & Xie, G. G. (2001). Network policy languages: a survey and a new approach. IEEE network, 15(1), 10-21.