Configure a Network Policy Server Infrastructure

Outline

- Plan Network Policy Server
- Configure Network Policy Server
- Manage Network Policy Server

What are network policies?

- Network policies are sets of conditions, constraints, and settings that allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
- Network policy is a collection of rules that govern the behaviors of network devices.

ttps://docs.microsoft.com/ms-my/windows-server/networking/technologies/nps/nps-np-overview

Network Policies in Windows

- Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication and authorization.
- Network Policies - An Ordered Set of Rules

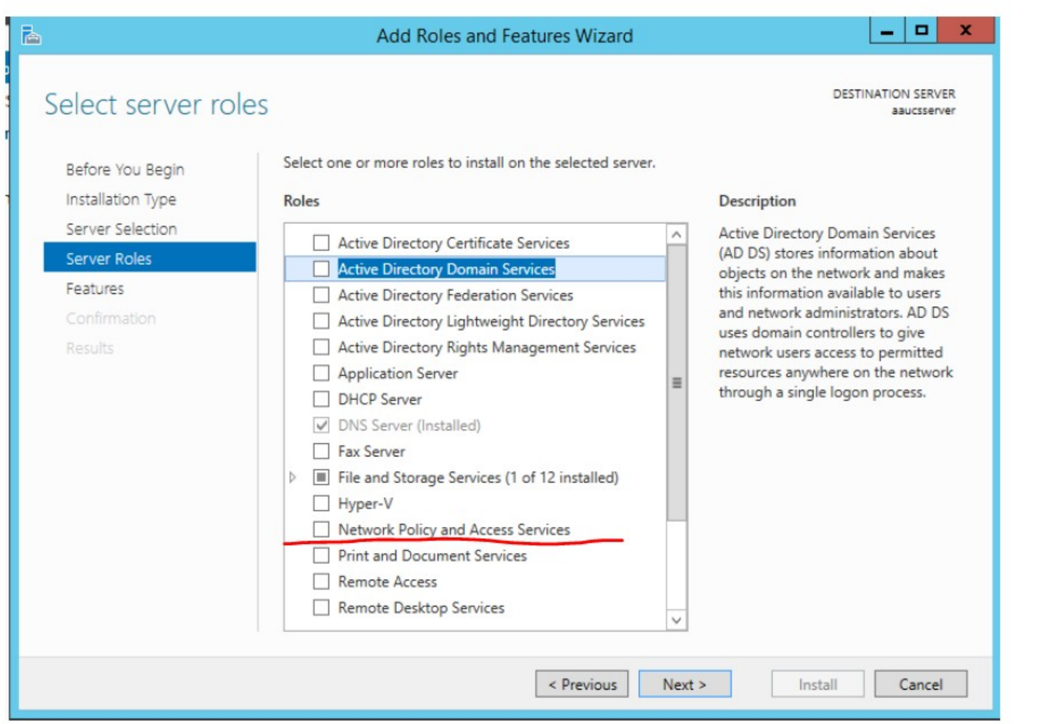
  Each rule has a set of conditions and settings.
- NPS compares the conditions of the rule to the properties of connection requests.
- If a match occurs between the rule and the connection request, the settings defined in the rule are applied to the connection.

Network Policies in Windows

- The primary purpose of a network security policy is to inform users and staff the requirements for protecting various assets.
- These assets take many forms, including passwords, documents, or even servers.
- These policies also lay guidelines for acquiring, configuring, and auditing computer systems and networks.

overview of Network Policy Server (NPS)

- in Windows Server 2016 and Windows Server 2019.
- NPS is installed when you install the Network Policy and Access Services (NPAS) feature in Windows Server 2016 and Server 2019.
- In Server Manager, select Tools, and then select Network Policy Server. The NPS console opens. In the NPS console, right-click NPS (Local), then select Register server ii The Network Policy Server dialog box opens



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
aaucsserver

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

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

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

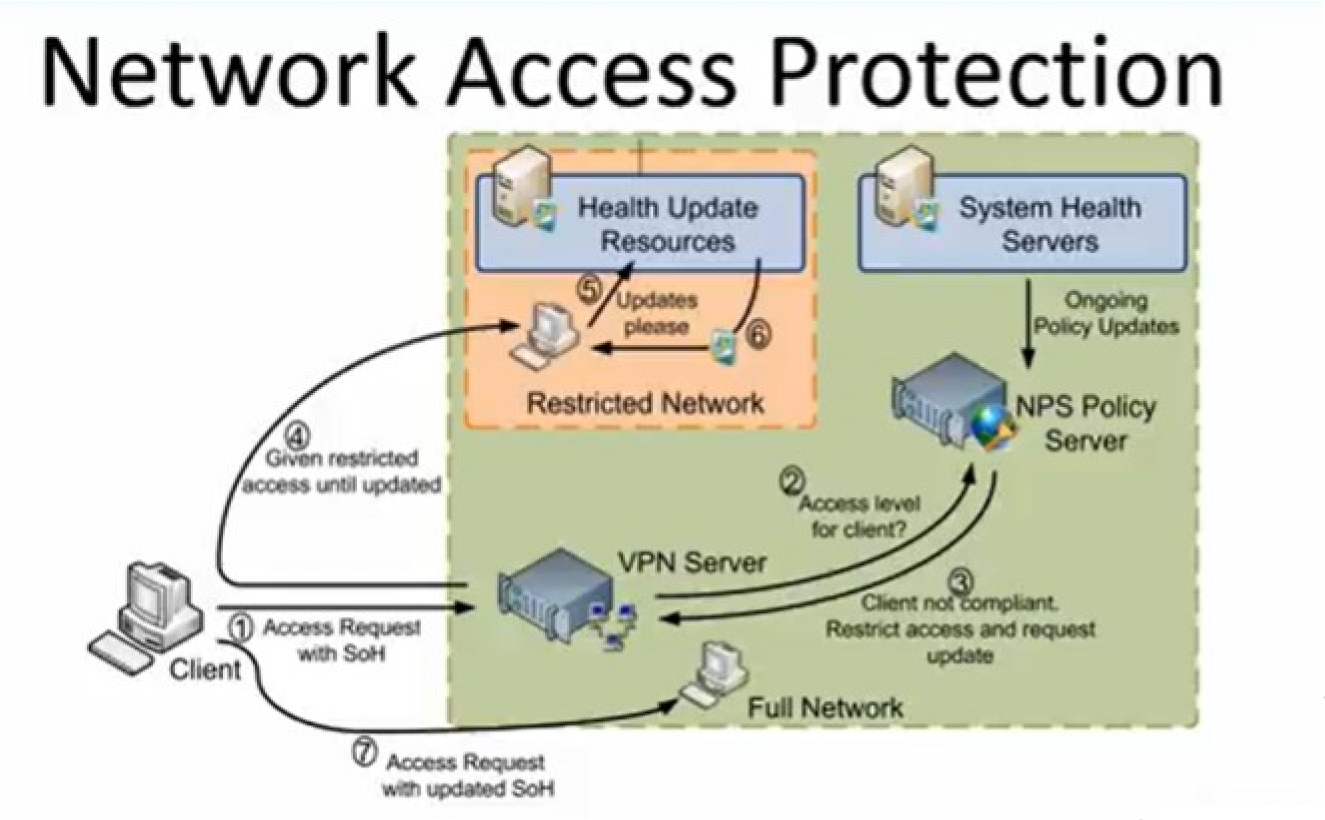
Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

< Previous | Next > | Install | Cancel

https://www.youtube.com/watch?v=GSAClWmg8y0

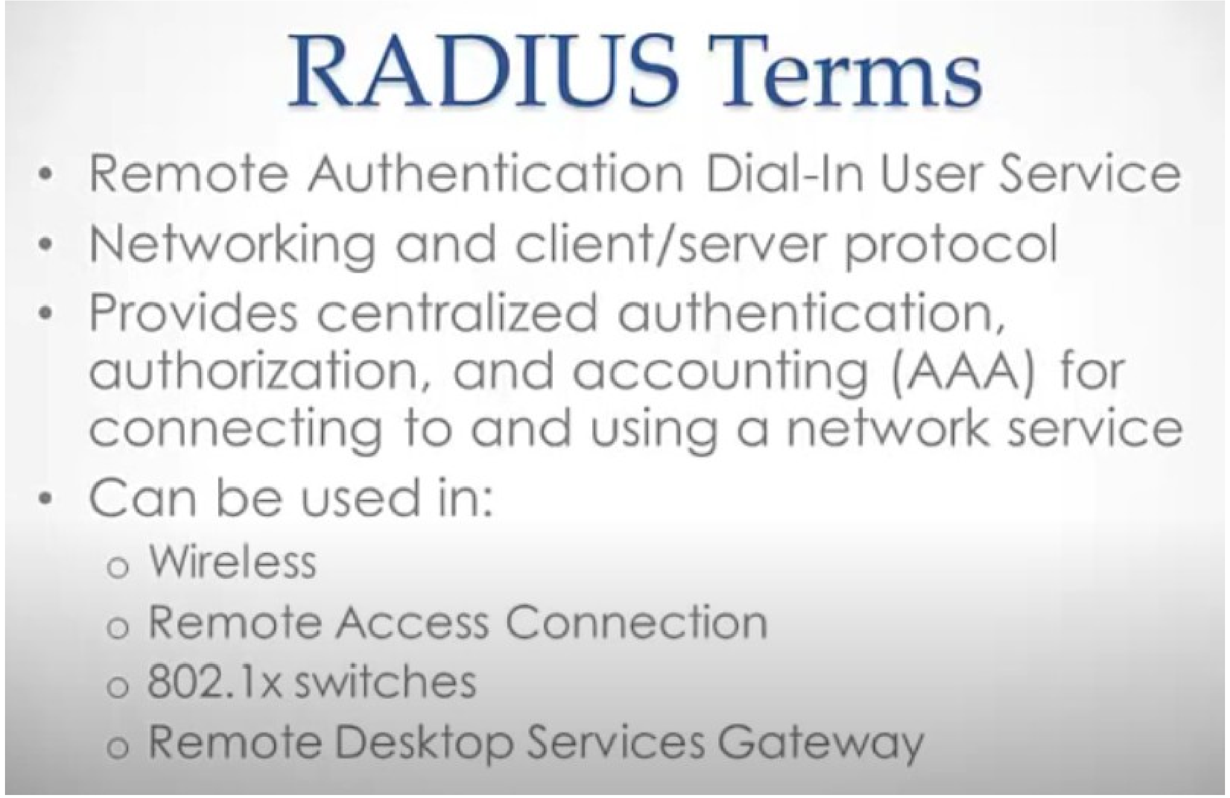
- Network Policy and Access Services (NPAS) is used to provide secure remote access.
- This access is provided via a few different methods.
- NPAS is used to deploy RADIUS, Network Access Protection (NAP), and secure access points.


Network Access Protection
Health Update Resources
System Health Servers
⑤ Updates please
⑥
Restricted Network
Ongoing Policy Updates
NPS Policy Server
④ Given restricted access until updated
② Access level for client?
VPN Server
③ Client not compliant. Restrict access and request update
① Access Request with SoH
Client
Full Network
⑦ Access Request with updated SoH

Network Policy Server (NPS)

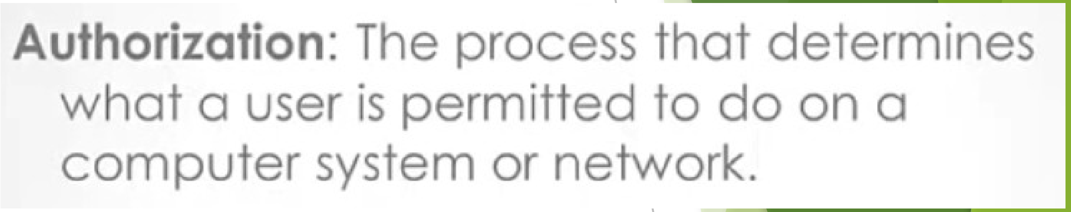
Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2019

- Network Policy Server (NPS) - to create and enforce organization-wide network access policies for connection request authentication and authorization.
- Configure NPS as a Remote Authentication Dial-In User Service (RADIUS) proxy to forward connection requests to a remote NPS or other RADIUS server so that it can load balance connection requests and forward them to the correct domain for authentication and authorization.



RADIUS Terms

- Remote Authentication Dial-In User Service
- Networking and client/server protocol
- Provides centralized authentication, authorization, and accounting (AAA) for connecting to and using a network service
- Can be used in:
  - Wireless
  - Remote Access Connection
  - 802.1x switches
  - Remote Desktop Services Gateway



Authorization: The process that determines what a user is permitted to do on a computer system or network.

https://www.youtube.com/watch?v=ZdQqIKoesas

Plan Network Policy Server

- Plan NPS as a RADIUS server
- Plan NPS as a RADIUS proxy

Network Policy Server (NPS)

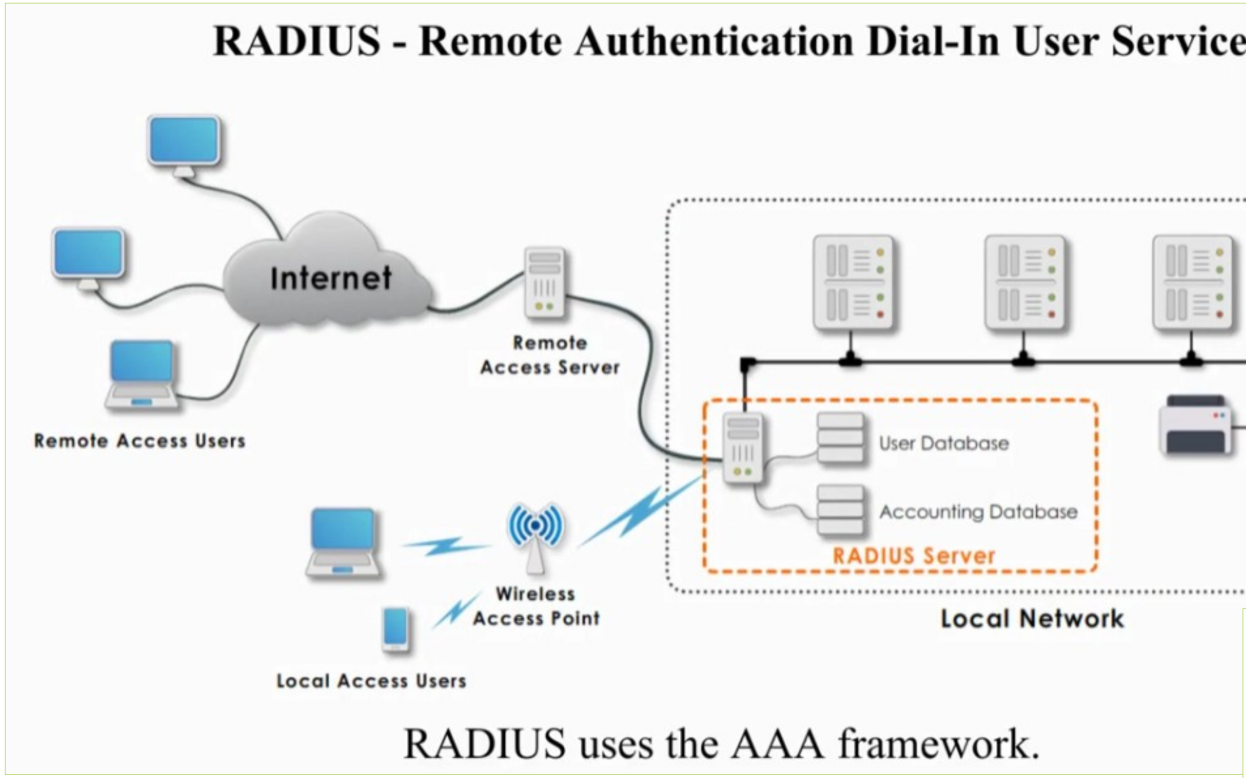
- **NPS allows centrally configure and manage network access authentication, authorization, and accounting with the following features:**

1. **RADIUS server.**

NPS performs centralized authentication, authorization, and accounting (AAA) for wireless, authenticating switch, remote access dial-up and virtual private network (VPN) connections.

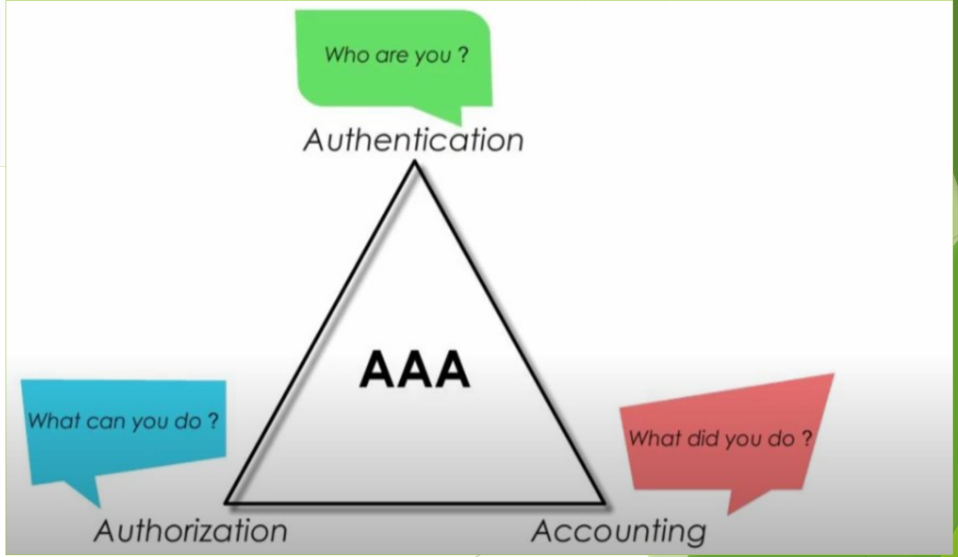
When NPS used as a RADIUS server, configure network access servers, such as wireless access points and VPN servers, as RADIUS clients in NPS.

Also, configure network policies that NPS uses to authorize connection requests, and can configure RADIUS accounting so that NPS logs accounting information to log files on the local hard disk or in a Microsoft SQL Server database.



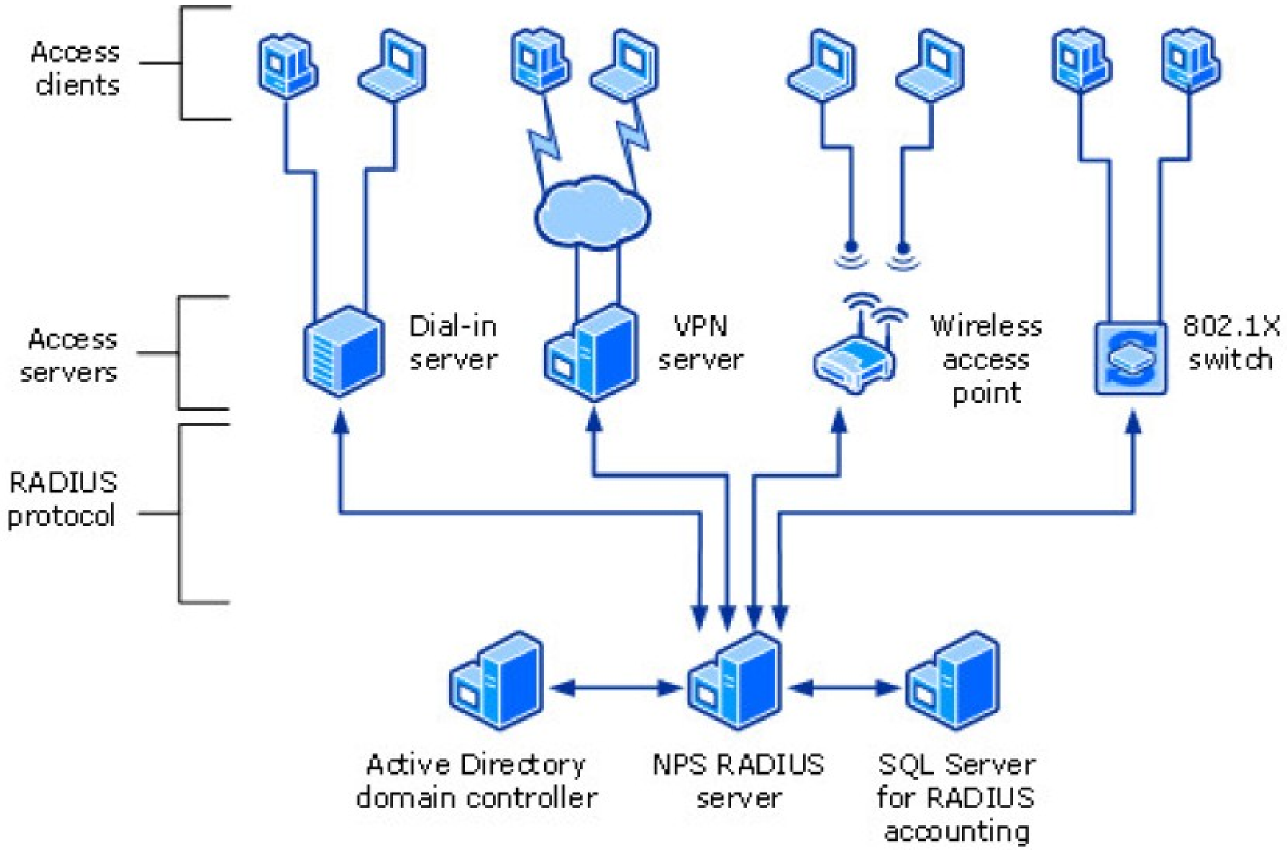
RADIUS - Remote Authentication Dial-In User Service

RADIUS uses the AAA framework.



https://www.youtube.com/watch?v=feHpDc1cLXM

The following illustration shows NPS as a RADIUS server for a variety of access clients.



- **You can use NPS as a RADIUS server when:**
- **You are using an AD DS domain or the local Security Access Manager (SAM) user accounts database as your user account database for access clients.**
- **You are using Remote Access on multiple dial-up servers, VPN servers, or demand-dial routers and you want to centralize both the configuration of network policies and connection logging and accounting.**
- **You are outsourcing your dial-up, VPN, or wireless access to a service provider. The access servers use RADIUS to authenticate and authorize connections that are made by members of your organization.**
- **You want to centralize authentication, authorization, and accounting for a heterogeneous set of access servers.**
- *** The Security Account Manager (SAM)**

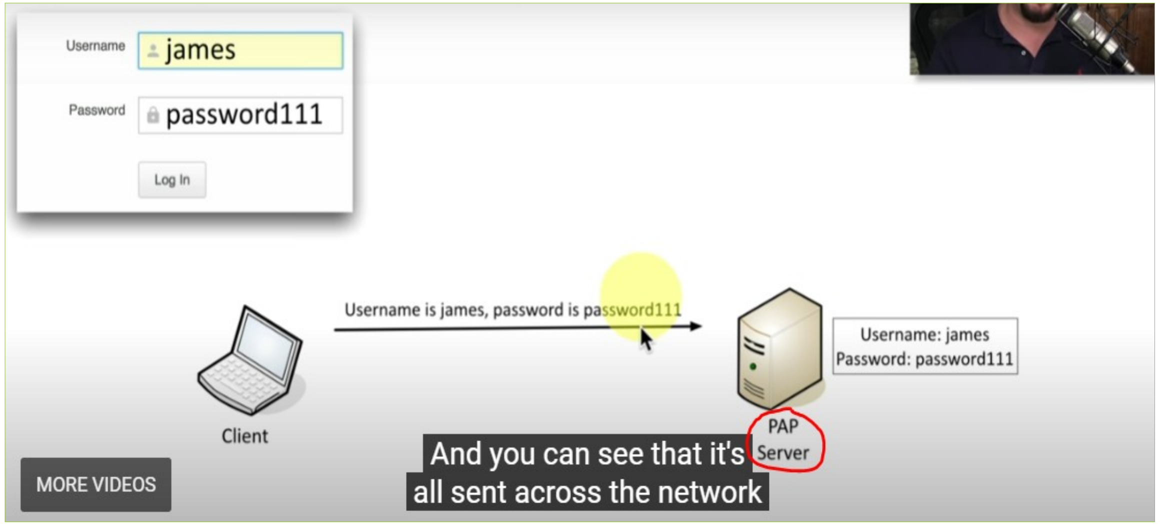
Ref: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top
https://www.youtube.com/watch?v=ZdQqIKoesas

Point-to-Point Protocol (PPP) Authentication protocols

- PAP stands for Password Authentication Protocol. PAP, on the end-user side, works as we all readily understand. For example: the user inputs a username and password. That information is provided by the user to the client who then sends it from the network access server (NAS) to the RADIUS server. Unfortunately, PAP is terribly insecure because it sends both the username and password in plaintext, meaning that anybody who has the ability to intercept packets between the NAS and RADIUS server would be able to discern the username and password easily.
- CHAP stands for Challenge Handshake Authentication Protocol. It is a more secure method of authentication than PAP (although it wasn’t hard to be more secure than a clear-text password communication).
- CHAP eliminates the process of sending clear-text passwords and instead utilizes encryption to mask the information being transferred.

https://www.professormesser.com/security-plus/sy0-501/pap-chap-and-ms-chap/

PAP VS CHAP



Username james

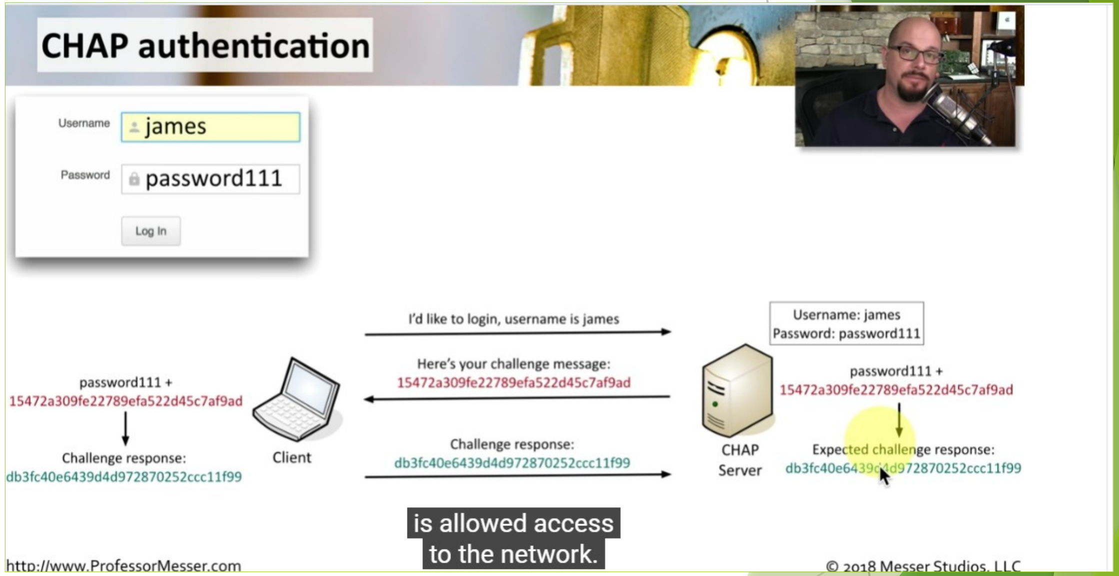
Password password111

Log In

Username is james, password is password111

Username: james
Password: password111

And you can see that it's all sent across the network



CHAP authentication

Username james

Password password111

Log In

Username: james
Password: password111

I'd like to login, username is james

Here's your challenge message:
15472a309fe22789efa522d45c7af9ad

Challenge response:
db3fc40e6439d4d972870252ccc11f99

password111 +
15472a309fe22789efa522d45c7af9ad

Challenge response:
db3fc40e6439d4d972870252ccc11f99

password111 +
15472a309fe22789efa522d45c7af9ad

Expected challenge response:
db3fc40e6439d4d972870252ccc11f99

is allowed access to the network.

http://www.ProfessorMesser.com

© 2018 Messer Studios, LLC

https://www.professormesser.com/security-plus/sy0-501/pap-chap-and-ms-chap/

- In computer networking, Point-to-Point Protocol (PPP) is a Data link layer (layer 2) communications protocol between two routers directly without any host or any other networking in between.
- It can provide connection authentication, transmission encryption, and compression.

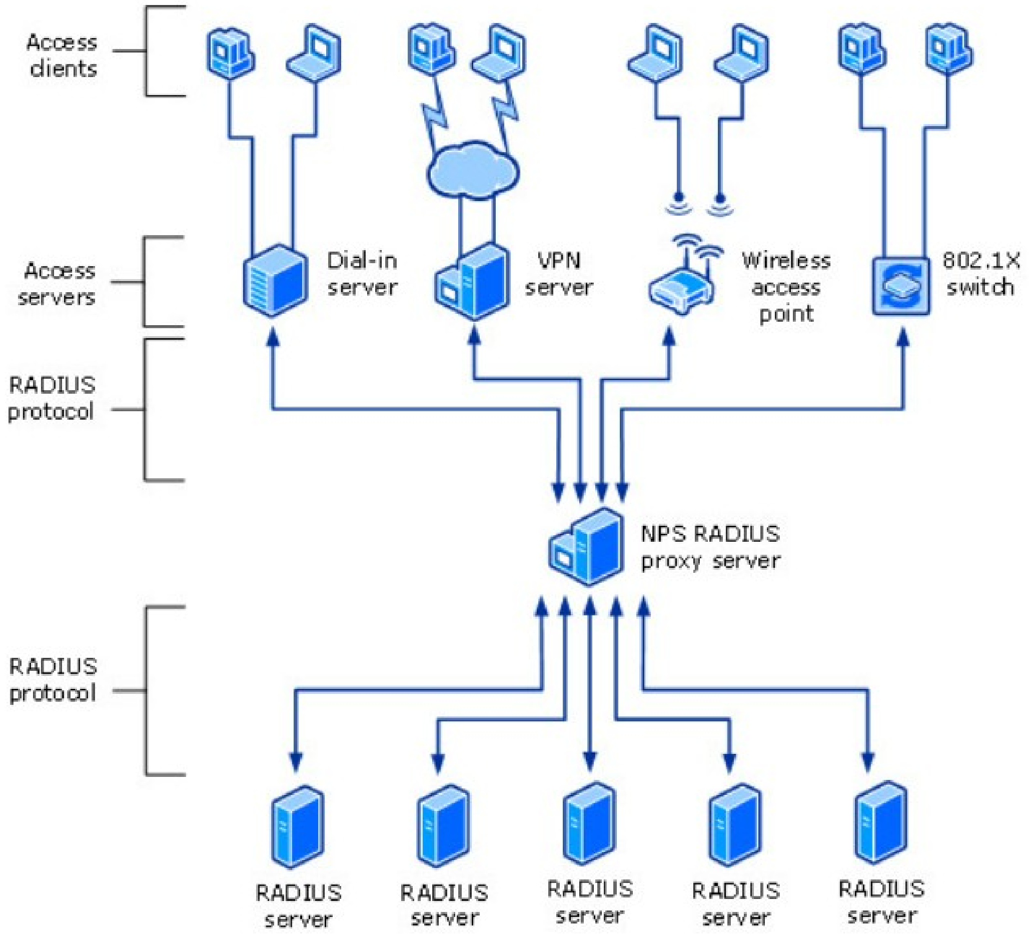
Network Policy Server (NPS)

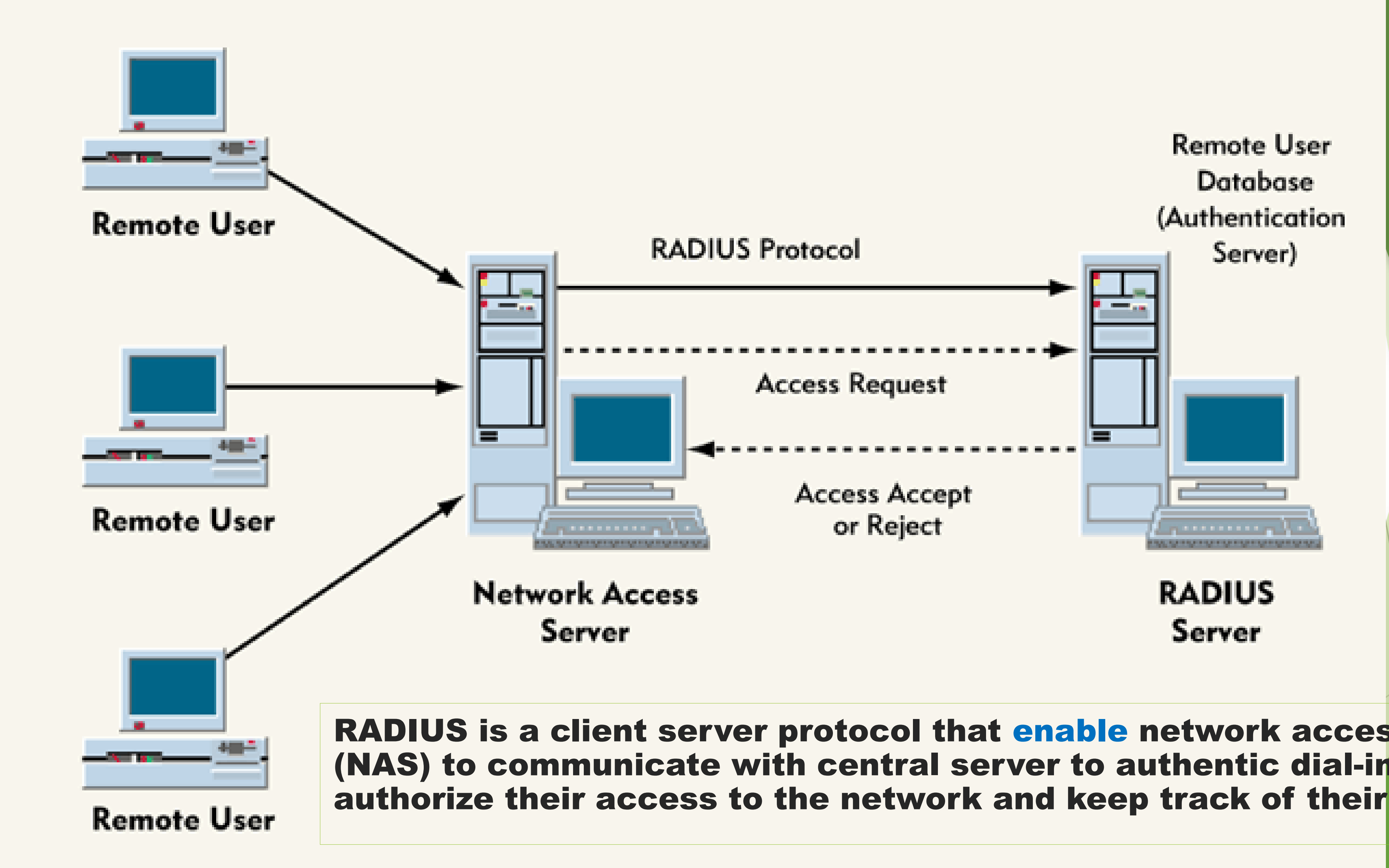
2. **RADIUS proxy.**

Use NPS as a RADIUS proxy when:

- a service provider who offers outsourced dial-up, VPN, or wireless network access services to multiple customers.
- to provide authentication and authorization for user accounts that are not members of either the domain
- to perform authentication and authorization by using a database that is not a Windows account database.
- to process a large number of connection requests.
- to provide RADIUS authentication and authorization for outsourced service providers and minimize intranet firewall configuration.

The following illustration shows NPS as a RADIUS proxy between RADIUS clients and RADIUS servers.





RADIUS is a client server protocol that enable network access server (NAS) to communicate with central server to authentic dial-in user, authorize their access to the network and keep track of their activities.

Ref: https://forum.huawei.com/enterprise/en/how-to-configure-the-radius-authentication/thread/450231-861

Network Policy Server (NPS)

- With NPS, organizations can also outsource remote access infrastructure to a service provider while retaining control over user authentication, authorization, and accounting.

- NPS configurations can be created for the following scenarios:
  - Wireless access
  - Organization dial-up or virtual private network (VPN) remote access
  - Outsourced dial-up or wireless access
  - Internet access
  - Authenticated access to extranet resources for business partners

Plan NPS as a RADIUS server

- **Guidelines to deploy NPS as a RADIUS server on the network**
  - **Plan NPS configuration.**
  - **Plan RADIUS clients.**
  - **Plan the use of authentication methods.**
  - **Plan network policies.**
  - **Plan NPS accounting.**

Ref: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-plan-server

Plan NPS as a RADIUS proxy

- **Guidelines to deploy NPS as a RADIUS proxy on the network**
  - **Plan NPS configuration.**
  - **Plan RADIUS clients.**
  - **Plan remote RADIUS server groups.**
  - **Plan attribute manipulation rules for message forwarding.**
  - **Plan connection request policies.**
  - **Plan NPS accounting.**

** Accounting relate to monitoring network resources, information needed for billing of services

Ref: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-plan-proxy

Configure Network Policy Server

- Deploy NPS Certificates for VPN and 802.1X Access
- Deploy NPS for 802.1X Wireless Access
- Deploy NPS for Windows 10 VPN Access

Manage Network Policy Server

1. Network Policy Server Management with Administration Tools
2. Configure Connection Request Policies
3. Configure Firewalls for RADIUS Traffic
4. Configure Network Policies
5. Configure Network Policy Server Accounting
6. Configure RADIUS Clients
7. Configure Remote RADIUS Server Groups
8. Manage Certificates Used with NPS
9. Manage NPSs
10. Manage NPS Templates

Network Policy Server Management with Administration Tools

1. Configure the Local NPS by Using the NPS Console
2. Manage Multiple NPSs by Using the NPS MMC Snap-in
3. Manage an NPS by Using Remote Desktop Connection
4. Use Netsh NPS commands to manage an NPS
5. Use Windows PowerShell to manage NPSs

Configure Connection Request Policies

- Add a Connection Request Policy
- Membership in Domain Admins, or equivalent, is the minimum required to complete this procedure.

Configure Firewalls for RADIUS Traffic

1. Windows Firewall on the local NPS
2. Other firewalls
3. Configuring the Internet firewall

Configure Network Policies

1. Add a Network Policy
2. Create Network Policies for Dial-Up or VPN with a Wizard
3. Create Network Policies for 802.1X Wired or Wireless with a Wizard
4. Configure NPS to Ignore User Account Dial-in Properties
5. Configure NPS for VLANs
6. Configure the EAP Payload Size

Configure Network Policy Server Acco unting

- There are three types of logging for Network Policy Server (NPS):

1. Event logging. Used primarily for auditing and troubleshooting connection attempts. Configure NPS event logging by obtaining the NPS properties in the NPS console.
2. Logging user authentication and accounting requests to a local file. Used primarily for connection analysis and billing purposes. Also useful as a security investigation tool because it provides a method of tracking the activity of a malicious user after an attack. Configure local file logging using the Accounting Configuration wizard.
3. Logging user authentication and accounting requests to a Microsoft SQL Server XML-compliant database. Used to allow multiple servers running NPS to have one data source. Also provides the advantages of using a relational database. Configure SQL Server logging by using the Accounting Configuration wizard.

Configure Network Policy Server Accounting

1. Use the Accounting Configuration wizard
2. Configure NPS Log File Properties
3. Configure NPS SQL Server Logging
4. Ping user-name

Configure RADIUS Clients

- On the NPS proxy, configure a remote RADIUS server group that contains the NPS.
- On the remote NPS, configure the NPS proxy as a RADIUS client.
- To perform the procedures in this topic, must have at least one network access server (VPN server, wireless access point, authenticating switch, or dial-up server) or NPS proxy physically installed on the network.

1. Configure the Network Access Server
2. Add the Network Access Server as a RADIUS Client in NP S
3. Configure RADIUS Clients by IP Address Range in Window s Server 2016 Datacenter

Configure Remote RADIUS Server Groups

- **Add a Remote RADIUS Server Group**
- **Create a new connection request policy that NPS uses to determine which connection requests to forward to other RADIUS servers.**
- **In addition, the connection request policy is configured by specifying a remote RADIUS server group that contains one or more RADIUS servers, which tells NPS where to send the connection requests that match the connection request policy.**

Manage Certificates Used with NPS

Enroll a server certificate to all NPSs. The server certificate must:

- Meet the minimum server certificate requirements as described in Configure Certificate Templates for PEAP and EAP Requirements
- Be issued by a certification authority (CA) that is trusted by client computers. A CA is trusted when its certificate exists in the Trusted Root Certification Authorities certificate store for the current user and local computer.

1. Change the Cached TLS Handle Expiry
2. Configure the TLS Handle Expiry Time on Client Computers
3. Configure the TLS Handle Expiry Time on NPSs
4. Obtain the SHA-1 Hash of a Trusted Root CA Certificate

Manage NPSs

- Configure NPS on a Multihomed Computer
- Configure NPS UDP Port Information
- Disable NAS Notification Forwarding
- Export an NPS Configuration for Import on Another Server
- Increase Concurrent Authentications Processed by NPS
- Install Network Policy Server
- NPS Proxy Server Load Balancing
- Register an NPS in an Active Directory Domain
- Unregister an NPS from an Active Directory Domain
- Use Regular Expressions in NPS
- Verify Configuration After NPS Changes

Manage NPS Templates

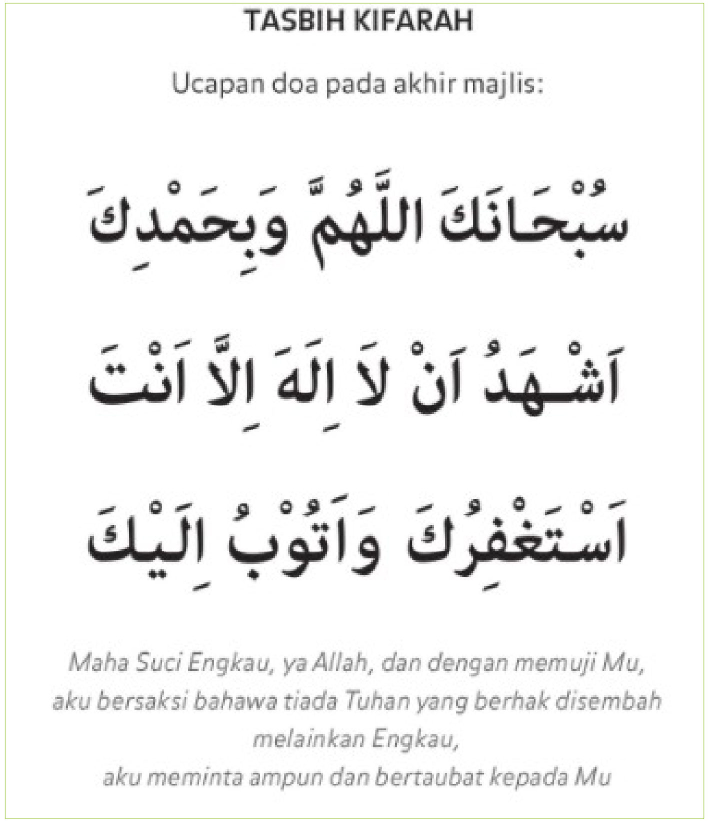
- Templates Management provides a node in the NPS console where you can create, modify, delete, duplicate, and view the use of NPS templates. NPS templates are designed to reduce the amount of time and cost that it takes to configure NPS on one or more servers.
- The following NPS template types are available for configuration in Templates Management.
  - Shared Secrets. To specify a shared secret that can reuse (by selecting the template in the appropriate location in the NPS console) when configure RADIUS clients and servers.
  - RADIUS Clients. To configure RADIUS client settings that can reuse by selecting the template in the appropriate location in the NPS console.
  - Remote RADIUS Servers. To configure remote RADIUS server settings that can reuse by selecting the template in the appropriate location in the NPS console.
  - IP Filters. To create Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) filters that can reuse (by selecting the template in the appropriate location in the NPS console) when configure network policies.

1. **Create an NPS Template**
2. **Apply an NPS Template**
3. **Export or Import NPS Templates**

After install NPS, administer NPSs via:

- Locally, by using the NPS Microsoft Management Console (MMC) snap-in, the static NPS console in Administrative Tools, Windows PowerShell commands, or the Network Shell (Netsh) commands for NPS.
- From a remote NPS, by using the NPS MMC snap-in, the Netsh commands for NPS, the Windows PowerShell commands for NPS, or Remote Desktop Connection.
- From a remote workstation, by using Remote Desktop Connection in combination with other tools, such as the NPS MMC or Windows PowerShell.

The End



TASBIH KIFARAH

Ucapan doa pada akhir majlis:

سُبْحَانَكَ اللَّهُمَّ وَبِحَمْدِكَ

اَشْـهَدُ اَنْ لاَ اِلَهَ اِلاَّ اَنْتَ

اَسْتَغْفِرُكَ وَاَتُوْبُ اِلَيْكَ

Maha Suci Engkau, ya Allah, dan dengan memuji Mu,
aku bersaksi bahawa tiada Tuhan yang berhak disembah
melainkan Engkau,
aku meminta ampun dan bertaubat kepada Mu