**Module 13**

**Networking with**

**Windows Server**

# Topic : Installing and configure DNS server

**1. Describe DNS operation**

DNS stands for a Domain Name System. DNS resolves names to numbers, to be more specific it resolves domain names to IP addresses. So by typing in a web address in web browser, DNS will resolve the name to a number because the only thing computers know are numbers.

For example, when searching for google.com on web browser DNS server will search through its cache to find a matching IP address for that domain name, and when it finds it it will resolve that domain name to IP address of Google web site, and once that is done then your computer is able to communicate with a Google web server and retrieve the webpage.

If web browser or operating system cannot find IP address in its own cache memory, it will send a query to next level to what is called resolver server. Resolver server is basically your ISP or Internet service provider, so when resolver receives this query, it will check its own cache memory to find an IP address for google.com, and if it cannot find it it will send query to next level which is root server. The root servers are the top most server in the DNS hierarchy.

There are 13 sets of these root servers from a.root-servers.net to m.root-servers.net. When root server receives query for IP address for google.com, root server is not going to know what IP address is, but root server does know where to send resolver to help it find IP address. So, root server will direct resolver to TLD or top-level domain server for .com domain. So, resolver will now ask TLD server for IP address for google.com.

**2. DNS query—Iterative and Recursive**

**DNS query :** A DNS query also known as a DNS requests a demand for information sent from a user's computer (DNS client) to a DNS server. In most cases a DNS request is sent, to ask for the IP address associated with a domain name. An attempt to reach a domain, is actually a DNS client querying the DNS servers to get the IP address, related to that domain.

**Types of queries :**

In general, there are two ways of resolving a host or a domain name to an IP address, using the domain name system **Recursive** query and **Iterative** query.

**(i) The Recursive query :**

It is when a DNS client directly gets the IP address of a domain, by asking the name server system to perform the complete translation. For example :

 A user opens up browser and enters www.co.in in the address bar. His computer does not know the IP address So, it sends a request to the user’s DNS resolver. The resolver does not know the IP address for that, so it will query one of the root DNS servers. The root servers know the locations of all the TLDs, such as .com, they do not know the IP o f that, so they return the location of the .com servers. Once the query reaches the .com TLD servers, it will find the Authoritative DNS server and will reply to the resolver with that server. The resolver will send a query to the Authoritative DNS server of the domain and will resolve it. The Authoritative DNS server of the domain will check within its database and will find an entry for www.co.in, which has an IP address. Finally the resolver will know the IP address for it and will send the result to the user's computer.

**(ii) Iterative query :**

It is when a DNS client contacts the name servers, one by one, until it finds the server, containing the needed information.

* An iterative DNS query is a request for a website name or uniform resource locator (URL) that the domain name system DNS server responds to with the IP address from its zone file cache, if possible. If the server doesn’t have the IP address requested, it forwards the request on to another DNS server. Iterative DNS queries are also known as non-recursive DNS queries.
* Iterative requests are made by both iterative DNS servers and recursive DNS server. Even the requests made by recursive servers to other DNS servers are iterative. At the level of root DNS, all servers are iterative because they are the end of the line and their availability is crucial to the function of the internet.

**3. what is forward lookup zone and its resource type**

Forward lookup zone contains a mapping between host names and IP addresses. When a computer requests an IP address by providing a host name, the forward lookup zone is queried to find the IP address for the given host name. The forward lookup zone contains A type resource records that can point out an IP address for a given host name.

For example, by typing google.com in browser, the forward lookup zone will be queried and the IP address will be returned, which is actually the IP address of that site. When a forward lookup is sent to the DNS server, the DNS server searches for an A type resource record associated with the host name provided by the request. An A type resource is a

DNS record that can be used to point the domain name and host names to a static IP address. If the DNS server finds a matching A type resource record, it will return that to the client, else it will forward the query to another DNS server.

**4. what is reverse lookup zone and its resource type**

Reverse lookup zone contains a mapping that relates IP addresses to host names. When a computer requests for a domain name by providing an IP address, the reverse lookup zone is queried to find the host name for the IP address given. The reverse lookup zone contains PTR records that can point out a host name for a given IP address.

For example, if a client wants to find the host name for the IP address 8.8.8.8, the reverse lookup zone will be queried and it will return the host name google.com. The reverse lookup zone contains PTR resource records. A PTR record allows doing a reverse lookup by pointing the IP address to a host/domain name.

**5. what is conditional forwarder**

Conditional forwarders are DNS servers that only forward queries for specific domain names. Instead of forwarding all queries it cannot resolve locally to a forwarder, a conditional forwarder is configured to forward name queries to query.

Forwarding according to domain names improves conventional forwarding by adding a name-based condition to the forwarding process. It enables improving name resolution between internal (private) DNS namespaces that aren't part of the DNS namespace of the internet.

**6. what is primary zone, secondary zone and stub zone** **Primary Zone** :

This is the main zone and has a read/write copy of the zone data. A Primary DNS zone is the original Read-Write Authoritative DNS zone of portion of a DNS Namespace. When a DNS Server hosts a primary zone, that DNS Server is considered as the Authoritative DNS Server and it is the primary source for information of that zone. Zone updates are possible only in a Primary DNS zone. Primary DNS zone is hosted in the Primary DNS Server.

All changes to the zone are made in the primary zone and are replicated to the secondary zones. The zone data is stored in a text file located in this folder c:\windows\system32\DNS on the Windows server running DNS.

**Secondary Zone :**

A secondary Zone is a read-only copy of the primary zone. This zone cannot process updates and can only retrieve updates from the primary zone. T or another Secondary Zone, kept in a Secondary DNS Server. A Secondary DNS Zone is used to reduce the load on Primary DNS Servers and also for preventing single point of failure.

This zone can answer DNS name resolution queries from clients nodes, this helps reduce the workload on the primary zone. Secondary zones cannot be active directory integrated.

**Stub Zone :**

Stub zones are like a secondary zone but only stores partial zone data. These zones are useful to help reduce zone transfers by passing the requests to authoritative servers. These zones only contain the SOA, NS, and A records.

**7. what is active directory integrated zone**

Active Directory Integrated Zones stores its zone data in Active Directory. Integrated zones can be replicated to all domain controllers in the domain and forest. Active Directory integrated zones use multi-master replication, this means any domain controller running the DNS server service can write updates to the zone for which they are authoritative.

**Advantages :**

* + Replication is faster, more secure and efficient.
  + Better redundancy due to zone data being copied to all Domain Controllers
  + Improved Security if secure dynamic update is enabled
  + No need to schedule or manage zone transfers

**8. primary server, secondary server, cache only server**   **Primary Server :**

The primary server is the authoritative server for the zone. All administrative tasks associated with the zone (such as creating subdomains within the zone, or other similar administrative tasks) must be performed on the primary server.

In addition, any changes associated with the zone or any modifications or additions to RRs in the zone files must be made on the primary server. For any given zone, there is one primary server, except when you integrate Active Directory services and Microsoft DNS Server.

**Secondary Servers :**

Secondary servers are backup DNS Servers. Secondary servers receive all of their zone files from the primary server zone files in a zone transfer. Multiple secondary servers can exist for any given zone, as many as necessary to provide, load balancing, fault tolerance and traffic reduction.

Additionally, any given DNS Server can be a secondary server for multiple zones. In addition to primary and secondary DNS Servers, additional DNS Server roles can be used when such servers are appropriate for a DNS infrastructure. These additional servers are caching servers and forwarders.

**Caching Servers :**

Caching servers also known as caching-only servers, perform as their name suggests; they provide only cached-query service for DNS responses. Rather than maintaining zone files like other secondary servers do, caching DNS Servers perform queries, cache the answers, and return the results to the querying client.

The primary difference between caching servers and other secondary servers is that other secondary servers maintain zone files (and do zone transfers when appropriate, thereby generating network traffic associated with the transfer), caching servers do not.

**9. what is aging and scavenging**  **Aging :**

It is a DNS feature that is used to identify the stale resource records from the DNS server. It uses two intervals namely Non-refresh interval and Refresh interval. The DNS record is considered a stale record when both these intervals are elapsed.

* **Non-Refresh Interval:** Non-Refresh Intervalis the interval during which the resource record cannot be refreshed. It is used to reduce the replication traffic during this interval to avoid the same information being replicated. By default, this is configured for 7 days and during this time, the timestamp cannot be updated.
* **Refresh interval:** Refresh Interval is the interval during which the resource record can be updated. By default, the refresh interval is set to 7 days. This value should be large to allow all clients to refresh their records. In this time any data in the DNS records can be updated including the time stamp.

**Scavenging :**

DNS Scavenging is the process of removing outdated DNS records. It looks at the timestamps of the DNS record in order to determine if the DNS record should be removed. This will occur after the No-refresh interval and Refresh interval, which is 14 days by default. The important thing to remember with Scavenging is that it is not configured by default. In order for Scavenging to work, a number of settings need to be configured in order for it to work at. If these settings are not configured correctly, Scavenging will not occur or can happen quite randomly.

**10. what is MX record**

A DNS mail exchange (MX) record directs email to a mail server. A mail exchanger record specifies the mail server responsible for accepting email messages on behalf of a domain name. It is a resource record in the Domain Name System. It is possible to configure several MX records, typically pointing to an array of mail servers for load balancing and redundancy.

The MX record indicates how email messages should be routed in accordance with the Simple Mail Transfer Protocol (SMTP, the standard protocol for all email). Like CNAME record, an MX record must always point to another domain. The 'priority' numbers in the domains for the MX records indicate preference, where the lower priority value is preferred.

**\*Practical**

1. installactive directory integrated dns

DONE

1. createsecondary dnsandzone transfer

DONE

1. create“A”record

DONE

1. createalias

DONE

1. createreverse lookupzone

DONE

1. makeapointer

DONE

1. applyconditional forwareder betwwen twodifferent domain

DONE

1. nslookupcommand

**DHCP**

**1. purpose of DHCP**

Dynamic Host Configuration Protocol (DHCP) is a standard protocol defined by RFC 1541. It’s purpose is to allows a server to dynamically distribute IP addressing and configuration information to clients. Normally the DHCP server provides the client with at least this basic information:

* IP Address
* Subnet Mask
* Vendor Class Identifier
* DNS Address

**2. what is DORA process?**

The DHCP negotiation process is known as DORA: Discover, Offer, Request, Acknowledge message.

1. **DHCP discover message :**

This is a first message generated in the communication process between server and client. This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long.

1. **DHCP offer message :**

The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also, a server ID is specified in the packet in order to identify the server.

1. **DHCP request message :**

When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address . A Client ID is also added in this message.

1. **DHCP acknowledgement message :**

In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.

**3. what is authorised DHCP server?**

An authorized DHCP server is a DHCP server that has been authorized in Active Directory to support DHCP clients. Authorizing a DHCP server provides with the ability to control the addition of DHCP servers to the domain.

Authorization must occur before a DHCP server can issue leases to DHCP clients. Requiring authorization of the DHCP servers prevents unauthorized DHCP servers from offering potentially invalid IP addresses to clients.

Active Directory is required to authorize a DHCP server. With Active Directory, unauthorized DHCP servers will not be able to support DHCP clients. The DHCP Server service, on a server that is a member of Active Directory, checks with the Active Directory Domain Controller to verify that the DHCP server is registered in Active Directory. If the DHCP server is not registered, then the DHCP Server service does not start, and therefore the DHCP server cannot support DHCP clients.

**4. describe scope, lease duration, DHCP option, exclude address**  **Scope :**

It is a consecutive range of IP addresses that a DHCP server can draw on to fulfill an IP address request from a DHCP client. By defining one or more scopes on your DHCP server, the server can manage the distribution and assignment of IP addresses to DHCP clients.

**Lease duration :**

This DHCP-assigned IP address is not permanent and expires in about 24 hours. This is called DHCP lease time. Unless otherwise mentioned, the DHCP server assumes that all

IP addresses are temporary and expire after some time. The biggest advantage with DHCP lease time is that the same IP address is not stuck to a device forever and is available for other devices, too when needed. The standard DHCP lease time is 24 hours, but you can change it to meet your network’s needs.

**DHCP Option :**

Supplying DHCP options is a smart way to configure network clients during the early phase of network access deployment. In addition to providing the IP address, the DHCP protocol is able to set a large bunch of options that are very useful for device configuration. Each option has a name and a numerical identifier to be transported in the protocol frames. DHCP server configuration can handle providing options to all devices asking for an IP address and also bound to a specific client identifier or mac address family. Here is the list of the most common DHCP options exchanged with clients:

* + DHCP option **1**: subnet mask to be applied on the interface asking for an IP address
  + DHCP option **3**: default router or last resort gateway for this interface
  + DHCP option **6**: which DNS (Domain Name Server) to include in the IP configuration for name resolution
  + DHCP option **51**: lease time for this IP address

**Exclude Address :**

An exclusion is an address or range of addresses taken from a DHCP scope that the DHCP server is not allowed to hand out. For example, if one has set a DHCP server to exclude the address range 192.168.0.1 to 192.168.0.10 then the only way a computer on network would get an address of 192.168.0.4 would be if you assigned it statically on that machine. This is because DHCP knows NOT to give this range of IP addresses out.

**5. what is reservation?**

A reservation is a specific IP addresses that is tied to a certain device through its MAC address. That is assigning a specific IP address for a specific device by its MAC address, which will remain same until changes.

For example, if there is a workstation on the network that requires a certain IP address,but user don’t want to go through to trouble of assigning it statically, then one can create a reservation for it. So if the MAC address of the NIC on the computer is AA-BB00-FF-CC-AA and want it to maintain the IP address of 192.168.0.100 then have to create a DHCP reservation under that particular scope saying that the IP address 192.168.0.100 is reserved only for the MAC address AA-BB-00-FF-CC-AA.

**6. what is DHCP relay agent?**

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet.

Relay agent forwarding is distinct from the normal forwarding of an IP router, relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway IP address (giaddr field of the DHCP packet) and, if configured, adds the relay agent information option (option82) in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing option 82.

**7. describe ipconfig command**

This command displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig** displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

This command is most useful on computers that are configured to obtain an IP address automatically. This enables users to determine which TCP/IP configuration values have been configured by DHCP, Automatic Private IP Addressing (APIPA), or an alternate configuration.

* + To display the basic TCP/IP configuration for all adapters, type: ipconfig

* + To display the full TCP/IP configuration for all adapters, type: ipconfig /all

* + To renew a DHCP-assigned IP address configuration for only the Local Area Connection adapter, type:

ipconfig /renew Local Area Connection

* + To flush the DNS resolver cache when troubleshooting DNS name resolution problems, type:

ipconfig /flushdns

* + To display the DHCP class ID for all adapters with names that start with Local, type: ipconfig /showclassid Local\*

* + To set the DHCP class ID for the Local Area Connection adapter to TEST, type: ipconfig /setclassid Local Area Connection TEST

• Practical

1. install DHCP sever and make authorize

DONE

1. create a scope and check on client by ipconfig

DONE

1. DHCP database and take backup

DONE

1. hcp failover

DONE

1. DHCP relay agent

DONE

1. DHCP filter

DONE

1. DHCP reservation

DONE

**IPAM**

**1. what is IPAM and purpose of IPAM IPAM :**

IP Address Management (IPAM) is an integrated suite of tools to enable end-to-end planning, deploying, managing and monitoring of your IP address infrastructure, with a rich user experience. IPAM automatically discovers IP address infrastructure servers and Domain Name System (DNS) servers on network and enables to manage them from a central interface.

**Purpose of IPAM :**

It is the administration of DNS and DHCP, which are the network services that assign and resolve IP addresses to machines in a TCP/IP network. Simply put, IPAM is a means of planning, tracking, and managing the Internet Protocol address space used in a network.

**2. why need dedicated server**

A dedicated server is a server that had been complete access to and control over. Instead of sharing server resources with other users all of the server resources can be used to power website. If site has outgrown a traditional shared hosting plan, then might consider upgrading to a dedicated server. This type of hosting is very beneficial for larger sites that receive a high volume of traffic, or those that require custom server configurations.

**Need of Dedicated Server :**

A dedicated server can provide a ton of advantages for the right kind of user. Here are some of benefits needed to a dedicated server:

* + High Level of Performance
  + Ability to Customize Your Server
  + Fast Site Loading Speeds
  + Improved Website Security

**3. policy for ipam sever**

If have chosen the Group Policy based provisioning method, must need to provide a GPO name prefix in the provisioning wizard. After providing a GPO name prefix, the wizard will display the GPO names that must be created in domains that will be managed by IPAM. The following GPOs are not created by the provisioning wizard and must be created in each domain that will be managed by the IPAM server, that is DHCP, DNS, and Domain controller NPS.

If chosen the manual provisioning method, it will allow to create IPAM provisioning GPOs and use them to apply access settings to managed servers. In this case, specific GPO names are not required. However, need to apply GPOs manually to managed servers by adding or removing the managed server to GPO security filtering as needed. For steps to modify GPO security filtering. This procedure is not necessary if chosen the automatic GPO-based provisioning method

create IPAM provisioning GPOs, Run the Invoke-IpamGpoProvisioning cmdlet at an elevated Windows PowerShell prompt. Invoke-IpamGpoProvisioning has the following parameters:

Invoke-IpamGpoProvisioning [-Domain] <String> [-GpoPrefixName] <String> [DelegatedGpoGroup <String[]> ] [-DelegatedGpoUser <String[]> ] [-DomainController <String> ] [-Force] [-IpamServerFqdn <String> ] [-PassThru] [ <CommonParameters>]

**4. which service monitor and manage by IPAM**

A big enterprise or organization which works with number of DNS server, Number of sites and domain controller can be monitored from a single location with IPAM services and it allows to manage certain interfaces and services such as, DHCP as well as DNS.

**• Practical**

1. Install IPAM

DONE

1. configure IPAM withs ix step

DONE

1. create Dhcp scope using IPAM 4 create DNS zone

DONE

1. check monitoring of services

DONE

# Topic : Remote connectivity and VPN

**1. what is VPN?**

VPN stands for Virtual Private Network. The VPN allows you to send your data via an encrypted, secure connection to an external server: the VPN server. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

**2. type of VPN**

There are two main type of VPN :

1. **A remote access :**

It VPN securely connects a device outside the corporate office. These devices are known as endpoints and may be laptops, tablets, or smartphones. Advances in VPN technology have allowed security checks to be conducted on endpoints to make sure they meet a certain posture before connecting. Think of remote access as computer to network.

1. **A site-to-site VPN :**

It connects the corporate office to branch offices over the Internet. Site-to-site VPNs are used when distance makes it impractical to have direct network connections between these offices. Dedicated equipment is used to establish and maintain a connection. Think of site-to-site access as network to network. There are another two base of Site to site VPN:

* + **Intranet based VPN:**

When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.

* + **Extranet based VPN:**

When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

**3. tunneling protocol**

**(i) Internet Protocol Security (IPSec):**

* Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection. IPSec runs in 2 modes:
* Transport mode
* Tunneling mode

**(ii) Layer 2 Tunneling Protocol (L2TP):**

 L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnel.

**(iii) Point–to–Point Tunneling Protocol (PPTP):**

 PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.

**(iv) SSL and TLS:**

 SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have “https” in the initial of the URL instead of “http”.

**(v)** **OpenVPN:**

 OpenVPN is an open source VPN that is commonly used for creating Point-to-Point and Site-to-Site connections. It uses a traditional security protocol based on SSL and TLS protocol.

**(vi) Secure Shell (SSH):**

 Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that the tunnel is encrypted. SSH connections are generated by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

**4. authentication protocol**

Protocols such as EAP, CHAP, PAP, and SPAP authenticates the identity of the remote user. For encryption purposes, however, it is best to use EAP or MS-CHAP for authentication because it allows link encryption.

**(i) Password Authentication Protocol (PAP):**

* PAP was one of the first authentication protocols created. It’s simple and takes relatively little computational power, but it’s also much more vulnerable than other protocols for authentication.
* In this, client initiates authentication by sending a packet with their credentials (username and password). The client continually sends authentication requests to the server until the server responds. The server checks the credentials and responds with authentication success or authentication failure.

**(ii)** **Challenge Handshake Authentication Protocol (CHAP):**

* CHAP uses a username and password combination, but it requires both the server and the client to run the password through a hash function along with a One Time Password (OTP) sent from the server.
* In this, At any time during a session, the server initiates authentication by sending an OTP (usually in the form of a 128-bit string).
* Often, this happens multiple times during a session, with the server re-authenticating the client for additional security. The client takes the OTP and runs it, plus their password, through an MD5 Hash function. Next, the client sends the resulting hash string and their username (in plaintext) back to the server.
* Finally, the server uses the username to look up the stored password in their database and computes the same MD5 hash function with that server and the OTP they initially sent. If the MD5 hash codes match, the client is authenticated. The server responds with authentication success or authentication failure.

**(iii) Extensible Authentication Protocol (EAP): 40 methods of authentication**

* PAP and CHAP are simple when compared with EAP, which is really more of an authentication framework than a security protocol. There are 40 different authentication methods, that can be used. In each request or response between the server and the client, a “type” for authentication is specified. Some of the types include EAP-MD-5, EAP-TLS, EAP-PEAP, EAP-TTLS, and EAP-Fast.
* In this, the server sends an authentication request to the client, including which of the 40 authentication methods it should use. The client then computes whatever it needs to, depending on the specified “type.” Next, the client sends the results back to the server, along with the type, so that the server knows what method it should use to check the output. If the server needs anything else, it will send another request—along with the type—back to the client until authentication is deemed a success or failure. Once the server determines the outcome, it sends an authentication success or an authentication failure back to the client.

**5. what is routing**

Routing is a process in which devices are connected in order to deliver the packet by choosing an optimal path from one network to another. A VPN router allows you to connect several devices at the same time, protecting them all with a secure, encrypted connection. It allows to link to it through either a Wi-Fi connection or Ethernet, depending on the device and how you want to use it. Because they can handle multiple devices, VPN routers for home can provide safer internet browsing for every member of your household.

• Practical

1. install routing and remote access

DONE

1. configure LAN routing

DONE

1. configure vpn connection (VPN client)

DONE

# Topic : Network policy server

**1. what is Radius server**

RADIUS (Remote Authentication Dial-In User Service) is a client-server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

RADIUS enables a to maintain user profiles in a central database that all remote servers can share. Having a central database provides better security, allow to set up a policy that can be applied at a single administered network point. A central database also makes it easier to track usage for billing for the network access or internet service provider and for keeping network statistics.

In the RADIUS protocol, remote network users connect to their networks through a network access server NAS. The NAS queries the authentication server to get authentication, authorization and configuration information about the remote user.

**2. what is authentication authorization and accounting**

AAA is a standard-based framework used to control who is permitted to use network resources (through authentication), what they are authorized to do (through authorization), and capture the actions performed while accessing the network (through accounting).

**Authentication :**

The process by which it can be identified that the user, which wants to access the network resources, valid or not by asking some credentials such as username and password. A network administrators can control how a user is authenticated if someone wants to access the network. Some of these methods include using the local database of that device (router) or sending authentication requests to an external server like the ACS server. To specify the method to be used for authentication, a default or customized authentication method list is used.

**Authorization :**

It provides capabilities to enforce policies on network resources after the user has gained access to the network resources through authentication. After the authentication is successful, authorization can be used to determine what resources is the user allowed to access and the operations that can be performed.

**Accounting :**

It provides means of monitoring and capturing the events done by the user while accessing the network resources. It even monitors how long the user has access to the network. The administrator can create an accounting method list to specify what should be accounted for and to whom the accounting records should be sent.

**3. RADIUS server operation method and radius client**

A **RADIUS Client** (or Network Access Server) is a networking device (like a VPN concentrator, router, switch) that is used to authenticate users.

A **RADIUS Server** is a background process that runs on a UNIX or Windows server. It lets you maintain user profiles in a central database. Hence, if you have a RADIUS Server, you have control over who can connect with your network.

When a user tries to connect to a RADIUS Client, the Client sends requests to the RADIUS Server. The user can connect to the RADIUS Client only if the RADIUS Server authenticates and authorizes the user.

* The working of the RADIUS Server depends on the exact nature of the RADIUS ecosystem. However, all servers have AAA capabilities (Authentication, Authorization, and Accounting). In some RADIUS ecosystems, a RADIUS Server can also act as a proxy client to other RADIUS Servers.
* RADIUS Servers offer businesses the ability to preserve the privacy and security of their system and their users, thus helping in security management and in creating policies for server administration.
* In the RADIUS protocol, remote network users connect to their networks through a network access server NAS. The NAS queries the authentication server to get authentication, authorization and configuration information about the remote user.  Unlike other client-server applications, where the client is often an individual user, RADIUS clients are the NAS systems used to access a network and the authentication server is the RADIUS server.

**4. RADIUS port number**

The port values of 1812 for authentication and 1813 for accounting are RADIUS standard ports. However, by default, many access servers use ports 1645 for authentication requests and 1646 for accounting requests.

**5. what is network policies (NPS)?**

Network policies are sets of conditions, constraints, and settings that allow to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

When processing connection requests as a Remote Authentication Dial-In User Service (RADIUS) server, NPS performs both authentication and authorization for the connection request. During the authentication process, NPS verifies the identity of the user or computer that is connecting to the network. During the authorization process, NPS determines whether the user or computer is allowed to access the network.

To make these determinations, NPS uses network policies that are configured in the NPS console. NPS also examines the dial-in properties of the user account in Active Directory Domain Services (ADDS) to perform authorization.

**• Practical**

1. P1configureRADIUSforwireless client

DONE

2. configure NPS for remote access

DONE

# Topic : IPv4 addressing and IPv6 addressing

**1. what is ip address? And type of ip address**

An IPv6 address is 128 bits. The preferred IP address format has 8 hexadecimal numbers representing 16 bytes, segregated by periods (.). They are expressed in the form of four pairs - an example address might be 255.255.255.255 wherein each set can range from 0 to 255. An IP address represents a unique address that distinguishes any device on the internet or any network from another. IP addresses are not produced randomly. They are generated mathematically and are further assigned by the IANA (Internet Assigned Numbers Authority), a department of the ICANN.

**Types of IP address :**

1. **Private IP address :**

All the devices that are linked with internet network are allocated a private IP address. It holds computers, desktops, laptops, smartphones, tablets, or even Wi-Fi-enabled gadgets such as speakers, printers, or smart Televisions. The router produces unique private IP addresses that act as an identifier for every device using internet network.

1. **Public IP address :**

A public IP address or primary address represents the whole network of devices associated with it. Every device included within with primary address contains their own private IP address. ISP is responsible to provide your public IP address to router. Typically, ISPs contains the bulk stock of IP addresses that they dispense to their clients. A public IP address is practiced by every device to identify network that is residing outside internet network. Public IP addresses are further classified into two categories- dynamic and static.

* **Dynamic IP address :**

As the name suggests, Dynamic IP addresses change automatically and frequently. With this types of IP address, ISPs already purchase a bulk stock of IP addresses and allocate them in some order to their customers. Periodically, they re-allocate the IP addresses and place the used ones back into the IP addresses pool so they can be used later for another client. The foundation for this method is to make cost savings profits for the ISP.

* **Static IP address :**

In comparison to dynamic IP addresses, static addresses are constant in nature. The network assigns the IP address to the device only once and, it remains consistent. Though most firms or individuals do not prefer to have a static IP address, it is essential to have a static IP address for an organization that wants to host its network server. It protects websites and email addresses linked with it with a constant IP address.

**2. class of ip address**

The class of an IP address can identify by looking at its first octet. Following are the ranges of Class A, B, C, and D Internet addresses, each with an example address:

* **Class A** networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. For example the address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.
* **Class B** networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. For example the address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.
* **Class C** networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. For example the address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.
* **Class D** IP addresses are not allocated to hosts and are used for multicasting. Multicasting allows a single host to send a single stream of data to thousands of hosts across the Internet at the same time. It is often used for audio and video streaming.

**3. public ip address and private ip address**

**Private IP address** of a system is the IP Address which is used to communicate within the same network. Using private IP data or information can be sent or received within the same network.

**Public IP address** of a system is the IP address which is used to communicate outside the network. Public IP address is basically assigned by the ISP (Internet Service Provider).

**Difference between Private and Public IP address:**

|  |  |
| --- | --- |
| **PRIVATE IP ADDRESS** | **PUBLIC IP ADDRESS** |
| Scope is local. | Scope is global. |
| It is used to communicate within the network. | It is used to communicate outside the network. |
| Private IP addresses of the systems connected in a network differ in a uniform manner. | Public IP may differ in uniform or nonuniform manner. |
| It works only in LAN. | It is used to get internet service. |
| It is used to load network operating system. | It is controlled by ISP. |
| It is available in free of cost. | It is not free of cost. |

**4. what is static ip address, DHCP and APIPA**  **Static IP address :**

In comparison to dynamic IP addresses, static addresses are constant in nature. The network assigns the IP address to the device only once and, it remains consistent.

 Though most firms or individuals do not prefer to have a static IP address, it is essential to have a static IP address for an organization that wants to host its network server. It protects websites and email addresses linked with it with a constant IP address.

**DHCP :**

Dynamic Host Configuration Protocol (DHCP) is allows a server to dynamically distribute IP addressing and configuration information to clients. When a device wants access to a network that’s using DHCP, it sends a request for an IP address that is picked up by a DHCP server.

 The server responds be delivering an IP address to the device, then monitors the use of the address and takes it back after a specified time or when the device shuts down. The IP address is then returned to the pool of addresses managed by the DHCP server to be reassigned to another device as it seeks access to the network.

**APIPA :**

Automatic Private IP Addressing (APIPA) is OS based feature of Windows that enables a Dynamic Host Configuration Protocol client to automatically assign an IP address to itself when there is no DHCP server available to perform that function.

 The IP address range for APIPA is (169.254.0.1 to

169.254.255.254) having 65,534 usable IP addresses, with the subnet mask of 255.255.0.0**.** APIPA serves as a DHCP server failover mechanism and makes it easier to configure and support small LANs.

**5. what is ipv6 address?**

IPv6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IP v4 exhaustion. IPv6 is a 128-bits address having an address space of 2^128, which is way bigger than IPv4.

In IPv6, it uses Colon-Hexa representation. All IPv6 addresses are 128 bits long, written as 8 sections of 16 bits each. They are expressed in hexadecimal representation, so the sections range from 0 to FFFF. Sections are delimited by colons, and leading zeroes in each section may be omitted. If two or more consecutive sections have all zeroes, they can be collapsed to a double colon, 8 groups of 16-bit hexadecimal values separated by colons (:). For example :FE80:CD00:0000:0CDE:1257:0000:211E:729C

In IPv6 representation, there are three addressing methods :

* + Unicast
  + Multicast
  + Anycast

**6. ipv6 DHCP process**

The DHCPv6 client-server model is similar to that of IPv4. DHCP clients and servers use a reserved, link-scoped multicast address to exchange DHCP messages. When a DHCP client needs to send messages to a DHCP server that is not attached to the same link, a DHCP relay agent can be used to relay messages between the client and server.

* Each IPv6 DHCP server and client has a unique DHCP unique identifier (DUID). DHCP servers use DUIDs to identify clients when providing configuration parameters, and clients use DUIDs to identify the source of the DHCP messages from servers.
* A DHCP client that needs an IPv6 address sends a Solicit message to the well-known multicast address.
* DHCPv6 servers then send Advertise messages to the client to indicate that they are available.
* The client sends a Request message to a specific DHCPv6 server to request IP addresses and configuration parameters.
* The DHCPv6 server responds with a Reply message that contains the IP addresses and configuration parameters.

**7. what is NAT?**

NAT stands for Network Address Translation, a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers. That is, masks the port number of the host with another port number.

If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

**8. what is gateway address?**

A gateway address is a node’s IP address on a computer network, a key stopping point for data coming to or going to other networks. In a workplace, the gateway is the computer that routes traffic from a workstation to the external network that serves the web pages. An entryway is a system hub utilized in broadcast communications that interfaces two systems with various transmission conventions. Gateways serve as entry and exit points for a network because all data must pass through or communicate with the gateway before it can be routed.

**9. what is loopback address?**

A loopback address is a distinct reserved IP address range that starts from 127.0.0.0 ends at 127.255.255.255 though 127.255.255.255 is the broadcast address for 127.0.0.0/8. The loopback addresses are built into the IP domain system, enabling devices to transmit and receive the data packets. The loopback address 127.0.0.1 is generally known as localhost.

**10. different type of ipv6 address.**

**Types of IPv6 addresses :** There are different types and formats of IPv6 addresses, of which, it's notable that there are no broadcast addresses in IPv6. Some examples of IPv6 formats include :

1. **Global unicast:** These addresses are routable on the internet and start with "2001:" as the prefix group. Global unicast addresses are the equivalent of IPv4 public addresses.

1. **Unicast address:** Used to identify the interface of an individual node.

1. **Anycast address:** Used to identify a group of interfaces on different nodes.

1. **Multicast address:** An address used to define multicast, Multicasts are used to send a single packet to multiple destinations at one time.

1. **Link local addresses :** One of the two internal address types that are not routed on the internet. Link local addresses are used inside an internal network, are self-assigned and start with "fe80:" as the prefix group.

1. **Unique local addresses:** This is the other type of internal address that is not routed on the internet. Unique local addresses are equivalent to the IPv4 addresses 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16.

**11. ipv6 tunnelling**

IPv6 Tunneling is a mechanism for encapsulating IPv6 packets within a site-to-site IPv6 VPN. It is used to form a virtual point-to-point link between two IPv6 nodes. IPv6 Tunnels are stateless and have no knowledge of the configuration or even existence of the remote tunnel endpoint. Once an IPv6 Tunnel is configured, packets are encapsulated and forwarded regardless of whether the decapsulating device is present or not.

IPv6 Tunneling allows hosts in one private IP network to communicate with hosts in another private IP network by providing a tunnel between two routers across the Internet. The IPv6 tunnel connection endpoints are terminated via a Virtual Tunnel Interface (VTI) configured in each device.

**• Practical**

l 1. Configure ipv6address manually and test with ping

DONE

1. IPv6addressautomatically

DONE

1. ping utility

DONE

1. ipconfig

DONE

1. tracert / traceroute

DONE

1. dhcpv6

DONE

# Topic : DFS

**1. what is DFS? And purpose of DFS**

A distributed file system (DFS) is a file system that is distributed on various file servers and locations. It permits programs to access and store isolated data in the same method as in the local files. It also permits the user to access files from any system. It allows network users to share information and files in a regulated and permitted manner. Although, the servers have complete control over the data and provide users access control.

DFS's primary goal is to enable users of physically distributed systems to share resources and information through the Common File System (CFS)**.** It is a file system that runs as a part of the operating systems. Its configuration is a set of workstations and mainframes that a LAN connects. The process of creating a namespace in DFS is transparent to the clients.

DFS has two components in its services, and these are as follows :

* 1. **Local Transparency :** It is achieved via the namespace component.
  2. **Redundancy :** It is achieved via a file replication component.

**2. Define DFS namespace and DFS replication**

DFS Namespaces and DFS Replication are role services in the File and Storage Services role.

**DFS Namespaces** : Enables to group shared folders that are located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders. There are two ways in which DFS can be implemented:

* + Standalone DFS namespace
  + Domain-based DFS namespace

**DFS Replication** :

DFS Replication is a role service in Windows Server that enables you to efficiently replicate folders (including those referred to by a DFS namespace path) across multiple servers and sites. DFS Replication is an efficient, multiple-master replication engine that you can use to keep folders synchronized between servers across limited bandwidth network connections. It replaces the File Replication Service (FRS) as the replication engine for DFS Namespace.

* Active Directory Domain Services (AD DS) uses DFS Replication for replicating the SYSVOL folder in domains that use the Windows Server 2008 or later domain functional level.
* DFS Replication uses a compression algorithm known as remote differential compression (RDC). RDC detects changes to the data in a file and enables DFS Replication to replicate only the changed file blocks instead of the entire file.

**3. what is folder target?**

A folder target is the Universal Naming Convention (UNC) path of a shared folder or another namespace that is associated with a folder in a namespace. Adding multiple folder targets increases the availability of the folder in the namespace.

**• Practical**

1. install DFS namespace and replication

DONE

1. configure common name space

DONE

1. configure replication and check

DONE

1. configure branch cache

DONE

# Advance Network

**1. what is SDN?**

Software-Defined Networking (SDN) is an approach to networking that uses softwarebased controllers or application programming interfaces (APIs) to communicatewith underlying hardware infrastructure and direct traffic on a network.

This model differs from that of traditional networks, which use dedicated hardware devices (i.e., routers and switches) to control network traffic. SDN can create and control a virtual network – or control a traditional hardware – via software.

While network virtualization allows organizations to segment different virtual networks within a single physical network, or to connect devices on different physical networks to create a single virtual network, software-defined networking enables a new way of controlling the routing of data packets through a centralized server.

**2. what is SCVMM?**

System Center Virtual Machine Manager, also known as System Center VMM, is a management tool developed by Microsoft to efficiently manage virtualized environments, particularly as a company's virtual machine and services deployment size increases. It does this by bringing the management and administration of virtual hosts and clusters under a single tool. It helps to provide a unified management experience across on-premises, service provider. VMM capabilities include:

* **Datacenter:** Configure and manage your datacenter components as a single fabric in VMM. Datacenter components include virtualization servers, networking components, and storage resources. VMM provisions and manages the resources needed to create and deploy virtual machines and services to private clouds.
* **Virtualization hosts:** VMM can add, provision, and manage Hyper-V, VMware, and Citrix XenServer virtualization hosts and clusters.
* **Networking:** Add networking resources to the VMM fabric, including network sites defined by IP subnets, virtual LANs (VLANs), logical switches, static IP address and MAC pools. VMM provides network virtualization, including support for creating and manage virtual networks and network gateways. Network virtualization allows multiple tenants to have isolated networks and their own IP address ranges for increased privacy and security. Using gateways, VMs on virtual networks can connect to physical networks in the same site or in different locations.
* **Storage:** VMM can discover, classify, provision, allocate, and assign local and remote storage. VMM supports block storage (fibre channel, iSCSI, and Serial Attached SCSI (SAS) storage area networks (SANs)).
* **Library resources:** The VMM fabric retains a library of file-based and non file-based resources that are used to create and deploy VMs and services on virtualization hosts. File-based resources include virtual hard disks, ISO images, and scripts. Non file-based resources include templates and profiles that are used to standardize the creation of VMs. Library resources are accessed through library shares