**Chapter-3: Advanced DHCP and DNS**

**Q. What is DNSSEC?**

Ans. Domain Name System Security Extensions (DNSSEC) adds security to DNS by enabling DNS servers to validate the responses given by other DNS servers. DNSSEC enables digital signatures to be used with DNS zones.

Or,

DNSSEC adds security to DNS using public key cryptography to sign DNS zones and resource records. When the DNS resolver issues a query for a record in a signed zone, the authoritative DNS server provides both the record and a digital signature that enables validation of that record.

Note:

DNSSEC provides clients with a way of verifying the integrity of the results of a DNS query. DNSSEC accomplishes this by cryptographically signing DNS zone data. When a client queries a record in a zone signed using DNSSEC, the DNS server returns both the record and the digital signature that enables the client to validate that record.

**Q. Which new resource records are created when we sign a zone?**

Ans. When you sign a zone, the following new resource records are created:

1. Resource Record Signature (RRSIG) record
2. DNSKEY
3. Next Secure (NSEC/NSEC3) record

**Q. When we implement DNSSEC which additional cryptographic keys are created?**

Ans. When you implement DNSSEC, the following additional cryptographic keys are created:

1. Trust Anchor
2. Key Signing Key (KSK)
3. Zone Signing Key (ZSK)

**Q. DNS event log:**

The DNS server log is located in the Applications and Services Logs folder in Event Viewer.

A DNS event log records DNS events such as service startup and shutdown as well as errors.

**Q. Write about DNS event log records information.**

Ans. DNS event log records information including:

1. Changes to the DNS service. For example when the DNS server service is stopped or started.
2. Zone loading and signing events.
3. Modifications to DNS server configuration.
4. DNS warning and error events.

By default the DNS server records all these events. It’s also possible to configure the DNS server to only log errors, or errors and warning events.

MCQ:

1. DNSSEC uses public key cryptography to sign DNS zones and resource records.
2. DNSSEC accomplishes this by cryptographically signing DNS zone data.
3. The DNS server log is located in the Applications and Services Logs folder in Event Viewer.
4. By default the DNS server records all events.

**Q. What are GlobalNames Zones?**

Ans. GlobalNames Zones provide single-label name resolution. Single-label name resolution allows  
single names to be translated to IP addresses. GlobalNames Zones are hosted on DNS servers and are intended as a replacement technology for WINS.

**Q.** **What types of DNS records a GlobalName Zone hosts?**

Ans. A GlobalName Zone hosts CNAME, also known as alias, records.

**Q. what is the purpose of global name zones?**

Ans.

* The GlobalNames zone can be replicated like any other DNS zone.

**Consider using GlobalNames Zones in the following circumstances:**

* You need to provide single-label name resolution when your network uses IPv6 addressing.
* WINS does not support IPv6, whereas a single-label record in the GlobalNames Zone are mapped to A or AAAA records, allowing both IPv4 and IPv6 name resolution.
* You need to provide single-label name resolution for a small number of hosts.
* Anadvantage of WINS is that it’s dynamically populated. You must populate the GlobalNames Zone manually by creating CNAME records.

**To deploy the GlobalNames Zone, you need to do the following:**

* Create a new Active Directory integrated forward lookup zone named GlobalNames  
  that you have configured to replicate throughout the forest.
* Manually activate the GlobalNames Zone on each DNS server in the forest by running  
  the following Windows PowerShell command (substituting DNSServerName name for  
  the FQDN of the DNS server):  
  Set-DNSServerGlobalNameZone –ComputerName DNSServerName –Enable $True

**Q. What is DNS socket pool?**

Ans. DNS socket pool is a technology that makes cache-tampering and spoofing attacks more difficult by using source port randomization when issuing DNS queries to remote DNS servers. A DNS server running on Windows Server 2012 uses a socket pool of 2,500 by default.

Or,

The DNS socket pool allows for port randomization with DNS requests as a way of protecting against spoofing attacks. A DNS server running on Windows Server 2012 uses a socket pool of 2,500 by default.

**Q. What is DNS cache locking?**

Ans. DNS Cache Locking blocks a record stored in the DNS server’s cache from being overwritten until a specified percentage of the record’s TTL has expired. By default, the DNS Cache Locking value is set to 100.

**Q. What is DNS recursion?**

Ans. You can enable DNS recursion as a way of hardening a DNS server against attacks that use recursion as a way of denying service.

**Q. What is Netmask ordering?**

Ans. Netmask ordering allows the DNS server to return a DNS record that is on the same IP subnet as the client if such a record exists.

MCQ:-

1. A DNS server running on Windows Server 2012 uses a socket pool of 2,500 by default.
2. You can use the **dnscmd** command-line tool to vary the socket pool between 0 and 10,000.
3. You must restart the DNS service before the reconfigured socket pool size is used.
4. By default, the DNS Cache Locking value is set to 100, but you can reset it using the  
   Set-DNSServerCache cmdlet with the LockingPercent option.
5. You can disable recursion on the Advanced tab of the DNS server’s properties
6. Netmask ordering is enabled by default on Windows Server 2012 DNS servers. You can  
   verify that netmask ordering is enabled by viewing the advanced properties of the DNS server

**Delegated administration:**

By default, members of the Domain Admins group are able to perform all DNS administration tasks on DNS servers within a domain. Members of the Enterprise Admins group are able to perform all DNS administration tasks on any DNS server in the forest.

**Q. What is Superscope?**

Ans. A superscope is a collection of individual DHCP scopes. You might create a superscope when  
you want to bind existing scopes together for administrative reasons.

**Q. What is multicast scope?**

A multicast address is one that allows one communication too many on a network. When you use multicast, multiple hosts on a network listen for traffic on a single multicast IP address.

Or, Multicast scopes enable you to provide multicast address ranges to applications that require multicast addresses.  
  
**Q. What is the range of multicast IP addresses in IPv4?**  
Ans. Multicast IP addresses are in the range 224.0.0.0 through to 239.255.255.255

**Q. What is MADCAP ?**

Multicast scopes are also known as MADCAP (Multicast Address Dynamic Client Allocation Protocol) scopes as applications that require access to multicast addresses support the MADCAP application programming interface (API).

**Note**: Windows Deployment Services (WDS) server with its own set of multicast addresses, and you don’t need to configure a special multicast scope in DHCP to support this role.

**Split Scope**

**Q. What is split Scope?**

Split scope is one method of providing fault tolerance for a DHCP scope. The idea behind a split scope is that you host one part of the scope on one DHCP server and a second smaller part of the scope on a second DHCP server.

Or, Split scopes enable you to host parts of the same scope on different DHCP servers. Split scopes provide high availability if DHCP servers don’t run the Windows Server 2012 operating system.

**Q. How it works?**

This split has 80% of the addresses on the first DHCP server and 20% of the addresses on the partner server. In this scenario, the DHCP server that hosts the 20% portion of the address space is usually located on a remote subnet.

**Q. What is Name Protection?**

DHCP Name Protection is a feature that enables you to ensure that the host names that a DHCP server registers with a DNS server are not overwritten in the event that a non-Windows operating system has the same name. DHCP Name Protection also protects names from being overwritten by hosts that use static addresses that conflict with DHCP-assigned addresses.

Or, Name protection enables you to configure DHCP so that names registered on behalf of Windows clients in DNS can’t be overwritten by hosts using non-Microsoft operating systems.

**Q. What is DHCP failover?**

Ans. DHCP failover enables you to configure DHCP to be highly available without using split scopes. DHCP failover is a feature (technology) new to Windows Server 2012. You have two options when configuring DHCP failover: (i) Hot Standby mode and (ii) Load Sharing mode.

Or, DHCP failover is a technology new to Windows Server 2012. It enables DHCP servers to be configured in a partner relationship. You have two options when configuring DHCP failover: (i) Hot Standby mode and (ii) Load Sharing mode.

**Q. Write the difference between Hot Standby mode and Load Sharing mode.**

Ans. In hot standby mode, one DHCP server serves as a hot standby for another server, only taking over if the first server becomes unavailable. The default value is 5% of the address ranges to be reserved on the standby server. The default value for the state switchover interval is 60 minutes.

In load sharing mode, the DHCP servers share IP address allocation duties for the same scope. The default is for each server to share 50% of the load.

MCQ

You want to make a DHCP scope highly available so that clients can still obtain address  
leases if one of these DHCP servers fail. Which of the following strategies should you  
implement to accomplish this goal?  
A. Configure DHCP failover. Use Hot Standby mode.  
B. Configure DHCP failover. Use Load Sharing mode.  
**C. Configure a split scope.**  
D. Configure a superscope.

**Q. What is IPAM?**

Ans: Internet Protocol address management (IPAM) is a method of tracking and modifying the information associated with a network's Internet Protocol address (IP address) space.

IPAM is a technology new to Windows Server 2012 that simplifies the process of managing multiple DHCP and DNS servers.

Or,

IPAM is a technology new to Windows Server 2012 that enables you to centralize the management of DHCP and DNS servers. Rather than managing each server separately, you can use IPAM to manage them from a single console.

Note:

1. IPAM enables you to centralize the management of DHCP and DNS servers.
2. You can use a single IPAM server to manage up to 150 separate DHCP servers and up to 500 individual DNS servers.
3. A single IPAM server is able to manage 6,000 separate DHCP scopes and 150 separate DNS zones.
4. You can only install the IPAM feature on a computer that is a member of an Active Directory domain.
5. IPAM is also not supported on computers that host the Domain Controller server role.
6. You should not deploy a DNS or DHCP server on the IPAM server if you want to manage those servers using IPAM.
7. IPAM is also limited so that you can only use it to manage DHCP and DNS servers that are members of the same Active Directory forest.
8. You can’t use IPAM to manage standalone servers or servers that are members of different forests.
9. If you use the GPO prefix IPAM, the three GPOs are named:

■ IPAM\_DC\_NPS

■ IPAM\_DHCP

■ IPAM\_DNS

1. Managing the IP address space: The benefit of IPAM is that it enables you to manage all of the IP addresses in your organization.
2. IPAM administration: You can delegate administrative permissions by adding user accounts to one of five local security groups on the IPAM server:

■ **IPAM Users:** Members of this group are able to view IPAM server information such as address space and operational event information, but they are unable to view IP address tracking information.  
■ **IPAM MSM Administrators:** MSM stands for Multi-Server-Management. They have read-only access to the IP address space. They are unable to view or perform IP address tracking tasks.  
■ **IPAM ASM Administrators** ASM stands for Address Space Administrator. They are also able to manage the IP address space. They cannot perform monitoring tasks and are unable to perform IP address tracking tasks.  
■ **IPAM IP Audit Administrators** Members of this group are able to manage server inventory and perform common management tasks, but they have read-only access to the IP address space and IP address tracking information.  
■ **IPAM Administrators** Members of this group are able to perform all tasks on the  
IPAM server including viewing IP address tracking information.

**Q. What is the work of IPAM?**

Ans. We can perform tasks such as creating address scopes, configuring address reservations, and managing DHCP and DNS options globally, rather than having to perform these tasks on a server-by-server basis.  
You can also use IPAM to search stored IP address lease data, MAC address data, and corresponding user sign on and sign off information.

**Q. What is IP Address tracking?**

Ans. IP address tracking enables you to figure out which user was associated with a specific IP address at a particular point of time, something that can be important when trying to determine the cause of unauthorized activity on the organizational network.

Or, You can use IP address tracking to search the IPAM database at a particular point of time on the basis of IP address, MAC address, computer name, or user name.

**Q. Write the parameters to track IP address records.**

You can search for IP address records using one of the following four parameters:

1. **Track by IP Address:** Track by IPv4 address, but IPAM does not support tracking on the basis of IPv6 address.
2. **Track by Client ID:** Track IP address activity on the basis of media access control (MAC) address.
3. **Track by Host Name:** Track by the computer’s name as registered in DNS.
4. **Track by User Name:** Track a user name by providing a host name.

**IPAM administration:** Members of the Domain Admins and Enterprise Admins groups have full administrative access to the IPAM server. There are five local security groups on the IPAM server that  
you can use to delegate administrative privileges.

**Q. Write the five local security groups to delegate administrative permissions on the IPAM server.**

Ans. The five local security groups to delegate administrative permissions on the IPAM server are:

1. IPAM Users
2. IPAM MSM Administrators
3. IPAM ASM Administrators
4. IPAM IP Audit Administrators
5. IPAM Administrators