**15\_SAS On IPv4 and IPv6**

**Self-Assessment Sheet**

1. How many bits are in an IPv4 address?

32

2. How many bits are in an IPv6 address?

128

3. What are the first 64 bits in an IPv6 address?

*In an IPv6 address, the first 64 bits represent the network prefix, while the remaining 64 bits represent the interface identifier (also known as the host portion). This division is a fundamental aspect of IPv6 addressing and is based on the recommendation in RFC 4291, which defines IPv6 addressing architecture.*

4. What are the second 64 bits in an IPv6 address?

*In an IPv6 address, the second 64 bits represent the Interface Identifier or host portion. This portion uniquely identifies a specific interface (host) on the network. Unlike IPv4, where the host portion varies in size depending on the subnet mask, IPv6 reserves a fixed 64 bits for the interface identifier.*

5. What is the highest possible digit/number for each byte in an IPv4 address?

*In an IPv4 address, each byte consists of 8 bits, allowing for a total of 256 possible values (2^8). However, since the counting starts from zero, the highest possible value for each byte in an IPv4 address is 255. Therefore, the decimal range for each byte in an IPv4 address is from 0 to 255.*

6. What settings to check when troubleshooting IPv4?

*When troubleshooting IPv4 connectivity issues, there are several settings and configurations that you should check. Here are some key settings to investigate:*

*IP Address Configuration:*

*Check the IP address configuration of the device (e.g., computer, router, server). Ensure that it has been assigned a valid IPv4 address, subnet mask, default gateway, and DNS server addresses.*

*Verify that the IP address is within the correct range for the network and that it is not conflicting with any other device on the network.*

*Subnet Mask:*

*Verify that the subnet mask is configured correctly. It should match the subnet mask used by other devices on the same network segment.*

*An incorrect subnet mask can lead to communication issues, such as the inability to reach devices on other subnets.*

*Default Gateway:*

*Confirm that the default gateway (router) address is configured correctly. The default gateway is used to send traffic to destinations outside the local subnet.*

*Ensure that the default gateway is reachable and properly configured to forward traffic to the correct destinations.*

*DNS Configuration:*

*Check the DNS server settings to ensure that the device can resolve domain names to IP addresses.*

*Verify that the DNS server addresses are correctly configured and reachable. Incorrect DNS settings can prevent access to websites and other network resources by domain name.*

*Network Connectivity:*

*Test network connectivity by pinging the local host (127.0.0.1) and the default gateway. This helps determine whether the network interface is functioning correctly.*

*Use the ping command to test connectivity to other devices on the local network and to remote hosts by IP address.*

*Firewall and Security Settings:*

*Check firewall settings to ensure that they are not blocking necessary traffic, such as ICMP (ping) or specific ports required for network services.*

*Review security policies and access control lists (ACLs) to identify any restrictions that may be affecting network traffic.*

*IP Conflict Detection:*

*Look for signs of IP address conflicts, such as duplicate IP addresses or network errors indicating address conflicts.*

*Use tools like ARP (Address Resolution Protocol) tables to detect duplicate IP addresses on the network.*

*Routing Tables:*

*Review the routing table to ensure that routes are configured correctly and that traffic is being forwarded to the appropriate destinations.*

*Check for any incorrect or missing routes that may be causing connectivity issues.*

*By checking these settings and configurations, you can identify and resolve common IPv4 connectivity issues effectively. If necessary, consult network documentation, contact your network administrator, or use network diagnostic tools for further troubleshooting.*

7. What is Dynamic Host Configuration Protocol (DHCP)?

*DHCP stands for Dynamic Host Configuration Protocol. It is a network protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network. DHCP simplifies the process of IP address management by dynamically allocating IP addresses to devices as they connect to the network, instead of requiring manual configuration of each device.*

8. What port does a device use to broadcast to a DHCP server?

*Devices use UDP (User Datagram Protocol) as the transport protocol for DHCP (Dynamic Host Configuration Protocol) communications. DHCP clients broadcast DHCP discover messages to discover available DHCP servers on the network. These discovered messages are sent to the destination IP address 255.255.255.255, which is the limited broadcast address, and to the destination port number 67.*

*So, to specifically answer your question, devices use port 67 (UDP) to broadcast DHCP discover messages.*

9. What port does DHCP server use to broadcast to a device?

*To summarize, the DHCP server uses port 67 (UDP) to send DHCP offer messages to clients, and clients use port 68 (UDP) to receive these messages from the DHCP server.*

10. What is a subnet mask?

*A subnet mask is a 32-bit number used in conjunction with an IP address to divide the IP address into network and host portions. It helps identify the network portion of an IP address and the host portion of the IP address. The subnet mask contains a series of contiguous binary 1s followed by contiguous binary 0s.*

*In IPv4, the subnet mask is expressed in dotted decimal notation, similar to an IP address. It consists of four octets (32 bits), where each octet represents eight bits. A subnet mask of 255.255.255.0, for example, indicates that the first 24 bits (or 3 octets) represent the network portion, and the remaining 8 bits (or 1 octet) represent the host portion.*

*The subnet mask is used in conjunction with the IP address to perform bitwise AND operation, resulting in the network address. The network address identifies the specific network to which the device belongs. The host portion of the IP address identifies the specific device (host) within that network.*

*Here's an example to illustrate how a subnet mask works:*

*IP Address: 192.168.1.100*

*Subnet Mask: 255.255.255.0*

*Performing a bitwise AND operation between the IP address and subnet mask:*

*yaml*

*Copy code*

*IP Address: 11000000.10101000.00000001.01100100*

*Subnet Mask: 11111111.11111111.11111111.00000000*

*Result: 11000000.10101000.00000001.00000000 (192.168.1.0)*

*In this example, the network portion of the IP address is 192.168.1, and the host portion is 100.*

*In summary, a subnet mask is used to determine the network and host portions of an IP address, enabling proper routing and communication within a network. It plays a crucial role in IP address allocation and network configuration.*

11. What is a default gateway?

*A default gateway is a network device (usually a router) that serves as an entry and exit point for traffic between a local network (LAN) and external networks such as the internet. It acts as a gateway or intermediary device that forwards packets from devices on the local network to destinations outside the local network and vice versa.*

*Here's how a default gateway works:*

*Outgoing Traffic: When a device on the local network wants to communicate with a device on an external network (e.g., accessing a website on the internet), it sends the data packets to the default gateway.*

*Routing Decision: The default gateway examines the destination IP address of the packets and makes a routing decision based on its routing table. If the destination is on a remote network, the default gateway forwards the packets to the appropriate network segment.*

*Internet Access: If the destination IP address is outside the local network (i.e., not within the subnet defined by the subnet mask), the default gateway forwards the packets to the internet through an upstream router or internet service provider (ISP).*

*Incoming Traffic: When responses or data packets from external networks are received by the default gateway, it forwards them to the appropriate device on the local network based on the source IP address of the packets.*

*In summary, a default gateway serves as the bridge between a local network and external networks, facilitating communication between devices on the local network and devices/services outside the local network. It is a critical component of network connectivity and internet access for devices connected to a LAN.*