**5.1.1-2 IP Configuration:**

IP Addresses operate at Layer 3, the Network layer. Unique hosts are assigned unique IP addresses. Each portion of an IP address is an octet made up of 8 bits. Subnet masks also have 4 octets, where first 2 identify the subnet and the second 2 identify host.

|  |  |  |
| --- | --- | --- |
|  | Default Example | Custom Example |
| Network Address | 188.50.0.0 | 188.50.0.0 |
| Subnet Mask | 255.255.0.0 | 255.255.255.0 |
| # of Subnet Addresses | One | 254 |
| # of Hosts per Subnet | 65,534 | 254 per subnet |
| Subnet Address(es) | 188.50.0.0 (only one) | 188.50.1.0 188.50.2.0 188.50.3.0 (and so on) |
| Host Address Range(s) | 188.50.0.1 to 188.50.255.254 | 188.50.1.1 to 188.50.1.254 188.50.2.1 to 188.50.2.254 188.50.3.1 to 188.50.3.254 (and so on) |

IP Address Classes:

**A:** 1-126 Subnet-255.0.0.0 **B:** 128-191 Subnet-255.255.0.0 **C:** 192-223 Subnet-255.255.255.0 **D:** 224-239 (Multicast, with multiple hosts on same IP) **E:** 240-255 (experimental)

**5.1.3-4 Subnetting:**

**Subnetting is process of dividing a large network into smaller networks called subnets.** 255 Is a Broadcast address so 254 is highest value available.

Subnetting is the process of dividing a large network into smaller networks called subnets. When you subnet a network, each network segment has a different network address (also called a subnet address). In practice, the terms network and subnet are used interchangeably to describe a physical network segment with a unique network address.

* Increase the number of devices that can be added to the LAN (to overcome the architecture limits),
* Decrease the number of devices on a single subnet (to reduce traffic congestion)
* Reduce the processing load placed on computers and routers
* Isolate sensitive systems on the network

Subnetting is also used to efficiently allocate available IP addresses. For example, an organization with a class B network ID is allocated enough addresses for 65,536 hosts. However, if the organization in practice uses only 10,000 of those host IDs, over 55,000 IP addresses are going unused. Subnetting provides a way to break the single class B network ID into multiple smaller network IDs.

* Subnetting uses custom subnet masks instead of the default subnet masks (e.g., using 255.255.255.0 with a Class B address instead of the default 255.255.0.0).

The following table shows how a Class B address can be subnetted to provide additional subnet addresses. Notice that by using a custom subnet mask, the Class B address looks like a Class C address.

While subnetting divides a large address space into multiple subnets, supernetting combines multiple small network addresses into a single larger network. Supernetting allows multiple Class C addresses to be combined into a single network.

**5.1.9 IP Address Assignment/Facts:**

Static and Dynamic IP Assignment can be used.

DHCP allows for clients to lease IP addresses, and the DHCP server automatically configures the client’s connection. Static assignment opens up the opportunity for mistakes and misconfiguration as clients are not automatically configured.

An IP Helper can be used to configure DHCP on other routers on same network.

When dealing with Subnetting a network. Focus on how many subnets are to be created, and then divide the last octet into that number.

**5.2 Alternative IP Addressing**

APIPA is Automatic Private IP Addressing. APIPA ranges from 169.254.0.0 – 169.254.255.254

After machine assigns itself an APIPA host address, it then sends out an ARP request to make sure that no other devices assigned themselves that same address.

If a host is configured to obtain its IP address from a DHCP server but that server is unreachable, then an alternate IP address assignment method may be employed. These are as follows:

|  |  |
| --- | --- |
| Method | Description |
| Automatic Private IP Addressing (APIPA) | APIPA provides an option for automatic IP address assignment without a DHCP server. APIPA is enabled by default on most modern operating systems, including Windows and Linux.  Using APIPA, hosts can assign themselves an IP address on the 169.254.0.0 network (with a mask of 255.255.0.0) if they can't locate a DHCP server. If a network host is configured to use dynamic IP addressing and a DHCP server can't be contacted, APIPA assigns a temporary IP address to the host. However, only the IP address and mask are assigned. Default gateway and DNS server addresses are not assigned. For this reason, APIPA can be used only to enable communications within a single subnet. Communication with other networks, including the Internet, will not be possible. In addition, communication with network infrastructure devices that use static IP addressing, such as servers, will not be possible even if they are on the same local subnet as the APIPA host. |
| Alternate IP Configuration | With an alternate IP configuration, static IP configuration values are used if a DHCP server cannot be contacted. When you configure an alternate IP address, APIPA is automatically disabled. It is recommended that, instead of APIPA, you use an alternate IP configuration, because it allows hosts to access other systems on the local subnet and on other networks, including the Internet. It also allows continued access to servers and other network infrastructure devices that use static IP addresses. |

**5.3 Configuring a DHCP Server**

In Windows Server 2012, a wizard is made available for users to configure DHCP services simply.

Remove Server Bindings to stop a server that also acts as a router from being a rogue DHCP server on the internet.

Afterwards, must create a scope that will be allowed to hand out addresses on the subnet. All addresses from 1-254 can be assigned (0 is router add, and 255 is broadcast). Exclusions can be made available to stop the server from handing out certain addresses.

To configure a scope, go to tools, then DHCP. Servers may have Hyper-V machines running alongside the server,

Right clicking on server options brings up options to enable or disable for the server.

The Dynamic Host Configuration Protocol (DHCP) centralizes management of IP addressing in a network by allowing a server to dynamically assign IP addresses to clients. DHCP also allows mobile users, who move from network to network, to easily obtain an IP address appropriate for each network they connect to.

|  |  |
| --- | --- |
| Broadcast | Description |
| DHCP Discover (D) | The client begins by sending out a DHCP Discover frame to identify DHCP servers on the network. |
| DHCP Offer (O) | A DHCP server that receives a Discover request from a client responds with a DHCP Offer advertisement, which contains an available IP address. If more than one DHCP server responds with an offer, the client usually responds to the first offer that it receives. |
| DHCP Request (R) | The client accepts the offered address by sending a DHCP Request back to the DHCP server. If multiple offers were sent, the DHCP Request message from the client also informs the other DHCP servers that their offers were not accepted and the IP addresses contained in their offers can be made available to other clients. |
| DHCP ACK (A) | The DHCP server responds to the request by sending a DHCP ACK (acknowledgement). At this point, the IP address is leased to and configured on the DHCP client. |

Because a DHCP client doesn't have an IP address when it initially boots, it must use broadcast frames to communicate with a DHCP server. The table below describes the method used to obtain an address from a DHCP server:

If the DHCP server is on a different subnet, additional configuration steps are required, since the DHCP broadcast frames are dropped by network routers by default.

Keep in mind the following when configuring a DHCP Server:

* The DHCP service needs to auto start when the server boots.
* It must have a static IP address.

For a DHCP server to deliver IP addresses, it must have a scope configured. A scope is the range of IP addresses that the DHCP server can assign to clients. When working with scopes, remember the following:

* There should be only one scope per network segment.
* The scope must be activated before the DHCP server can assign addresses to clients. After you activate a scope, you should not change it.
* A scope has a subnet mask that determines the subnet for a given IP address. You cannot change the subnet mask of an existing DHCP scope; to change the subnet mask used by a scope, you must delete and recreate the scope.
* Lease duration values are part of the scope properties, and they determine the length of time a client can use an IP address leased through DHCP.

In addition to providing IP addresses, a DHCP server can also provide clients with additional IP configuration parameters using options. Commonly used DHCP options include the subnet mask, the default gateway address, and a DNS server address. The following three levels of options can be configured:

* Server options are applied to all computers that get an IP address from the DHCP server, regardless of which scope they obtain the address from. (e.g., if your organization has only one DNS server, then all DHCP clients need the same DNS server address.)
* Scope options are applied to all computers that get an IP address from a particular scope on the DHCP server. (e.g., because scopes are associated with specific subnets, each scope needs to be configured with the appropriate default gateway address option.)
* Client options are applied to a specific DHCP client. The client's MAC address is used to identify which system receives the option.

The DHCP console provides context-sensitive icons to reflect DHCP server status as follows:

* A check mark in a green circle indicates that the DHCP server is connected and authorized.
* A red down arrow indicates that the DHCP server is connected but not authorized.
* A horizontal white line inside a red circle indicates that the DHCP server is connected, but the current user does not have the administrative credentials necessary to manage the server.
* An exclamation point inside a yellow triangle indicates that 90% of available addresses for server scopes are either in use or leased.
* An exclamation point inside a blue circle indicates that 100% of available addresses for server scopes are either in use or leased.

Because a DHCP client doesn't have an IP address assigned when it initially boots, it must use broadcast frames to communicate with a DHCP server. If the server is on a different subnet from the client, then the DHCP requests sent by the client will not be able to reach the server, because broadcast frames are dropped by network routers. If your network is configured in this manner, you can implement one of the following mechanisms to forward DHCP broadcasts through network routers to a remote DHCP server on a different subnet:

|  |  |
| --- | --- |
| Option | Description |
| RFC 1542 Compliant Router | An RFC 1542 compliant router listens for DHCP traffic and routes any received DHCP frames to the appropriate subnet. For example, on a Cisco router, you can enable this functionality by using the ip helper-address command. The syntax is:  ip helper-address [server\_address]  Replace [server\_address] with the IP address of the remote DHCP server. |
| DHCP Relay Agent | If you are using a Windows server in your network, then you can install the Routing and Remote Access service (RRAS) role on the server and enable the DHCP Relay Agent role service. The DHCP Relay Agent sends the DHCP packets it receives to a remote DHCP server on a different subnet. To configure the DHCP Relay Service, you must do the following:   * Specify which server network interface the agent listens on for DHCP messages. * Specify the IP address of the remote DHCP server where the agent should forward DHCP messages to. |

**5.5 DNS Resolution**

DNS is a system by which logical names are translated to actual IP addresses on the web. DNS servers handle requests for name->ip translations.

**5.6 IP Version 6**

Dual stack is where a server is configured to handle both IPv4 and IPv6 packets. Packets can be encapsulated as IP

Teredo is a host to host tunneling protocol that handles encapsulation and decapsulation

Miredo is a host to host tunneling protocol used on Linux systems that handles.

6to4 tunneling can be used between IPv6 and IPv6 networks. The routers must be dual stack and will convert IPv6 to IPv4 so that it can be transferred across a network.

4to6 tunneling can be used with IPv6 and IPv6 networks. The routers must be dual stack and will convert IPv6 to IPv4 so that it can be transferred across a network.

The addresses available under the current IPv4 addressing standard have been exhausted. In response to this situation, a new IP addressing system (IP version 6, or IPv6) has been developed. An IPv6 address is a 128-bit binary number. A sample IPv6 IP address looks like the following: 35BC:FA77:4898:DAFC:200C:FBBC:A007:8973.

The following list describes the features of an IPv6 address:

* It is made up of 32 hexadecimal numbers organized into 8 quartets.
* The quartets are separated by colons.
* Each quartet is represented as a hexadecimal number between 0 and FFFF. Each quartet represents 16 bits of data (FFFF = 1111 1111 1111 1111).
* Leading zeros can be omitted in each section. For example, the quartet 0284 could also be written as 284.
* An address with consecutive zeros can be expressed more concisely by substituting a double colon for the group of zeros. For example:
  + FEC0:0:0:0:78CD:1283:F398:23AB
  + FEC0::78CD:1283:F398:23AB (concise form)

This is also called address compression. Address compression is when you take a fully-notated IPv6 address and remove empty octets from it, replacing them with a colon.

* If an address has more than one consecutive location where one or more quartets are all zeros, only one location can be abbreviated. For example, FEC2:0:0:0:78CA:0:0:23AB can be abbreviated as:
  + FEC2::78CA:0:0:23AB  
    or
  + FEC2:0:0:0:78CA::23AB  
    but not
  + FEC2::78CA::23AB
* The 128-bit address contains two parts:

|  |  |
| --- | --- |
| **Component** | **Description** |
| Prefix | The first 64 bits are known as the *prefix*.   * + The prefix can be divided into various parts that identify things such as geographic region, the ISP, the network, and the subnet.   + The *prefix length* identifies the number of bits in the relevant portion of the prefix. To indicate the prefix length, add a slash (/) followed by the prefix length number. Full quartets with trailing 0s in the prefix address can be omitted (e.g., 2001:0DB8:4898:DAFC::**/**64).   + Because addresses are allocated based on physical location, the prefix generally identifies the location of the host. The 64-bit prefix is often referred to as the *global routing* prefix. |
| Interface ID | The last 64 bits are known as the *interface ID*. This is the unique address assigned to an interface.   * + Addresses are assigned to interfaces (network connections), not to the host. Technically, the interface ID is not a host address.   + In most cases, individual interface IDs are not assigned by ISPs but are rather generated automatically or managed by site administrators.   + Interface IDs must be unique within a subnet, but they can be the same if they are on different subnets.   + On Ethernet networks, the interface ID can be automatically derived from the MAC address. Using the automatic host ID simplifies administration.   To ensure that the interface ID is unique for every host on the network, IPv6 uses the Extended Unique Identifier 64 (EUI-64) format. The following are some details of the EUI-64 format:   * + Each host has a unique 48-bit hardware address called a *MAC address* (also called the *burned-in*address) that is assigned to each device by the vendor. The MAC address is guaranteed to be unique through design. The EUI-64 format uses the unique MAC address by:     1. Splitting the MAC address into 24-bit halves.     2. Inserting 16 bits (represented by hex FFFE) between the two halves.   For example, a host with a MAC address of 20-0C-FB-BC-A0-07 would start with the following EUI-64 interface ID: 200C:FB**FF**:**FE**BC:A007.   * + 1. To be complete, the EUI-64 format requires setting the seventh bit in the first byte to binary 1 (reading from left to right, this is the second hex value in the interface ID). This bit is called the *universal/local (U/L) bit*.        - When the U/L bit is set to 0, the MAC address is a burned-in MAC address.        - When the U/L bit is set to 1, the MAC address has been configured locally. EUI-64 requires the U/L bit to be set to 1.   Review the following examples:   * + - * 200C:FBFF:FEBC:A007 (Incorrect interface ID, as the U/L bit is still set to 0)       * 220C:FBFF:FEBC:A007 (Correct interface ID) |

IPv6 adds the following features not included in IPv4:

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Auto-configuration | Because hardware IDs are used for node IDs, IPv6 nodes simply need to discover their network IDs. This can be done by communicating with a router. |
| Built-in Quality of Service | Built-in support for bandwidth reservations makes guaranteed data transfer rates possible. (Quality of service features are available as add-ons within an IPv4 environment but are not part of the native protocol.) |
| Built-in Security Features | IPv6 has built-in support for security protocols such as IPsec. (IPsec security features are available as add-ons within an IPv4 environment.) |
| Source Intelligent Routing | IPv6 nodes have the option to include addresses that determine part or all of the route a packet will take through the network. |

In IPv6, addresses are assigned to interfaces (network connections). All interfaces are required to have an IPv6 address, and each interface can have more than one IPv6 address. IPv6 defines the following types of addresses:

|  |  |  |
| --- | --- | --- |
| **Address Type** | **Description** | |
| Unicast | *Unicast* addresses are assigned to a single interface, for the purpose of allowing that one host to send and receive data. Packets sent to a unicast address are delivered to the interface identified by that address.  Three types of unicast IPv6 addresses are as follows: | |
| Link-local | *Link-local* addresses (also known as *local link* addresses) are addresses that are valid on only the current subnet. Details include the following:   * Link-local addresses have an FE80::/10 prefix. This includes any address beginning with FE8, FE9, FEA, or FEB. * All nodes must have at least one link-local address, although each interface can have multiple addresses. * Link-local addresses are used for automatic address configuration, for neighbor discovery, or for subnets that have no routers.   Do not use link-local IPv6 addressing on routed networks. Routers never forward packets destined for link-local addresses to other subnets. |
| Unique local | *Unique local* addresses are private addresses used for communication within a site or between a limited number of sites. In other words, unique local addressing is commonly used for network communications that do not cross a public network; they are the equivalent of private addressing in IPv4. Details include the following:   * Because unique local addresses are not registered with IANA, they cannot be used on a public network (such as the Internet) without address translation. * Addresses beginning with a prefix of FC00 or FD00 are unique local addresses. * Following the prefix, the next 40 bits are used for the Global ID. The Global ID is generated randomly, creating a high probability of uniqueness on the entire Internet. * Following the Global ID, the remaining 16 bits in the prefix are used for subnet information. * Unique local addresses are likely to be globally unique, but they are not globally routable. Unique local addresses might be routed between sites by a local ISP.   The process for designing a network addressing scheme when using unique local addresses is similar to that used for global unicast addresses. The key difference is how the prefix is defined. Because the address range is not registered, a global routing prefix does not have to be requested from an ISP. Instead, each organization defines its own prefix. |
| Global unicast | *Global unicast* addresses are addresses that are assigned to individual interfaces that are globally unique. All IPv6 addresses that haven't been specifically reserved for other purposes are defined as global unicast addresses. The global routing prefix assigned to an organization by an ISP is typically 48 bits long (/48), but it could be as short as /32 or as long as /56, depending on the ISP. All subnet IDs within the same organization must begin with the same global routing prefix, but they must also be uniquely identified using a different value in the subnet field.  Using this addressing scheme allows organizations to define a large number (216) of IPv6 subnets. When designing an IPv6 network, separate IPv6 subnets should be defined by the following:   * Network segments separated by routers * VLANs * Point-to-point WAN links |
| Multicast | *Multicast* addresses represent a dynamic group of hosts. Packets sent to a multicast address are sent to all interfaces identified by that address. If different multicast addresses are used for different functions, only the devices that need to participate in a particular function will respond to the multicast; devices that have no need to participate in the function will ignore the multicast. Details include the following:   * All multicast addresses have an FF00::/8 prefix. * Multicast addresses that are restricted to the local link have only an FF02::/16 prefix. Packets starting with FF02 are not forwarded by routers. * Multicast addresses with an FF01::/16 prefix are restricted to a single node.   The following are well-known multicast addresses:   * FF02::1 is for all nodes on the local link. This is the equivalent of the IPv4 subnet broadcast address. FF01::1 is for all interfaces on a node. * FF02::2 is for all routers on the local link. FF01::2 is for all routers on node-local. * FF02::1:2 is for all DHCP servers or DHCP relay agents on the local link. DHCP relay agents forward these packets to other subnets.   There are no broadcast addresses in IPv6. IPv6 multicast addresses are used instead of broadcast addresses. | |
| Anycast | The *anycast* address is a unicast address that is assigned to more than one interface, typically belonging to different hosts. An anycast packet is routed to the nearest interface having that address (based on routing protocol decisions). Details include the following:   * An anycast address is the same as a unicast address. Assigning the same unicast address to more than one interface makes it an anycast address. * You can have a link-local, unique local, or global unicast anycast address. * When you assign an anycast address to an interface, you must explicitly identify the address as an anycast address (to distinguish it from a unicast address). * Anycast addresses can be used to locate the nearest server of a specific type (e.g., the nearest DNS or network time server). | |
| Loopback | The local loopback address for the local host is 0:0:0:0:0:0:0:1 (also identified as ::1 or ::1/128). The local loopback address is not assigned to an interface. It can be used to verify that the TCP/IP protocol stack has been properly installed on the host. | |

Unicast:

* Dig is a command utility used on Linux systems. Nslookup is generally used on Windows systems.