Book reference:

1. Chapter 5 from tcp/ip or, ccna book

2. Abdus sattar slide( note is in copy)

Subnetting:(from chatgpt)

Certainly! Subnetting is a way to divide a larger computer network into smaller, more manageable parts called subnets. Think of it like dividing a big neighborhood into smaller blocks, each with its own unique addresses and houses. Subnetting helps make networks more organized, efficient, and secure. Here's a simple breakdown:

Subnet:

* A subnet is like a smaller neighborhood within a larger one.
* It has its own range of IP addresses for devices, like houses in a neighborhood.
* Devices in the same subnet can communicate directly with each other without involving devices in other subnets.

Subnetting:

* Subnetting is the process of splitting a big network into these smaller subnets.
* It's like dividing the big neighborhood into smaller blocks.
* Subnetting uses a technique that borrows bits from the host part of an IP address to create subnet addresses.

Why Subnetting?

* Address Flexibility: Subnetting gives flexibility to network administrators to allocate addresses more efficiently. They can assign addresses to different parts of the network as needed.
* Reduced Traffic: By creating smaller subnets, broadcast messages (like announcements) are limited to just that subnet, reducing unnecessary traffic across the whole network.
* Security: Subnets can help isolate different parts of a network, enhancing security by controlling which devices can communicate with each other.
* Better Management: Managing smaller subnets is easier than managing a single large network. It allows administrators to apply rules and policies more effectively.

Imagine you have a big field (network) with lots of people (devices). Instead of having everyone interact with everyone else, you divide the field into smaller sections (subnets) with their own separate spaces. This way, people in one section can interact easily without affecting others. That's what subnetting does for computer networks – it divides, organizes, and streamlines communication.

Example in the slide-

'll break down the process step by step to help you understand how Host X communicates with Host Z in a scenario where they are on different networks.

* Network Setup:
  + Host X is on network 200.1.1.0 with IP address 200.1.1.5.
  + Host Z is on network 200.1.2.0 with IP address 200.1.2.8.
  + Both hosts are connected to hubs or switches, and there's a router that connects these two networks.
* Sending a Packet:
  + Host X wants to send a packet to Host Z. Since they are on different networks, Host X realizes it cannot send the packet directly to Host Z.
* Default Gateway:
  + Host X knows it needs to use its "Default Gateway" to reach Host Z. The default gateway is a router that connects Host X's network (200.1.1.0) to other networks.
  + Host X's default gateway is the router interface with IP address 200.1.1.1 on network 200.1.1.0.
* Router Routing:
  + Host X sends the packet to its default gateway (router interface with IP 200.1.1.1).
  + The router receives the packet and examines the destination IP address (200.1.2.8).
* ANDing Process:
  + The router performs a process called "ANDing" using the subnet mask associated with the source network (200.1.1.0) to determine which network the destination IP address (200.1.2.8) belongs to.
  + In binary, the subnet mask for 200.1.1.0 is usually something like 255.255.255.0, which is equivalent to 11111111.11111111.11111111.00000000 in binary.
  + The ANDing process involves performing a bitwise AND operation between the destination IP address and the subnet mask. This helps the router identify the network part of the address.
* Routing Decision:
  + The router determines that the destination IP address 200.1.2.8 is not in the same network as Host X (200.1.1.0).
  + The router consults its routing table to determine the next hop (next router interface) that will get the packet closer to the destination.
* Forwarding the Packet:
  + The router forwards the packet to the appropriate interface that will lead the packet closer to the destination network 200.1.2.0.
* Destination Network:
  + The packet goes through a series of routers, each making similar routing decisions based on the destination IP address until it reaches the router that connects to the network 200.1.2.0.
* Delivery to Host Z:
  + The router in network 200.1.2.0 receives the packet and delivers it to Host Z with IP address 200.1.2.8.

In summary, Host X sends the packet to its default gateway (router), which uses the subnet mask to determine that the destination is on a different network. The router forwards the packet to the appropriate interfaces, ultimately reaching the router connected to the destination network, where it's then delivered to Host Z.

Host X's default gateway is the router interface with IP address 200.1.1.1 on network 200.1.1.0. how to determnie that?

The determination of Host X's default gateway, in this case, is usually configured manually or through a DHCP (Dynamic Host Configuration Protocol) server. Here's how it could be determined:

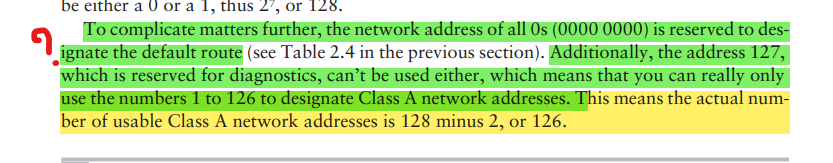
* Manual Configuration:
  + Network administrators often manually configure the default gateway on devices within a network.
  + In this scenario, the administrator would configure Host X to use the IP address 200.1.1.1 as its default gateway.
  + This information is entered in the network settings of Host X.
* DHCP Configuration:
  + If the network uses DHCP, which is a common protocol to automatically assign IP addresses and network settings to devices, the default gateway can be provided by the DHCP server.
  + When Host X connects to the network, it sends a DHCP request, and the DHCP server responds with an IP address, subnet mask, DNS servers, and the default gateway.
  + The DHCP server would be configured to assign 200.1.1.1 as the default gateway to devices within the 200.1.1.0 network.

In either case, the determination of the default gateway involves configuring the network settings of Host X to point to the router interface with the IP address 200.1.1.1. This ensures that when Host X needs to send data to a destination on a different network, it knows to send the data through the specified router interface.

It's important to note that the specific configuration method can vary based on the network setup and the practices of the network administrators.

Regenerate

Book tcp/ip(explaination of some confusing lines in book)



->Additionally, the address 127, which is reserved for diagnostics, can’t be used either, which means that you can really only use the numbers 1 to 126 to designate Class A network addresses. This means the actual number of usable Class A network addresses is 128 minus 2, or 126. why the address127 cant be used?

The address 127.0.0.1 (or any IP address in the range 127.0.0.0 to 127.255.255.255) is reserved for a special purpose known as loopback addressing. In computer networking, loopback addressing allows a device to send data to itself, effectively creating a loopback network interface. This is commonly used for testing and diagnostics.

When you send data to the loopback address (127.0.0.1), it doesn't actually go out onto a physical network. Instead, it's processed internally by the network stack of the operating system and then sent back to the application that generated it. This is extremely useful for testing network-related functionalities of applications and troubleshooting network issues without involving an external network.

Due to the importance of loopback addressing for testing and diagnostics, the entire range 127.0.0.0/8 (127.0.0.0 to 127.255.255.255) is reserved for loopback purposes and is not usable as regular network addresses. This is why the address 127 cannot be used for general networking purposes, as it's dedicated to loopback functionality.

->To complicate matters further, the network address of all 0s (0000 0000) is reserved to designate the default route what is this deafault route?

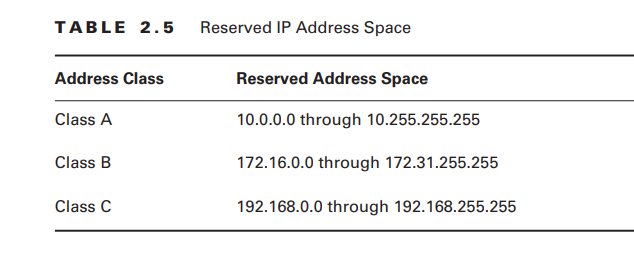
The default route, often referred to as the default gateway, is a concept in computer networking that specifies where network traffic should be sent if there is no specific route entry in the routing table for the destination IP address. In simpler terms, it's the path that network traffic takes when there's no more specific information available about where to send it.

When a device wants to send data to a destination IP address, it first checks its routing table to find a matching entry. If it doesn't find an exact match, it uses the default route to forward the traffic. This is especially useful for sending traffic to destinations outside of the local network or subnet.

The default route is typically configured on routers or gateways that connect different networks together. For example, in a home network setup, your router's IP address could be set as the default route on all devices within your local network. When a device in your network wants to access a website on the internet, it checks its routing table, doesn't find a specific route for the destination IP (since it's outside the local network), and then sends the traffic to the default route (your router). The router is responsible for forwarding the traffic to the appropriate destination on the wider internet.

In terms of the network address of all zeros (0000 0000), it's used to represent the default route in a routing table. This is because a network address of all zeros matches any destination IP address. When a device encounters a destination IP address that doesn't match any specific routes in its table, it uses the default route entry (often represented by an all-zero network address) to determine where to send the traffic.

To sum up, the default route is a crucial element in networking that ensures proper forwarding of network traffic when no specific route entry is available



Class B 172.16.0.0 through 172.31.255.255 this is referred as the reserved space for B my q is how this 16 and 31 are determined?

The IP address space is divided into different classes (Class A, Class B, Class C, etc.) to efficiently allocate addresses based on the size of networks. The division into these classes is done based on the leading bits of the IP address. However, with the introduction of Classless Inter-Domain Routing (CIDR), the traditional strict boundaries between classes have become more flexible, and the concept of subnetting is used to allocate IP addresses more efficiently.

The address range 172.16.0.0 through 172.31.255.255 falls within what was traditionally considered as Class B address space. However, these ranges are not actually determined by the values 16 and 31. Instead, they were chosen based on practical considerations and the need for flexibility in address allocation.

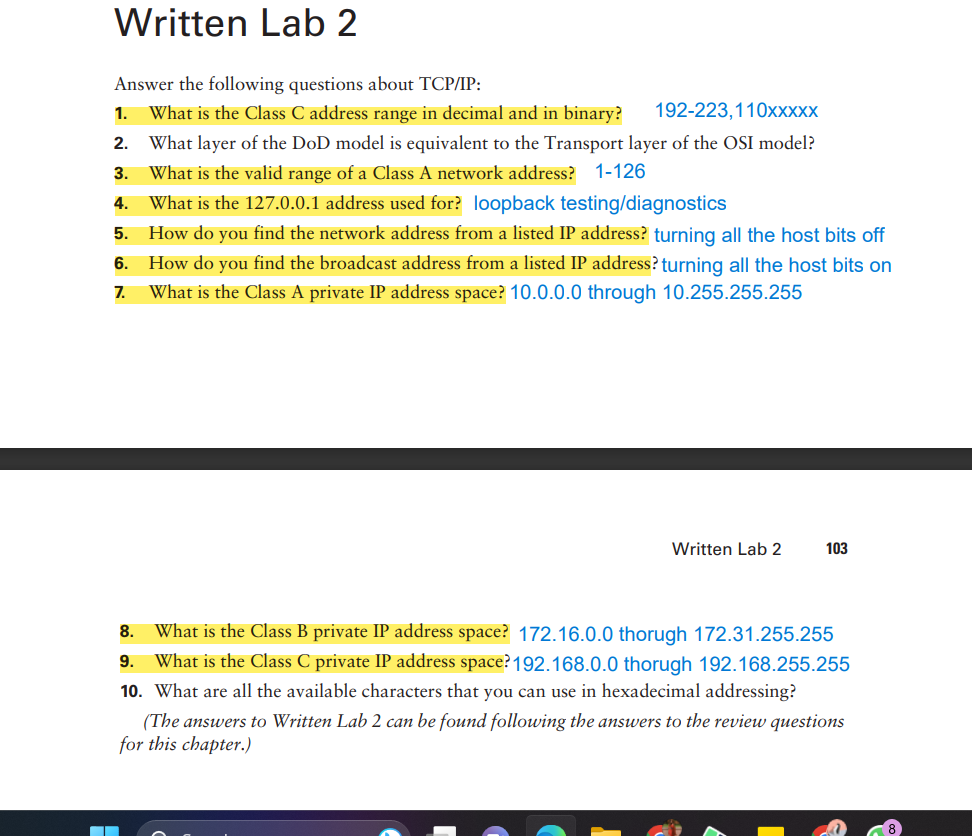
In the early days of IP addressing, the address classes were defined based on the number of bits used for the network part and the host part of the address. Class A addresses had the first octet reserved for the network portion, Class B addresses had the first two octets reserved for the network portion, and Class C addresses had the first three octets reserved for the network portion.

For Class B addresses, the first two bits of the first octet were always set to '10'. This means the range of possible values for the first octet was 128 to 191 (binary: 10000000 to 10111111).

The specific range of 172.16.0.0 to 172.31.255.255 was likely chosen because it allows for a substantial number of IP addresses to be allocated within that range, while still adhering to the constraints of the address class definitions. The addresses within this range are often used for private networks, such as those in organizations, without the need to obtain public IP addresses.

Remember, as networking technology has evolved, CIDR has become the more prevalent method of addressing, which allows for more flexible allocation of address ranges. The concept of strict address classes has become less significant in modern networking, as subnetting allows for finer control over address allocation.

Question answer of this chapter 2 of CCNA



TCP/IP

About NAT (network addess translation) from chatgpt

Network Address Translation (NAT) is a networking technique that allows multiple devices within a private network to share a single public IP address when communicating with resources on the internet. NAT serves as an intermediary between the private local network and the public internet, enabling devices with private IP addresses to access the global network.

Here's how NAT works:

* Private Network and Private IP Addresses: Devices within a local network are assigned private IP addresses. These private IP addresses are not globally unique and are used only within the confines of the local network. These addresses are typically from the reserved address ranges like 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8.
* Public IP Address: The router or gateway device of the local network is assigned a public IP address by the Internet Service Provider (ISP). This public IP address is unique and serves as the identifier for the entire local network when communicating with external servers on the internet.
* Outgoing Data Packets: When a device from the local network wants to access a resource on the internet, the NAT device (router) modifies the source IP address of the data packet. The private IP address of the sending device is replaced with the public IP address of the NAT device. This change allows the data packet to be routed through the internet using the public IP address.
* Incoming Data Packets: When a response is received from the internet, the NAT device looks at the destination port number of the incoming data packet. Using a translation table, it determines which private IP address within the local network the response should be forwarded to. The NAT device changes the destination IP address of the data packet to the appropriate private IP address.

NAT serves several key purposes:

* Conservation of Public IP Addresses: Since public IP addresses are limited, NAT allows many devices within a private network to share a single public IP address. This helps to mitigate the exhaustion of available public IP addresses.
* Security and Privacy: Devices within the private network are not directly accessible from the internet because they are using private IP addresses. This provides a layer of security by hiding the structure of the local network.
* Address Multiplexing: Multiple devices can use the same internal private IP addresses without conflict, as long as they are communicating with different external servers on the internet.
* Port Mapping: NAT often involves not only translating IP addresses but also port numbers. This enables many devices to share the same public IP address by differentiating connections based on port numbers.

It's important to note that while NAT provides a way for devices with private IP addresses to communicate with the internet, it can introduce complexities, particularly for certain types of network applications like online gaming or peer-to-peer communication, where direct connections between devices are desired.

Relation between NAT and private address

I apologize for any confusion. Let's clarify the relationship between NAT and private address space:

* Private Address Space: Private address space refers to the reserved IP address ranges that are designated for use within private networks. These ranges are not routable on the public internet and are intended for local use only. The three common private address ranges are:
  + 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
  + 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
  + 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)
* Network Address Translation (NAT): NAT is a technique used to allow multiple devices with private IP addresses to share a single public IP address when accessing resources on the internet. NAT involves the translation of IP addresses in data packets as they travel between a private network and the public internet.

Now, here's how NAT and private address space are related:

* Private address space is used within local networks to assign IP addresses to devices. These IP addresses are not globally unique and can be reused in different private networks.
* NAT is used by routers or gateway devices to translate the private IP addresses of devices within a local network into the public IP address of the router when those devices communicate with resources on the internet.
* NAT enables devices with private IP addresses to communicate with the internet without requiring each device to have its own unique public IP address. Instead, all outgoing traffic from the devices in the local network appears to originate from the single public IP address of the router.

In summary, private address space provides a pool of addresses that can be used within local networks, and NAT is a technique that allows these devices to access the public internet using a shared public IP address. NAT ensures that communication between the private network and the public internet is possible by translating IP addresses in both outgoing and incoming data packets.

Classless addressing

→subnetting and supernetting in the classful addressing didnt really solve the address depletion problem and made the distribution of addresses and routing process more difficult.t

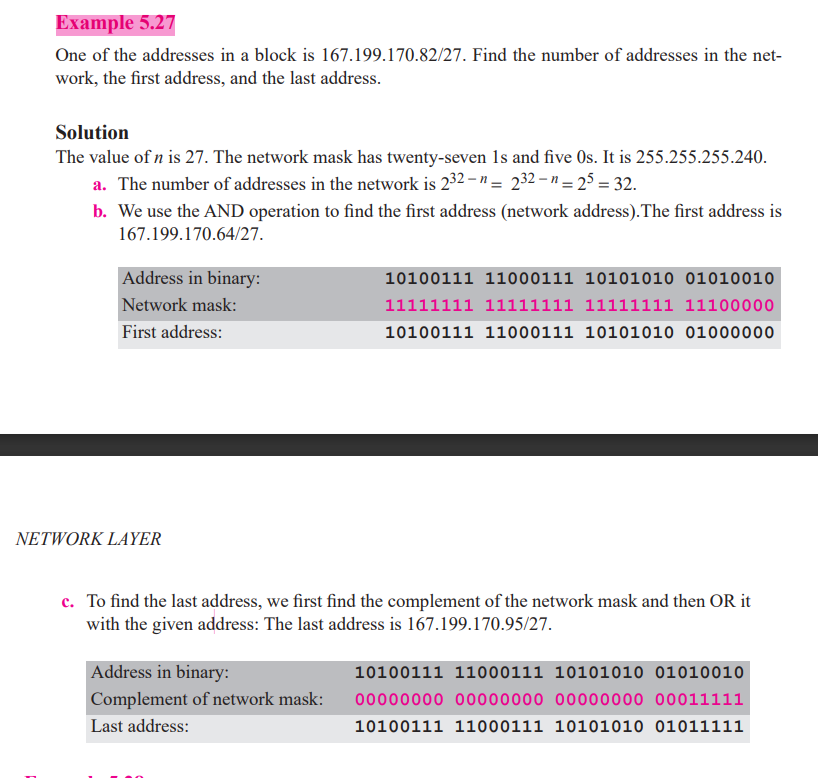
→the class privilege was removed from the distribution to compensate for the address depletion

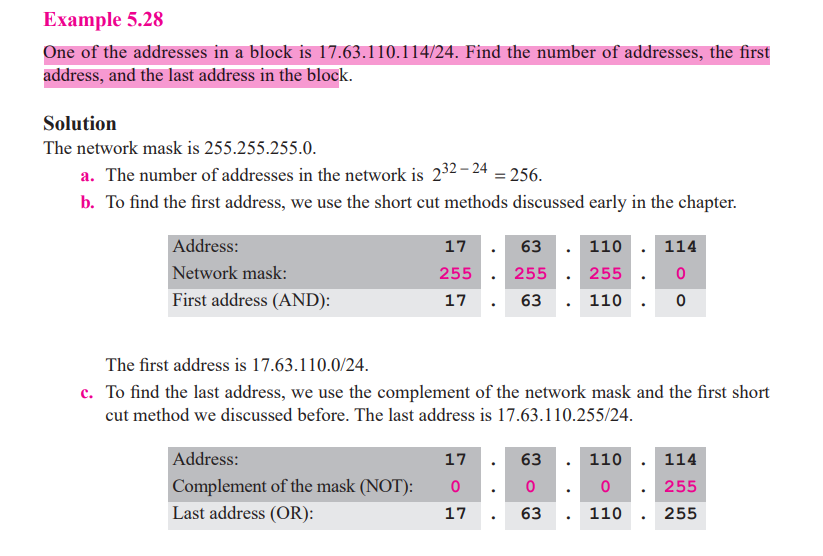
→in classless addressing the whole address space is divided in to variable length blocks, the only restriction is the number of addresses in a block needs to be a power of 2

→in classless address divided into 2 parts - prefix defines network address and suffix defines host

→ in classless addressing we need to include prefix length to find the block of an address.prefix length is aded to the address separated by a slash. This is referred to as slash notation

→ the slash notation is formally referred to as classless interdomain routing or CIDR notation





Address aggregation

One of the advantages of cidr architecture is address aggregation.ICANN assigns a large block of address to an ISP.Each ISP in turn divides its assign block into smaller subblocks and grants the subblocks to its customers,many blocks of addresses are aggregated in one block and granted to one ISP