MODULE (lecture)

Week 8

SA321

ACADEMIC YEAR 2023-2024

MODULE IN SA321

Credits **: 3 units**
Pre-Requisite **:** SIA311– Systems Integration and Architecture 1

Lesson Title: Networking I
a. Layers
b. Networking I: IPv4 Basics & CIDR subnetting
c. Networking I: IPv6 Basics

Layers

OSI MODEL LAYERS

What is the OSI Model?

The Open Systems Interconnection (OSI) model is a conceptual framework that divides network communications functions into seven layers. Sending data over a network is complex because various hardware and software technologies must work cohesively across geographical and political boundaries. The OSI data model provides a universal language for computer networking, so diverse technologies can communicate using standard protocols or rules of communication. Every technology in a specific layer must provide certain capabilities and perform specific functions to be useful in networking. Technologies in the higher layers benefit from abstraction as they can use lower-level technologies without having to worry about underlying implementation details.

Why is the OSI model important?

The layers of the Open Systems Interconnection (OSI) model encapsulate every type of network communication across both software and hardware components. The model was designed to allow two standalone systems to communicate via standardized interfaces or protocols based on the current layer of operation.

Shared understanding of complex systems

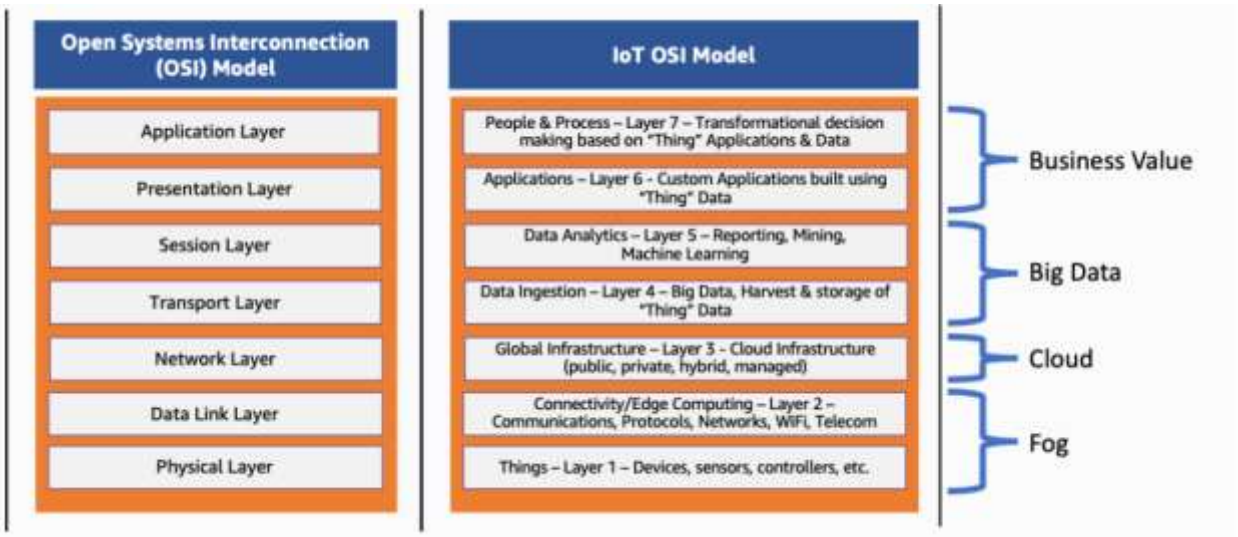
Engineers can use the OSI model to organize and model complex networked system architectures. They can separate the operating layer of each system component according to its main functionality. The ability to decompose a system into smaller, manageable parts via abstraction makes it easier for people to conceptualize it as a whole.

Faster research and development

With the OSI reference model, engineers can understand their work better. They know which technological layer (or layers) they're developing for when they create new, networked systems that need to communicate with each other. Engineers can develop networked systems and take advantage of a series of repeatable processes and protocols.

Flexible standardization

The OSI model does not specify the protocols to use between levels, but rather the tasks that protocols perform. It standardizes network communication development so people can rapidly understand, build, and decompose highly complex systems—all without prior knowledge of the system. It also abstracts details, so engineers don't require the understanding of every aspect of the model. In modern applications, the lower levels of networking and protocols are abstracted away to simplify system design and development. The following image shows how the OSI model is used in modern application development.

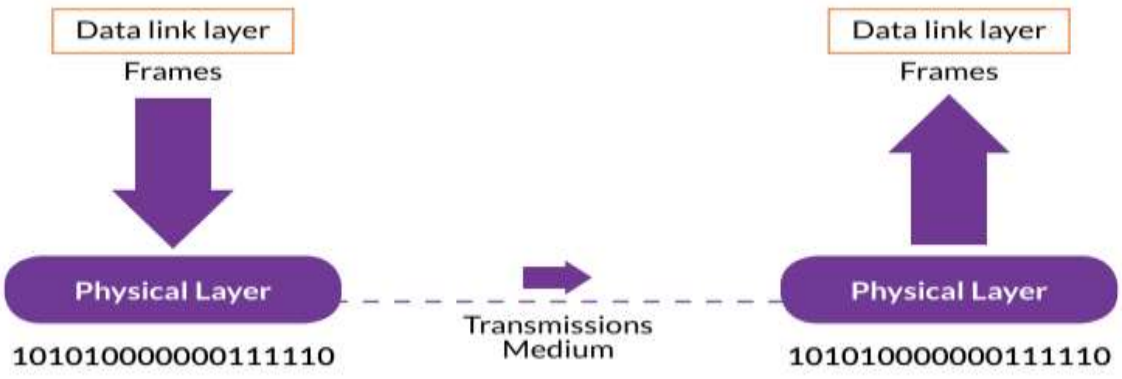


What are the seven layers of the OSI model?

The Open Systems Interconnection (OSI) model was developed by the International Organization for Standardization and others in the late 1970s. It was published in its first form in 1984 as ISO 7498, with the current version being ISO/IEC 7498-1:1994. The seven layers of the model are given next.

Physical Layer – Layer 1

- In charge of sending digital bits from source to destination device
- Composed of cables, connectors, NIC, repeaters and Hubs
- Does encoding and decoding
- Sends electrical impulses made up of 1s and 0s



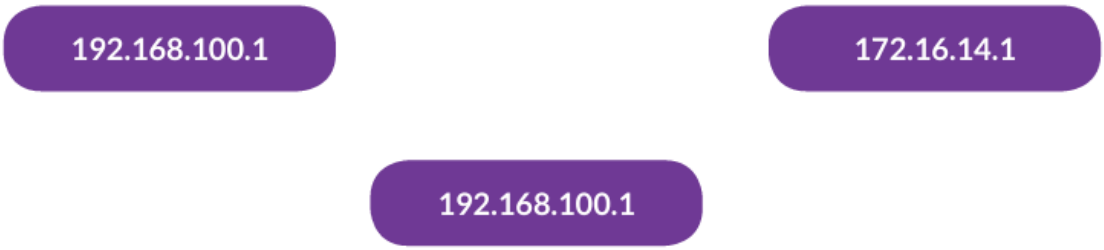
This is the first layer, stacked at the bottom of the OSI model. It has to be present in the source and destination devices during the communication. The source defines triggers the transmission of bits to the destination device. A system has to work with various physical components, such as cables, network interface cards (NICs), switches, and routers. When a system is connected to a switch via a cable, it can send the bits to the destination system. When the bits, 0 and 1, are sent out by a source system to the destination system, their bits are encoded into electrical signals on a wired network. Instead of electrical signals, the bits are converted into electromagnetic waves on a wireless network.

The **Data Link layer** is the 2nd layer that passes the information above the layer to the physical layer.

Data Link Layer – Layer 2

- Is responsible for communication between Network and Physical layer.
- Is divided into two sublayers:
  - LLC – Logical Link Control Sublayer
  - MAC Sublayer

Layer 2, or the Data Link layer has a key responsibility. It receives the information from the Network layer and passes it to the Physical layer. This is nothing but layer-to layer communication. One layer sends the information to the next layer. A layer in the OSI model can communicate with the layer above or below it. When the Data Link layer sends the information, it creates frames and adds physical addresses. The frame that it creates is used to determine the data structure for the network. The Data Link layer comprises two sublayers – Logical Link Control (LLC) and MAC sublayers. Both sublayers play an essential role. The LLC sublayer determines whether the communication is connection-oriented or connectionless. The MAC sublayer contains the MAC address, the physical address of a network interface card, which is eventually used for communication with the other nodes on the networks. Switches use the MAC addresses to locate the destination systems.



The Network layer is the mediator of data transmission between the Transport and the Data Link layers. It receives the information from the Transport layer and then passes it to the Data Link layer, which works with the MAC or the physical address unique to every network interface card. On the other side, the Network layer works with the logical addressing, which can be assigned and changed. When you move a laptop or a system from one network to the other network, the system's physical address does not change – unless you change the network interface card. However, the logical address changes. The packet

addressing and the conversion of physical to logical addressing occur at the Network layer. No matter which network you are connected to, even though the logical address changes, the physical address remains the same. Then comes the source to destination delivery. The source and destination networks can be different. For example, a system may be sending data to a system on the Internet. The physical address cannot be used in this case, but the logical address is used to find the route to the destination system. The physical addresses are used when the destination system is located on the same network. If it is a different network, then the logical address is used. This is why it is often said to be Layer 3 routing – it allows the different networks to connect. Using the routing, the best path to the destination can also be determined using the routers located on the connected networks.

Transport Layer – Layer 4

- Accepts services from the session layer and passes them to the network layer below
- Is responsible for:
  - End-to-end message delivery - handles message acknowledgment and traffic control.
  - Error checking - packets arrive without duplication or corruption, and in the correct order
- Contains the TCP and UDP protocols

The fourth layer in the OSI model is the Transport layer, which is responsible for:

- Receiving services from the Session layer, which is located above it as the 5th layer
- Provides services to the Network layer, which is located below it as the 3rd layer The Transport layer performs two essential functions: End-to-end message delivery - handles message acknowledgment and traffic control. Error checking - packets arrive without duplication or corruption and in the correct order A system can be performing several tasks at once. For example, it may be using a Web browser to browse a page on the Internet and copying data from another system on the network. A lot of data packets are arriving at the system. How does the system segregate the data packets and send them to the correct applications, such as a Web browser? In this scenario, the identification of the data packets contains a port number so that the data packets can be sent to the correct application. The data packet differentiation cannot be done with only one IP address because each data packet is meant for the same system that has the same IP address. The Transport layer is also responsible for ensuring an error-checking method is in place. **Its error-checking method ensures:**

- Packets arrive in the order they were supposed to arrive in
- There is no duplication of the data packets
- The data packets are not corrupt The Transport layer contains two key protocols, TCP and UDP. The TCP acronym denotes Transmission Control Protocol. The UDP acronym denotes User Datagram Protocol.

Session Layer – Layer 5

- Manages communication between two devices on a network
  - Regulates the start, continuation, and end of a session
- Ensures all security concerns are met
- Manages dialog control, such as:

- Simplex
- Half-Duplex
- Full-Duplex
- Contains some of the following protocols: NetBIOS, DNS, RPC, and NF

Now let's look at the OSI model's fifth layer, the session layer, that manages the communication between two devices on a network. It regulates the start, continuation, and end of a session. It performs the following tasks: Establish a session between two devices Maintain the session while the communication between the devices is taking place Terminate the session when the communication between the devices is over It also regulates the data exchange between two devices. It simply acts as a moderator that determines who can transfer the data and how long the transfer should take place. It ensures that there is security for the session being established. It also ensures that the security concerns are taken care of. The security can be determined by a login, for example. It also determines the type of dialog control that will be used. For example, it can be one of the following dialog controls:

- Simplex
- Half-Duplex
- Full-Duplex

Some of the key protocols on this layer are NetBIOS, DNS, RPC, and NFS

Presentation Layer – Layer 6

- Represents data in a uniform format to an application
- Is also known as the "translation layer"
- Uses methods
  - American Standard Code for Information Interchange - ASCII
  - Extensible Markup Language – XML
- Compresses data for transmission
- Encrypts data for security purposes

The 6th layer or the Presentation layer works according to the name it has been given. It presents the data in a format that is understood by the applications. It formats the data in a uniform format by hiding the differences that the data format differences between two devices that are communicating. The data formatting is performed for the Application layer, the 7th layer of the OSI model. The data received may be different than the Application layer at the receiving system can understand. The Presentation layer formats the data so that the Application layer can comprehend it. The Presentation layer is also known as the Translation layer because of its capabilities of translating the data from one format to the commonly used format methods, such as:

- American Standard Code for Information Interchange - ASCII
- Extensible Markup Language - XML

Using either of these methods converts the data into 0s and 1s. It also reduces the number of bits transmitted on the network by applying compression to the data. It also encrypts the data for security purposes.

Application Layer – Layer 7

- Is the layer where the user interacts with the devices
- Serves as an interface for the applications, such as:
  - Email applications
  - Web browsers
- Example of protocols running on Layer 7:
  - FTP
  - DHCP
  - DNS
  - SMTP
  - HTTP

The Application layer is the OSI model's final layer, the 7th layer. It serves as the interface for users and application processes to access network services. Using the Application layer, the users can communicate with the applications. Let's see how it works. The Application layer allows the users to work or interact with the applications installed on a system. When a user interacts, the data is passed on to the user in a standard format. Even if the user accesses the application from a different network, the data is still standardized for presentation.

The following protocols exist on the Application layer:

- File Transfer Protocol (FTP)
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- Simple Mail Transfer Protocol (SMTP)
- Hypertext Transfer Protocol (HTTP

Networking I: IPv4 Basics & CIDR subnetting

What is IPv4?

IP stands for Internet Protocol and v4 stands for Version Four (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.

IP version four addresses are 32-bit integers which will be expressed in decimal notation.

Example- 192.0.2.126 could be an IPv4 address.

Parts of IPv4

Network part:

The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.

Host Part:

The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.

For each host on the network, the network part is the same, however, the host half must vary.

Subnet number:

This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

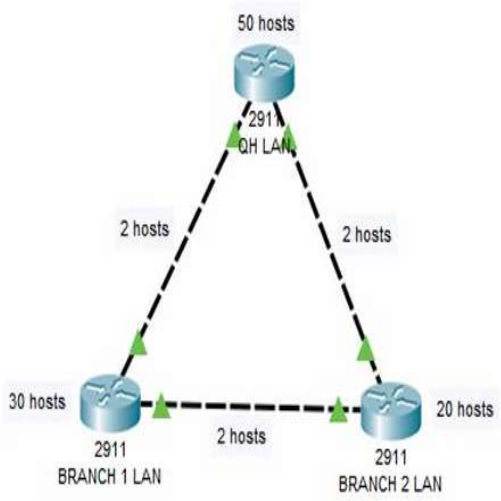
Advantages of IPv4

- IPv4 security permits encryption to keep up privacy and security.
- IPV4 network allocation is significant and presently has quite 85000 practical routers.
- It becomes easy to attach multiple devices across an outsized network while not NAT.
- This is a model of communication so provides quality service also as economical knowledge transfer.
- IPV4 addresses are redefined and permit flawless encoding.
- Routing is a lot of scalable and economical as a result of addressing is collective more effectively.
- Data communication across the network becomes a lot of specific in multicast organizations.
- Limits net growth for existing users and hinders the use of the net for brand new users.
- Internet Routing is inefficient in IPv4.
- IPv4 has high System Management prices and it's labor-intensive, complex, slow & frequent to
- errors.
- Security features are nonobligatory.
- Difficult to feature support for future desires as a result of adding it on is extremely high
- overhead since it hinders the flexibility to attach everything over IP.

Limitations of IPv4

- IP relies on network layer addresses to identify end-points on network, and each network has a unique IP address.
- The world's supply of unique IP addresses is dwindling, and they might eventually run out theoretically.
- If there are multiple host, we need IP addresses of next class.
- Complex host and routing configuration, non-hierarchical addressing, difficult to re-numbering addresses, large routing tables, non-trivial implementations in providing security, QoS (Quality of Service), mobility and multi-homing, multicasting etc. are the big limitation of IPv4 so that's why IPv6 came into the picture.

IPV4 Subnetting/CIDR subnetting



Classless (Variable-length Subnet Mask

- Subnet Mask:
  - Determine if a host is on the same network or not
  - Is a 32-bit address
- Variable-length Subnet Mask (VLSM)
  - Allows subnets to be variable in size
  - Allows hosts to be variable in numbers in each subnet
  - Uses only classless routing protocols
  - Uses different configurations for different subnet masks

Before understanding the concept of classless, let's understand the concept of subnet masks. A subnet mask determines the network of a system. It determines whether a system is on the same network or a different network. It is a 32-bit address that is made of ones and zeros. The value of 1 is used as the network prefix, and the value of 0 determines the host. For example, if you /24, the network prefix consists of 24 ones and 8 zeros. VLSM is a short name for Variable Length Subnet Mask. Consider a scenario of having more than one subnet mask in a single subnet. This is achieved using VLSM, which is subnetting the subnet. VLSM:

- Allows subnets to be variable in size
- Allows hosts to be variable in numbers in each subnet
- Uses only classless routing protocols
- Uses different configurations for different subnet masks Without the use of VLSM, you will end up wasting IP addresses. For example, if a subnet requires only 10 IP addresses, you will still end up assigning 254, which will waste 244 IP addresses. Using VLSM, you can assign the subnet mask as 255.255.255.240, which will give only 16 IP addresses, out of which 14 will be useful. VLSM is mainly used with IPv4 public IP addresses.

Understanding Variable Length Subnet Masks (VLSM)

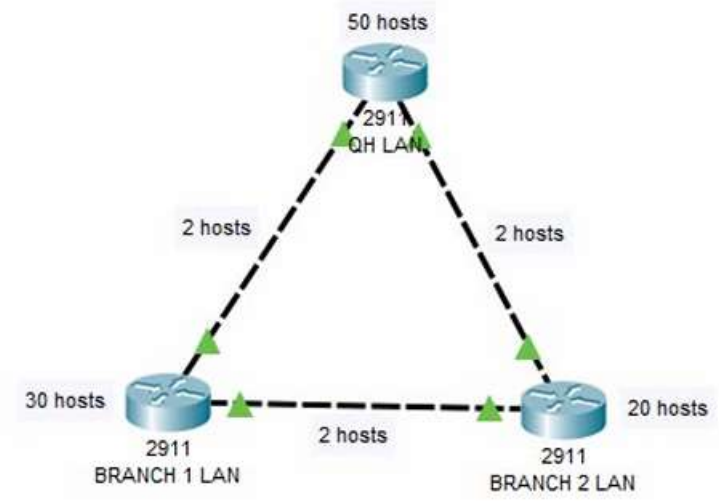
We have a limited number of private IPv4 addresses that can be used in every organization. As the Internet and most organizations are aggressively growing, we need a way to eliminate wasting IPv4 addresses. One of the ways that we can maximize the use of private IPv4 addresses in the organization is through subnetting.

The reason why we need subnetting is to efficiently distribute an IPv4 address with the least wastage and to create more networks with the smaller broadcast domains. To efficiently use subnetting, we can use Variable-Length Subnet Mask (VLSM).

Steps to Implement Variable-Length Subnet Mask (VLSM)

We will use the below network topology as we go through the steps of the Variable-Length Subnet Masking (VLSM).

With Variable-Length Subnet Mask (VLSM), we can allot the closest required number of IP addresses into a subnetwork in our LAN. We don't need to use a /23 subnet mask in all of our subnets, for example.



Step 1. **Identify the host requirement.** How many hosts or IP addresses are needed by the subnets in our LAN? We can arrange them from the highest host requirement to the lowest, as we will perform VLSM subnetting starting from the subnet with the highest host requirement. Don't forget to include the point-to-point (WAN) links as well.

- HQ LAN – 50 hosts
- BRANCH 1 – 30 hosts
- BRANCH 2 – 20 hosts
- WAN 1 (HQ to BRANCH 1) – 2 hosts
- WAN 2 (HQ to BRANCH 2) – 2 hosts
- WAN 3 (BRANCH 1 to BRANCH 2) – 2 hosts

The total host requirement for our network is 106 hosts, and we will perform VLSM subnetting on the HQ LAN subnetwork first.

Step 2. Determine the class of IP subnet. We need to determine the class of IP subnet that we will use based on the required number of hosts.

Class A has 16,777,216, Class B has 65,536, and Class C has 256 IP addresses. As per our network requirement, we need only 106 hosts, therefore we will use a Class C IP address space. In our example, we will use 192.168.10.0. It could also be that the organization bought an IP address space from the IP address authorities.

Step 3. Identify the host bits for every subnet. In our network topology example, HQ LAN has 50 hosts requirement, therefore we would have 6 host bits.

2^6 host bits will give us 64 hosts, minus 2 for the network address and broadcast address, which is equal to 62 usable host addresses. It suffices our 50 hosts requirement for HQ LAN.

Step 4. Calculate the subnet mask. Identify the network bits and determine the subnet mask of the subnet. We can get the subnet mask by subtracting the host bits from 32 (the total IPv4 address bits). For HQ LAN, it's 32 – 6 host bits, which is equal to a /26. The subnet mask for HQ LAN is /26 and its long format is 255.255.255.192

Step 5. Get the increment. To determine in which block of number should we go up, we can use the formula of **2^host bits**. For HQ LAN, it is 2^6 host bits, which will give us an increment of 64.

Step 6. Determine the network address, broadcast address, and IP address range. Starting from the base IP address, we will go up or increment in the value computed in Step 5.
For our network, we have a base IP address of 192.168.10.0. For HQ LAN, we will increment in a block of 64 as calculated in Step 5. Moreover, since it is in the Class C IP address space, as identified in Step 2, we will increment in the 4th octet.
That will be:
192.168.10.0 + 64 (Current subnet)
192.168.10.64 (Base IP address for the next subnet)
We determined that the network address for HQ LAN subnet is 192.168.10.0. The broadcast address will be 1 less than the next IP subnet. That's 192.168.10.64 – 1, which is 192.168.10.63.
Finally, to get the HQ LAN usable IP address range, it is the IP address range in between the network address and the broadcast address, 192.168.10.1 to 192.168.10.62.

Completing the Variable-Length Subnet Mask Subnetting Process

Now, we are done with subnetting the HQ LAN. To fully implement VLSM, we need to do subnetting as well on the remaining LAN and WAN networks, which are BRANCH 1 LAN, BRANCH 2 LAN, WAN 1, WAN 2, and WAN 3.

The next subnet to be subnetted in VLSM will be the BRANCH 1 LAN as it has the next highest number of hosts. We will start with 192.168.10.64 as our network address as it is where we ended with our first IP subnet, HQ LAN.

Follow the steps we did on HQ LAN to perform VLSM subnetting on the remaining LAN and WAN subnets in our network diagram.

Below are the host bits, subnet mask, increment, network address, broadcast address, and usable IP address ranges of each subnet of the network topology we used in our example:

HQ LAN:
Number of Hosts – 50
Host Bits – 6 bits
Subnet Mask – /26 or 255.255.255.192
Increment – 64
Network Address – 192.168.10.0
Broadcast Address – 192.168.10.63
Usable IP Addresses – 192.168.10.1 to 192.168.10.62

BRANCH 1 LAN:
Number of Hosts – 30
Host Bits – 5 bits
Subnet Mask – /27 or 255.255.255.224
Increment – 32
Network Address – 192.168.10.64

Broadcast Address – 192.168.10.95
Usable IP Addresses – 192.168.10.65 to 192.168.10.94

BRANCH 2 LAN:
Number of Hosts – 20
Host Bits – 5 bits
Subnet Mask – /27 or 255.255.255.224
Increment – 32
Network Address – 192.168.10.96
Broadcast Address – 192.168.10.127
Usable IP Addresses – 192.168.10.97 to 192.168.10.126

WAN 1:
Number of Hosts – 2
Host Bits – 2 bits
Subnet Mask – /30 or 255.255.255.252
Increment – 4
Network Address – 192.168.10.128
Broadcast Address – 192.168.10.131
Usable IP Addresses – 192.168.10.129 to 192.168.10.130

WAN 2:
Number of Hosts – 2
Host Bits – 2 bits
Subnet Mask – /30 or 255.255.255.252
Increment – 4
Network Address – 192.168.10.132
Broadcast Address – 192.168.10.135
Usable IP Addresses – 192.168.10.133 to 192.168.10.134

WAN 3:
Number of Hosts – 2
Host Bits – 2 bits
Subnet Mask – /30 or 255.255.255.252
Increment – 4
Network Address – 192.168.10.136
Broadcast Address – 192.168.10.139
Usable IP Addresses – 192.168.10.137 to 192.168.10.138

Classful

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

This slide displays the classful IP address divided into five classes, namely Class A to Class E. It is important to note that only Class A to C is used. The slide also displays the starting and ending addresses of each class. For example, Class B has a 128.0.0.0, and the ending address is 191.255.255.255. There are fewer networks in Class A but more hosts per network. Similarly, Class C has fewer networks, but there are more hosts per network. The slide also displays the number of bits used for networks and hosts. Class A has only 8 bits for the network, whereas Class C has 24 bits for networks. In the Addresses Per Network column, the number mentioned in the parentheses is the number of hosts per network. You must subtract two addresses from the total number of hosts, 0.0.0.0 and 127.0.0.1, as they cannot be allocated.

Classless Inter-Domain Routing (CIDR) Notation

- Is used for allocation of IP addresses
- Is based on VLSM
- Breaks the IP addresses into two parts:
    - Network address: Is used as a prefix
    - Remaining address: Is used as a suffix with the number of bits remaining in the address
- Overall improves the efficiency of IPv4 allocation without wasting IP addresses

The CIDR notation is used for allocating IP addresses without wasting too many IP addresses. In the previous slide, you look at the VLSM method that reduces wastage by allocating only the required IP addresses. You also looked at the example of 255.255.255.240, which will allocate only 16 IP addresses. If you do not use VLSM, the total IP address allocated will be 256, which means you will waste 246 IP addresses if you need just 10 of them. So, in a nutshell, CIDR uses the VLSM method for IP address distribution. CIDR breaks the IP address into two parts: Network Address: This is used as a prefix Remaining address: This is used as a suffix with the number of bits remaining in the address For example, you have 192.168.1.0/24 – you get a total of 256 IP addresses. However, you have to remove two IP addresses and, therefore, are left with 254. Let's simplify the concept of CIDR. You know that there are three classes of IP addresses:

- Class A - 16 million hosts
- Class B - 65,535 hosts
- Class C - 254 hosts Suppose you need to use a class B IP address but require only 5000 IP addresses. In this scenario, you would waste nearly 60000 IP addresses. So, what is the solution? You use the CIDR notation to reduce the wastage of the IP address. With the CIDR notation of /19, you will get 8192 IP

addresses. Even though you still waste a little more than 3000 IP addresses, it is still better than wasting 60000.

CIDR Block Size	Exponential Notation	Number of Addresses
/24	2^8	256
/23	2^9	512
/22	2^{10}	1,024
/21	2^{11}	2,048
/20	2^{12}	4,096
/19	2^{13}	8,192
/18	2^{14}	16,384
/17	2^{15}	32,768
/16	2^{16}	65,536

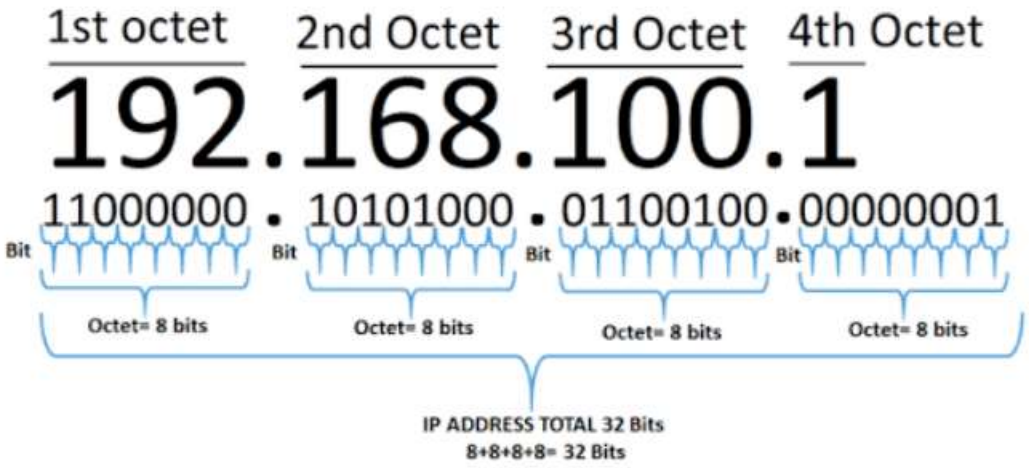
CIDR block definition

CIDR stands for Classless Inter-Domain Routing, which is an IP address allocation method that enhances data routing efficiency. CIDR notation is used in IP addressing to define a range of IP addresses.

What is an IP address?

To understand a CIDR block fully, we need to understand IP addresses. An IP address is the numerical representation of a location in a network. Similarly to how your phone number identifies your cell phone, your IP address identifies your device, your server, and your network interface. Computers only understand binary numbers (comprised of zeros and ones), therefore an IP address is just a sequence of zeros and ones. An IP address uses a combination of 32 zeros and ones, 32 bits.

Humans, however, need another format. That's why that binary number is split into four blocks or bytes and each block is represented with a decimal value. Each decimal number goes from 0 to 255 (decimal representation of eight 1s). Because of that, you always see an IP address as a combination of four decimal numbers, something like: 192.168.1.1.



A depiction of an IP address

Creating a CIDR block for your Private Space

Whether you're well-versed or need a refresher, we need to know what a Private Space and Private networks are before discussing how CIDR blocks are set up, which is crucial for configuring these networks.

- **Private Space:** Think of this as your own private corner of the internet. This is how you extend your company's network to MuleSoft's Anypoint Platform. It is a virtual, private, and isolated logical space in CloudHub 2.0 to run your apps in. You can create multiple private spaces either in the same or different regions.
- **Private Network:** When setting up a private network, you assign a range of IP addresses for applications within your private space to utilize, specify the region in which they will operate, and optionally designate internal DNS servers to handle requests for custom domains. You can configure multiple private spaces within a single region, allowing for the creation of distinct and isolated networks for different environments, like development or staging, in addition to the production environment.

CIDR block sizing

The size of a Private Space is determined by the CIDR block. When you create a private space, you must specify the CIDR block. For Private Spaces, the size of this CIDR needs to be a number between 24 (256 IPs) and 16 (65,536 IPs). Having a short block might cause your deployment to run out of IPs, meaning it won't be able to deploy apps in the Private Space. From that perspective, setting your VPC size to the maximum CIDR block would be the best solution.

However, the moment you connect a Private Space to your Private Network using Anypoint Virtual Private Network or Transit Gateway Attachments, the CIDR block will become part of your internal network and consume private IP addresses from your internal addressing space. It's important not to oversize your Private Space as it will take out more IPs than necessary from your internal network.

For many organizations, if you consider the amount of SaaS solutions that require a private connection, it becomes a challenge to reserve big CIDR blocks for all of them. You can't resize or change the CIDR

block after you create a Private Space. For this reason, ensure that you correctly anticipate your requirements before configuring this parameter.

To further clarify, here's a table with CIDR block sizes and their corresponding number of IP addresses:

CIDR Block Size	Exponential Notation	Number of Addresses
/24	2^8	256
/23	2^9	512
/22	2^{10}	1,024
/21	2^{11}	2,048
/20	2^{12}	4,096
/19	2^{13}	8,192
/18	2^{14}	16,384
/17	2^{15}	32,768
/16	2^{16}	65,536

How to estimate the number of IPs needed for your CIDR block

Considering the above, how do we estimate the number of IPs we need for our Mule deployment? Start from the number of applications you'll deploy onto that Private Space. The key is to understand that there's not a one-to-one relation between apps and IPs. It's likely that one application will consume more than one IP. Here are the key concepts to understand to do a proper estimation for the CIDR block:

Number of workers

A Mule app is deployed to one or more workers. Every worker gets its own IP address, so an app deployed to one worker will get one IP and the same app deployed to four workers will get four IPs

Horizontal scaling and high availability

You need to estimate how many workers your app needs. There are mainly two reasons to add more than one worker to your app:

- **Horizontal scaling:** Some apps, due to their type of processing, require more than one worker to distribute the load between the workers and get better performance.
- **High availability:** If your app is critical, you need to add additional workers so if one worker fails, the app can continue serving requests.

Fault tolerance

Redundancy is a critical technique for achieving **fault tolerance** in CloudHub 2.0. By providing multiple availability zones, CloudHub 2.0 can deploy redundant resources across different zones. In the event of a failure in one zone, traffic can be seamlessly redirected to another zone, ensuring high availability of services. Providing more than a worker for an app will give fault tolerance at the worker level, but if we require fault tolerance for the whole region, we need to provide one worker per AZ.

Zero downtime deployment

Zero downtime deployment is a deployment style that allows CloudHub to deploy new versions of an application without causing any interruption to the consumers of the application. The goal here is to be able to quickly make changes to the environment without impacting the SLAs.

With this technique, we can deploy a new version of our app or update the runtime with no service interruption. It's also useful if you need to scale your app vertically or horizontally. Zero downtime leverages a side-by-side deployment. For any of those operations, CloudHub starts up a new worker with the new version of the app and keeps both workers (the new and the old one) until the old one is removed and the new one remains.
In this process, the new worker will require a new IP; for a short time, you will have two workers and two IPs running. So zero downtime affects the required size of your CIDR block. You need to have enough free IPs in the IP range of your VPC so that you can duplicate the number of IPs assigned to existing apps when a bulk update happens. A few must-answer questions are:

- How many apps would you be updating in parallel?
- Do you need to update your apps in groups?
- Do you update your runtimes periodically? How many different versions of the mule runtime do you keep in your deployment?
- How does security and continuous patching affect your apps?
- What type of traffic do you have for your apps? Is there a group of critical apps in your deployment that you typically scale vertically or horizontally to accommodate peaks of traffic?

Answering all these questions gives a better understanding of the block of IPs you need to maintain unused in your CIDR block for zero downtime operations.

Number of environments

In practice, software applications are typically deployed across multiple environments, with at least two: one for production and another for non-production. It's also not uncommon to have multiple non-production environments. When determining the appropriate CIDR block size, you need to consider the number of environments your applications are expected to be deployed on.

Considerations

When specifying CIDR blocks, ensure that they:

- Are from a private IP space
- Don't overlap with any other CIDR blocks assigned to your other private spaces
- Don't overlap with any CIDR blocks in use in your corporate network

You can't use the following reserved CIDR blocks:

```
172.17.0.0/16
100.64.0.0/10
198.19.0.0/16
224.0.0.0/4
169.254.0.0/16
127.0.0.0/8
0.0.0.0/8
```

Example of reserved CIDR blocks

Networking I: IPv6 Basics

What is IPv6?

The most common version of the Internet Protocol currently in use, IPv4, will soon be replaced by IPv6, a new version of the protocol. The well-known IPv6 protocol is being used and deployed more often, especially in mobile phone markets. IP address determines who and where you are in the network of billions of digital devices that are connected to the Internet.

IPv6 or Internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. IPv6 was designed by Internet Engineering Task Force (IETF) in December 1998 with the purpose of superseding the IPv4 due to the global exponentially growing internet users.

The next generation Internet Protocol (IP) address standard, known as IPv6, is meant to work in tandem with IPv4, which is still in widespread use today, and eventually replace it. To communicate with other devices, a computer, smartphone, home automation component, Internet of Things sensor, or any other Internet-connected device needs a numerical IP address. Because so many connected devices are being used, the original IP address scheme, known as IPv4, is running out of addresses.

IPv4 vs IPv6

The common type of IP address (is known as IPv4, for "version 4"). Here's an example of what an IP address might look like:

```
25.59.209.224
```

An IPv4 address consists of four numbers, each of which contains one to three digits, with a single dot (.) separating each number or set of digits. This group of separated numbers creates the addresses that let you and everyone around the globe to send and retrieve data over our Internet connections. The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses which is more than 4 billion addresses. To date, it is considered the primary Internet Protocol and carries 94% of Internet traffic. Initially, it was assumed it would never run out of addresses but the present situation paves a new way to IPv6, let's see why? An IPv6 address consists of eight groups of four hexadecimal digits. Here's an example IPv6 address:

```
3001:0da8:75a3:0000:0000:8a2e:0370:7334
```

This new IP address version is being deployed to fulfil the need for more Internet addresses. With 128-bit address space, it allows 340 undecillion unique address space.

IPv6 support a theoretical maximum of 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456. To keep it straightforward, we will never run out of IP addresses again.

The next iteration of the IP standard is known as Internet Protocol version 6 (IPv6). Although IPv4 and IPv6 will coexist for a while, IPv6 is meant to work in tandem with IPv4 before eventually taking its place. We need to implement IPv6 in order to proceed and keep bringing new gadgets and services to the Internet. We can only move forward with an innovative and open Internet if we implement it, which was created with the needs of a global commercial Internet in mind.

Types of IPv6 Address

Now that we know about what is IPv6 address let's take a look at its different types.

- Unicast addresses : Only one interface is specified by the unicast address. A packet moves from one host to the destination host when it is sent to a unicast address destination.
- Multicast addresses It represents a group of IP devices and can only be used as the destination of a datagram.
- Anycast addresses The multicast address and the anycast address are the same. The way the anycast address varies from other addresses is that it can deliver the same IP address to several servers or devices. Keep in mind that the hosts do not receive the IP address. Stated differently, multiple interfaces or a collection of interfaces are assigned an anycast address.

Advantages of IPv6

- Faster Speeds: IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- Stronger Security: IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.
- Routing efficiency
- Reliability
- Most importantly it's the final solution for growing nodes in Global-network.
- The device allocates addresses on its own.
- Internet protocol security is used to support security.
- Enable simple aggregation of prefixes allocated to IP networks; this saves bandwidth by enabling the simultaneous transmission of large data packages.

Disadvantages of IPv6

- Conversion: Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
- Communication: IPv4 and IPv6 machines cannot communicate directly with each other.

- Not going backward Compatibility: IPv6 cannot be executed on IPv4-capable computers because it is not available on IPv4 systems.
- Conversion Time: One significant drawback of IPv6 is its inability to uniquely identify each device on the network, which makes the conversion to IPV4 extremely time-consuming.
- Cross-protocol communication is forbidden since there is no way for IPv4 and IPv6 to communicate with each other.

Difference Between IPv6 and IPv4

IPv6	IPv4
IPv6 has a 128-bit address length	IPv4 has a 32-bit address length
It supports Auto and renumbering address configuration	It Supports Manual and DHCP address configuration
The address space of IPv6 is quite large it can produce 3.4×1038 address space	It can generate 4.29×109 address space
Address Representation of IPv6 is in hexadecimal	Address representation of IPv4 is in decimal
In IPv6 checksum field is not available	In IPv4 checksum field is available
IPv6 has a header of 40 bytes fixed	IPv4 has a header of 20-60 bytes.
IPv6 does not support VLSM.	IPv4 supports VLSM(Variable Length subnet mask).

References

PLSP Library
Computer Applications 2nd Edition (2023) :Dan Piestun
Computer Applications (2023): Victor Borodin
Networking All-In-One for DUMMIES(2016) : Dough Lowe
Online
C615 System Administration (Jan 29,2022): Jan Shauman
learn.microsoft: October 31,2023
COMPTIA NETWORK + [N10-008] WORKBOOK(2021)