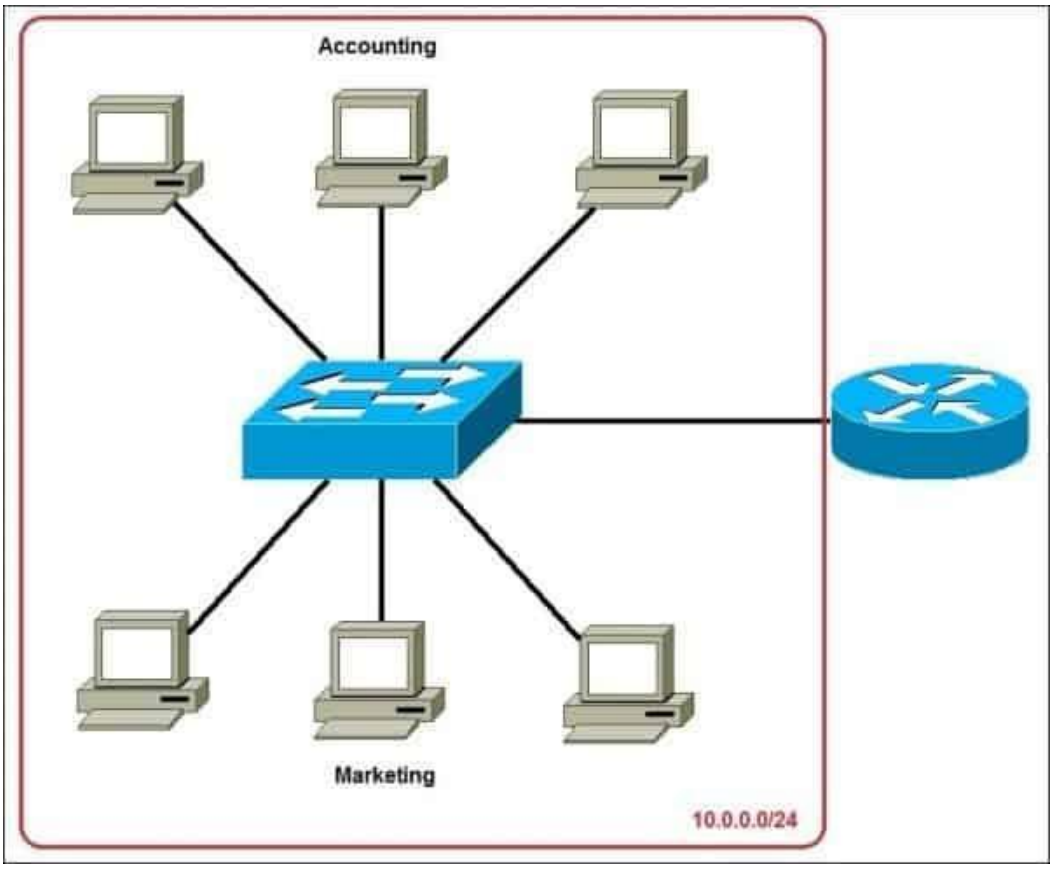
1)What is subnetting? explain it with example.

Subnetting is the practice of dividing a network into two or more smaller networks. It increases routing efficiency, enhances the security of the network and reduces the size of the broadcast domain.

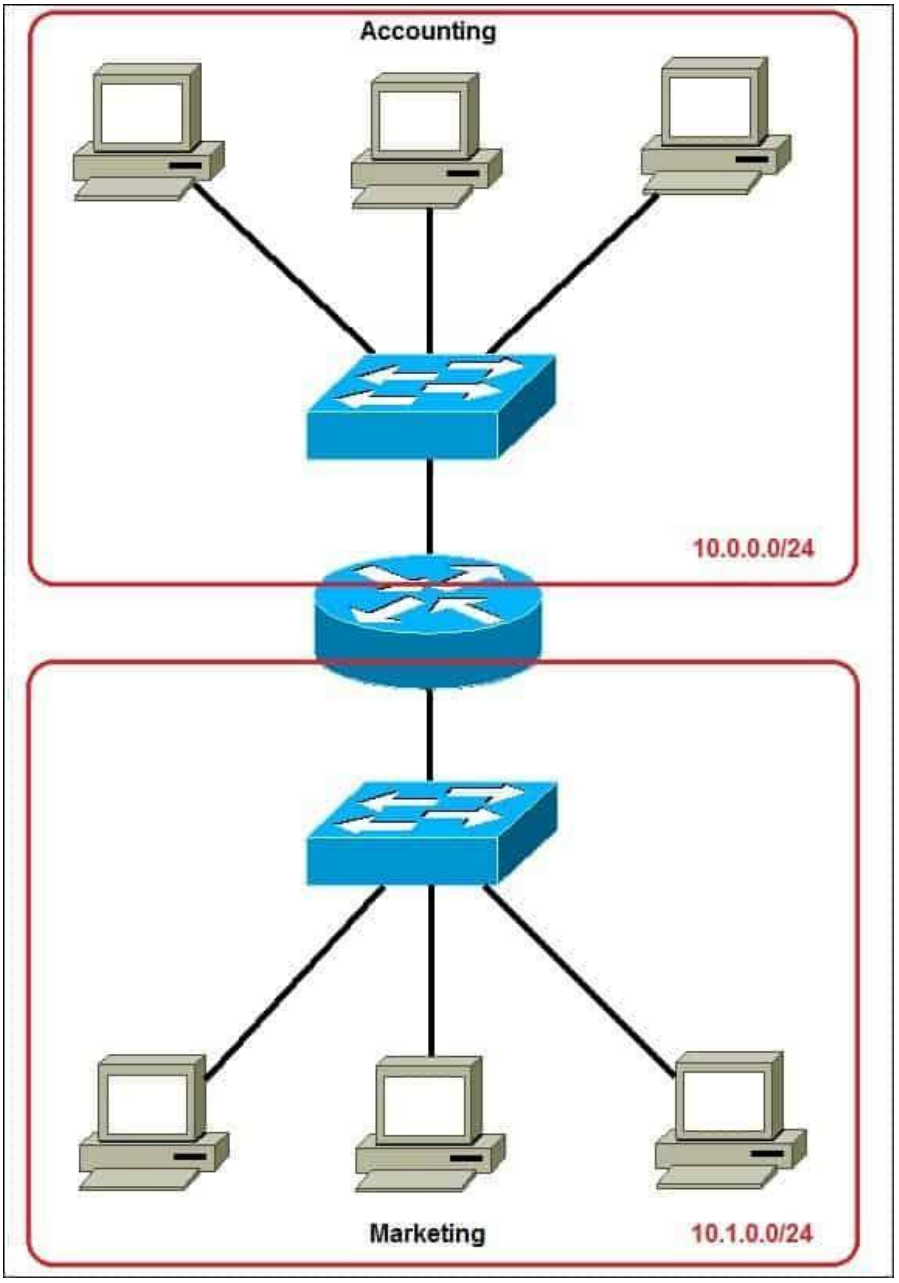
Consider the following example:



In the picture above we have one huge network: **10.0.0.0/24**. All hosts on the network are in the same subnet, which has the following disadvantages:

- **a single broadcast domain** – all hosts are in the same broadcast domain. A broadcast sent by any device on the network will be processed by all hosts, creating lots of unnecessary traffic.
- **network security** – each device can reach any other device on the network, which can present security problems. For example, a server containing sensitive information shouldn't be in the same network as user's workstations.
- **organizational problems** – in a large networks, different departments are usually grouped into different subnets. For example, you can group all devices from the **Accounting** department in the same subnet and then give access to sensitive financial data only to hosts from that subnet.

The network above could be subnetted like this:



Now, two subnets were created for different departments: **10.0.0.0/24** for Accounting and **10.1.0.0/24** for Marketing. Devices in each subnet are now in a different broadcast domain. This will reduce the amount of traffic flowing on the network and allow us to implement packet filtering on the router.

2)What is supernetting? Explain with example.

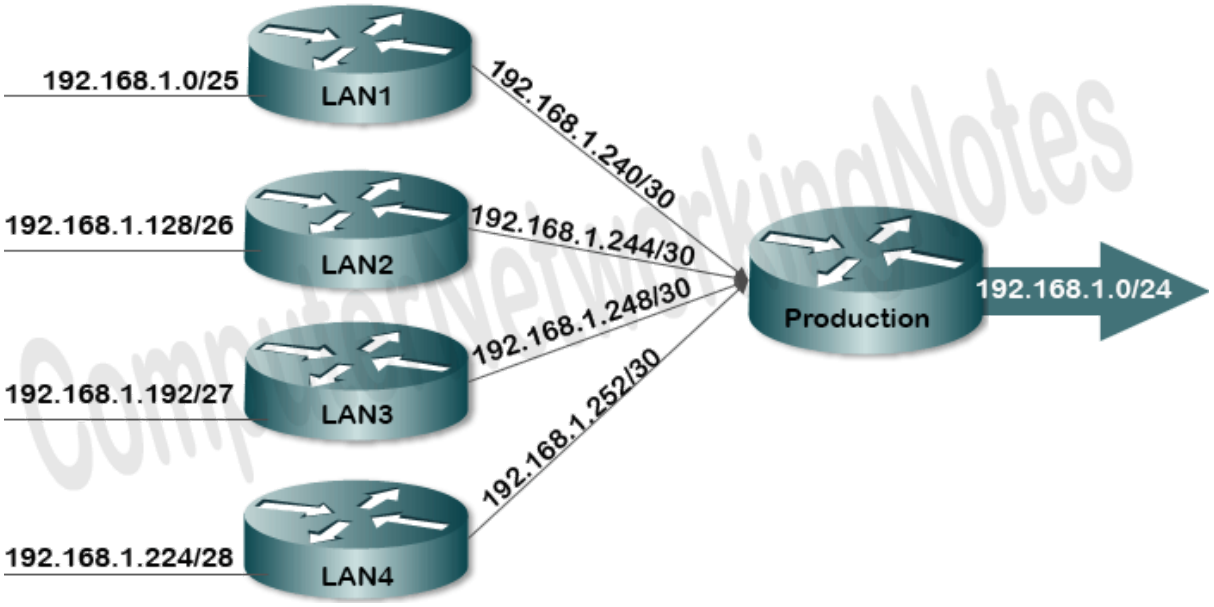
Supernetting Tutorial: – Supernetting Explained with Examples

This tutorial explains Supernetting, route summarization and route aggregation in detail with examples. Learn how Supernetting is done step by step along with the fundamental and the basic concepts of Supernetting such as what is Supernetting, why Supernetting is done and what are the advantages of Supernetting.

What is Supernetting?

Supernetting is the process of summarizing a bunch of contiguous Subnetted networks back in a single large network. Supernetting is also known as route summarization and route aggregation.

Following figure shows an example of Supernetting.



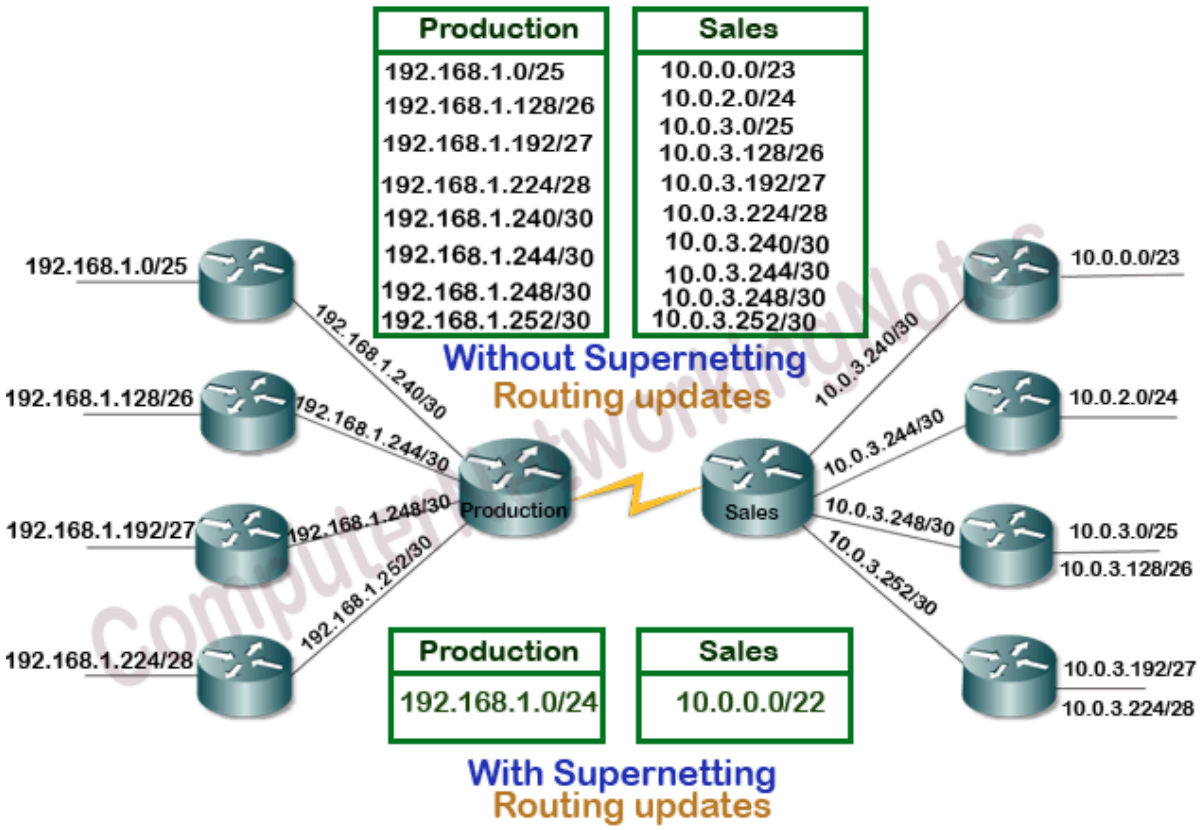
In above example, 8 subnets are summarized in single subnet.

Why Supernetting is done?

Supernetting is mainly done for optimizing the routing tables. A routing table is the summary of all known networks. Routers share routing tables to find the new path and locate the best path for destination.

Without Supernetting, router will share all routes from routing tables as they are. With Supernetting, it will summarize them before sharing. Route summarization reduces the size of routing updates dramatically.

Following figure shows an example of route summarization.



Advantage of Supernetting

Supernetting provides following advantages.

- It reduces the size of routing updates.
- It provides a better overview of network.
- It decreases the use of resources such as Memory and CPU.
- It decreases the required time in rebuilding the routing tables.

Supernetting components

Each route advertises a certain number of addresses including network ID, broadcast ID and subnet mask. We can use a term Block size to refer all these addresses collectively.

In order to perform the Supernetting, we need Network ID, CIDR Value, Broadcast ID, Subnet Mask and Block Size of each route.

- Network ID and broadcast ID are used to check the alignment of routes. Supernetting can be performed only if routes are sequential.

- Block size is used to calculate the summarized route from given routes.
- Subnet mask and CIDR value is the same thing in different notations. Both are used to find the ON network bits in IP address. In exam, question may use any notation. While preparing for Cisco exam, you should practice with both.

Since an advertise route is the combination of network ID and CIDR value, we only need to figure out the broadcast ID, subnet mask and block size.

For block size use following formulas:-

```
32 – CIDR Value = Number of host bits
Block size = 2^Number of host bits
```

For example if CIDR value is 25 then block is 128.

```
32 -25 = 7
2^7 = 128
```

Broadcast ID is the last address of network. Once you know the block size, to calculate the broadcast ID, simply count the addresses starting from network ID till the last address of the block.

For example if network ID is 192.168.1.0/25 and block size is 128 and then broadcast ID will be 192.168.1.127/25.

In counting, the 0 is used as a number. For example, [0, 1 and 2] are 3 numbers.

Following table lists all CIDR values along with subnet mask and block size.

Supernetting chart

CIDR	Subnet mask	Block Size
/8	255.0.0.0	16777216
/9	255.128.0.0	8388608
/10	255.192.0.0	4194304
/11	255.224.0.0	2097152
/12	255.240.0.0	1048576
/13	255.248.0.0	524288
/14	255.252.0.0	262144
/15	255.254.0.0	131072
/16	255.255.0.0	65536
/17	255.255.128.0	32768
/18	255.255.192.0	16384
/19	255.255.224.0	8192
/20	255.255.240.0	4096
/21	255.255.248.0	2048
/22	255.255.252.0	1024
/23	255.255.254.0	512
/24	255.255.255.0	256

/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4

This tutorial is the last part of the article "IP Subnetting in Computer Network Step by Step Explained with Examples". Other parts of this article are following.

This tutorial is the first part of the article. It explains IP addressing and network addressing such as IP address, subnet mask, IP address types and IP classes in detail.

Basic Subnetting in Computer Networks Explained

This tutorial is the second part of the article. It explains what Subnetting is and why it is necessary in computer network along with the advantages of Subnetting.

Subnetting Tutorial - Subnetting Explained with Examples

This tutorial is the third part of the article. It explains the Subnetting concepts and terms such as network id, broadcast id, total hosts, valid hosts, power of 2, block size and CIDR in detail.

Subnetting Tricks Subnetting Made Easy

This tutorial is the fourth part of the article. It explains the easiest and the fastest way of performing Subnetting in Cisco exams and interviews.

VLSM Subnetting Explained with Examples

This tutorial is the fifth part of the article. It explains what VLSM Subnetting is and how to perform it step by step along with differences between FLSM Subnetting and VLSM Subnetting.

VLSM Subnetting Examples and Calculation Explained

This tutorial is the sixth part of the article. It explains VLSM Subnetting examples step by step in detail including VLSM Subnetting practice questions and answers.

Key points of Supernetting

Supernetting can be done only in same address space. If address space is completely different between two or more routes, they cannot be summarized in a single route. For example, we can't summarize the route 192.168.1.0/25 with the route 193.168.1.128/25.

A route can be summarized only in a route which is bigger than it in block size. For example we can't summarize a route of block size 64 in a route of block size 32 but we can summarize two routes of block size 32 in a single route of block size 64.

The easiest way of calculating the summarized route is adding the block size of all sequential routes and using the Subnetting which provides the block size that is equal to the result of addition. For example if we have two sequential routes of block size 16, we can summarize them in a single route of block size 32.

Summarization can be done only in available bock sizes. For example if we have 5 routes of block size 8, we cannot summarize them in single route of block size 40 (8x5). 40 is not a valid block size. For valid block sizes see the Supernetting chart give above. In this case, the best choice is summarizing first four routes is single summarized route of block size 32 and keeping the fifth route as it is.

Just like block size, network ID of summarized route must be matched with the network ID of first sequential route. To calculate the valid network in summarized block size, simply count in block size starting from 0.

For example, if summarized block size is 32 then valid network IDs are 0, 32, 64, 96, 128, 160, 192 and 224. If the first sequential route of routes which we are summarizing doesn't start with any one of these network IDs, they can't be summarized in a single route of block size 32, even they satisfy the block size requirement.

For instance the route 192.168.1.16/28 and the route 192.168.1.32/28 can't be summarized in a single route of block size 32 even they are sequential and their collective block size (16+16) is equal to the 32.

Any sequential routes which start with any one of these network IDs can be summarized with this block size. For instance route 192.168.1.0/28 and the route 192.168.1.16/28 can be summarized in a single route 192.168.1.0/27 of block size 32

Never select a block size which does not cover all addresses unless it is clearly mentioned in question that remaining addresses will be used behind the router where summarization will be performed.

For example, if we have two routes with block size of 16 and 8, we can't summarize them in a single route of block size 32. If we do that, router will advertise a summarized route that says this router have network path for 32 addresses while in reality it have network path only for 24 (16+8) addresses.

Let's take another example. If we have three routes with block size of 16, instead of summarizing all of them in single route of block size 64 (16+16+16 = 48), we should summarize only first two routes in a single route of block size 32 (16+16 =32). In this case, router will advertise two routes; one summarized route of block size 32 and other original route. Advertising two correct routes is better than advertising a single incorrect route.

Supernetting Examples Explained Step by Step

Above we took the two examples of Supernetting. Let's understand how Supernetting was performed in them step by step.

Arrange all the routes in ascending order based on their after slash value (also known CIDR value). If CIDR value is same in two or more routes, use their IP addresses for ordering.

Supernetting Example 1	After slash value or CIDR Value	Supernetting Example 2	After slash va
192.168.1.0/25	25	10.0.0.0/23	23

192.168.1.128/26	26	10.0.2.0/24	24
192.168.1.192/27	27	10.0.3.0/25	25
192.168.1.224/28	28	10.0.3.128/26	26
192.168.1.240/30	30	10.0.3.192/27	27
192.168.1.244/30	30	10.0.3.224/28	28
192.168.1.248/30	30	10.0.3.240/30	30
192.168.1.252/30	30	10.0.3.244/30	30
		10.0.3.248/30	30
		10.0.3.252/30	30

Write the CIDR value, Subnet Mask, Network ID, Broadcast ID and block size of each route.

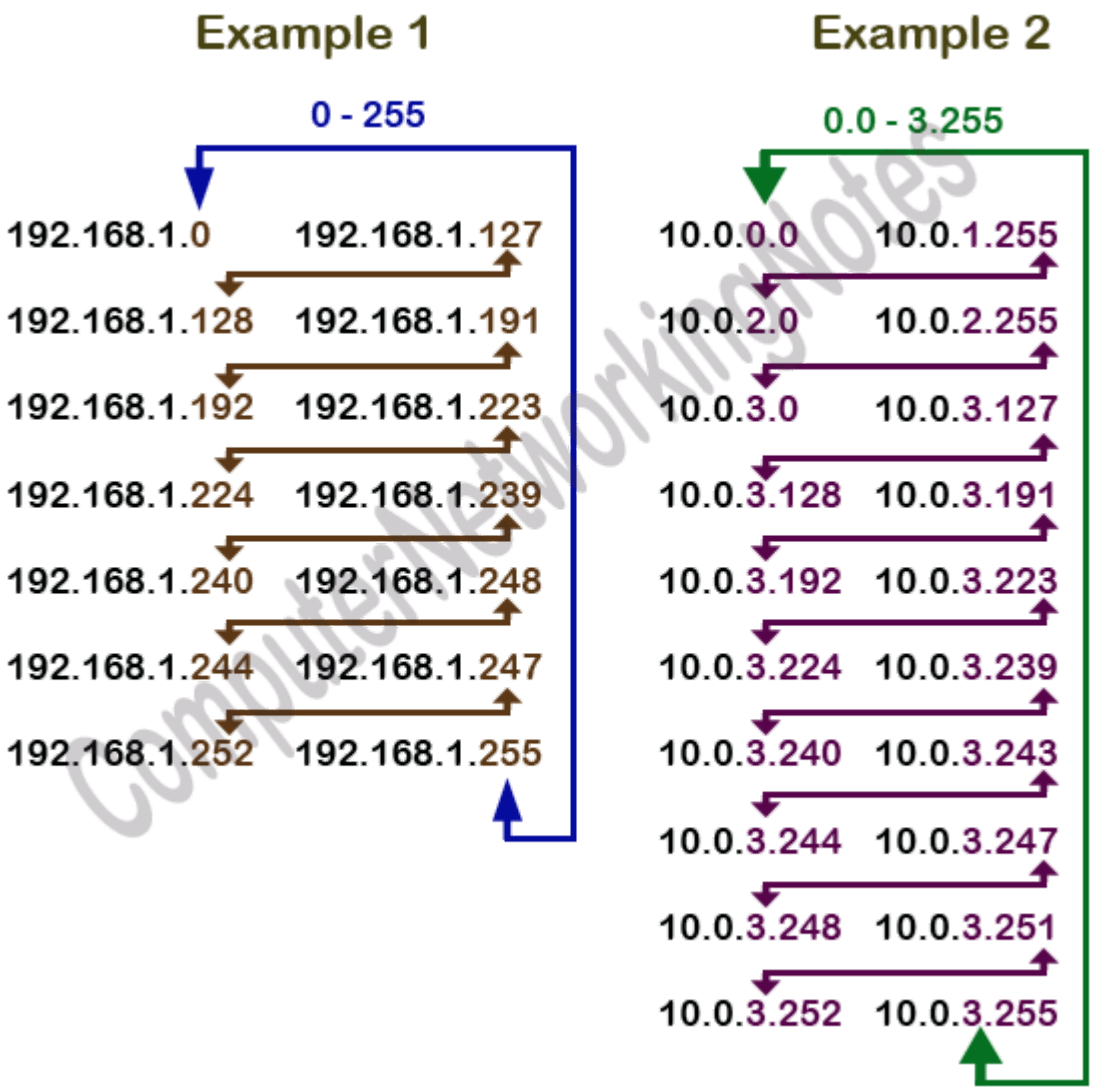
Supernetting Example 1

Route	CIDR value	Subnet Mask	Network ID	Broadcast ID
192.168.1.0/25	25	255.255.255.128	192.168.1.**0**	192.168.1.**127**
192.168.1.128/26	26	255.255.255.192	192.168.1.**128**	192.168.1.**191**
192.168.1.192/27	27	255.255.255.224	192.168.1.**192**	192.168.1.**223**
192.168.1.224/28	28	255.255.255.240	192.168.1.**224**	192.168.1.**239**
192.168.1.240/30	30	255.255.255.252	192.168.1.**240**	192.168.1.**248**
192.168.1.244/30	30	255.255.255.252	192.168.1.**244**	192.168.1.**247**
192.168.1.248/30	30	255.255.255.252	192.168.1.**248**	192.168.1.**251**
192.168.1.252/30	30	255.255.255.252	192.168.1.**252**	192.168.1.**255**

Supernetting Example 2

Route	CIDR value	Subnet Mask	Network ID	Broadcast ID
10.0.0.0/23	23	255.255.254.0	10.0.0.**0**	10.0.1.**255**
10.0.2.0/24	24	255.255.255.0	10.0.2.**0**	10.0.2.**255**
10.0.3.0/25	25	255.255.255.128	10.0.3.**0**	10.0.3.**127**
10.0.3.128/26	26	255.255.255.192	10.0.3.**128**	10.0.3.**191**
10.0.3.192/27	27	255.255.255.224	10.0.3.**192**	10.0.3.**223**
10.0.3.224/28	28	255.255.255.240	10.0.3.**224**	10.0.3.**239**
10.0.3.240/30	30	255.255.255.252	10.0.3.**240**	10.0.3.**243**
10.0.3.244/30	30	255.255.255.252	10.0.3.**244**	10.0.3.**247**
10.0.3.248/30	30	255.255.255.252	10.0.3.**248**	10.0.3.**251**
10.0.3.252/30	30	255.255.255.252	10.0.3.**252**	10.0.3.**255**

Group the routes based on sequence. If a route's network ID starts from where previous route's broadcast ID ends, it is a sequential route. But if it does not start from where previous route ends, it is not a sequential route.



Add the block size of all sequential routes.

In first example, sum of block sizes is 256 and in second example it is 1024.

Check the nearest valid block size which provides equal or less number of addresses. The block size 256 and 1024 exactly match with our requirement. The Subnetting of /24 and /22 give us the block size of 256 and 1024 respectively.

To write the summarize route, use the network ID of first route with the CIDR value or the subnet mask of the summarized route.

In first example, network ID of the first route is 192.168.1.0 and the CIDR value of summarized route is /24. Thus, the summarized route for first example will be 192.168.1.0/24.

Same way in second example, network ID of first route is 10.0.0.0 and the CIDR value of summarized route is /22. So, the summarize route for second example will be 10.0.0.0/22.

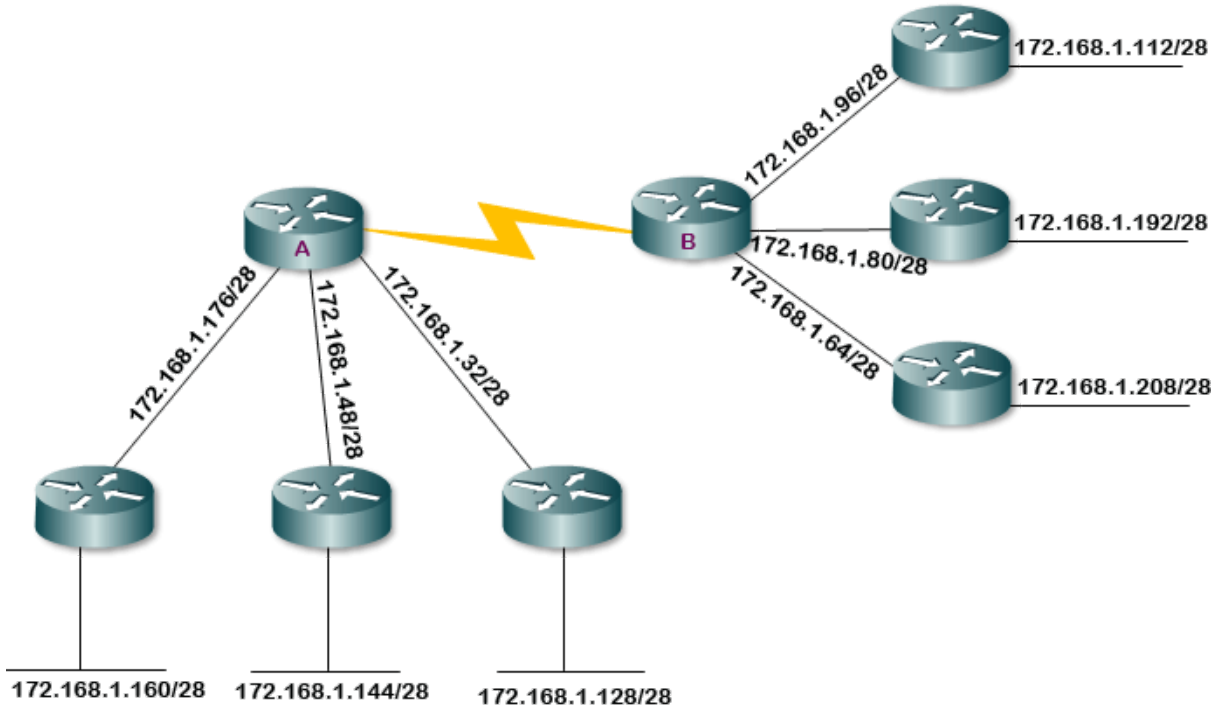
Complex Supernetting Examples

If IP addressing is planed correctly, Supernetting is simple and straightforward as we have seen in above examples. It becomes difficult only if unplanned IP addressing is used in network.

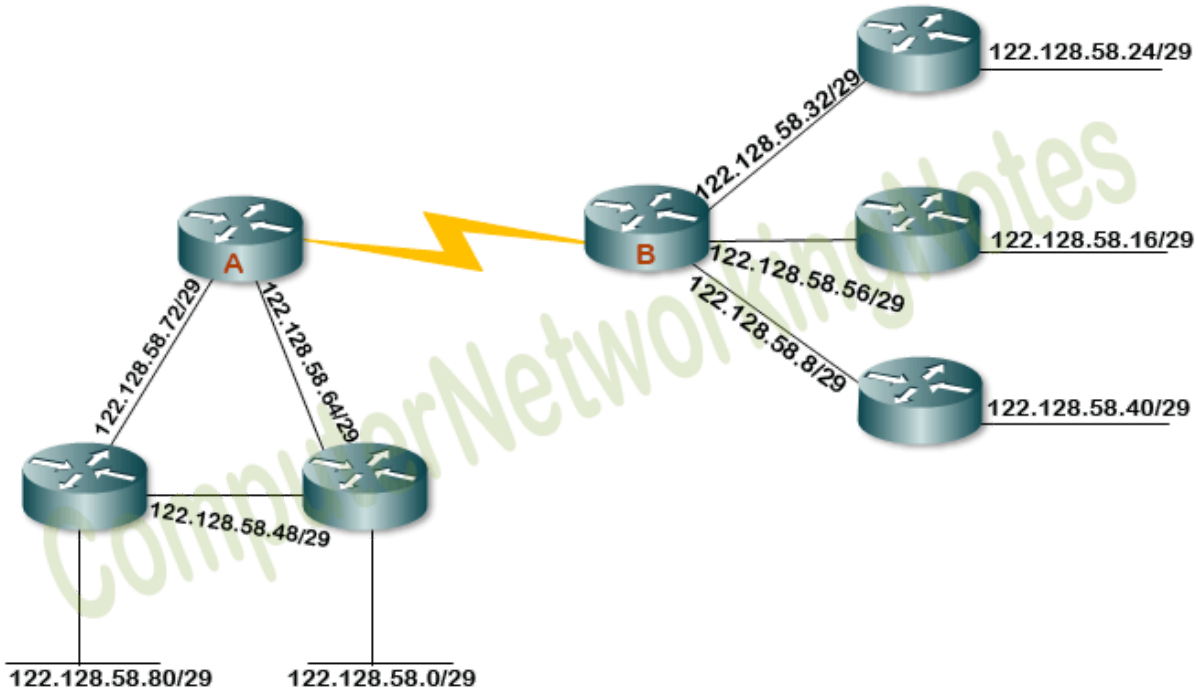
If you are preparing for Cisco exam, you should practice with unplanned IP addressing. To test candidates' caliber, Cisco usually puts complex and unplanned networks in Supernetting related questions.

To get an overview of how Supernetting questions could be difficult in Cisco exam, let's have two examples of complex Supernetting. These examples are based on Supernetting questions asked in CCNA Routing and Switching exam.

Supernetting Example 3



Supernetting Example 4



Step 1: - Arrange all routes in ascending order.

Supernetting Example 3		Supernetting Example 4	
Router A	Router B	Router A	Router B
172.168.1.32/28	172.168.1.64/28	122.128.58.0/29	122.128.
172.168.1.48/28	172.168.1.80/28	122.128.58.48/29	122.128.
172.168.1.128/28	172.168.1.96/28	122.128.58.64/29	122.128.
172.168.1.144/28	172.168.1.112/28	122.128.58.72/29	122.128.
172.168.1.160/28	172.168.1.192/28	122.128.58.80/29	122.128.
172.168.1.176/28	172.168.1.208/28	122.128.58.56/29	

Step 2: - Write the network ID, broadcast ID, CIDR value, subnet mask and block size of each route.

Supernetting Example 3 (Router A)

Route	CIDR	Subnet mask	Network ID	Broadcast ID
172.168.1.32	28	255.255.240.0	172.168.1.32	172.168.1.47
172.168.1.48	28	255.255.240.0	172.168.1.48	172.168.1.63
172.168.1.128	28	255.255.240.0	172.168.1.128	172.168.1.143
172.168.1.144	28	255.255.240.0	172.168.1.144	172.168.1.159
172.168.1.160	28	255.255.240.0	172.168.1.160	172.168.1.175
172.168.1.176	28	255.255.240.0	172.168.1.176	172.168.1.191

Supernetting Example 3 (Router B)

Route	CIDR	Subnet mask	Network ID	Broadcast ID
172.168.1.64	28	255.255.240.0	172.168.1.64	172.168.1.79

172.168.1.80	28	255.255.240.0	172.168.1.80	172.168.1.95
172.168.1.96	28	255.255.240.0	172.168.1.96	172.168.1.111
172.168.1.112	28	255.255.240.0	172.168.1.112	172.168.1.127
172.168.1.192	28	255.255.240.0	172.168.1.192	172.168.1.207
172.168.1.208	28	255.255.240.0	172.168.1.208	172.168.1.223

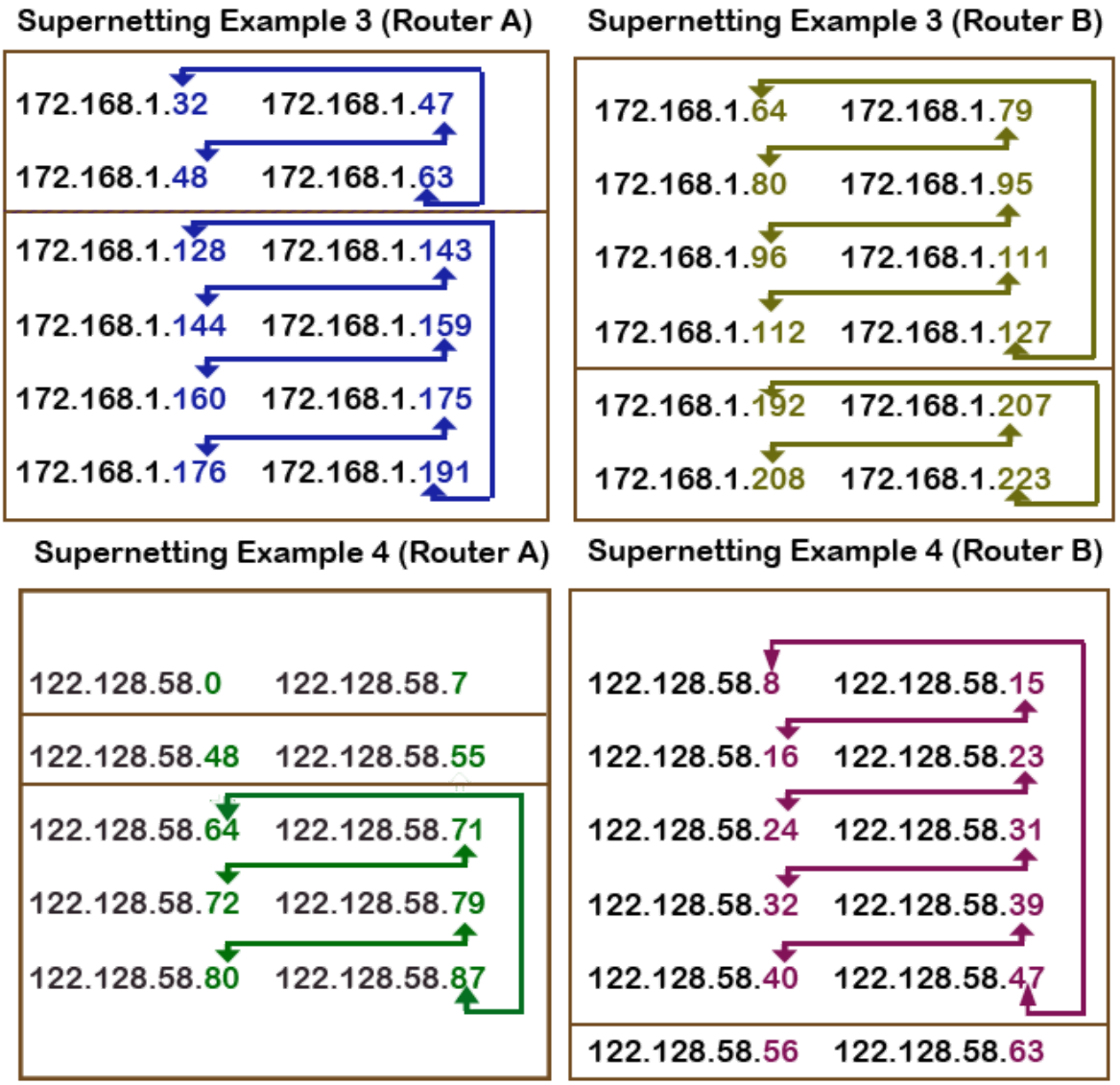
Supernetting Example 4 (Router A)

Route	CIDR	Subnet mask	Network ID	Broadcast ID
122.128.58.0	29	255.255.255.248	122.128.58.0	122.128.58.7
122.128.58.48	29	255.255.255.248	122.128.58.48	122.128.58.55
122.128.58.64	29	255.255.255.248	122.128.58.64	122.128.58.71
122.128.58.72	29	255.255.255.248	122.128.58.72	122.128.58.79
122.128.58.80	29	255.255.255.248	122.128.58.80	122.128.58.87

Supernetting Example 4 (Router B)

Route	CIDR	Subnet mask	Network ID	Broadcast ID
122.128.58.8	29	255.255.255.248	122.128.58.8	122.128.58.15
122.128.58.16	29	255.255.255.248	122.128.58.16	122.128.58.23
122.128.58.24	29	255.255.255.248	122.128.58.24	122.128.58.31
122.128.58.32	29	255.255.255.248	122.128.58.32	122.128.58.39
122.128.58.40	29	255.255.255.248	122.128.58.40	122.128.58.47
122.128.58.56	29	255.255.255.248	122.128.58.56	122.128.58.63

Step 3: - Based on network ID and Broadcast ID make the group of sequential routes.



Step 4: - Summarize each group of sequential routes in a single or multiple summarized routes.

- Add the block size of all sequential routes in group.
- Find the valid block which is equal or less in size.
- Starting from 0, count in valid block size and check whether the network ID of first sequential route exists in result or not.
- If network ID of first sequential route exists in result, use the valid block size to summarize the routes.
- For summarization use the CIDR value which provides this block size.
- If network ID of first sequential route does not exist in result, use smaller valid block size and count again. Repeat this step until the network ID of first sequential route does not fall in result.

Supernetting example 3 (Router A)

As we can see in above figure, there are two groups of sequential routes in this router.

In first group, there are two sequential routes; 32 and 48. Both routes have a block size of 16. The sum of block sizes is 32 (16+16). 32 is a valid block size. The network ID of first sequential route is 32 which is a valid network ID in block size 32 (0, **32**, 64,...). Block size 32 is associated with CIDR value /27. Let's use this block size for summarization.

Summarize the routes 172.168.1.32/28 and the route 172.168.1.48/28 in a single route 172.168.1.32/27 of block size 32.

In second group, there are 4 sequential routes 128, 144, 160 and 176 of block size 16. The sum of all block sizes is 64. 64 is a valid block size. Network ID of first sequential route (128) is also in the range of block size 64 (0, 64, **128**, 192 .....). Thus, we can use the block size 64 to summarize these routes. CIDR value of block size 64 is /26. Let's use it to summarize these routes.

Summarize the routes 172.168.1.128/28, 172.168.1.144/28, 172.168.1.160/28 and 172.168.1.176/28 in a single route 172.168.1.128/26 of block size 64.

Supernetting example 3 (Router B)

This router also has the two groups of sequential routes. In first group there are 4 sequential routes 64, 80, 96 and 112 of block size 16 and in second group there are 2 sequential routes 192 and 208 of block size 16.

The sum of block sizes is 64 (16+16+16+16) in first group and 32 (16+16) in second group. Both 64 and 32 are valid block sizes and the network ID of first sequential route in both groups is also a valid network ID in both block sizes.

Summarize the routes 172.168.1.64/28, 172.168.1.80/28, 172.168.1.96/28 and 172.168.1.112/28 a single route 172.168.1.64/26 of block size 64.

Summarize the routes 172.168.1.192/28 and the route 172.168.1.208/28 in a single route 172.168.1.192/27 of block size 32.

Supernetting example 4 (Router A)

There are total 5 routes behind this router. Since first two routes 0 and 48 have no sequential routes, we have to advertise them individually. We can't summarize a route which has no sequential route.

Remaining 3 routes 64, 72 and 80 are sequential with the block size 8. The sum of block sizes (8+8+8) is 24. Since 24 is not a valid block size, we have to exclude the routes from summarization until the sum of block sizes becomes equal to a valid block size. If we exclude one route from summarization, the sum of block sizes reduces to 16 which is a valid block size.

In block size 16, 64 (the network ID of first sequential route) is a valid network ID (0, 16, 32, 48, **64**, 80.....).

Summarize first two routes in a summarize route 122.128.58.64/28 of block size 16 and advertise the remaining third route 122.128.58.80/29 independently.

Supernetting example 4 (Router B)

There are total 6 routes behind this router. Since last route 56 has no sequential route, it can't be summarized.

Remaining five routes 8, 16, 24, 32 and 40 are sequential. Total numbers of address in these routes are 40 (8+8+8+8+8). 40 is not a valid block size. The nearest valid block size is 32. So if we exclude one route (8+8+8+8-8 = 32), can we use the block size 32 for remaining routes?

No, even 32 is a valid block size, still it can't be used. In order to use it, network ID of first route must be any one ID form 0, 32, 64, 96, 128, 160, 192 and 224. While in this case, network ID of first route is 8. Thus the block size 32 can't be used for summarization.

Our next valid block size is 16. If we use this block size, we have to create two summarized routes and skip one sequential route from the summarization. Each summarized route of block size 16 will summarize the 2 sequential routes of the block size 8.

Since in order to use the block size 16, we have to skip one route from the five sequential routes and due to the same reason explained above in block size 32 we can't summarize the first route 8, exclude the first route from summarization.

Summarize remaining 4 routes (16, 24, 32, and 40) of block size 8 in two separate summarized routes 122.128.58.16/28 and 122.128.58.32/28 of block size 16.

Following table lists the summarized routes for all four routers.

Example3 (Router A)	Example3 (Router B)	Example4 (Router A)	Example
172.168.1.32/27	172.168.1.64/26	*122.128.58.0/29*	*122.128.*
172.168.1.128/26	192.168.1.192/27	*122.128.58.48/29*	122.128.
		122.128.58.64/28	122.128.
		122.128.58.80/29	*122.128.*

The routes which couldn't be summarized are formatted in bold and italic.

That's all for this tutorial. If you have any feedback, suggestion or comment about this tutorial, please mail me. If you like this tutorial, don't forget to share it through your favorite social platform.

By ComputerNet

3)What is Reliable communication?

(not complete ans)

Peoples are naturally communicators but devices are not. In the Internet of Things (IoT) architecture, the smart devices (SDs), sensors, programs and association of smart objects are connected together to transfer information among them. The SD is designed as physical device linked with computing resources that are capable to connect and communicate with

another SD through any medium and protocol. The communication among intelligent physical things is a challenging task to exchange information that guaranteed to reach to the destination completely in a real time with the same order as sending without corruption. The reliable communication between physical things can be built in the transmission control protocol (TCP) layers. In TCP layer, the reliable communication is required the error detection, correction and confirmation to exchange information among smart devices. In this paper, the author represents a framework to deal with reliability issues to enable the

adoption of IoT devices. The results found the improvement in reliability.

4)What is multicast ,broadcast ,anycast and unicast?

Multicasting in Computer Network

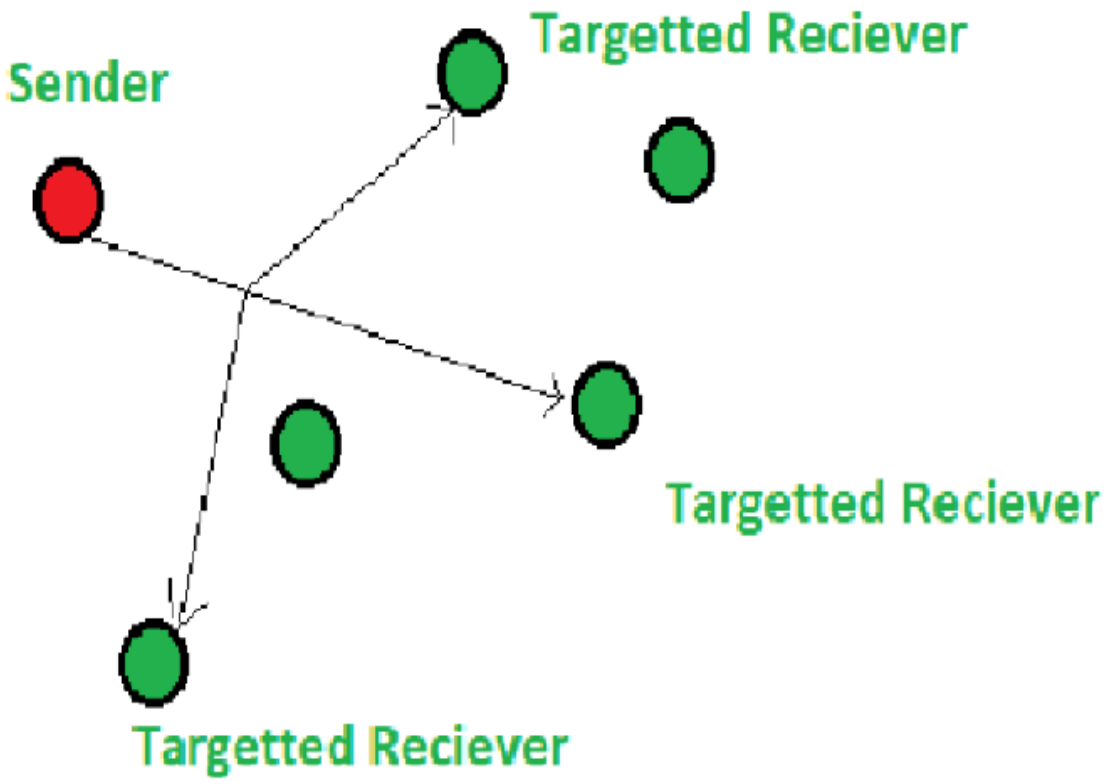
- Difficulty Level : Easy
- Last Updated : 10 May, 2020

Read

Discuss

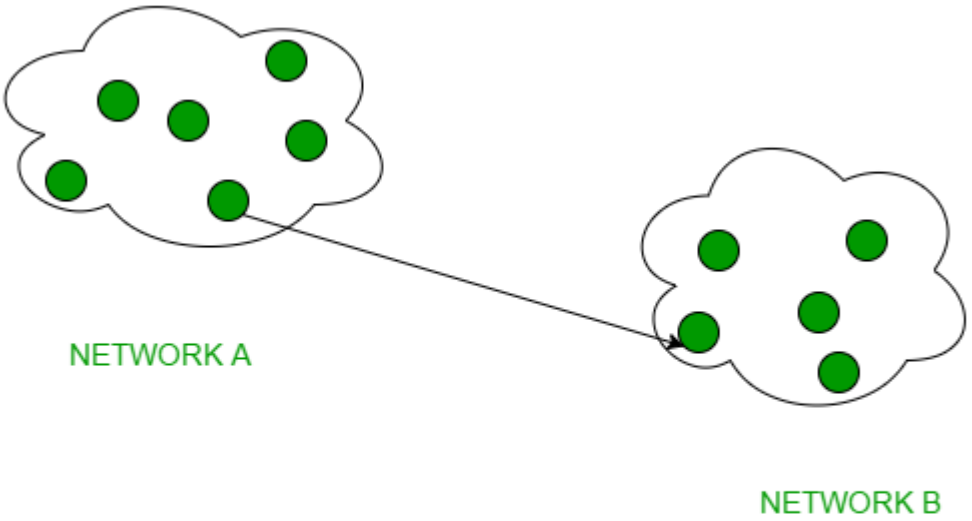
Multicast is a method of group communication where the sender sends data to multiple receivers or nodes present in the network simultaneously. Multicasting is a type of one-to-many and many-to-many communication as it allows sender or senders to send data packets to multiple receivers at once across LANs or WANs. This process helps in minimizing the data frame of the network.

Multicasting works in similar to Broadcasting, but in Multicasting, the information is sent to the targeted or specific members of the network. This task can be accomplished by transmitting individual copies to each user or node present in the network, but sending individual copies to each user is inefficient and might increase the network latency. To overcome these shortcomings, multicasting allows a single transmission that can be split up among the multiple users, consequently, this reduces the bandwidth of the signal.



1. Unicast –

This type of information transfer is useful when there is a participation of a single sender and a single recipient. So, in short, you can term it as a one-to-one transmission. For example, if a device having IP address 10.1.2.0 in a network wants to send the traffic stream(data packets) to the device with IP address 20.12.4.2 in the other network, then unicast comes into the picture. This is the most common form of data transfer over the networks.

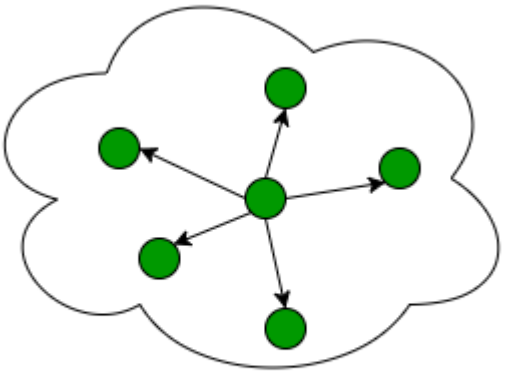


UNICAST EXAMPLE

2. Broadcast –

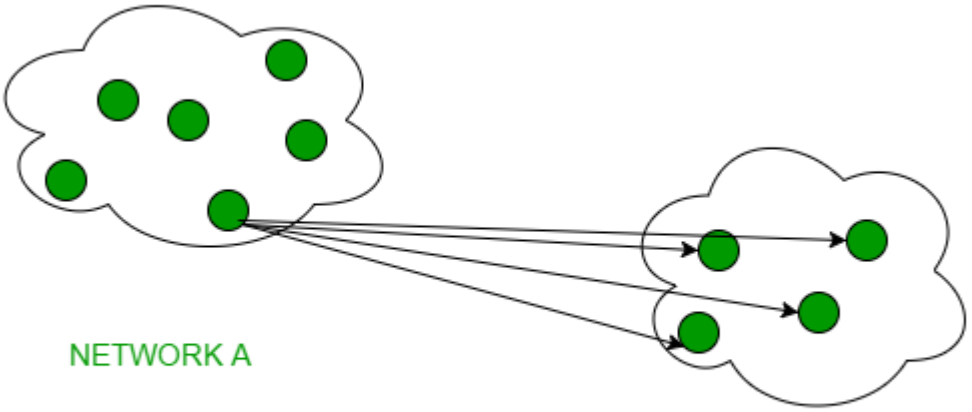
Broadcasting transfer (one-to-all) techniques can be classified into two types :

- **Limited Broadcasting –**
  Suppose you have to send a stream of packets to all the devices over the network that you reside, this broadcasting comes in handy. For this to achieve, it will append 255.255.255.255 (all the 32 bits of IP address set to 1) called as **Limited Broadcast Address** in the destination address of the datagram (packet) header which is reserved for information transfer to all the recipients from a single client (sender) over the network.



NETWORK CLUSTER

- **Direct Broadcasting –**
  This is useful when a device in one network wants to transfer packet stream to all the devices over the other network. This is achieved by translating all the Host ID part bits of the destination address to 1, referred to as **Direct Broadcast Address** in the datagram header for information transfer.



NETWORK A

NETWORK B

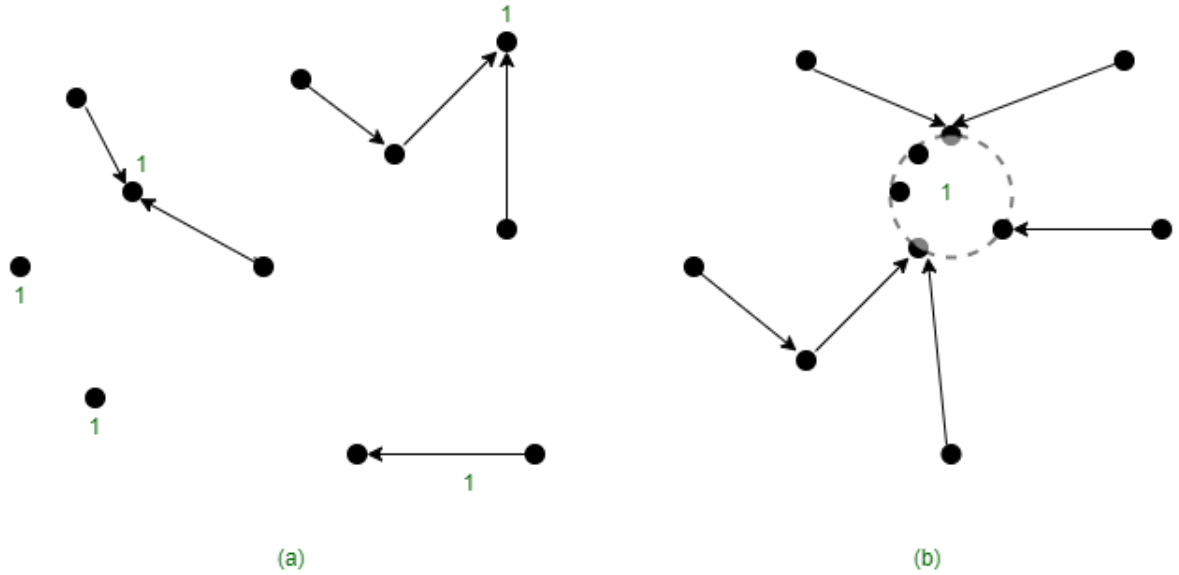
This mode is mainly utilized by television networks for video and audio distribution.
One important protocol of this class in Computer Networks is Address Resolution Protocol (ARP) which is used for resolving an IP address into a physical address which is necessary for underlying communication

Anycast Routing

- Difficulty Level : Basic
- Last Updated : 07 Jul, 2022

Read
Discuss

A packet is delivered to the nearest member of a group, in anycast. **Anycast routing** finds these paths. Sometimes nodes provide a service, such as time of day or content distribution for which it is getting the right information all that matters, not the node that is contacted; any node will do. For example, anycast is used in the internet as part of DNS. **Topology :** Regular distance vector and link state routing can produce anycast routes because there is no need to devise new routing schemes for anycast. Suppose we want to anycast to the members of group 1. They will be given the address “1”, instead of different addresses. Distance vector routing will distribute vectors as usual, and nodes will choose the shortest path to destination 1. This will result in nodes sending to the nearest instance of destination 1. That is, it believes that all the instances of node 1 are the same node, as in the topology shown in figure below.



(a) Anycast routes to group 1 (b) Topology seen by the routing protocol

This procedure works for link state routing as well, although there is the added consideration that the routing protocol must not find seemingly short paths that pass through node 1. This would result in jumps through hyperspace, since the instances of node 1 are really nodes located in different parts of the network. However, link state protocols already make this distinction between routers and hosts. We glossed over this fact earlier because it was not needed for our discussion.

5)What is crc?

. **CRC :** CRC or Cyclic Redundancy Check is the error detection method to detect the errors and this method is used by upper layer protocols. It contains **Polynomial Generator** on both sender and receiver side. The polynomial generator is of the type x^3+x^2+x+1.

CRC is a thorough concept for detection and reporting of errors

It is capable of detecting double digits errors

It follows a complex computation method.

Due to complex computation, it can detect more errors.

t is based on hash approach. It is widely used in analog transmission for data validation

Cyclic Redundancy Check (CRC)

By Dinesh Thakur

Cyclic Redundancy Check (CRC) An error detection mechanism in which a special number is appended to a block of data in order to detect any changes introduced during storage (or transmission). The CRe is recalculated on retrieval (or reception) and compared to the value originally transmitted, which can reveal certain types of error. For example, a single corrupted bit in the data results in a one-bit change in the calculated CRC, but multiple corrupt bits may cancel each other out.

A CRC is derived using a more complex algorithm than the simple CHECKSUM, involving MODULO ARITHMETIC (hence the 'cyclic' name) and treating each input word as a set of coefficients for a polynomial.

• CRC is more powerful than VRC and LRC in detecting errors.

• It is not based on binary addition like VRC and LRC. Rather it is based on binary division.

• At the sender side, the data unit to be transmitted IS divided by a predetermined divisor (binary number) in order to obtain the remainder. This remainder is called CRC.

• The CRC has one bit less than the divisor. It means that if CRC is of n bits, divisor is of n+ 1 bit.

• The sender appends this CRC to the end of data unit such that the resulting data unit becomes exactly divisible by predetermined divisor *i.e.* remainder becomes zero.

• At the destination, the incoming data unit *i.e.* data + CRC is divided by the same number (predetermined binary divisor).

• If the remainder after division is zero then there is no error in the data unit & receiver accepts it.

• If remainder after division is not zero, it indicates that the data unit has been damaged in transit and therefore it is rejected.

• This technique is more powerful than the parity check and checksum error detection.

• CRC is based on binary division. A sequence of redundant bits called CRC or CRC remainder is appended at the end of a data unit such as byte.

Requirements of CRC :

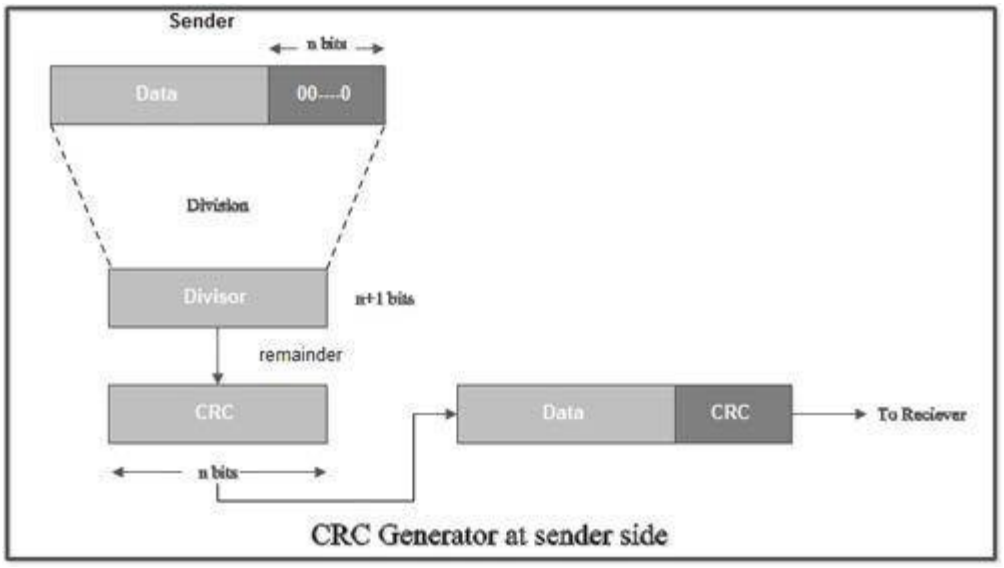
A CRC will be valid if and only if it satisfies the following requirements:

1. It should have exactly one less bit than divisor.
2. Appending the CRC to the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.

• The various steps followed in the CRC method are

1. A string of n as is appended to the data unit. The length of predetermined divisor is n+ 1.

2. The newly formed data unit *i.e.* original data + string of n as are divided by the divisor using binary division and remainder is obtained. This remainder is called CRC.



3. Now, string of n Os appended to data unit is replaced by the CRC remainder (which is also of n bit).

4. The data unit + CRC is then transmitted to receiver.

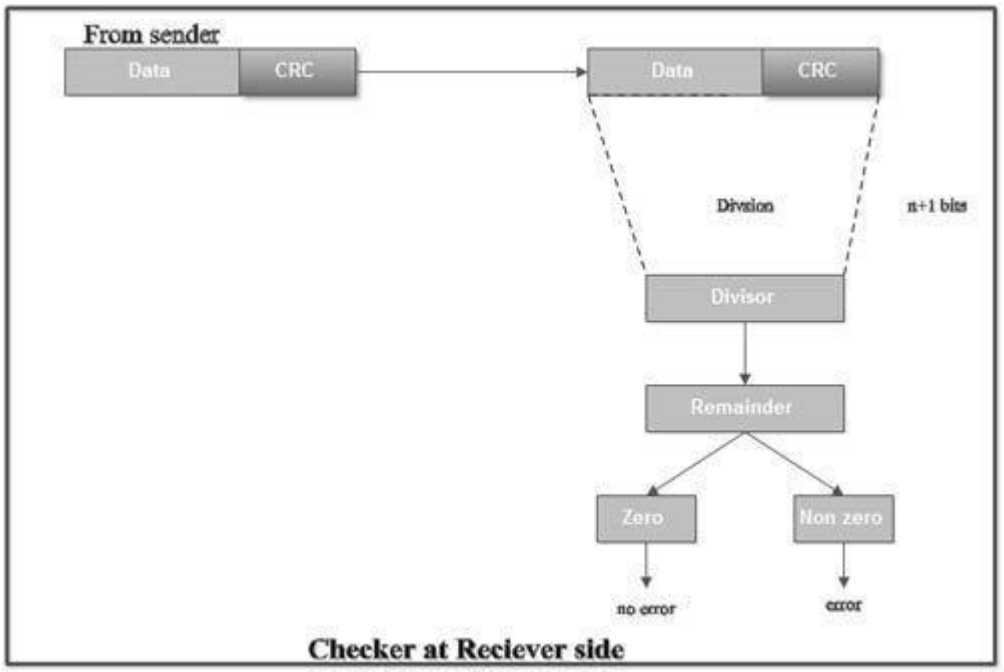
5. The receiver on receiving it divides data unit + CRC by the same divisor & checks the remainder.

6. If the remainder of division is zero, receiver assumes that there is no error in data and it accepts it.

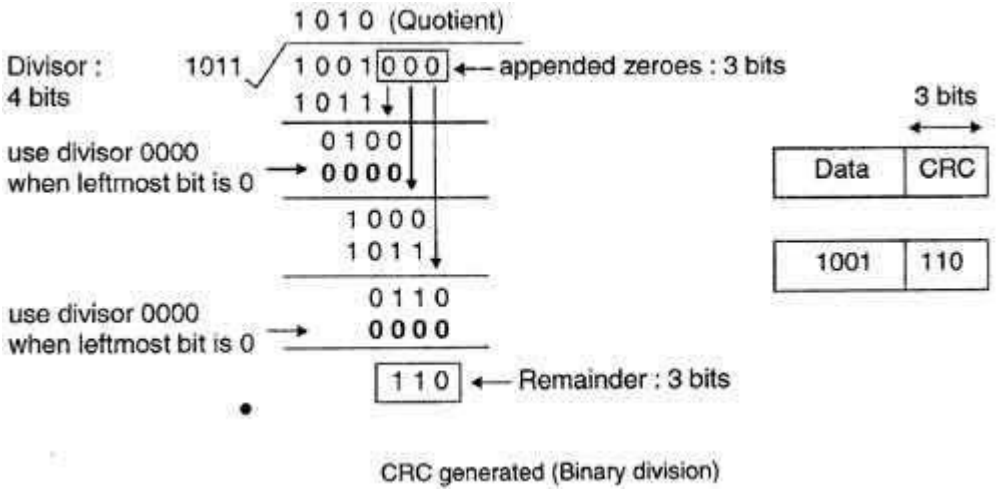
7. If remainder is non-zero then there is an error in data and receiver rejects it.

• For example, if data to be transmitted is 1001 and predetermined divisor is 1011. The procedure given below is used:

1. String of 3 zeroes is appended to 1011 as divisor is of 4 bits. Now newly formed data is 1011000.



1. Data unit 1011000 is divided by 1011.



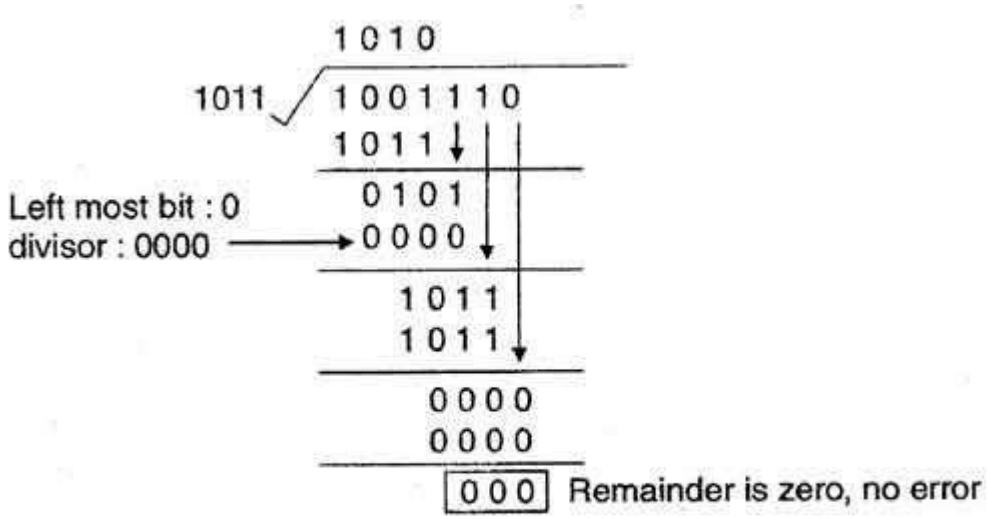
CRC generated (Binary division)

2. During this process of division, whenever the leftmost bit of dividend or remainder is 0, we use a string of Os of same length as divisor. Thus in this case divisor 1011 is replaced by 0000.

3. At the receiver side, data received is 1001110.

4. This data is again divided by a divisor 1011.

5. The remainder obtained is 000; it means there is no error.



CRC decoded (binary division)

• CRC can detect all the burst errors that affect an odd number of bits.

• The probability of error detection and the types of detectable errors depends on the choice of divisor.

• Thus two major requirement of CRC are:

(a) CRC should have exactly one bit less than divisor.

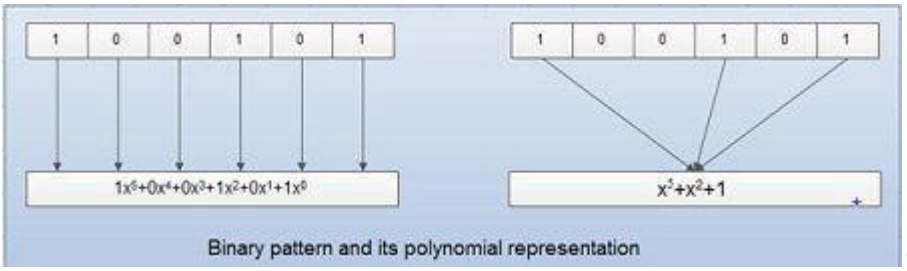
(b) Appending the CRC to the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.

Polynomial codes

• A pattern of Os and 1s can be represented as a polynomial with coefficient of o and 1.

• Here, the power of each term shows the position of the bit and the coefficient shows the values of the bit.

• For example, if binary pattern is 100101, its corresponding polynomial representation is $x^5 + x^2 + 1$. Figure shows the polynomial where all the terms with zero coefficient are removed and x J is replaced by x and XO by 1.



• The benefits of using polynomial codes is that it produces short codes. For example here a 6-bit pattern is replaced by 3 terms.

• In polynomial codes, the degree is 1 less than the number of bits in the binary pattern. The degree of polynomial is the highest power in polynomial. For example as shown in fig degree of polynomial $x^5 + x^2 + 1$ are 5. The bit pattern in this case is 6.

• Addition of two polynomials is based on modulo-2 method. In such as case, addition and subtraction is same.

• Addition or subtraction is .done by combining terms and deleting pairs of identical terms. For example adding $x^5 + x^4 + x^2$ and $x^6 + x^4 + x^2$ give $x^6 + x^5$. The terms x^4 and x^2 are deleted.

• If three polynomials are to be added and if we get a same term three times, a pair of them is detected and the third term is kept. For example, if there is x^2 three times then we keep only one x^2

• In case of multiplication of two polynomials, their powers are added. For example, multiplying $x^5 + x^3 + x^2 + x$ with $x^2 + x + 1$ yields:

$(X^5 + x^3 + x^2 + x)(x^2 + x + 1)$

$= x^7 + x^6 + x^5 + x^5 + x^4 + x^3 + x^4 + x^3 + x^2 + x^3 + x^2 + x$

$= X^7 + x^6 + x^3 + X$

In this, first polynomial is multiplied by all terms of second. The result is then simplified and pairs of equal terms are deleted.

• Incase of division, the two polynomials are divided as per the rules of binary division, until the degree of dividend is less than that of divisor.

CRC generator using polynomials

• If we consider the data unit 1001 and divisor or polynomial generator 1011their polynomial representation is:

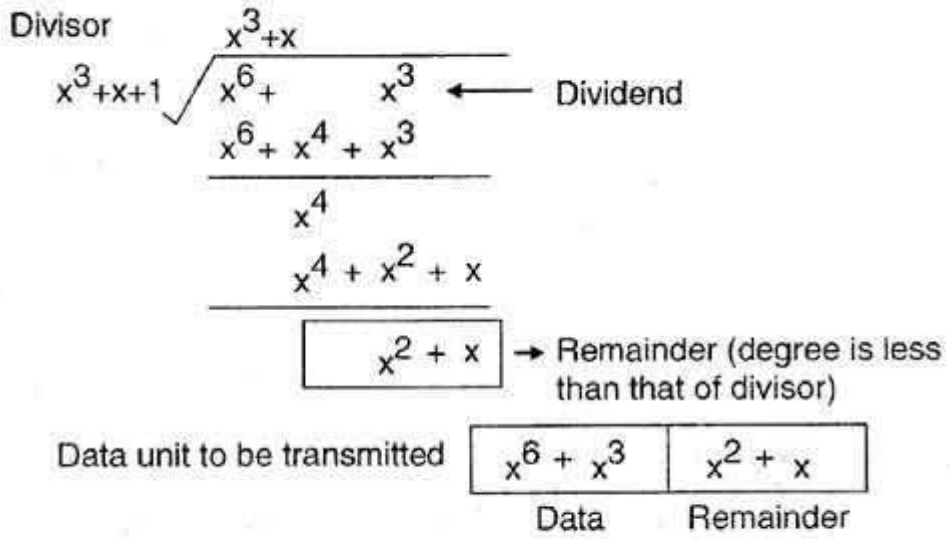
• Now string of n 0s (one less than that of divisor) is appended to data. Now data is 1001000 and its corresponding polynomial representation is $x^6 + x^3$.

• The division of $x^6 + x^3$ by $x^3 + x + 1$ is shown in fig.

• The polynomial generator should have following properties:

1. It should have at least two terms.

Data	1001	$x^3 + 1$
Division (polynomial generator)	1011	$x^3 + x + 1$



CRC division using polynomial

2. The coefficient of the term x^0 should be 1.

3. It should not be divisible by x.

4. It should be divisible by x+ 1.

• There are several different standard polynomials used by popular protocols for CRC generation. These are:

Name	Polynomial	Application
CRC-8	$x^8 + x^2 + x + 1$	ATM header
CRC-10	$x^{10} + x^9 + x^5 + x^4 + x^2 + 1$	ATM AAL
CRC-16	$x^{16} + x^{12} + x^5 + 1$	HDLC
CRC-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	LANs

6)Which layers is having security protocol?

What is Transport Layer Security (TLS)?

Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP). In this article we will focus on the role of TLS in web application security.

TLS was proposed by the Internet Engineering Task Force (IETF), an international standards organization, and the first version of the protocol was published in 1999. The most recent version is TLS 1.3, which was published in 2018.

What is the difference between TLS and SSL?

TLS evolved from a previous encryption protocol called Secure Sockets Layer (SSL), which was developed by Netscape. TLS version 1.0 actually began development as SSL version 3.1, but the name of the protocol was changed before publication in order to indicate that it was no longer associated with Netscape. Because of this history, the terms TLS and SSL are sometimes used interchangeably.

What is the difference between TLS and HTTPS?

HTTPS is an implementation of TLS encryption on top of the HTTP protocol, which is used by all websites as well as some other web services. Any website that uses HTTPS is therefore employing TLS encryption.

Why should businesses and web applications use the TLS protocol?

TLS encryption can help protect web applications from data breaches and other attacks. Today, TLS-protected HTTPS is a standard practice for websites. The Google Chrome browser gradually cracked down on non-HTTPS sites, and other browsers have followed suit. Everyday Internet users are more wary of websites that do not feature the HTTPS padlock icon.

What does TLS do?

There are three main components to what the TLS protocol accomplishes: Encryption, Authentication, and Integrity.

- **Encryption:** hides the data being transferred from third parties.
- **Authentication:** ensures that the parties exchanging information are who they claim to be.
- **Integrity:** verifies that the data has not been forged or tampered with.

How does TLS work?

For a website or application to use TLS, it must have a TLS certificate installed on its origin server (the certificate is also known as an "SSL certificate" because of the naming confusion described above). A TLS certificate is issued by a certificate authority to the person or business that owns a domain. The certificate contains important information about who owns the domain, along with the server's public key, both of which are important for validating the server's identity.

A TLS connection is initiated using a sequence known as the TLS handshake. When a user navigates to a website that uses TLS, the TLS handshake begins between the user's device (also known as the *client* device) and the web server.

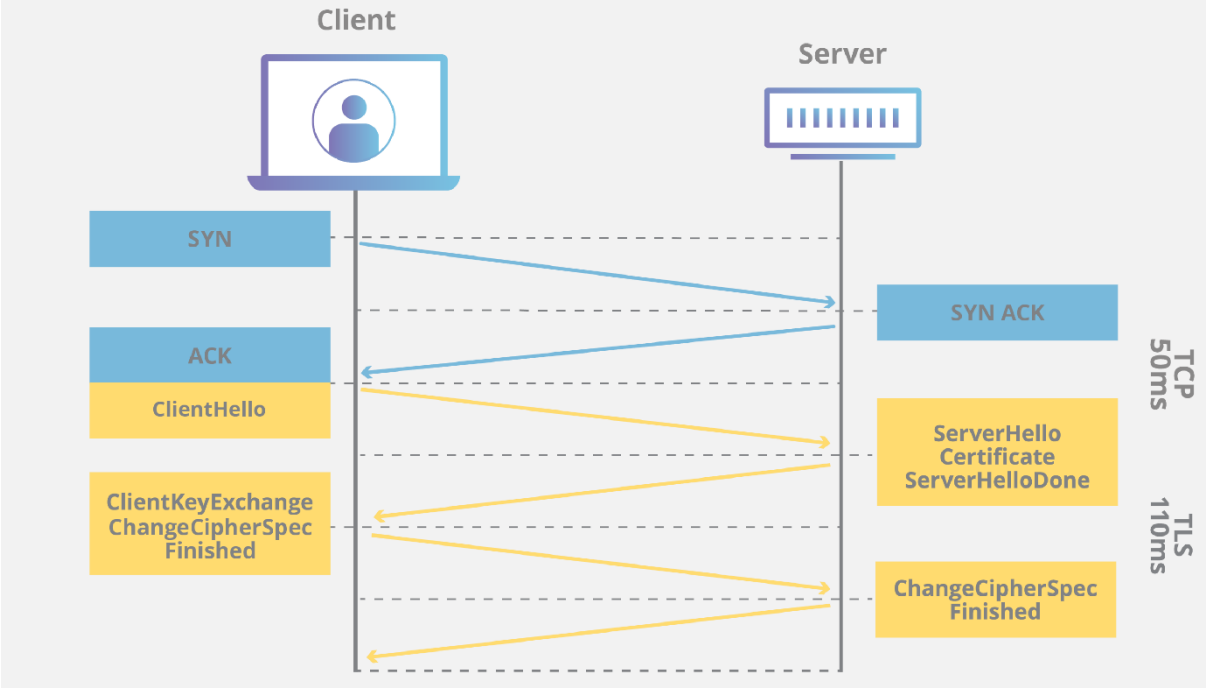
During the TLS handshake, the user's device and the web server:

- Specify which version of TLS (TLS 1.0, 1.2, 1.3, etc.) they will use
- Decide on which cipher suites (see below) they will use
- Authenticate the identity of the server using the server's TLS certificate
- Generate session keys for encrypting messages between them after the handshake is complete

The TLS handshake establishes a cipher suite for each communication session. The cipher suite is a set of algorithms that specifies details such as which shared encryption keys, or session keys, will be used for that particular session. TLS is able to set the matching session keys over an unencrypted channel thanks to a technology known as public key cryptography.

The handshake also handles authentication, which usually consists of the server proving its identity to the client. This is done using public keys. Public keys are encryption keys that use one-way encryption, meaning that anyone with the public key can unscramble the data encrypted with the server's private key to ensure its authenticity, but only the original sender can encrypt data with the private key. The server's public key is part of its TLS certificate.

Once data is encrypted and authenticated, it is then signed with a message authentication code (MAC). The recipient can then verify the MAC to ensure the integrity of the data. This is kind of like the tamper-proof foil found on a bottle of aspirin; the consumer knows no one has tampered with their medicine because the foil is intact when they purchase it.



How does TLS affect web application performance?

The latest versions of TLS hardly impact web application performance at all.

Because of the complex process involved in setting up a TLS connection, some load time and computational power must be expended. The client and server must communicate back and forth several times before any data is transmitted, and that eats up precious milliseconds of load times for web applications, as well as some memory for both the client and the server.

However, there are technologies in place that help to mitigate potential latency created by the TLS handshake. One is TLS False Start, which lets the server and client start transmitting data before the TLS handshake is complete. Another technology to speed up TLS is TLS Session Resumption, which allows clients and servers that have previously communicated to use an abbreviated handshake.

These improvements have helped to make TLS a very fast protocol that should not noticeably affect load times. As for the computational costs associated with TLS, they are mostly negligible by today's standards.

TLS 1.3, released in 2018, has made TLS even faster. TLS handshakes in TLS 1.3 only require one round trip (or back-and-forth communication) instead of two, shortening the process by a few milliseconds. When the user has connected to a website before, the TLS handshake has zero round trips, speeding it up still further.

How to start implementing TLS on a website

Cloudflare offers free TLS/SSL certificates to all users. Anyone who does not use Cloudflare will have to acquire an SSL certificate from a certificate authority, often for a fee, and install the certificate on their origin servers.

For more on how TLS/SSL certificates work, see What is an SSL certificate? Check if a website is using TLS encryption at the Cloudflare Diagnostic Center.

7)What is port no .Different types port nos.

What is a port?

A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

What is a port number?

Ports are standardized across all network-connected devices, with each port assigned a number. Most ports are reserved for certain protocols — for example, all Hypertext Transfer Protocol (HTTP) messages go to port 80. While IP addresses enable messages to go to and from specific devices, port numbers allow targeting of specific services or applications within those devices.

How do ports make network connections more efficient?

Vastly different types of data flow to and from a computer over the same network connection. The use of ports helps computers understand what to do with the data they receive.

Suppose Bob transfers an MP3 audio recording to Alice using the File Transfer Protocol (FTP). If Alice's computer passed the MP3 file data to Alice's email application, the email application would not know how to interpret it. But because Bob's file transfer uses the port designated for FTP (port 21), Alice's computer is able to receive and store the file.

Meanwhile, Alice's computer can simultaneously load HTTP webpages using port 80, even though both the webpage files and the MP3 sound file flow to Alice's computer over the same WiFi connection.

Are ports part of the network layer?

The OSI model is a conceptual model of how the Internet works. It divides different Internet services and processes into 7 layers. These layers are:

Ports are a transport layer (layer 4) concept. Only a transport protocol such as the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) can indicate which port a packet should go to. TCP and UDP headers have a section for indicating port numbers. Network layer protocols — for instance, the Internet Protocol (IP) — are unaware of what port is in use in a given network connection. In a standard IP header, there is no place to indicate which port the data packet should go to. IP headers only indicate the destination IP address, not the port number at that IP address.

Usually, the inability to indicate the port at the network layer has no impact on networking processes, since network layer protocols are almost always used in conjunction with a transport layer protocol. However, this does impact the functionality of testing software, which is software that "pings" IP addresses using Internet Control Message Protocol (ICMP) packets. ICMP is a network layer protocol that can ping networked devices — but without the ability to ping specific ports, network administrators cannot test specific services within those devices.

Some ping software, such as My Traceroute, offers the option to send UDP packets. UDP is a transport layer protocol that can specify a particular port, as opposed to ICMP, which cannot specify a port. By adding a UDP header to ICMP packets, network administrators can test specific ports within a networked device.

Why do firewalls sometimes block specific ports?

A firewall is a security system that blocks or allows network traffic based on a set of security rules. Firewalls usually sit between a trusted network and an untrusted network; often the untrusted network is the Internet. For example, office networks often use a firewall to protect their network from online threats.

Some attackers try to send malicious traffic to random ports in the hopes that those ports have been left "open," meaning they are able to receive traffic. This action is somewhat like a car thief walking down the street and trying the doors of parked vehicles, hoping one of them is unlocked. For this reason, firewalls should be configured to block network traffic directed at most of the available ports. There is no legitimate reason for the vast majority of the available ports to receive traffic.

Properly configured firewalls block traffic to all ports by default except for a few predetermined ports known to be in common use. For instance, a corporate firewall could only leave open ports 25 (email), 80 (web traffic), 443 (web traffic), and a few others, allowing internal employees to use these essential services, then block the rest of the 65,000+ ports.

As a more specific example, attackers sometimes attempt to exploit vulnerabilities in the RDP protocol by sending attack traffic to port 3389. To stop these attacks, a firewall may block port 3389 by default. Since this port is only used for remote desktop connections, such a rule has little impact on day-to-day business operations unless employees need to work remotely.

What are the different port numbers?

There are 65,535 possible port numbers, although not all are in common use. Some of the most commonly used ports, along with their associated networking protocol, are:

- **Ports 20 and 21:** File Transfer Protocol (FTP). FTP is for transferring files between a client and a server.
- **Port 22:** Secure Shell (SSH). SSH is one of many tunneling protocols that create secure network connections.
- **Port 25:** Simple Mail Transfer Protocol (SMTP). SMTP is used for email.
- **Port 53:** Domain Name System (DNS). DNS is an essential process for the modern Internet; it matches human-readable domain names to

machine-readable IP addresses, enabling users to load websites and applications without memorizing a long list of IP addresses.

- **Port 80:** Hypertext Transfer Protocol (HTTP). HTTP is the protocol that makes the World Wide Web possible.

- **Port 123:** Network Time Protocol (NTP). NTP allows computer clocks to sync with each other, a process that is essential for encryption.

- **Port 179:** Border Gateway Protocol (BGP). BGP is essential for establishing efficient routes between the large networks that make up the Internet (these large networks are called autonomous systems). Autonomous systems use BGP to broadcast which IP addresses they control.

- **Port 443:** HTTP Secure (HTTPS). HTTPS is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443. Network services that use HTTPS for encryption, such as DNS over HTTPS, also connect at this port.

- **Port 500:** Internet Security Association and Key Management Protocol (ISAKMP), which is part of the process of setting up secure IPsec connections.

- **Port 3389:** Remote Desktop Protocol (RDP). RDP enables users to remotely connect to their desktop computers from another device.

The Internet Assigned Numbers Authority (IANA) maintains the full list of port numbers and protocols assigned to them.

8)How many no of servers are there?

Network Server Types Explained

Network servers became common in the early 1990s, as businesses increasingly began using PCs to provide services formerly hosted on larger mainframes or minicomputers.
A network server, today, is a powerful computer that provides various shared resources to workstations and other servers on a network. The shared resources can include disk space, hardware access and email services. Any computer can be a “network server,” but what separates a server from a workstation is not the hardware, but rather the function performed by the computer.

In general, a workstation is any computer used by an individual person to perform his or her job duties, while a network server is any computer that provides users with access to shared software or hardware resources.

Servers are usually built with more powerful components than individual workstations. For example, a server will usually have more RAM installed than a workstation or will use a more robust operating system designed to run 24/7. While this may increase the price of the server relative to a single workstation, the overall cost can be significantly lower to an organization.

Below are 13 of the most common server types used today:

---

1. Application Servers
Sometimes referred to as a type of middleware, application servers occupy a large chunk of computing territory between database servers and the end user, and they often connect the two.
2. Client Servers
In the client/server programming model, a server is a program that awaits and fulfills requests from client programs in the same or other computers. A given application in a computer may function as a client with requests for services from other programs and also as a server of requests from other programs.
3. Collaboration Servers
In many ways, collaboration software, once called ‘groupware,’ demonstrates the original power of the Web. Collaboration software designed to enable users to collaborate, regardless of location, via the Internet or a corporate intranet and to work together in a virtual atmosphere.
4. FTP Servers
One of the oldest of the Internet services, File Transfer Protocol, makes it possible to move one or more files securely between computers while providing file security and organization as well as transfer control.
5. List Servers
List servers offer a way to better manage mailing lists, whether they be interactive discussions open to the public or one-way lists that deliver announcements, newsletters or advertising.

6. Mail Servers

Almost as ubiquitous and crucial as Web servers, mail servers move and store mail over corporate networks (via LANs and WANs) and across the Internet.

7. Open Source Servers

From your underlying open source server operating system to the server software that help you get your job done, open source software is a critical part of many IT infrastructures.

8. Proxy Servers

Proxy servers sit between a client program (typically a Web browser) and an external server (typically another server on the Web) to filter requests, improve performance, and share connections.

9. Real-Time Communication Servers

Real-time communication servers, formerly known as chat servers or IRC Servers, and still sometimes referred to as instant messaging (IM) servers, enable large numbers users to exchange information near instantaneously.

10. Server Platforms

A term often used synonymously with operating system, a platform is the underlying hardware or software for a system and is thus the engine that drives the server.

11. Telnet Servers

A Telnet server enables users to log on to a host computer and perform tasks as if they're working on the remote computer itself.

12. Virtual Servers

In 2009, the number of virtual servers deployed exceeded the number of physical servers. Today, server virtualization has become near ubiquitous in the data center. From hypervisors to hybrid clouds, ServerWatch looks at the latest virtualization technology trends.

13. Web Servers

At its core, a Web server serves static content to a Web browser by loading a file from a disk and serving it across the network to a user's Web browser. This entire exchange is mediated by the browser and server talking to each other using HTTP.

Exchange Server

Built to deliver the enterprise-grade security and reliability that businesses require, Microsoft Exchange provides email, calendar and contacts on your PC, phone and web browser.

Lync Server

Lync Server is an enterprise real-time communications server software, providing the infrastructure for enterprise instant messaging, presence, VoIP, ad hoc and structured conferences (audio, video and web conferencing) and PSTN connectivity through a third-party gateway or SIP trunk.

SharePoint Server

A server product that relies on SharePoint Foundation technology to provide a consistent, familiar framework for lists and libraries, site administration, and site customization. SharePoint Server includes all the features of SharePoint Foundation plus additional features and capabilities such as Enterprise Content Management, business intelligence, enterprise search, personal sites, and Newsfeed.

SQL Server

SQL Server is a relational database management system (RDBMS) from Microsoft that's designed for the enterprise environment. As a database, it is a software product whose primary function is to store and retrieve data as requested by other software applications: those on the same computer or those running on another computer across a network (including the cloud).

Windows Server

As the server version of Windows 8, Windows Server 2012 redefines the server category, delivering hundreds of new features and enhancements spanning virtualization, networking, storage, user experience, cloud computing, automation, and more.

So what's a server? In a sense, there's really no such thing as just a server. There's always some type of resource that's being served, which is either explicit or implied. A server is just a computer that's been selected and probably optimized to perform a specific task in service to others. And it's that task that makes all the difference.
Was this information helpful to you? Is there something else around servers worth discussing? Your comments are always welcome!

At New Horizons, we're talking about IT everyday—and not just with a variety of clients, but with leading vendors—about industry trends and real-life challenges. And because of our these close partnerships, New Horizons is positioned to help businesses like yours leverage our knowledge experts to discuss strategies, implementation and troubleshooting.

Click here if you would like to learn about o

How many resoling techniques are there for dns?

How many layers in dns tree?

What is DNS and the DNS Hierarchy

By Jithin on August 22nd, 2016

The DNS is an integral part of the Internet as it would not exist without it. The DNS is in a hierarchy in which the members of it are ranked according to the relative status. We are going to see the DNS hierarchy in detail here.

What is DNS?

The DNS stands for Domain Name System. The prominent intention of DNS is to translate domain names to the IP addresses. Even though there are there are domain names for all the websites, there are IP addresses also for them.The Internet uses this IP addresses to identify the websites. The IP address is a numerical data incorporated with four parts separated by dots(.). This numerical value is not easy to remember, so domain names were created, which are easily memorable. The DNS is responsible for translating these domain names to the IP addresses.

The DNS is a worldwide network that collectively forms a database of domain names and IP addresses. This database is a global one. The hierarchy consists of DNS servers. A DNS server can be defined as the following.

DNS Server

A DNS server is also a web server. Its primary objective is to interact with the aforementioned database. These DNS servers translate the domain name entered into the URL area of a web browser to the corresponding IP address. There are thousands of DNS servers worldwide which form the Domain Name System which currently is the largest digital database.

Fully Qualified Domain Name (FQDN)

It is essential to know about Fully Qualified Domain Name (FQDN), to understand the DNS hierarchy. A FQDN is the domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels including the top-level domain and the root zone. It consists of two parts, the host name and the domain name. An example of FQDN in a mail server is "*mail.mydomain.com*" where "*mail"* is the host name and the "*mydomain.com"* is the domain name. A fully qualified domain name is supposed to have little ambiguity. FQDN is otherwise called an absolute domain name.

DNS Hierarchy

The DNS hierarchy is comprised of the following elements:

1) Root Level

2) Top Level Domains

3) Second Level Domains

4) Sub-Domain

5) Host

DNS Root Zone

The DNS root zone is the highest level in the DNS hierarchy tree. The root name server is the name server for the root zone. It answers the requests for records in the

root zone and answers other requests by providing a list of authoritative name servers for the appropriate TLD (top-level domain). The root nameservers are very important because they are the first step in resolving a domain name. These are the authoritative nameservers which serve the DNS root zone. These servers contain the global list of the top-level domains. The root zone contains the following:

1) Organizational hierarchy such as .com, .net, .org.

2) Geographic hierarchy such as .uk, .fr, .pe.

The root DNS servers are operated by 12 different organizations.

1) Verisign

2) University of Southern California

3) Cogent

4) University of Maryland

5) NASA AMES Research Center

6) Internet Systems Consortium

7) US Department of Defense

8) US Army Research Lab

9) Netnod

10) RIPE

11) ICANN

12) WIDE

Top Level Domains

The next level in the DNS hierarchy is Top level domains. There are many TLDs available at the moment. As we have seen the TLDs are classified as two sub categories. They are organizational hierarchy and geographic hierarchy. Let us see each in detail.

Organizational Hierarchy

Domain	Purpose
com	Commercial organizations
edu	Educational institutions
gov	Government institutions
mil	Military groups
net	Major network support centers
org	Nonprofit organizations and others
int	International organizations

Geographic hierarchy

In the geographic hierarchy, each country is assigned with two letter codes. These codes are used to identify countries.

For example, take the domain name ***images.google.com***

Here, the ".com" is the top-level domain. It is called as tld in short. This is the next component in the DNS hierarchy. A TLD can have many domains under it. For example, a .com tld can have linux.com, centos.com, ubuntu.com, etc.

Sometimes, there is a second level hierarchy to a tld. They deal with the type of entity intended to register an SLD under it. For example, for the .uk tld, a college or other academic institution would register under the .ac.uk ccSLD, while companies would register under .co.uk.

Second Level Domains

The next level in the DNS hierarchy is the Second Level Domains. This is the domain that is directly below the tld. This is the main part of the domain name. It can vary according to the buyer. There are no limits here as the tlds. Once the domain is available anyone can purchase it. If the domain is unavailable at the moment, same 2nd level name with other tlds is the best option.

Sub-domain

The sub-domain is the next level in the DNS hierarchy. The sub-domain can be defined as the domain that is a part of the main domain. The only domain that is not also a sub-domain is the root domain. Suppose two domains. *one.example.com* and *two.example.com*. Here, both the domains are the sub-domains of the main domain *example.com* and the *example.com* is also a subdomain of the *com* top level domain.

This is the DNS hierarchy and elements of the DNS hierarchy.

If you need any further assistance please reach our support department.

What is the length of string in dns tree?

12)What is ARP and RARP and where does it work

RP vs RARP: Know the Difference between ARP and RARP

These are both protocols of the network layer. When an IP datagram needs to be sent between one host to another, the sender would require the receiver's physical address as well as its logical address. Here, with dynamic mapping, we get two protocols, namely, ARP and RARP. But there is a significant difference between ARP and RARP.

The difference is that when we provide ARP with the receiver's logical address, it would obtain that receiver's physical address. On the other hand, when we provide RARP with the host's physical address, then it would obtain the host's logical address from the available server.

What is ARP?

The term ARP is an abbreviation for Address Resolution Protocol. It is a protocol of the network layer. Since it is a dynamic type of mapping protocol, every host available in the network would be aware of another host's logical address. Now, let us suppose that the host has to send

another host an IP datagram. Here, the IP datagram needs to be encapsulated into a frame. It needs to be done so that the datagram can easily pass via the physical network available between the receiver and the sender.

What is RARP?

The term RARP is an abbreviation for Reverse ARP. The RARP is also a protocol of the network layer. It's a TCP/IP protocol, allowing any of the hosts to obtain its actual IP address from our network server. As the name already suggests, the RARP is an adaptation of the ARP protocol. It is basically the reverse of the ARP protocol.

Difference between ARP and RARP

Let us talk about the difference between ARP and RARP. To make this topic more understandable and clear, we are comparing both of the terms based on their individual characteristics in a table.

Parameters	ARP	RARP
Full Form	The term ARP is an abbreviation for Address resolution protocol.	The term RARP is an abbreviation for Reverse Address Resolution Protocol.
Basics	The ARP retrieves the receiver's physical address in a network.	The RARP retrieves a computer's logical address from its available server.
Broadcast Address	The nodes use ARP broadcasts in the LAN with the help of the MAC address.	The RARP utilises IP addresses for broadcasting.
Table Maintained By	The ARP table is maintained by the Local Host.	The RARP table is maintained by the RARP Server.
Usage	The router or the host uses ARP to find another router/host's address (physical address) in LAN.	RARP is used by thin clients that have limited facilities.
Reply Information	The primary use of the ARP reply is to update the ARP table.	The primary use of the RARP reply is to configure the local host's IP address.
Mapping	The ARP maps the node's IP address (32-bit logical address) to the MAC address/physical address (48-bit address).	The RARP maps the 48-bit address (MAC address/physical address) to the logical IP address (32-bit).

13)What are different IPC ? name some.

Inter-process communication (IPC) & IPC types in OS

Software Engineering Operating System
Up

In this article, we have explained **Inter-process communication (IPC) in Operating System**, why is IPC needed and various ways to achieve IPC like using shared memory, message passing, buffering, pipes and more.

Table of contents:

Let us get started with Inter-process communication & it's types in Operating System.

Processes and communication

The processes that occur ***concurrently*** in the Operating systems can be of 2 types :

- **Independent:** These do not share any data with any other process.
- **Cooperating:** These processes share data with other processes. Clearly they can affect and get affected themselves too by other processes.

Why need communication among processes ?

There are several reasons for the same. Some of them are :

- **Information sharing:** There may be a possibility that processes may need the same piece of information at the same time for their execution. **For example**, Copying and Pasting.
- **Computation speed:** It is very important to have high speed in computation. If a task is subdivided into tasks which are executed parallely, it enhances the speed and throughput of system.
- **Modularity:** Modularity means dividing the functions of operating system into separate processes called Threads, to achieve improved throughput.

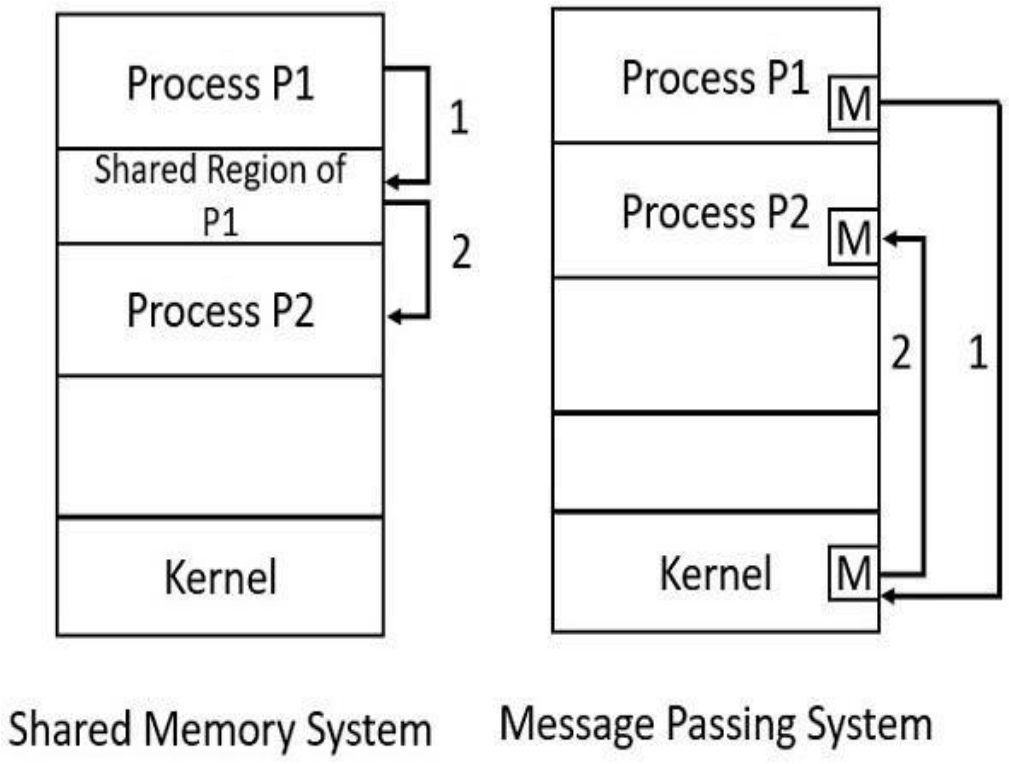
What is Inter-process communication ?

Inter-process communication (IPC) helps to achieve the communication among the processes or threads in a system.
It is useful mainly in the environment where the processes reside on different computer systems connected via any type of network. A very simple and self explanatory example is the chat system used in World Wide Web.

There are 2 basic models for IPC:

- **Shared Memory**
- **Message Passing**

SHARED MEMORY	MESSAGE PASSING
A region of memory is shared among the processes.	Messages are exchanged among the processes.
Faster than message-passsing systems.	Useful for exchanging smaller amounts of data.
Only require to establish shared-memory regions.	Require more time consuming task of kernel intervention.



1. IPC in Shared-Memory Systems

A process creates the shared-memory region in it's own address space. Other processes communicate by attaching the address space to their own address space.

Processes communicate by Reading and Writing data in the shared area. Operating system does not have any control over data or location. It is solely determined by the processes.

A very famous problem called Producer Consumer Problem is used to illustrate the inner working of Shared-Memory systems. Briefly explaining :

- A producer process produces information that is to be consumed by the consumer.
- By shared memory, both producer and consumer share a memory space called Buffer.
- A producer produces an item at a time and consumer consumes another item at that time.
- Both producer and consumer are synchronized so that consumer does not consume an item that has not yet been produced.

- A simple example to understand the problem is Client-server system. Considering Server as a Producer and Client as a consumer. For example, A Web server produces web content such as HTML files and images which are consumed by the client web browser.
- 2 types of buffers can be used : **Bounded buffer**(Fixed buffer size) and **Unbounded buffer**(No limit on buffer size).

The POSIX API uses Shared-memory IPC for communication.

2. IPC in Message-Passing Systems

Message passing provides a mechanism to allow processes to communicate and to synchronize their actions without sharing the same address space.
It is very useful in case where the tasks or processes reside on different computers and are connected by a network.

Messages can be of fixed or variable size. Methods for message passing operations:

1. Direct and Indirect communication
In Direct communication,
Each task explicitly pass the message along with passing name of process to which it is passing.

```
send(task name, message)
receive(task name, message)
```

In Indirect communication, Message passing is through mailboxes. The tasks communicating should have a shared mailbox.

```
send(mailbox name, message)
receive(mailbox name, message)
```

2. Synchronous and Asynchronous communication
Tasks make calls to each other for communication. Synchronous means blocking and Asynchronous means non-blocking.

There are 4 cases:
->*Blocking send:* The sending process is blocked until message is received by receiver task.

->*Non-Blocking send:* The sending process sends the message according to it's requirement without considering whether message is received or not at receiver end.
->*Blocking receive:* The receiving process is blocked until message is available.
->*Non-Blocking receive:* The receiving goes on accepting either the message or null information continuously.
When there are both receiving and sending blocked, that case is called *Rendezvous.*

3. Buffering

The messages to be exchanged reside in temporary queue. It can be implemented in 3 ways:

- *Zero capacity:* Maximum length of queue is zero, so messages can't wait in it. Means sender will be blocked until the receiver receives the message.
- *Bounded capacity:* Queue will be having finite length, and atmost that number of messages will only reside in it. Sender can send messages until queue is not filled.
- *Unbounded capacity:* Queue's length is infinite, so any number of messages can wait in it. Sender will never block.

4. Pipes

Pipes act as a channel between 2 processes to communicate. These were one of the first IPC mechanisms in early UNIX. Pipes allow a mechanism in which output of one process is input of another process. Pipes function as FIFO.

There are 2 types of pipes:

1. Ordinary pipes: It allows communication in producer-consumer fashion. The producer writes to one end, and consumer reads from the other. It allows only undirectional flow. For 2-way, we will have to use 2 ordinary pipes. On Windows systems, ordinary pipes are termed as *Anonymous pipes* and the communicating processes have a parent-child relationship. These can be used only for communication between processes on same machine. Once processes finish, ordinary pipes don't exist.
2. Named pipes: These can be bidirectional, require no parent-child relationship and is used for communication for several processes. These

pipes continue to exist after communicating processes have finished. Named pipes are referred to as FIFOs in UNIX.

5. Sockets

Just as pipes are of two tastes (i.e. named and ordinary), Sockets also do. Similarly these enable channel-based communication for processes on same device. But Network sockets allow IPC for processes on different hosts via networking. A socket consists of an IP address and a port number.

Generally sockets use client-server architecture. The server here waits for client request by listening to a specified port. After receiving the request, server accepts the connection and the connection is completed. The client process has a port assigned to it by host computer.

For example, client on host A with IP address 130.44.3.60 wishes to establish a connection with web server which is listening at port 70 at address 151.33.50.9 .

6. Semaphores

Semaphores are used to lock/unlock the critical region which is shared among processes. If a single region is shared by multiple processes, there is a possibility of deadlock. Thus semaphore comes into play to manage message passing.
Semaphores are of 2 types: *Binary semaphores*(having 2 states 0 or 1) and *Counting semaphores*(different resource counts).
A very basic example for implementation of semaphores is: Consider the case of printing. We are having 5 printers(assuming 1 printer will print 1 at a time). We request to print 3 jobs. These jobs will be given to 3 printers. Again 4 jobs came into request while previous was executing. So now the 2 printers free will schedule the 2 requests and other 2 requests will be executed when one of the printers will be free. This is how counting semaphores are implemented. Semaphores manage the entry and exit of processes in critical section (or the execution).

With this article at OpenGenus, you must have a strong idea of Inter-process communication & it's types in Operating System.

14.

15)Different data link layer protocol?

Examples of Data Link Layer Protocols

- Difficulty Level : Easy
- Last Updated : 05 Aug, 2020

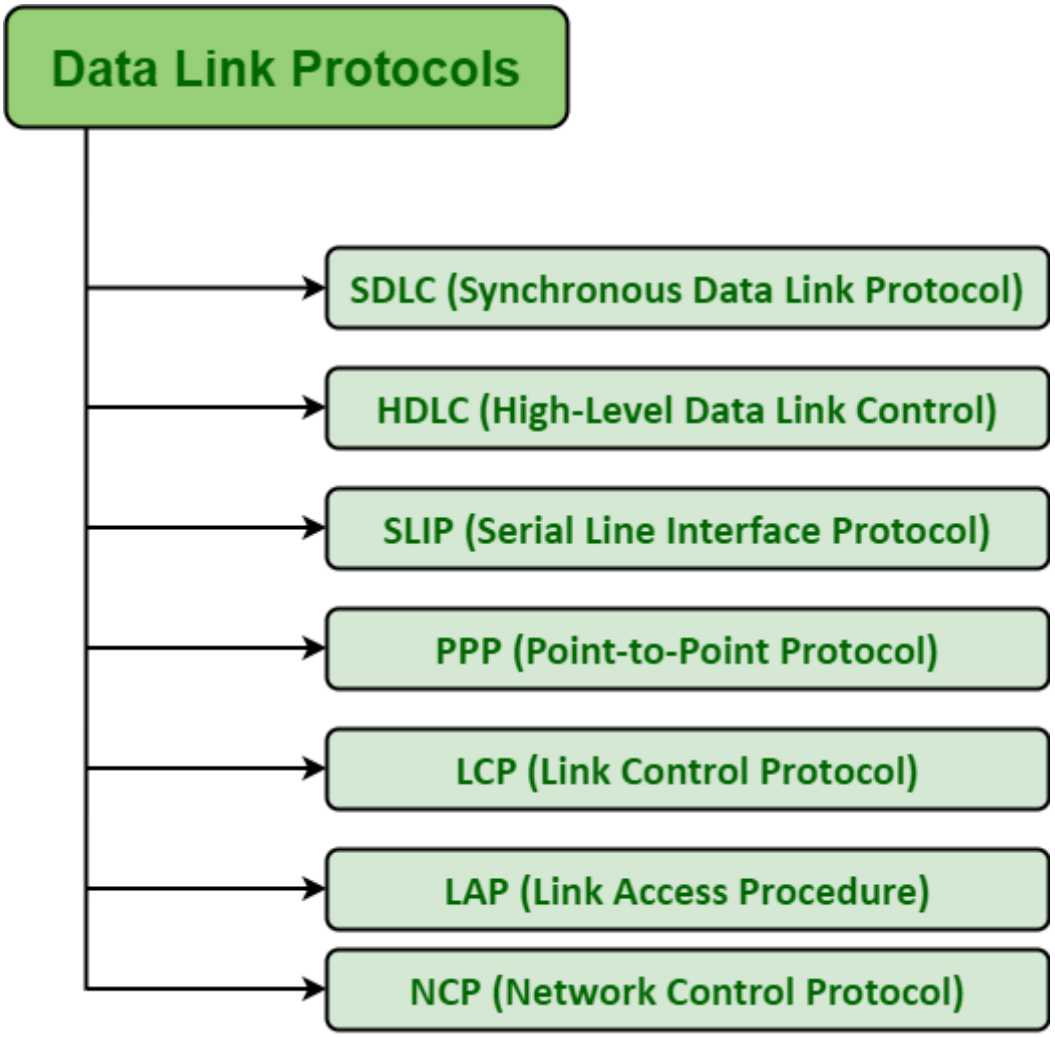
Read

Discuss

Data Link Layer protocols are generally responsible to simply ensure and confirm that the bits and bytes that are received are identical to the bits and bytes being transferred. It is basically a set of specifications that are used for implementation of data link layer just above the physical layer of the Open System Interconnections (OSI) Model.

Some Common Data Link Protocols :

There are various data link protocols that are required for Wide Area Network (WAN) and modem connections. Logical Link Control (LLC) is a data link protocol of Local Area Network (LAN). Some of data link protocols are given below :



1. Synchronous Data Link Protocol (SDLC) –
   SDLC is basically a communication protocol of computer. It usually supports multipoint links even error recovery or error correction also. It is usually used to carry SNA (Systems Network Architecture) traffic and is present precursor to HDLC. It is also designed and developed by IBM in 1975. It is also used to connect all of the remote devices to mainframe computers at central locations may be in point-to-point (one-to-one) or point-to-multipoint (one-to-many) connections. It is also used to make sure that the data units should arrive correctly and with right flow from one network point to next network point.

2. High-Level Data Link Protocol (HDLC) –
   HDLC is basically a protocol that is now assumed to be an umbrella under which many Wide Area protocols sit. It is also adopted as a part of X.25 network. It was originally created and developed by ISO in 1979. This protocol is generally based on SDLC. It also provides

best-effort unreliable service and also reliable service. HDLC is a bit-oriented protocol that is applicable for point-to-point and multipoint communications both.

3. Serial Line Interface Protocol (SLIP) **–**
   SLIP is generally an older protocol that is just used to add a framing byte at end of IP packet. It is basically a data link control facility that is required for transferring IP packets usually among Internet Service Providers (ISP) and a home user over a dial-up link. It is an encapsulation of the TCP/IP especially designed to work with over serial ports and several router connections simply for communication. It is some limitations like it does not provide mechanisms such as error correction or error detection.
4. Point to Point Protocol (PPP) **–**
   PPP is a protocol that is basically used to provide same functionality as SLIP. It is most robust protocol that is used to transport other types of packets also along with IP Packets. It can also be required for dial-up and leased router-router lines. It basically provides framing method to describe frames. It is a character-oriented protocol that is also used for error detection. It is also used to provides two protocols i.e. NCP and LCP. LCP is used for bringing lines up, negotiation of options, bringing them down whereas NCP is used for negotiating network-layer protocols. It is required for same serial interfaces like that of HDLC.

5. **Link Control Protocol (LCP) –**
   It was originally developed and created by IEEE 802.2. It is also used to provide HDLC style services on LAN (Local Area Network). LCP is basically a PPP protocol that is used for establishing, configuring, testing, maintenance, and ending or terminating links for transmission of data frames.

6. **Link Access Procedure (LAP) –**
   LAP protocols are basically a data link layer protocols that are required for framing and transferring data across point-to-point links. It also includes some reliability service features. There are basically three types of LAP i.e. LAPB (Link Access Procedure Balanced), LAPD (Link Access Procedure D-Channel), and LAPF (Link Access Procedure Frame-Mode Bearer Services). It is actually originated from IBM SDLC, which is being submitted by IBM to the ISP simply for standardization.

7. **Network Control Protocol (NCP) –**
   NCP was also an older protocol that was implemented by ARPANET. It basically allows users to have access to use computers and some of the devices at remote locations and also to transfer files among two or more computers. It is generally a set of protocols that is forming a part of PPP. NCP is always available for each and every higher-layer protocol that is supported by PPP. NCP was replaced by TCP/IP in the 1980s.

NFC stands for Near Field Communication. It enables short range communication between compatible devices. At least one transmitting device and another receiving device is needed to transmit the signal. Many devices can use the NFC standard and are considered either passive or active.

So NFC devices can be classified into 2 types:

1. **Passive NFC devices –**
   These include tags, and other small transmitters which can send information to other NFC devices without the need for a power source of their own. These devices don't really process any information sent from other sources, and can not connect to other passive components. These often take the form of interactive signs on walls or advertisements.

2. **Active NFC devices –**
   These devices are able to both the things i.e. send and receive data. They can communicate with each other as well as with passive devices. Smartphones the best example of active NFC device. Card readers in public transport and touch payment terminals are also good examples of the technology.

How does NFC work?
Like other wireless signals Bluetooth and WiFi, NFC works on the principle of sending information over radio waves. Near Field Communication is another standard for wireless data transition which means devices must adhere to certain specifications in order to communicate with each other properly. The technology used in NFC is based on older technology which is the RFID (Radio-frequency identification) that used electromagnetic induction in order to transmit information.
This creates one major difference between NFC and Bluetooth/WiFi. NFC can be used to induce electric currents within passive components rather than just send data. This means that their own power supply is not required by passive devices. Instead they can be powered by the electromagnetic field produced

by an active NFC component when it comes into range. NFC technology unfortunately does not command enough inductance to charge our smartphones, but QI charging is based on the same principle.

The transmission frequency is 13.56 megahertz for data across NFC. Data can be sent at either 106, 212, or 424 kilobits per second which is quick enough for a range of data transfers like contact details to swapping pictures and music.

The NFC standard currently has three distinct modes of operation to determine what sort of information will be exchanged between devices.

1. The most common used in smartphones is the peer-to-peer mode. Exchange of various piece of information is allowed between 2 devices. In this mode both devices switch between active when sending data and passive when receiving.

2. The second mode i.e. read/write mode is a one-way data transmission. The active device, possibly your smartphone, links up with another device in order to read information from it. NFC advertisement tags use this mode.

3. The third mode of operation is card emulation. The NFC device can function as a smart or contactless credit card and make payments or tap into public transport systems.

Comparisons with Bluetooth –
There are several important technological differences between NFC and bluetooth but NFC has some significant benefits in certain circumstances. The major advantage of NFC over bluetooth is that it requires much less power consumption than Bluetooth. This makes NFC perfect for passive devices, such as the advertising tags as they can operate without a major power source.

But this power saving does have some major drawbacks. First and the foremost is that the range of transmission of NFC is much shorter than Bluetooth which is a major drawback. NFC has a range of around 10 cm, just a few inches whereas Bluetooth connections can transmit data up to 10 meters or more from the source. Another drawback is that NFC is quite a bit slower than Bluetooth. NFC can transmit data at a maximum speed of just 424 kbit/s, whereas Bluetooth 2.1 can transmit 2.1 Mbit/s and with Bluetooth Low Energy around 1 Mbit/s .

NFC has one another major advantage i.e. faster connectivity. It uses inductive coupling(i.e. the absence of manual pairing) which takes less than one tenth of a second to establish a connection between two devices. While

modern Bluetooth connects pretty fast, NFC is still super handy for certain scenarios as mobile payments.

Samsung Pay, Android Pay, and even Apple Pay use NFC technology though Samsung Pay works a bit differently than the others. While Bluetooth works better for connecting devices together for file transfers, sharing connections to speakers, and more, we anticipate that NFC will always have a place in this world thanks to mobile payments — a quickly expanding technology.

What is Wi-Fi?

- Last Updated : 28 Dec, 2021

Read

Discuss

We all know about **Wi-Fi**, in our mobile, laptop everywhere Wi-Fi is supported. Wi-Fi is a wireless networking technology, by which we can access networks or connect with other computers or mobile using a wireless medium. In Wi-Fi, data are transferred over radio frequencies in a circular range.
Wi-Fi, a brand name given by the Wi-Fi Alliance (formerly Wireless Ethernet Compatibility Alliance), is a generic term that refers to the communication standard for the wireless network which works as a Local Area Network to operate without using the cable and any types of wiring. It is known as **WLAN**. The communication standard is **IEEE 802.11**. Wi-Fi works using Physical Data Link Layer.
Nowadays in all mobile computing devices such as laptops, mobile phones, also digital cameras, smart TVs has the support of Wi-Fi. The Wi-Fi connection is established from the access point or base station to the client connection or any client-to-client connection within a specific range, the range depends on the router which provides the radio frequency through Wi-Fi. These frequencies operate on 2 types of bandwidth at present, 2.4 GHz and 5 GHz.

All the modern laptops and mobiles are capable of using both bandwidths, it depends on the Wi-Fi adapter which is inside the device to catch the Wi-Fi signal. 2.4 GHz is the default bandwidth supported by all the devices. 2.4 GHz can cover a big range of areas to spread the Wi-Fi signal but the frequency is low, so in simple words, the speed of the internet is less and 5 GHz bandwidth is for a lower range of area but the frequency is high so the speed is very high.

Let’s say, if there is an internet connection of 60 MB/s bandwidth, then for 2.4 GHz bandwidth, it provides approx 30 to 45 MB/s of bandwidth connection and for 5 GHz bandwidth, it provides approx 50 to 57 MB/s bandwidth.

History:

The concept of Wi-Fi is very old but its implementation is not so old. At first **ALOHA System** is a wireless network system that is used to connect Hawaii island via a network in the year 1971. Where the protocol is used for this was ALOHA protocol and the network used packet transfer. Later it's converted to IEEE 802.11 protocol.
Then in 1985, the Federal Communications Commission (FCC) released a new network for general uses which works on 900 Mhz, 2.4 GHz, and 5.8 GHz bandwidth. This is known as the *ISM band*. Also, IBM introduced a *Token Ring LAN* network for connecting several computers, it can transfer data at 4 Mb/s speed. Then in 1988, a wireless cashier system was invented based on the Token Ring LAN network known as *waveLAN*, it operates at 900MHz or 2.4 GHz band and offers speeds of 1 to 2 Mbps. Then it was converted to *IEEE 802.11LAN/MAN* standards in 1989. ?Then in 1990, IEEE 802.11 Working Group for Wireless LANs is established by **Vic Hayes**, who was known as the **"Father of WiFi"**.
Then in 1994, *Dr. Alex Hills* introduced a research project on the wireless network, which provided coverage of the network to 7 buildings wirelessly.
Then in 1996 *Commonwealth Scientific and Industrial Research Organization (CSIRO)* introduced a wireless network based on the same protocol 802.11, later it was known as IEEE 802.11a standards.
Then after all this in 1997 the first version of Wi-Fi is released officially which is 802.11 and it can support a maximum of 2 Mb/s link speed. Then in 1999, the link speed is increased to 11 Mb/s over the 2.4 GHz frequency band, this version is known as *802.11b*
Then after a month, the IEEE 802.11a standard is approved officially, which provides up to 54 Mb/s link speed over the 5 GHz band, but the signal range is weaker than the 2.4 GHz band.

Then in 2003, the speed is increased in a new version, known as *802.11g*. The speed offers up to 54 to 108 Mb/s over 2.4 GHz.
After this two more versions were introduced that are, *802.11i and 802.11e*. In 802.11i, the security mechanism was increased and in 802.11e, Voice over Wireless LAN and multimedia streaming are involved.
Then in 2009, 802.11n is developed, which supports both 2.4 GHz and 5 GHz radiofrequency. And these are used simultaneously by dual-band routers and can reach maximum speeds of 600 Mbps.

Then in 2014, a new version was introduced that offers a potential speed of 1733 Mb/s in the 5 GHz band. This version is known as *802.11ac*. Till now this is the latest version of Wi-Fi.

Applications of Wi-Fi :

Wi-Fi has many applications, it is used in all the sectors where a computer or any digital media is used, also for entertaining Wi-Fi is used. Some of the

applications are mentioned below –

- Accessing Internet: Using Wi-Fi we can access the internet in any Wi-Fi-capable device wirelessly.
- We can stream or cast audio or video wirelessly on any device using Wi-Fi for our entertainment.
- We can share files, data, etc between two or more computers or mobile phones using Wi-Fi, and the speed of the data transfer rate is also very high. Also, we can print any document using a Wi-Fi printer, this is very much used nowadays.
- We can use Wi-Fi as **HOTSPOTS** also, it points Wireless Internet access for a particular range of area. Using Hotspot the owner of the main network connection can offer temporary network access to Wi-Fi-capable devices so that the users can use the network without knowing anything about the main network connection. Wi-Fi adapters are mainly spreading radio signals using the owner network connection to provide a hotspot.
- Using Wi-Fi or WLAN we can construct simple wireless connections from one point to another, known as Point to point networks. This can be useful to connect two locations that are difficult to reach by wire, such as two buildings of corporate business.
- One more important application is **VoWi-Fi**, which is known as **voice-over Wi-Fi**. Some years ago telecom companies are introduced VoLTE (Voice over Long-Term Evolution). Nowadays they are introduced to VoWi-Fi, by which we can call anyone by using our home Wi-Fi network, only one thing is that the mobile needs to connect with the Wi-Fi. Then the voice is transferred using the Wi-Fi network instead of using the mobile SIM network, so the call quality is very good. Many mobile phones are already getting the support of VoWi-Fi.
- Wi-Fi in offices: In an office, all the computers are interconnected using Wi-Fi. For Wi-Fi, there are no wiring complexities. Also, the speed of the network is good. For Wi-Fi, a project can be presented to all the members at a time in the form of an excel sheet, ppt, etc. For Wi-Fi, there is no network loss as in cable due to cable break.
- Also using W-Fi a whole city can provide network connectivity by deploying routers at a specific area to access the internet. Already schools, colleges, and universities are providing networks using Wi-Fi because of its flexibility.
- Wi-Fi is used as a *positioning system* also, by which we can detect the positions of Wi-Fi hotspots to identify a device location.

Types of Wi-Fi:

Wi-Fi has several types of standards, which are discussed earlier, here just the name of the standards are defined,

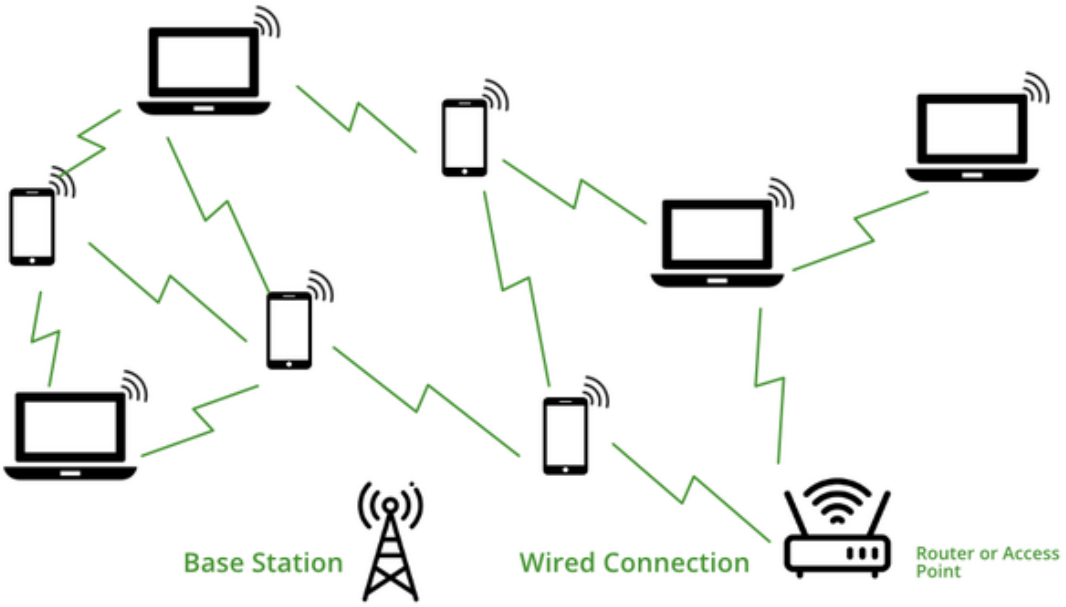
Standards	Year of Release	Description
Wi-Fi-1 (802.11b)	1999	This version has a link speed from 2Mb/s to 11 Mb/s over a 2.4 GHz frequency band
Wi-Fi-2 (802.11a)	1999	After a month of release previous version, 802.11a was released and it provide up to 54 Mb/s link speed over 5 Ghz band
Wi-Fi-3 (802.11g)	2003	In this version the speed was increased up to 54 to 108 Mb/s over 2.4 GHz
802.11i	2004	This is the same as 802.11g but only the security mechanism was increased in this version
802.11e	2004	This is also the same as 802.11g, only Voice over Wireless LAN and multimedia streaming are involved
Wi-Fi-4 (802.11n)	2009	This version supports both 2.4 GHz and 5 GHz radio frequency and it offers up to 72 to 600 Mb/s speed
Wi-Fi-5 (802.11ac)	2014	It supports a speed of 1733 Mb/s in the 5 GHz band

A new version will release in 2020 named *802.11ax* developed by **Huawei**, which can support, a maximum of 3.5 Gb/s. it will know **Wi-Fi 6**.

How does Wi-Fi work?

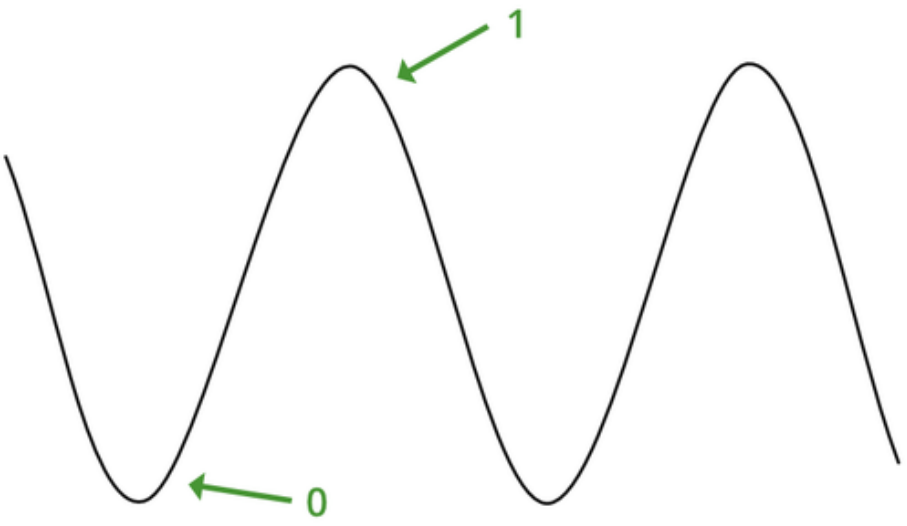
Wi-Fi is a wireless technology for networking, so it uses Electromagnetic waves to transmit networks. We know that there are many divisions of Electromagnetic waves according to their frequency such as X-ray, Gamma-ray, radio wave, microwave, etc, in Wi-Fi, the radio frequency is used. For transmitting Wi-Fi signal there is three medium,

- **Base station network or an Ethernet(802.3) connection:** It is the main host network from where the network connection is provided to the router.
- **Access point or router:** it is a bridge between a wired network and a wireless network. It accepts a wired Ethernet connection and converts the wired connection to a wireless connection and spreads the connection as a radio wave.
- **Accessing devices:** It is our mobile, computer, etc from where we use the Wi-Fi and surfing internet.



Working of Wi-Fi

All the electronics devices read data in binary form, also router or our devices, here routers provide radio waves and those waves are receive by our devices and read the waves in binary form. We all know how a wave looks like, the upper pick of the wave is known as 1 and the lower pick of the wave is known as 0 in binary. Like below:

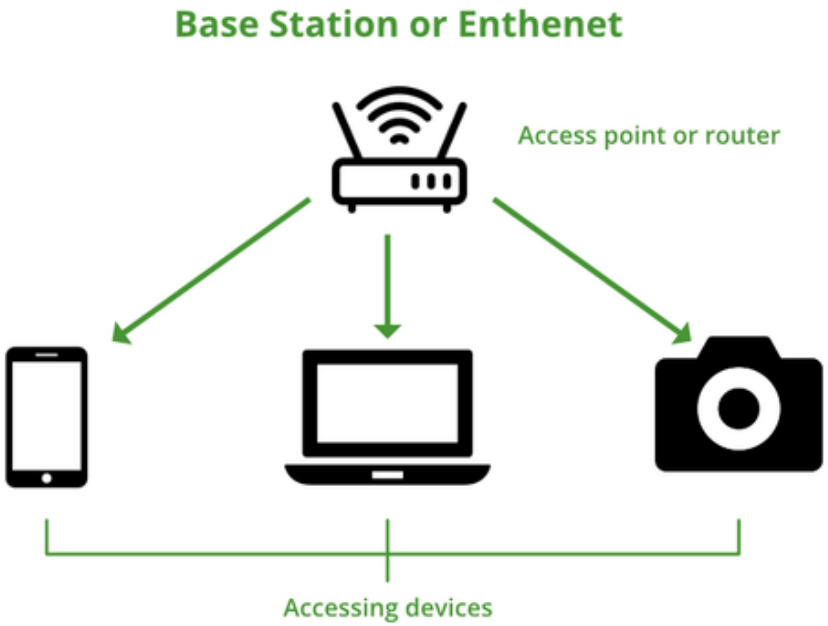


Data transmission

Some more terminologies

- **SSID (Service Set Identifier)**: It is a 32 character name that identifies the Wi-Fi network and differentiates one Wi-Fi from another Wi-Fi. All the devices are attempting to connect a particular SSID. Simply, SSID is the name of the wireless network.
- **WPA-PSK (Wi-Fi Protected Access- Pre-Shared Key):** It is a program developed by the Wi-Fi Alliance Authority to secure wireless networks with the use of Pre-Shared Key(PSK) authentication. WPA has 3 types, such as WPA. WPA2, WPA3. It is a way of encrypting the Wi-Fi signal to protect from unwanted users.
- Wi-Fi uses **Ad-Hoc** networks to transmit. It is a point-to-point network without any interface.

How signals are reached to our devices?



WiMax in Computer Network

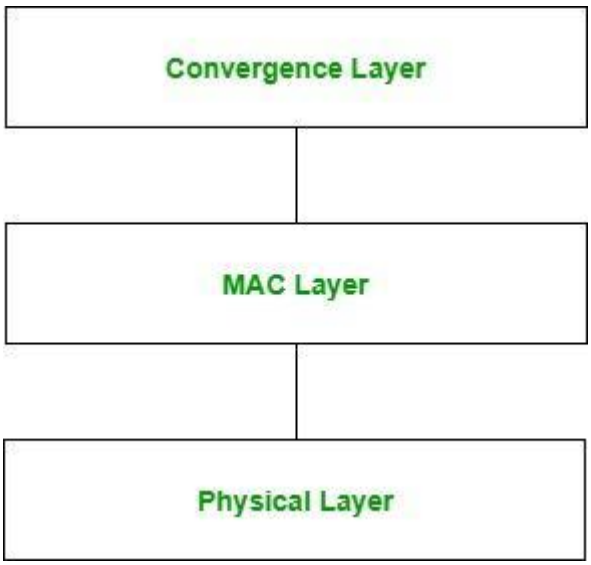
- Last Updated : 25 Nov, 2020

Read

Discuss

WiMax stands for **Worldwide Inter-operability for Microwave Access**. This technology is based on IEEE 802.16. It is used to provide higher data rates with increased coverage. It is based on MAN (Metropolitan Area Network) technology. Its range is upto 50 Km. It may provide speed upto 70 Mbps and it can operate in Non-Line-of-Sight. This technology is fast, convenient and cost effective.

Architecture:



1. **Physical Layer:**
   This layer is responsible for encoding and decoding of signals and manages bit transmission and reception. It converts MAC layer frames into signals to be transmitted. Modulation schemes which are used on this layer includes: QPSK, QAM-16 and QAM-64.

2. **MAC Layer:**
   This layer provides and interface between convergence layer and physical layer of WiMax protocol stack. It provides point to multipoint communication and is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

3. **Convergence Layer:**
   This layer provides the information of the external network. It accepts higher layer protocol data unit (PDU) and converts it to lower layer PDU. It provides functions depending upon the service being used.

Applications:

- Video streaming
- VoIP
- Video Conference
- E-Learning

18)Where csma/cd and csma/ca ?

Difference between CSMA CA and CSMA CD

CSMA is a mechanism that senses the state of the shared channel to prevent or recover data packets from a collision. It is also used to control the flow of data packets over the network so that the packets are not get lost, and data integrity is maintained. In CSMA, when two or more data packets are sent at the same time on a shared channel, the chances of collision occurred. Due to the collision, the receiver does not get any information regarding the sender's data packets. And the lost information needs to be resented so that the receiver can get it. Therefore we need to sense the channel before transmitting data packets on a network. It is divided into two parts, **CSMA CA** (Collision Avoidance) and **CSMA CD** (Collision Detection).

CSMA CD

The **Carrier Sense Multiple Access/ Collision Detection** protocol is used to detect a collision in the media access control (**MAC**) layer. Once the collision was detected, the CSMA CD immediately stopped the transmission by sending the signal so that the sender does not waste all the time to send the data packet. Suppose a collision is detected from each station while broadcasting the packets. In that case, the CSMA CD immediately sends a jam signal to stop transmission and waits for a random time context before transmitting another data packet. If the channel is found free, it immediately sends the data and returns it.

Advantage and Disadvantage of CSMA CD

Advantages of CSMA CD:

1. It is used for collision detection on a shared channel within a very short time.

2. CSMA CD is better than CSMA for collision detection.
3. CSMA CD is used to avoid any form of waste transmission.
4. When necessary, it is used to use or share the same amount of bandwidth at each station.
5. It has lower CSMA CD overhead as compared to the CSMA CA.

Disadvantage of CSMA CD

1. It is not suitable for long-distance networks because as the distance increases, CSMA CD' efficiency decreases.
2. It can detect collision only up to 2500 meters, and beyond this range, it cannot detect collisions.
3. When multiple devices are added to a CSMA CD, collision detection performance is reduced.

CSMA/CA

CSMA stands for **Carrier Sense Multiple Access** with **Collision Avoidance**. It means that it is a network protocol that uses to avoid a collision rather than allowing it to occur, and it does not deal with the recovery of packets after a collision. It is similar to the CSMA CD protocol that operates in the media access control layer. In CSMA CA, whenever a station sends a data frame to a channel, it checks whether it is in use. If the shared channel is busy, the station waits until the channel enters idle mode. Hence, we can say that it reduces the chances of collisions and makes better use of the medium to send data packets more efficiently.

Advantage and Disadvantage of CSMA CA

Advantage of CSMA CA

1. When the size of data packets is large, the chances of collision in CSMA CA is less.
2. It controls the data packets and sends the data when the receiver wants to send them.
3. It is used to prevent collision rather than collision detection on the shared channel.
4. CSMA CA avoids wasted transmission of data over the channel.
5. It is best suited for wireless transmission in a network.
6. It avoids unnecessary data traffic on the network with the help of the RTS/ CTS extension.

The disadvantage of CSMA CA

1. Sometime CSMA/CA takes much waiting time as usual to transmit the data packet.
2. It consumes more bandwidth by each station.
3. Its efficiency is less than a CSMA CD.

Difference between CSMA CA and CSMA CD

S. No	CSMA CD	CSMA CA
1.	It is the type of CSMA to detect the collision on a shared channel.	It is the type of CSMA to avoid collision on a shared channel.
2.	It is the collision detection protocol.	It is the collision avoidance protocol.
3.	It is used in 802.3 Ethernet network cable.	It is used in the 802.11 Ethernet network.
4.	It works in wired networks.	It works in wireless networks.
5.	It is effective after collision detection on a network.	It is effective before collision detection on a network.
6.	Whenever a data packet conflicts in a shared channel, it resends the data frame.	Whereas the CSMA CA waits until the channel is busy and does not recover after a collision.
7.	It minimizes the recovery time.	It minimizes the risk of collision.
8.	The efficiency of CSMA CD is high as compared to CSMA.	The efficiency of CSMA CA is similar to CSMA.
9.	It is more popular than the CSMA CA protocol.	It is less popular than CSMA CD.