COMPUTER NETWORKS 2

STAGE THREE

CHAPTER ONE

SUBNETTING

Subnetting

Subnetting is a process of breaking large network into smaller, more manageable subnetworks **(subnets)**. This helps improve network performance, security, and efficient IP address allocation.

Why Subnetting is Used

1. Efficient IP Address Management – Reduces wastage of IP addresses.
2. Improved Network Performance – Limits broadcast domains, reducing network congestion.
3. Enhanced Security – Allows network segmentation, reducing unauthorized access.
4. Simplified Troubleshooting – Makes network management and fault isolation easier.

Method of subnetting

In subnetting we need to find the following:

a. Finding the subnet mask

To find the subnet mask, we

1) need to write down the default subnet mask,

2) find the host bits borrowed to create subnets,

3) put the borrowed bits (1s bits) in the left side instead of the 0s bits.

For example: find the subnet mask of address 188.25.45.48/20

1. The default subnet mask is 255.255.0.0 (/16),

2. The number of borrowed bits from HostId portion is 4 (20 - 16 = 4).

3. The subnet mask in binary would be 11111111. 11111111. 11110000. 00000000.

Then subnet mask in decimal is 255.255.240.0

IP address: 188.25.45.48/20 subnet mask: 255.255.240.0

b. Finding the number of subnets

To calculate the number of subnets (sub-networks) provided by given subnet mask we use 2b, where b = number of bits borrowed from HostId bits to create subnets.

For example: find the number of subnets in 192.168.1.0/27 The number of borrowed bits is 3 because 27-24=3. (24 is the default value of Class C IP).

Then the number of subnets is 23 = 8
This means that we can make 8 sub-networks with the IP range 192.168.1.0/27.

c. Finding the total hosts

Total hosts are the hosts available per subnet. 2H = Total hosts. H is the number

of host bits. For example, in address 192.168.1.0/26 we have 32 - 26 = 6 (where

32 is the total bits in IP address). Total hosts per subnet would be 26 = 64.

Valid number of hosts

As we mentioned previously, we need to reduce two addresses per block (or

subnet), one for network ID and another for broadcast ID. Therefore,

Valid hosts = Total hosts - 2.

In above example we have 64 hosts per subnet, so valid hosts in each subnet

would be 64 - 2 = 62.

network ID → 192.168.1.0 broadcast ID → 192.168.1.63 (First subnet)

network ID → 192.168.1.64 broadcast ID → 192.168.1.127 (Second subnet)

network ID → 192.168.1.128 broadcast ID → 192.168.1.191 (Third subnet)

network ID → 192.168.1.192 broadcast ID → 192.168.1.255 (Forth subnet)

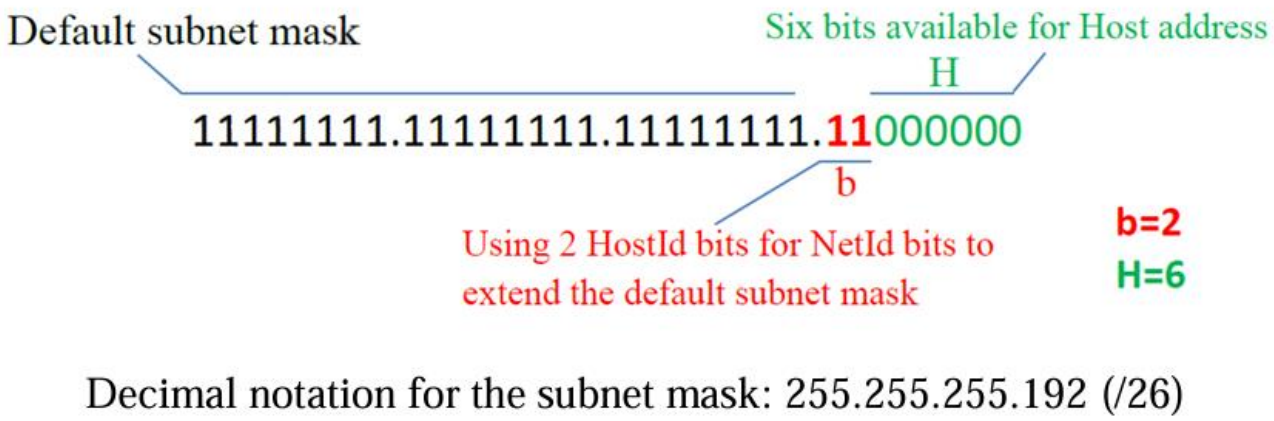
In the following we include some examples only from class C **(Class C Subnetting).**

Example

assume an organization has purchased the IP range: 192.168.55.0 and they need to use this IP range through four buildings with 55 host computer in each building. Find the 1) suitable subnet mask, 2) number of subnet, 3) number of hosts in each subnet, 4) valid number of hosts, 5) the network ID, broadcast ID and unused IPs of the third subnet.

Solution

Because we need to distribute the IP range through four buildings or networks, then the number of bits that will be borrowed from HostId is 2 as shown in the following:



Decimal notation for the subnet mask: 255.255.255.192 (/26)

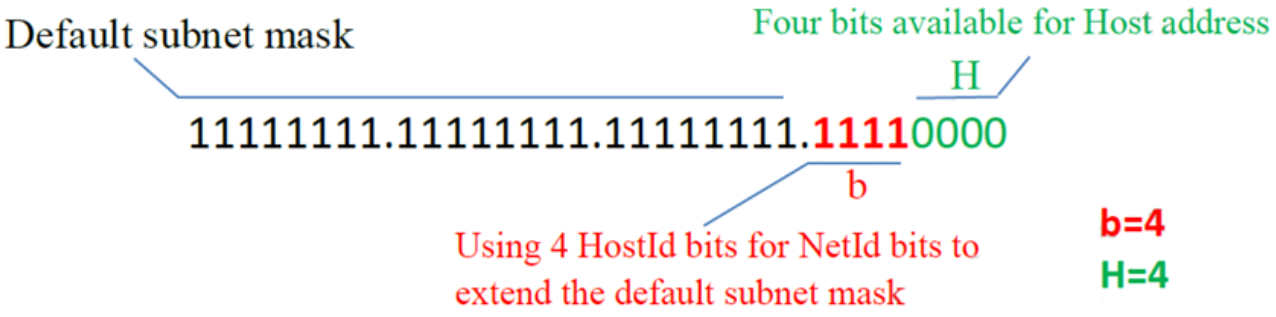
1) Subnet mask: 255.255.255.192 (/26) IP address: 192.168.55.0/26
2) Number of subnet: 2b = 22 = 4
3) Number of host in each subnet: 2H = 26 = 64 available hosts
4) Valid number of hosts: 64-2=62
5) Network ID → 192.168.1.128 , broadcast ID → 192.168.1.191 (for third subnet) Unused IP addresses: 62-55 = 7

Example

assume that we have the IP address 200.10.73.0/28, find each of following: Find the
1) subnet mask,
2) number of subnets,
3) number of hosts in each subnet,
4) valid number of hosts,
5) the network ID, broadcast ID of the second subnet.

Solution

The **binary notation** for the subnet mask is as shown below:



Binary notation for the subnet mask: 255.255.255.240 (/28)

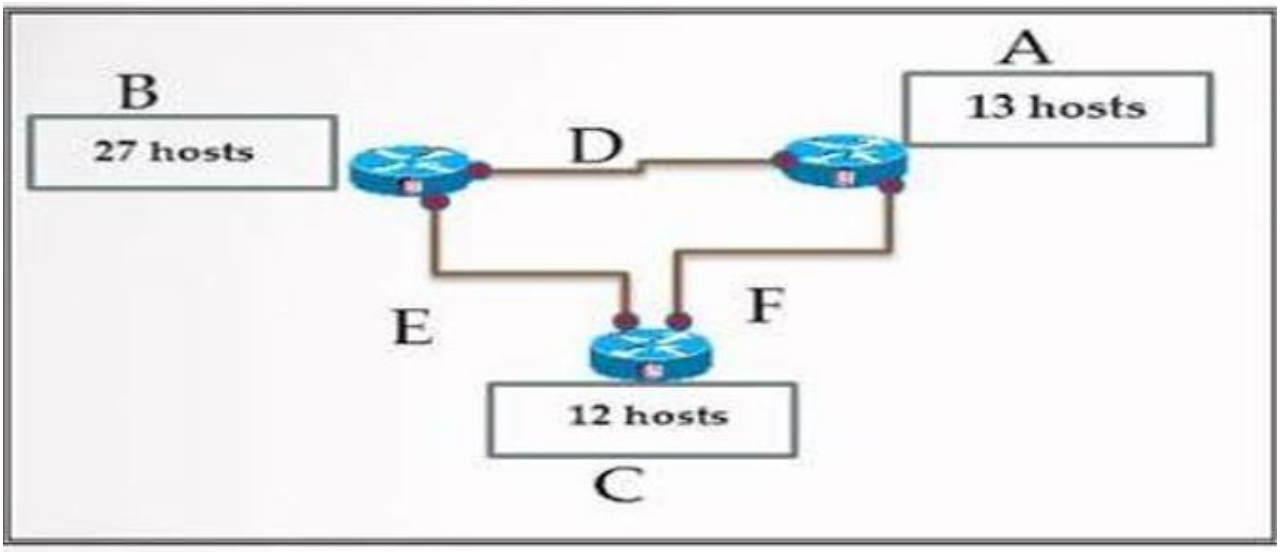
1) Subnet mask: 255.255.255.240 (/28) IP address: 200.10.73.0/28
2) Number of subnets: 2b = 24 = 16
3) Number of host in each subnet: 2H = 24 = 16 available hosts
4) Valid number of hosts: 16-2=14
5) Network ID → 192.168.1.16 , broadcast ID → 192.168.1.31 (for second subnet).

VLSM (Variable-Length Subnet Masking)

VLSM stands for Variable Length Subnet Mask where the subnet design uses more than one mask in the same network which means more than one mask is used for different subnets of a single class A, B, C or a network. It is used to increase the usability of subnets as they can be of variable size. It is also defined as the process of subnetting of a subnet.

Example 1

Network: 192.168.10.0 255.255.255.0 by using (VLSM)



1- NET B (27 HOSTS)

192.168.10.0/24 255.255.255.0

Net = > (27host)

Number of host = 2 ^ h -2 =2 ^ 5-2=30

11111111.11111111.11111111.11100000

255.255.255.224

Block size : 256-224 = 32

NETWORK B Subnet mask	192.168.10.0 /27 255.255.255.224
First	192.168.10.1 /27
Last	192.168.10.30 /27
Broadcast	192.168.10.31 /27

2- NET A (13 HOSTS)

192.168.10.0

255.255.255.0

Net = > (13host)

Number of hosts = 2 ^ h -2 =2 ^ 4-2=14

11111111.11111111.11111111.11110000

255.255.255.240

Block size: 256-240 = 16

NETWORK A Subnet mask	192.168.10.32 /28 255.255.255.240
First	192.168.10.33 /28
Last	192.168.10.46 /28
Broadcast	192.168.10.47 /28

3- NET C (12 HOSTS)

192.168.10.0 255.255.255.0

Net = > (12host)

No of host = 2 ^ h -2 =2 ^ 4-2=14

11111111.11111111.11111111.11110000

255.255.255.240

Block size :256-240 = 16

NETWORK C Subnet mask	192.168.10.48 /28 255.255.255.240
First	192.168.10.49 /28
Last	192.168.10.62 /28
Broadcast	192.168.10.63 /28

4- NET D (2 HOSTS)

192.168.10.0 255.255.255.0

Net = > (2host)

No of host = 2 ^ h -2 =2 ^ 2-2=2

11111111.11111111.11111111.11111100

255.255.255.252

Block size : 256-252 = 4

NETWORK D Subnet mask	192.168.10.64 /30 255.255.255.252
First	192.168.10.65 /30
Last	192.168.10.66 /30
Broadcast	192.168.10.67 /30

Example 2

Network: 169.200.0.0 /16 by using (VLSM)

NET A :60 Host NET B :200 Host NET C: 2 Host NET D: 500 Host NET E: 1000 Host

1- NET E (1000 HOSTS)

169.200.0.0 /16 255.255.255.0

Net = > (1000host)

Number of host = 2 ^ h -2 =2 ^ 10-2=1022

11111111.11111111.11111100. 00000000

255.255.252.0

Block size : 256-252 = 4

Network E	169.200.0.0 /22
First	169.200.0.1 /22
Broadcast	169.200.3.255 /22
Last	169.200.3.254 /22

2- NET D (500 HOSTS)

169.200.0.0 /16 255.255.0.0

Net = > (500host)

Number of hosts = 2 ^ h -2 =2 ^ 9-2=510

11111111.11111111.11111110. 00000000

255.255.254.0

Block size: 256-254 = 2

Network D	169.200.4.0 /23
First	169.200.4.1 /23
Broadcast	169.200.5.255 /23
Last	169.200.5.254 /23

3- NET B (200 HOSTS)

169.200.0.0 /16 255.255.0.0

Net = > (200host)

Number of hosts = 2 ^ h -2 =2 ^ 8-2=254

11111111.11111111.11111111. 00000000

255.255.255.0

Block size: 256-255 = 1

Network B	169.200.6.0 /24
First	169.200.6.1 /24
Broadcast	169.200.6.255 /24
Last	169.200.6.254 /24

4- NET A (60 HOSTS)

169.200.0.0 /16 255.255.0.0

Net = > (60host)

Number of hosts = 2 ^ h -2 =2 ^ 6-2=62

11111111.11111111. 11111111. 11000000

255.255.255.192

Block size: 256-192 = 64

Network B	169.200.7.0 /26
First	169.200.7.1 /26
Broadcast	169.200.7.63 /26
Last	169.200.7.62 /26

5- NET C (2 HOSTS)

169.200.0.0 /16 255.255.0.0

Net = > (2 host)

Number of host = 2 ^ h -2 =2 ^ 2-2=2

11111111.11111111. 11111111. 11111100 255.255.255.252

Block size : 256-252 = 4

Network B	169.200.7.64 /30
First	169.200.7.65 /30
Broadcast	169.200.7.67 /30
Last	169.200.7.66 /30

COMPUTER NETWORKS 2

المرحلة الثالثة

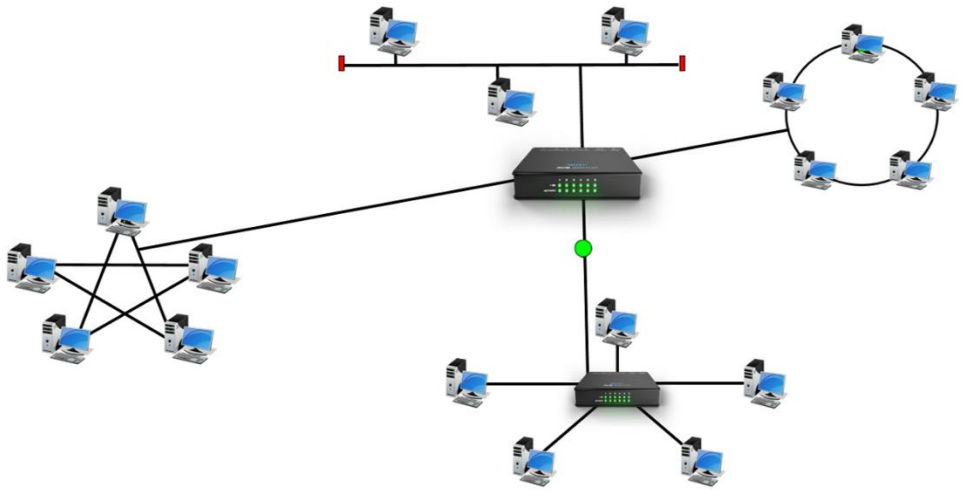
CHAPTER TOW

Routing

Routing in Computer Network

Routing is a mechanism that selects a way for data to be transmitted from the source to the destination. **The router** is a specific device that does routing.

A **Router** is a networking device that forwards data packets between computer networks. This device is usually connected to two or more different networks. When a data packet comes to a router port, the router reads the address information in the packet to determine which port the packet will be sent to. For example, a router provides you with internet access by connecting your LAN to the Internet.



When a packet arrives at a Router, it examines the destination IP address of a received packet and makes routing decisions accordingly. Routers use **Routing Tables** to determine out which interface the packet will be sent to. A routing table lists all networks for which routes are known. Each router's routing table is unique and stored in the RAM of the device.

Routing algorithms are used to route packets. The routing algorithm is just a piece of software that determines the best path by which a packet may be sent.

The measure is used by routing systems to identify the **optimum path** for packet delivery. The **metric** is the unit of measurement utilized by the routing algorithm to identify the best way to the destination, such as **hop count**, **bandwidth**, **latency**, **current load on the network**, and so on.

The routing algorithm creates and maintains the routing table for the path decision process.

Routing Table:`

A **routing table** is a set of rules, often viewed in a table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. See below a Routing Table:

Destination	Subnet mask	Interface
128.75.43.0	255.255.255.0	Eth0
128.75.43.0	255.255.255.128	Eth1
192.12.17.5	255.255.255.255	Eth3
default		Eth2

The entry corresponding to the default gateway configuration is a network destination of 0.0.0.0 with a network mask (netmask) of 0.0.0.0. The Subnet Mask of the default route is always 255.255.255.255.

Entries of a Routing Table:

A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. Routing Table provides the device with instructions for sending the packet to the next hop on its route across the network.
Each entry in the routing table consists of the following entries:

1. **Network ID:** The network ID or destination corresponding to the route.
2. **Subnet Mask:** The mask that is used to match a destination IP address to the network ID.
3. **Next Hop:** The IP address to which the packet is forwarded
4. **Outgoing Interface:** Outgoing interface the packet should go out to reach the destination network.
5. **Metric:** A common use of the metric is to indicate the ***minimum number of hops*** (routers crossed) to the network ID.

Routing table entries can be used to store the following types of routes:

- Directly Attached Network IDs
- Remote Network IDs
- Host Routes
- Default Route
- Destination

When a router receives a packet, it examines the destination IP address and looks up into its Routing Table to figure out which interface packet will be sent out.

Metrics of Routing:

There are many different metrics used to define and measure the efficiency of routing. Some of them are as follows:

1. Hop Count:

A hop count is a statistic that describes the number of trips through internetworking devices such as routers that a packet must make in order to go from source to destination. If the routing protocol uses hop count as a major metric value, the path with the fewest hops will be deemed the optimal way to take from source to destination.

2. Delay:

It is the amount of time it takes a router to process, queue, and transmit a datagram to an interface. This measure is used by protocols to calculate the delay values for all links along the path from beginning to finish. The path with the shortest delay will be deemed the best path.

3. Bandwidth:

The bandwidth of the link is the capacity of the link. Bits per second are used to measure bandwidth. A link with a greater transfer rate, such as gigabit, is chosen over a link with a lesser capacity, such as 56 kb. The protocol will assess the bandwidth capacity of each connection along the way, and the route with the highest total bandwidth will be regarded as the optimal route.

4. Load:

Load refers to how busy a network resource, such as a router or network link, is. It may be calculated in a number of ways, including CPU usage and packets processed per second. If the volume of traffic grows, so will the load value. The load value varies in response to variations in traffic.

5. Reliability:

Reliability is a metric factor that might have a set value. It is determined by the network links, and its value is calculated dynamically. Some networks fail more frequently than others. Some network links recover more easily than others after a network breakdown.

Any dependability factor can be used to provide reliability ratings, which are typically quantitative values assigned by the system administrator.

Types of Routing:

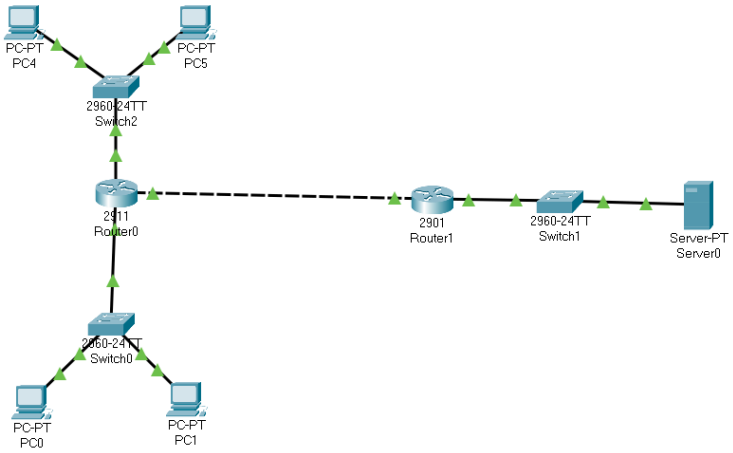
1. Static Routing:

Nonadaptive Routing is another name for static routing. It is a method in which an administrator manually enters routes into a routing database. The packets for the destination can be sent by a router following the path set by the administrator. This method does not make routing decisions based on network state or topology.

Advantages:

- No Overhead: There is no overhead on the router's CPU use. As a result, the less expensive router may be utilized to get static routing.
- Bandwidth consumption: There is no bandwidth usage between the routers.

- Security: It offers security since the system administrator is only authorized to regulate routing to a certain network.



Disadvantages:

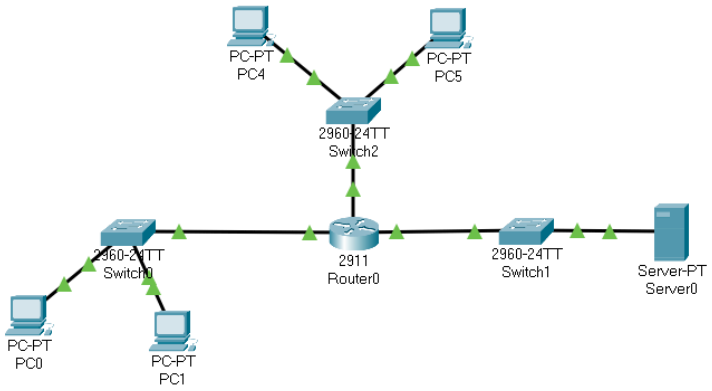
- Adding each route manually to the routing database becomes quite complex in a big network. To manually create each route, the system administrator should be well-versed in topology.

2. Default Routing:

Default Routing is a routing strategy in which a router is set to deliver all packets to the same hop device, regardless of whether it belongs to a specific network or not. A packet is sent to the device for which default routing is enabled.

When networks have a single exit point, default routing is utilized. It is also beneficial when a large number of transmission networks must send data to the same HP device.

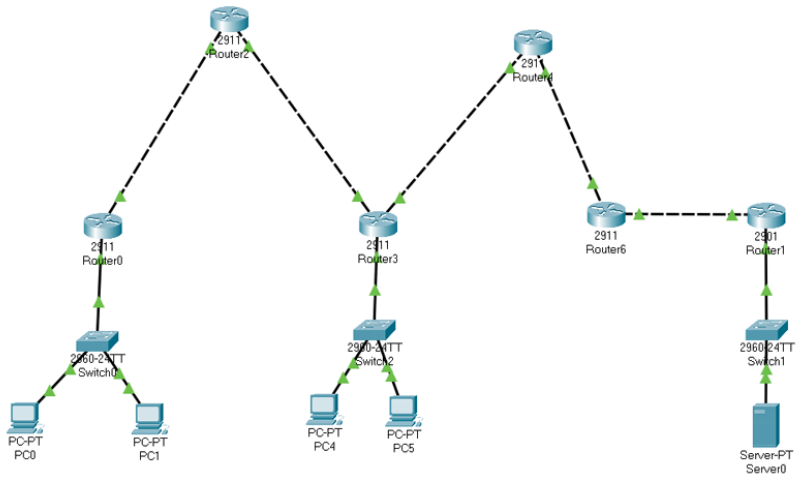
When a specific route is listed in the routing table, the router will take that route instead of the default route. When a specific route is not listed in the routing table, the default route is used.



3. Dynamic Routing:

It is sometimes referred to as Adaptive Routing. It is a technique in which a router creates a new route in the routing table for each packet in response to changes in the network's condition or topology.

Dynamic protocols are utilized to find new paths to the goal. RIP and OSPF are the protocols used in Dynamic Routing to discover new routes.
If any of the routes fails, an automated modification will be performed to get to the destination.



Requirements for Dynamic Routing:

To exchange routes, all routers must use the same dynamic routing protocol. If the router detects a change in the condition or topology, it broadcasts this information to all other routers.

Advantages:

- It is simpler to set up.
- It is more successful in determining the optimum path in response to changes in the condition or topology.

Disadvantages:

- In terms of CPU and bandwidth use, it is more costly.
- It is less secure than default and static routing.

Differences between automatic, manual, and dynamic routing

The following table lists the differences between automatic routing, manual routing, and dynamic routing.

Automatic routing	Static or manual routing	Dynamic routing
Automatic routing is the easiest. The router does all jobs. You don't need to do anything.	Manual routing is easier than dynamic routing but harder than automatic routing. You have to manage all routing-related information manually.	Dynamic routing is easy. You have to configure a routing protocol. The routing protocol manages all routing-related information automatically.
No routing knowledge is required.	You must know how to add and manage routes in the routing table.	You must know how to configure and manage the routing protocol.
A router does not know routes available outside the router. It can only add routes that are available on its interfaces.	An administrator knows all routes available in the network. The administrator can add or remove routes as per the requirement.	A routing protocol uses its mechanism to discover all routes in the network. The administrator can configure this mechanism to meet the network requirement.
By default, automatic routing is enabled on all routers.	Static routing is not enabled by default.	Dynamic routing is also not enabled by default.
Automatic routing is a good option if you have only one router in the network.	Static routing is a good option if you have only some routers in the network.	Dynamic routing is a good option if you have many routers in the network.
Automatic routing does not use additional hardware resources.	Static routing also does not use additional hardware resources.	Dynamic routing uses hardware resources to learn and manage routes.

An Overview of Routing Protocols

A routing protocol is a method of negotiation between two routers to select a route between two nodes based on different conditions. Different categories of routing protocols exist today. Most of the routing protocols that exist can be assigned to any of these categories mentioned below based on their properties.

- Interior Gateway Protocol (IGP)
- Exterior Gateway Protocol (EGP)

• Interior Gateway Protocol (IGP)

As its name suggests, Interior Gateway Protocol, also known as IGP, is used to exchange information among the routers/ gateways within an autonomous system. An autonomous system is a designated network area that is managed by a single network administrator and can have different routing devices.

There are mainly two broad types of interior gateway protocols:

- **Distance Vector Routing Protocol**
- **Link State Routing Protocol**

1. Distance Vector Routing Protocol

As its name suggests, the distance vector routing protocol utilizes two of its features in the routing process.

- **Direction**
- **Distance**

How does the distance vector routing protocol work?

Based on the bellman-ford algorithm, this routing protocol builds up a table at the router which contains a table of distance to different routers from a particular router. The table also contains the distance vector to all the routers in the networks via all the other routers.

For example, if there are three routers in the network, then the table for one of the routers, let's say router 1, will look something like this:

From Router 1	Via Router 1	Via Router 2	Via Router 3
To Router 1			
To Router 2		25	75
To Router 3		48	52

The above lists out the distance from router 1 to routers 2 and 3. As you can see the shortest path to all of the routers from router 1 (except itself) is via router 2.

Question: Can you find the distance between router 2 and router 3?

Route Calculation

In the beginning, when all the routers are booted up, they discover their immediate neighbors which are directly connected to them. They make a table out of it and broadcast their distances to other directly connected routers on the network.

Upon receiving a broadcast, the router compares its tables and updates for any shortest path.

Countdown to infinity problem

One of the major loopholes of the distance vector routing protocol is that it suffers from the countdown to infinity problem.

Scenario

Let us say there are four routers in a network Router A, B, C, and Router D. Let us assume that router A is down. After some time, when router B does not receive any update from

router A, it marks the router down. But router C still has the path to A via router B in its table.

So, router C broadcasts to router B that it knows a path to router A, and let us say, that is two hops away. In this scenario, though router C has counted the path via router B, router B is not aware of it. So, router B broadcasts its table by adding one more hop (for itself) and says that router A is three hops away from me.

When router C receives the broadcast and it finds out that router B has updated its distance, it also increments its distance accordingly and broadcasts the new distance again to router B. In turn, router B again broadcasts the new distance. This way, the distance keeps on increasing forever in a loop. This problem is called the **countdown to infinity problem**.

Question: Can you guess the solution to the countdown to infinity problem? If you have found one, then mention it in the comments at the end of the article.

Examples of Distance vector routing protocols:

- RIP (Routing Information Protocol)
- IGRP
- EIGRP

2. Link State Routing Protocol

Imagine a situation when there would be tens of routers inside an autonomous system. The route calculation would take a lot of time to converge when the distance between the routers is not stable and keeps on changing frequently. This was the problem with the Distance vector routing protocol and was addressed in the link state routing protocol.

Link state routing protocol works in two phases.

- Phase one: Reliable flooding
    - Initial state and,
    - final state
- Phase two: Route calculation

Reliable flooding

When the routers are booted up, the first thing that the routers do is determine which ports they are connected to. So, they reach each neighboring router personally. Once the router has an idea of what all ports they are connected to, they start advertising its connectivity and distributing it across the network so that each other node can receive the advertisement and build the network topology.

This flooding/ broadcast has been called here “reliable” because if any of the nodes advertise any false information, that will lead to a false network topology diagram.

Link Discovery Challenges

As already mentioned above, the first challenge is reliability. Other prominent challenges are **avoiding loops and minimizing the packet exchanges so as to avoid network overflooding.**

Solutions

The solutions to the above problem are:

- Each packet needs to have a unique ID
- Do not reply on the port from where you receive a broadcast. It is managed using a flag.

Thus, in the final state of reliable flooding, all the nodes have information about the entire topology.

Route Calculation

Route calculation in the link state protocol uses some variant of the Dijkstra algorithm. Once a node has the topology, it runs the Dijkstra algorithm to find the shortest path to all the other nodes in the network.

Just like the Distance Vector Routing Protocol, this routing protocol also has some limitations, though it tries to resolve some of the issues arising in the former one.

- Link state routing protocol reduces the network data overhead, unlike distance vector routing protocol, by using partial computation when a link metrics changes in the network.

Examples of Link state routing protocol

- Open Shortest Path First (OSPF) and,
- IS-IS (Intermediate System to Intermediate System)

- Exterior Gateway Protocol (EGP)

Exterior Gateway protocols are used to communicate to the different networks unlined IGPs which work only for an autonomous system.

Working of EGP

Internet hosts used EGP for data table routing exchanges before BGP was introduced. Available routers, addresses, cost metrics, and each optimal route selection path are all listed in the EGP routing table. The EGP model is designed to automate limited events, actions, and transitions.

The EGP mechanisms are as follows −

- Obtain neighbors
- Keep an eye on your neighbors.
- Data is exchanged via update messages.

EGP allows neighboring routers in different domains to share information, whereas Interior Gateway Protocols are utilized within a domain.

The Advanced Research Projects Agency Network's main routers use EGP to convey reachability to and from them (ARPANET). Individual source nodes in separate Internet administrative domains known as autonomous systems (ASs) sent information to the core routers, then relayed down via the backbone until it reached the destination network within another AS.

Unlike most other protocols, EGP is solely concerned with network reachability and uses no metrics to choose the optimum way.

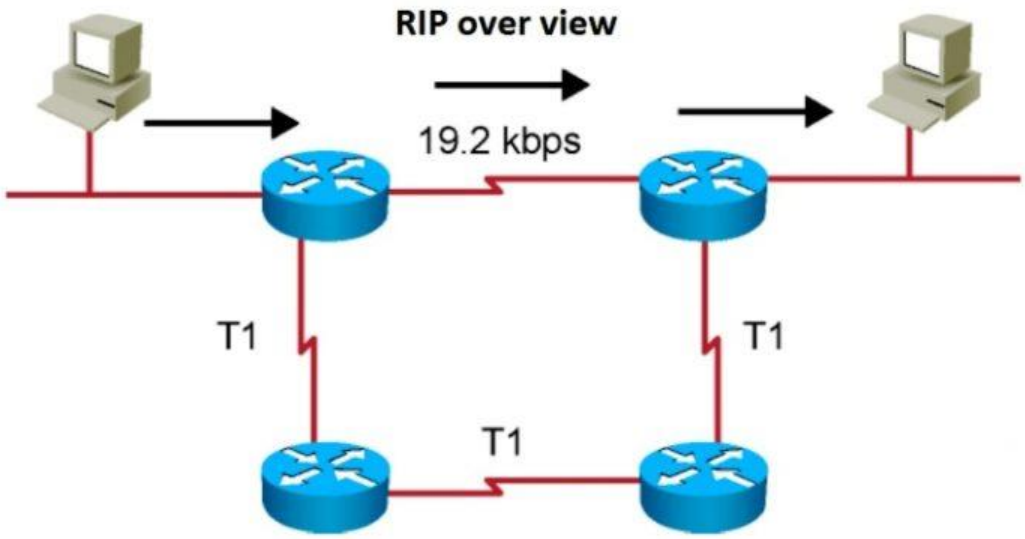
Pros and Cons of EGP

EGP was the first exterior gateway protocol to gain general popularity on the Internet, and it has several pros and disadvantages. The routing table remains stable with minimum changes because the protocol does not react to faults within the Autonomous system.

EGP is a simple reachability protocol limited to tree-like topologies and does not support multipath networking settings, making it less efficient than newer distance-vector and path-vector protocols.

As this routing system is designed to be centrally managed, it has limited scalability, a significant disadvantage in today's rapidly increasing Internet. The commercialized Internet is not under the supervision of any central authority. The Internet is made up of several interconnected networks. In a distributed architecture, autonomous systems require internal and external routing protocols to make intelligent routing decisions. As a result, EGP has fallen out of favor.

RIP (Routing Information Protocol)



Routing Information Protocol (RIP) is one of the earliest routing protocols which was a part of the **Interior Gateway Protocols**. It can also be classified as a type of **distance**

vector protocol where routing metrics are dependent on the distance calculated in some forms.

Routing Information Protocol uses **hop count** as the distance metric. RIP addresses that issue by setting up the maximum hop count as 15. A hop count of 16 is counted as infinity in the case of RIP. However, setting up a limitation on the hop count also comes at a cost. It limits the number of networks that can be supported in the RIP to 15.
RIP uses some of the fundamental concepts which are utilized in its routing protocols.

RIP fundamentals

Let us have a look at the fundamental concepts so that we can understand the rudimentary of this protocol.

Periodic Updates

As already discussed in the interior gateway protocol, all routers broadcast their routing tables to the directly connected routers on their interfaces. In the case of RIP, it sends periodic updates every 30 seconds to all other routers which are directly connected to it. Even if there are no network changes, these updates are still sent every 30 seconds.

The updates are sent only to the configured interfaces on a router. Also, the update is sent periodically as a broadcast (255.255.255.255) to all the hosts.

Administrative Distance

Routers use administrative distance as a metric when sending packets from one to another router. It is a special number that is associated with every routing protocol which enables a router to know which routing protocol another router is running.
Different routing protocols have been assigned different administrative distances. For RIP, it is 120. So, when another router receives the update and reads the administrative distance, it comes to know the other router is running what protocol.

RIP Limitations

Classful Routing

RIP uses classful routing and it does not support classless routing. For example, if a network that is connected to a router running RIP is using VLSM, all the nodes/hosts on that network should use the same network mask.

Router Authentication

There was no support for the authentication on RIP version 1 which made the routers vulnerable to attacks. With RIP version 2, MD5 authentication came into place, and instead of plain text passwords, encrypted passwords were used for the authentication.

Router authentication is used when a router receives a route update from its neighbor router. However, other mechanisms were implemented to prevent wrong information from being populated to other routers in RIP v2.

Split horizon route advertisement

To prevent the routing loops, routers do not broadcast the update on the interfaces it receives an update from.

Route Poisoning with Hold down timer

The concepts of route poisoning and hold-down timer are utilized to prevent packet looping and make sure that no routers send a packet to an invalid router.

Scenario
When a Router, Let's say Router A, detects that one of the networks connected directly to its interface is down, it sets its distance as 16 (hop count of 16 is counted as infinity in RIP) and broadcasts the update to other connected routers.

It might take some time in the network for the route poisoned messages to reach every other router. In the meantime, the router that advertised the message, in this case, Router A, would not accept any update from any other router until the hold-down timer expires.

Once the hold-down timer expires, the router starts accepting updates from other routers. In the case of RIP, the hold-down timer is 180 seconds, six times the update timer.

RIP Routing Table

As discussed before, this routing protocol uses different A router running the RIP protocol keeps the following set of information about every node

IP address: The destination IP address
Gateway: The first gateway along the path to the destination
Interface: The router interface to which the router is connected
Metric: At a distance of the number of hops on which another router is situated.
Timer: The time when the entry was last updated

RIP Timers

timers to keep track of other nodes and updates. Here is a list of the timers that are used by RIP

Update Timer

The update timer is the frequency at which every active router makes its routing table broadcast to every other directly connected router to its interfaces. As already discussed earlier in this article, RIP has the update timer set as 30 seconds by default.

Invalid Timer

The invalid timer comes into play when one of the routers in the network has been marked as unreachable. The router is marked unreachable and invalid by setting up its hops distance as 16. Though the route is still retained in the routing table the connected router still waits for a period of 180 seconds or six update periods (30 seconds x 6 = 180 seconds) before marking the router as poisoned and unreachable.

Flush Timer

The flush timer, as evident from its name, is used to flush out an entry from the routing table after a particular router has been marked as invalid using the invalid timer. By default, the flush timer is 240 seconds, which is 60 seconds longer than the invalid timer.

Hold down Timer

Hold down timer along with the route poisoning properties of the RIP is used in making sure that there is no looping in the network. Once a router goes down, a router waits another 180 seconds for the unreachable router to respond/ send some updates before making it unreachable.

COMPUTER NETWORKS 2

المرحلة الثالثة

CHAPTER THREE

SWITCH, HUB &ACCESS POINT

Ethernet Hub

A **hub** in computer networks is a basic networking device that connects multiple computers or network devices in a **Local Area Network (LAN)**. It operates at the **Physical Layer (Layer 1)** of the **OSI model** and is used to transmit data between devices connected to it.

How a Hub Works:

- When a device connected to the hub sends data, the hub **broadcasts** it to **all connected devices**.
- Only the device with the correct destination address processes the data; the rest **ignore** it.
- Hubs **do not filter data** or use MAC addresses for data delivery.

Types of Hubs:

1. **Passive Hub:**
   - Simply connects devices without amplifying signals.
2. **Active Hub:**
   - Regenerates and strengthens signals before forwarding.
3. **Intelligent Hub:**
   - Provides additional features like remote management and network diagnostics
   -

Advantages of Network Hubs

- It is less expensive.
- It does not impact network performance.
- Hub support different network media.

Disadvantages of Network Hubs

- It cannot find the best/ shortest path of the network.
- No mechanism for traffic detection.
- No mechanism for data filtration.
- Not capable of connecting to different network topologies like token ring, ethernet, etc.

Access Point

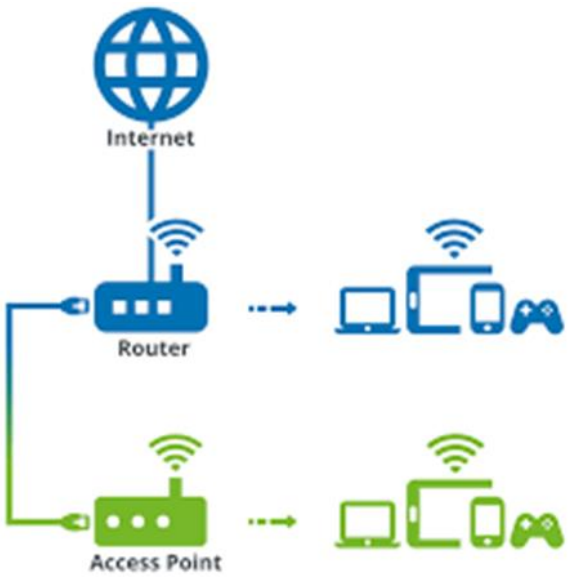
An Access Point (AP) in networking is a hardware device that allows wireless devices to connect to a wired network using Wi-Fi. It acts as a bridge between wireless devices (like laptops, smartphones, and tablets) and the wired network, enabling communication between them.

Key Features of an Access Point:

- **Wireless Connectivity**: Provides Wi-Fi access to devices within its coverage area.
- **Bridge Functionality**: Connects wireless clients to the wired Local Area Network (LAN).
- **SSID Broadcasting**: Transmits the network name (SSID = service set identifier, is your Wi-Fi network name) so devices can discover and join the network.
- **Security Options**: Supports security protocols like WPA3, WPA2, and WEP to protect wireless communications.

Where are Access Points Used?

- Offices: To provide Wi-Fi across large areas with multiple APs for seamless roaming.
- Schools & Universities: Ensures stable wireless connections for many users.
- Public Spaces: Airports, cafes, and malls use APs to offer guest Wi-Fi.



Network Switch

A network switch (also called switching hub, bridging hub, Ethernet switch, and, by the IEEE, MAC bridge) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.

A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

Unlike hubs, which broadcast the same data out of each port and let the devices pick out the data addressed to them, a network switch learns the Ethernet addresses of connected devices and then only forwards data to the port connected to the device to which it is addressed.

Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended. Each networked device connected to a switch can be identified by its network address, allowing the switch to direct the flow of traffic maximizing the security and efficiency of the network.

Bridging

Bridging in a **network switch** refers to the process of connecting multiple network segments to operate as a single, unified network. A **network bridge** (often implemented through a switch) filters and forwards traffic between network segments based on the **MAC addresses** of devices, allowing efficient communication without unnecessary data transmission across the entire network.

How Bridging Works in a Switch

1. **Learning** – The switch learns the MAC addresses of connected devices and stores them in a MAC address table.
2. **Forwarding** – When a frame arrives, the switch checks the destination MAC address and forwards it only to the appropriate port instead of broadcasting it to all ports.
3. **Filtering** – If the destination MAC address is on the same segment as the sender, the switch blocks unnecessary forwarding, reducing network congestion.

Why Bridging is Important in Switches:

1. Enhances network performance by reducing unnecessary traffic.
2. Improves security by isolating segments.
3. Increases scalability of large networks.
4. Facilitates network segmentation for better traffic management.

Advantages of Switches

1. They increase the available bandwidth of the network.
2. They help in reducing workload on individual host PCs.
3. They increase the performance of the network.
4. Networks which use switches will have less frame collisions. This is due to the fact that switches create collision domains for each connection.
5. Switches can be connected directly to workstations

Disadvantages of Switches

Following are the **disadvantages of Switches**:

1. They are more expensive compare to network bridges.
2. Network connectivity issues are difficult to be traced through the network switch.
3. Broadcast traffic may be troublesome.
4. If switches are in promiscuous mode, they are vulnerable to security attacks e.g., spoofing IP address or capturing of ethernet frames.
5. Proper design and configuration is needed in order to handle multicast packets.
6. While limiting broadcasts, they are not as good as routers.