15. Which device is commonly used to connect a computer to a telephone line for internet access?
   a) Router
   b) Gateway
   c) CSU/DSU
   d) Modem

16. Which device is responsible for assigning unique IP addresses to devices on a network?
   a) Router
   b) Gateway
   c) CSU/DSU
   d) DHCP server

17. What is the purpose of a CSU (Channel Service Unit) in a CSU/DSU device?
   a) It converts analog signals to digital signals.
   b) It provides clock synchronization for data transmission.
   c) It encrypts data packets for secure transmission.
   d) It assigns IP addresses to network devices.

18. What is the primary function of a gateway?
   a) Packet forwarding
   b) Signal regeneration
   c) IP address assignment
   d) Connecting networks with different protocols

19. Which device is commonly used to connect multiple devices within a local network?
   a) Router
   b) Gateway
   c) CSU/DSU
   d) Switch

20. What is the purpose of a CSU/DSU device in a network setup?
   a) It provides firewall capabilities.
   b) It converts analog signals into digital signals.
   c) It connects a local network to the internet.
   d) It routes network traffic between networks.

Terminal Questions:

1. What is the role of a router in a network? How does it facilitate communication between different networks?
2. What is the difference between a router and a gateway?
3. What is the purpose of a CSU/DSU in a network setup? How does it facilitate communication over digital leased lines?
4. What are some common issues that can arise with CSU/DSU devices, and how can they be resolved?
5. How can you secure a router or gateway to protect against unauthorized access and potential security threats?

Summary:

A wired router is a networking device that connects multiple wired devices within a local area network (LAN) and forwards data packets between these devices. It operates at the Network Layer (Layer 3) of the OSI model and uses routing tables to determine the best path for data

transmission. Wired routers typically have Ethernet ports to connect devices via Ethernet cables, and they can also connect to the internet through a modem. Wired routers are commonly used in homes and small to medium-sized businesses to share internet connectivity and enable communication between devices within the local network. A wireless router, also known as a Wi-Fi router, is a networking device that performs the same functions as a wired router but additionally provides wireless connectivity to devices within its coverage area. In addition to Ethernet ports for wired connections, a wireless router has built-in antennas that broadcast Wi-Fi signals, allowing Wi-Fi-enabled devices like smartphones, laptops, and tablets to connect to the network wirelessly. Wireless routers are widely used in homes, offices, and public spaces to offer the convenience of wireless internet access and enable seamless mobility for connected devices. A gateway is a networking device that acts as an entry and exit point between two different networks, enabling communication and data exchange between them. It can connect networks that use different communication protocols or architectures, effectively bridging the gap between incompatible networks. Gateways are often used in large-scale enterprise networks and the internet, where they play a crucial role in connecting local networks to the external world and facilitating the exchange of data between disparate networks. CSU/DSU is a pair of networking devices used to connect a digital data terminal equipment (DTE), such as a router or switch, to a digital data communication circuit, such as a T1 or T3 line. The Channel Service Unit (CSU) and Data Service Unit (DSU) perform separate functions but are typically housed in a single physical unit. The CSU handles line conditioning and termination, ensuring the quality and integrity of the data signals, while the DSU provides clocking and framing, facilitating proper data transmission over the digital circuit. CSU/DSU devices are commonly used in telecommunications and wide area networks (WANs) to connect businesses to their service provider's digital communication lines and ensure reliable and efficient data transmission.

Answer Keys:

1. a	2. b	3. c	4. a	5. c	6. a	7. d	8. b	9. b	10. b
11. b	12. c	13. c	14. c	15. d	16. d	17. a	18. d	19. d	20. b

Topic 5: Routing Protocols

ROUTING ALGORITHMS:
The **routing algorithm** is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.

PROPERTIES OF ROUTING ALGORITHM:
Correctness, simplicity, robustness, stability, fairness, and optimality

FAIRNESS AND OPTIMALITY.

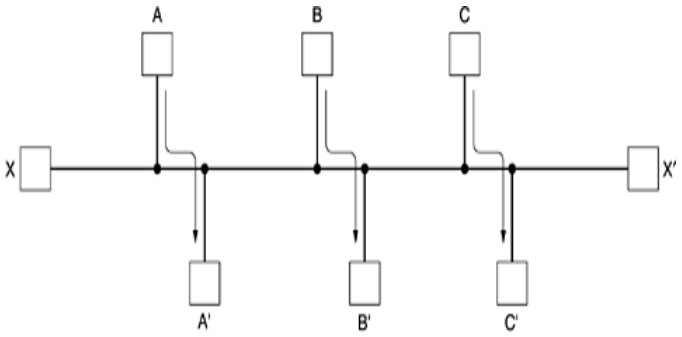


Fig 5.1 :Fairness & Optimality

Fairness and optimality may sound obvious, but as it turns out, they are often contradictory goals. There is enough traffic between A and A', between B and B', and between C and C' to saturate the horizontal links. To maximize the total flow, the X to X' traffic should be shut off altogether. Unfortunately, X and X' may not see it that way. Evidently, some compromise between global efficiency and fairness to individual connections is needed.

CATEGORY OF ALGORITHM

Routing algorithms can be grouped into two major classes: **nonadaptive and adaptive.**

Nonadaptive algorithms do not base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use to get from I to J is computed in advance, off-line, and downloaded to the routers when the network is booted.

This procedure is sometimes called **Static routing**.

Adaptive algorithms, in contrast, change their routing decisions to reflect changes inthe topology, and usually the traffic as well

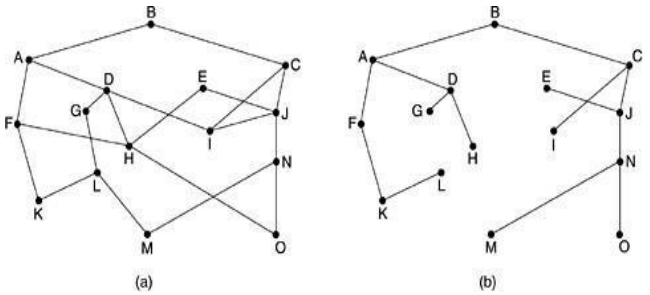
This procedure is sometimes called **dynamic routing**

THE OPTIMALITY PRINCIPLE

If router J is on the optimal path from router I to router K, then the optimal path fromJ to K also falls along the same route.

The set of optimal routes from all sources to a given destination form a tree rooted atthe destination. Such a tree is called a sink tree.

Fig 15.2 (a) A subnet. (b) A sink tree for router B.



As a direct consequence of the optimality principle, we can see that the set of optimal routes from all sources to a given destination form a tree rooted at the destination.

Such a tree is called a **sink tree** where the distance metric is the number of hops. Note that a sink tree is not necessarily unique; other trees with the same path lengths may exist.

The goal of all routing algorithms is to discover and use the sink trees for all routers.

SHORTEST PATH ROUTING

A technique to study routing algorithms: The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line (often called a link).
To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.
One way of measuring path length is the number of hops. Another metric is the geographic distance in kilometers. Many other metrics are also possible. For example, each arc could be labeled with the mean queuing and transmission delay for some standard test packet as determined by hourly test runs.
In the general case, the labels on the arcs could be computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measured delay, and other factors. By changing the weighting function, the algorithm would then compute the "shortest" path measured according to any one of a number of criteria or to a combination of criteria.

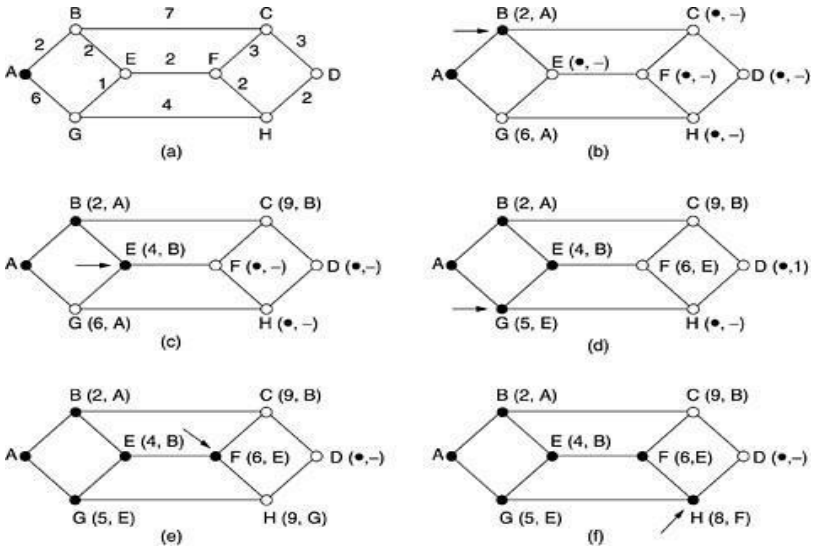


Fig. 14.2: Steps for computation of shortest path

FLOODING
Another static algorithm is **flooding**, in which every incoming packet is sent out on every outgoing line except the one it arrived on.
Flooding obviously generates vast numbers of duplicate packets, in fact, an infinite number unless some measures are taken to damp the process.
One such measure is to have a hop counter contained in the header of each packet, whichis decremented at each hop, with the packet being discarded when the counter reaches zero.

Ideally, the hop counter should be initialized to the length of the path from source to destination. If the sender does not know how long the path is, it can initialize the counter to the worst case, namely, the full diameter of the subnet.

DISTANCE VECTOR ROUTING

Distance vector routing algorithms operate by having each router maintain a table (i.e., a vector) giving the best-known distance to each destination and which line to use to get there. These tables are updated by exchanging information with the neighbors.
The distance vector routing algorithm is sometimes called by other names, most commonly the distributed **Bellman-Ford** routing algorithm and the **Ford-Fulkerson** algorithm, after the researchers who developed it (Bellman, 1957; and Ford and Fulkerson, 1962).
It was the original ARPANET routing algorithm and was also used in the Internet under the name RIP

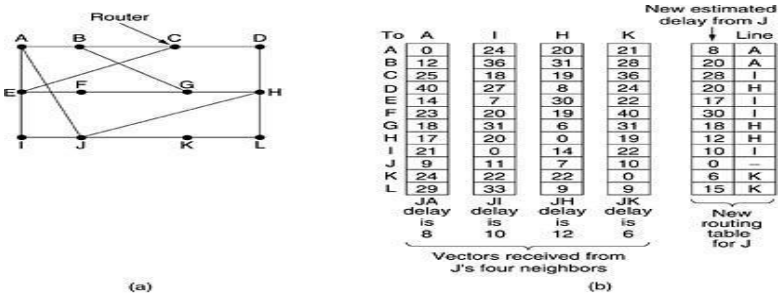


Fig.4.3: (a) A subnet. (b) Input from A, I, H, K, and the new routing table for J.

LINK STATE ROUTING
The idea behind link state routing is simple and can be stated as five parts. Each router must do the following:
Discover its neighbors and learn their network addresses.
Measure the delay or cost to each of its neighbors.
Construct a packet telling all it has just learned.
Send this packet to all other routers.
Compute the shortest path to every other router

1. Learning about the Neighbours
When a router is booted, its first task is to learn who its neighbours are. It accomplishes this goal by sending a special HELLO packet on each point-to-point line. The router on the other end is expected to send back a reply telling who it is.

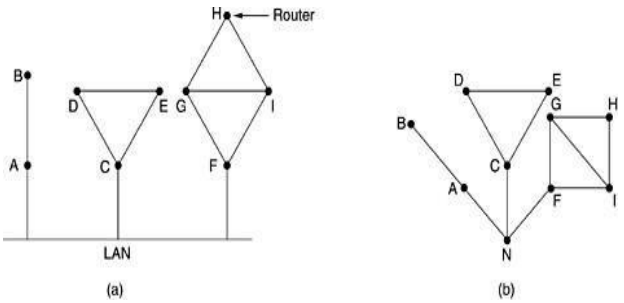


Fig. 4.4: (a) Nine routers and a LAN. (b) A graph model of (a).

2. Measuring Line Cost
The link state routing algorithm requires each router to know, or at least have a reasonable estimate of, the delay to each of its neighbors. The most direct way to determine this delay is to send over the line a special ECHO packet that the other side is required to send back immediately.

By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay.
For even better results, the test can be conducted several times, and the average used. Of course, this method implicitly assumes the delays are symmetric, which may not always be the case.
Building Link State Packets

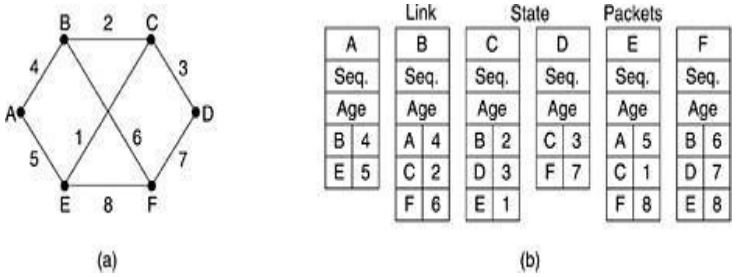


Fig.4.5: (a) A subnet. (b) The link state packets for this subnet.

Once the information needed for the exchange has been collected, the next step is foreach router to build a packet containing all the data.
The packet starts with the identity of the sender, followed by a sequence number and age(to be described later), and a list of neighbours.
For each neighbour, the delay to that neighbour is given.
An example subnet is given in Fig. 4.5(a) with delays shown as labels on the lines. The corresponding link state packets for all six routers are shown in Fig. 4.5 (b).

Distributing the Link State Packets

Source	Seq.	Age	Send flags A	Send flags C	Send flags F	ACK flags A	ACK flags C	ACK flags F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Fig 4.6: The packet buffer for router* B *in Fig. 4.5.

In Fig. 4.6, the link state packet from *A* arrives directly, so it must be sent to *C* and *F* and acknowledged to *A*, as indicated by the flag bits.
Similarly, the packet from *F* has to be forwarded to *A* and *C* and acknowledged to *F*.

HIERARCHICAL ROUTING

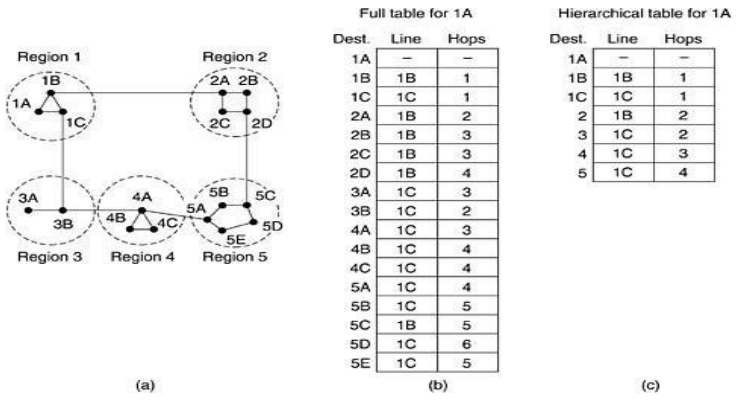


Fig 4.7: Hierarchical routing

The routers are divided into what we will call regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.

For huge networks, a two-level hierarchy may be insufficient; it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and so on, until we run out of names for aggregations.

Figure 4.7 gives a quantitative example of routing in a two-level hierarchy with five regions. The full routing table for router 1*A* has 17 entries, as shown in Fig. 4.7(b).

When routing is done hierarchically, as in Fig. 4.7(c), there are entries for all the local routers as before, but all other regions have been condensed into a single router, so all traffic for region 2 goes via the 1*B* -2*A* line, but the rest of the remote traffic goes via the 1*C* -3*B* line.

Hierarchical routing has reduced the table from 17 to 7 entries. As the ratio of the number of regions to the number of routers per region grows, the savings in table space increase.

BROADCAST ROUTING

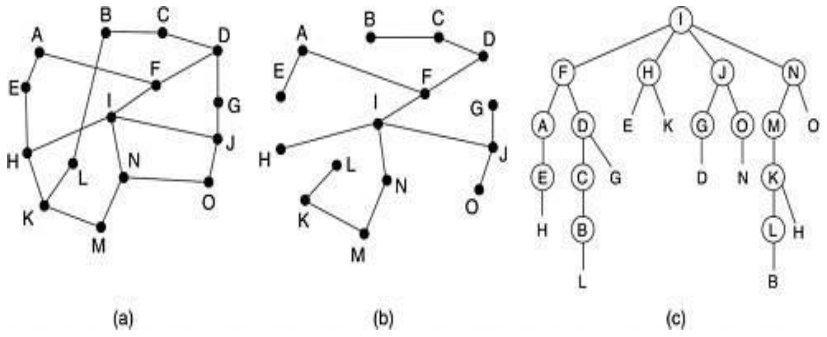


Fig. 4.8: Reverse path forwarding.
(a) A subnet.
(b) A sink tree.
(c) The tree built by reverse pathforwarding.

Sending a packet to all destinations simultaneously is called broadcasting.

The source simply sends a distinct packet to each destination. Not only is the method wasteful of bandwidth, but it also requires the source to have a complete list of all destinations.

Flooding.

The problem with flooding as a broadcast technique is that it generates too many packetsand consumes too much bandwidth.

Part (a) shows a subnet, part (b) shows a sink tree for router *I* of that subnet, and part (c)shows how the reverse path algorithm works.

When a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line that is normally used for sending packets to the source of the broadcast. If so, there is an excellent chance that the broadcast packet itself followed the best route from the router and is therefore the first copy to arrive at the router.

This being the case, the router forwards copies of it onto all lines except the one it arrived on. If, however, the broadcast packet arrived on a line other than the preferred one for reaching the source, the packet is discarded as a likely duplicate.

MULTICAST ROUTING

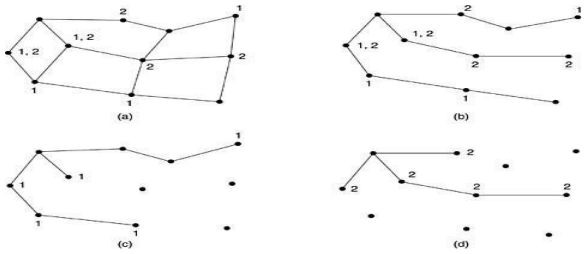


Fig. 4.9: Multicast routing

To do multicast routing, each router computes a spanning tree covering all other routers. For example, in Fig. 4.9 (a) we have two groups, 1 and 2.

Some routers are attached to hosts that belong to one or both of these groups, asindicated in the figure.

A spanning tree for the leftmost router is shown in Fig. 4.9 (b). When a process sends a multicast packet to a group, the first router examines its spanning tree and prunes it, removing all lines that do not lead to hosts that are members of the group.

In our example, Fig. 4.9 (c) shows the pruned spanning tree for group 1. Similarly, Fig. 4.9 (d) shows the pruned spanning tree for group 2. Multicast packets are forwardedonly along the appropriate spanning tree.

SAQ's-Self Assessment Questions

1. A _____ is a device that forwards data that is not explicitly destined to it.

A. hub
B. switch
C. router
D. All of the above

2. There exists _____ forms of routing protocols.

A. 1
B. 2
C. 3
D. 4

3. Routing protocols can be divided in _____ categories.

A. 2
B. 3
C. 4
D. 5

4. RIPng stands for _____.

A. Routing Information Path Next Generation
B. Routing Interior Protocol Next Generation
C. Routing Information Protocol Next Gateway
D. Routing Information Protocol Next Generation

5. An _____ distributes routing information between two different autonomous systems or organization.

A. Interior Routing Protocol
B. Exterior Routing Protocol
C. Link-State Routing Protocol
D. Distance Vector Routing Protocol

6. _____ is an upgraded implementation of ICMP to accommodate IPv6 requirements.

A. ICMPv6
B. DHCPv6
C. DNS
D. None of the above

7. Which type of Ethernet framing is used for TCP/IP and DEC net?

A. Ethernet 802.3
B. Ethernet 802.2
C. Ethernet II
D. Ethernet SNAP

8. Which NetWare protocol works on layer 3–network layer—of the OSI model?

A. IPX
B. NCP
C. SPX
D. NetBIOS

9. Which NetWare protocol provides link-state routing?

A. RIP
B. SAP
C. NCP
D. NLSP

10. A Distance Vector router running distance vector protocol advertises its connected routes and learns new routes from its neighbors.

A. Yes
B. No
C. Can be yes or no
D. Cannot say

11. Which layer is responsible for determining routes?
A. Physical Layer
B. Transport Layer
C. Network Layer
D. Transmission Layer

12. Routing decisions in the adaptive algorithm are taken by considering _____?
A. Network Traffic
B. Topology
C. Data
D. a & b

13 Which of the following is not the requirement of the routing function?
A. Correctness
B. Robustness
C. Delay time
D. Stability

14 The Open Shortest Path First(OSPF) protocol is an intra-domain routing protocol based on …….. routing.
A. distance vector
B. link state
C. path vector
D. non-distance vector

15. An/A …….routing scheme is designed to enable switches to react to changing traffic patterns on the network.
A. static routing
B. fixed alternative routing
C. standard routing
D. dynamic routing

16. The term …….. refers to which node or nodes in the network are responsible for the routing decision.
A. decision place
B. routing place
C. node place
D. switching place

17. The technique which requires no network information required is…
A. flooding

B. variable routing
C. fixed routing
D. random routing

18. When a direct delivery is made, both the deliverer and receiver have the same…
A. routing table
B. host id
C. IP address
D. Net id

19) In OSPF, a …… link is a network with several routers attached to it.
A. point-to-point
B. transient
C. stub
D. multipoint

20) In ……. the router forwards the received packet through only one of its interfaces.
A. unicasting
B. multicasting
C. broadcasting
D. point to point

Terminal Questions

Consider the network of Fig. 14.3 (a). Distance vector routing is used, and the following vectors have just come into router C: from B: (5, 0, 8, 12, 6, 2); from D: (16, 12, 6,0,9,10); and from E:(7,6,3,9,0,4). The cost of the links from C to B, D, and E, are 6, 3, and 5, respectively. What is C's new routing table? Give both the outgoing line to use and the cost.

Explain the difference between routing, forwarding, and switching.

Two machines on the same network try to use the same port number to communicate with a server on another network. Is this possible? Explain why (not). What changes if these machines are separated from other networks by a NAT box?

Consider the network of Fig. 5-12(a). Distance vector routing is used, and the follow- ing link state packets have just come in at router D: from A: (B: 5, E: 4); from B: (A: 4, C: 1, F: 5); from C: (B: 3, D: 4, E: 3); from E: (A: 2, C: 2, F: 2); from F: (B: 1, D: 2, E: 3). The cost of the links from D to C and F are 3 and 4 respectively. What is D's new routing table? Give both the outgoing line to use and the cost.

Answer Keys:

1	2	3	4	5	6	7	8	9	10
C	B	A	D	B	A	C	A	D	A
11	12	13	14	15	16	17	18	19	20
C	D	C	B	C	A	A	D	B	B

Topic 6: Subnetting

The Subnetting course is designed to provide students with a comprehensive understanding of the subnetting concept and its application in IP network design and management. The course covers the fundamental principles of subnetting, subnet mask calculation, and subnetting techniques. It is basically dealing with how to divide IP networks into smaller subnets to optimize network resources, improve scalability, and enhance network security.
The session on subnetting introduces the concept of subnetting and its importance in IP network design and management. It highlights the challenges faced in traditional IP addressing and how subnetting addresses those challenges. The session sets the foundation for understanding subnetting principles, subnet mask calculations, and subnetting techniques that will be covered in detail throughout the course.

SAQ's-Self Assessment Questions

1. What is subnetting?
   a. Dividing a network into multiple smaller subnetworks
   b. Combining multiple networks into a larger network
   c. Allocating IP addresses for devices in a network
   d. Creating virtual private networks

   Answer: a. Dividing a network into multiple smaller subnetworks

2. What is the purpose of subnetting?
   a. To improve network security
   b. To increase network performance
   c. To optimize IP address allocation
   d. All of the above

   Answer: d. All of the above

3. Which of the following is not a benefit of subnetting?
   a. Efficient use of IP addresses
   b. Improved network scalability
   c. Enhanced network reliability
   d. Reduced network latency

   Answer: d. Reduced network latency

4. What is a subnet mask?
   a. A unique identifier for a subnet
   b. A set of numbers used to divide a network into subnets
   c. A hardware device used in subnetting
   d. A protocol used to communicate between subnets

   Answer: b. A set of numbers used to divide a network into subnets

5. Which classful IP address range supports subnetting?
   a. Class A
   b. Class B
   c. Class C
   d. All classes

Answer: d. All classes

6. How many bits are borrowed from the host portion to create subnets in Class C networks?
a. 4 bits
b. 6 bits
c. 8 bits
d. 10 bits

Answer: c. 8 bits

7. What is the maximum number of subnets that can be created with a Class B network address using subnetting?
a. 256
b. 512
c. 1024
d. 2048

Answer: c. 1024

8. How many host addresses are available in each subnet when using a subnet mask of 255.255.255.192?
a. 30
b. 62
c. 126
d. 254

Answer: b. 62

9. Which subnet mask is associated with a /27 network prefix?
a. 255.255.255.192
b. 255.255.255.224
c. 255.255.255.240
d. 255.255.255.248

Answer: d. 255.255.255.248

10. Which subnetting technique allows for the creation of subnets with different sizes?
a. Fixed-length subnetting
b. Variable-length subnetting
c. Classful subnetting
d. Dynamic subnetting

Answer: b. Variable-length subnetting

11. What is the broadcast address for a subnet with a subnet mask of 255.255.255.224?
a. Last usable address
b. First usable address
c. Network address
d. All ones in the host portion

Answer: d. All ones in the host portion

12. How many usable host addresses are available in a subnet with a subnet mask of 255.255.255.240?

a. 14
b. 15
c. 16
d. 30

Answer: b. 15

13. Which subnetting technique involves dividing a network into equal-sized subnets?
a. Fixed-length subnetting
b. Variable-length subnetting
c. Classful subnetting

d. Hierarchical subnetting

Answer: a. Fixed-length subnetting

14. What is the default subnet mask for a Class C network?
a. 255.0.0.0
b. 255.255.0.0
c. 255.255.255.0
d. 255.255.255.255

Answer: c. 255.255.255.0

15. Which of the following is a private IP address range?
a. 10.0.0.0 - 10.255.255.255
b. 172.16.0.0 - 172.31.255.255
c. 192.168.0.0 - 192.168.255.255
d. All of the above

Answer: d. All of the above

16. What is supernetting?
a. Combining multiple subnets into a larger network
b. Dividing a network into smaller subnets
c. Allocating IP addresses for devices in a network
d. Creating virtual private networks

Answer: a. Combining multiple subnets into a larger network

17. Which protocol is commonly used for automatic assignment of IP addresses in subnetted networks?
a. DHCP
b. DNS
c. ARP
d. ICMP

Answer: a. DHCP

18. What is the network address of a subnet with a subnet mask of 255.255.255.0?
a. First usable address
b. Last usable address
c. Broadcast address

d. All zeros in the host portion

Answer: d. All zeros in the host portion

19. Which of the following is not a valid subnet mask?
a. 255.255.255.255
b. 255.255.0.0
c. 255.255.255.192
d. 255.255.255.224

Answer: a. 255.255.255.255

20. Which of the following is true about subnetting?
a. It reduces the size of a network
b. It increases the size of a network
c. It does not affect the size of a network
d. It only affects network performance

Answer: b. It increases the size of a network

21. What is a default gateway?
a. The first host address in a subnet
b. The last host address in a subnet
c. The network address of a subnet
d. The device used to connect one network to another
Answer: d. The device used to connect one network to another
22. Which of the following is not a valid IPv4 address?
a. 192.168.0.256
b. 10.0.0.1
c. 172.16.0.0
d. 255.255.255.0
Answer: a. 192.168.0.256
23. What is the maximum number of host addresses that can be assigned in a subnet with a /26 subnet mask?
a. 62
b. 126
c. 254
d. 510
Answer: a. 62
24. Which of the following is a valid IPv6 address?
a. 192.168.0.1
b. 2001:0db8:85a3:0000:0000:8a2e:0370:7334
c. 10.0.0.1
d. 172.16.0.0

Answer: b. 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Terminal Questions

1. What is subnetting?
2. What is the purpose of subnetting?
3. What is a subnet mask?
4. How does subnetting help in efficient use of IP addresses?
5. What is the default subnet mask for a Class C network?

6. How many bits are borrowed from the host portion to create subnets in a Class C network using subnetting?
7. What is the maximum number of subnets that can be created with a Class B network address using subnetting?

Summary
Subnetting is the process of dividing a network into smaller subnetworks called subnets. It allows for efficient use of IP addresses, improved network performance, and enhanced network security. Subnetting involves using subnet masks to determine the network and host portions of an IP address.

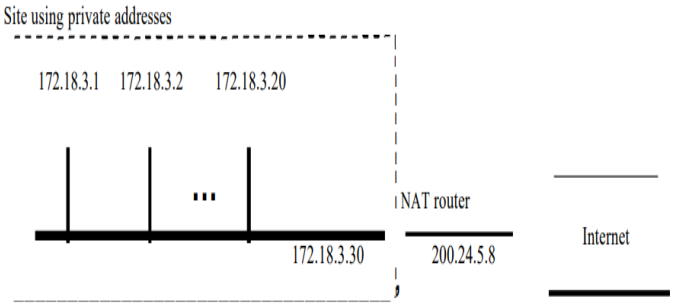
Topic 7: NAT, ARP & PAT

The number of home users and small businesses that want to use the Internet is ever increasing. In the beginning, a user was connected to the Internet with a dial-up line, which means that she was connected for a specific period of time. An ISP with a block of addresses could dynamically assign an address to this user. An address was given to a user when it was needed. But the situation is different today. Home users and small businesses can be connected by an ADSL line or cable modem. In addition, many are not happy with one address; many have created small networks with several hosts and need an IP address for each host. With the shortage of addresses, this is a serious problem.
A quick solution to this problem is called network address translation (NAT). NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally. The traffic inside can use the large set; the traffic outside, the small set.
To separate the addresses used inside the home or business and the ones used for the Internet, the Internet authorities have reserved three sets of addresses as private addresses, shown in Table 19.3.

Table Addresses for private networks

Range			**Total**
10.0.0.0	to	10.255.255.255	224
172.16.0.0	to	172.31.255.255	220
192.168.0.0	to	192.168.255.255	216

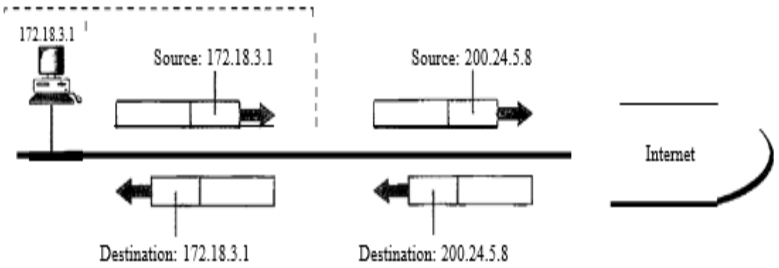
Any organization can use an address out of this set without permission from the Internet authorities. Everyone knows that these reserved addresses are for private net• works. They are unique inside the organization, but they are not unique globally. No router will forward a packet that has one of these addresses as the destination address.
The site must have only one single connection to the global Internet through a router that runs the NAT software. Below figure shows a simple implementation of NAT.
Below figure shows, the private network uses private addresses. The router that connects the network to the global address uses one private address and one global address. The private network is transparent to the rest of the Internet; the rest of the Internet sees only the NAT router with the address 200.24.5.8.
A NAT implementation



Address Translation

All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address. All incoming packets also pass through the NAT router, which replaces the destination address in the packet (the NAT router global address) with the appropriate private address. Figure below shows an example of address translation.

Addresses in a NAT

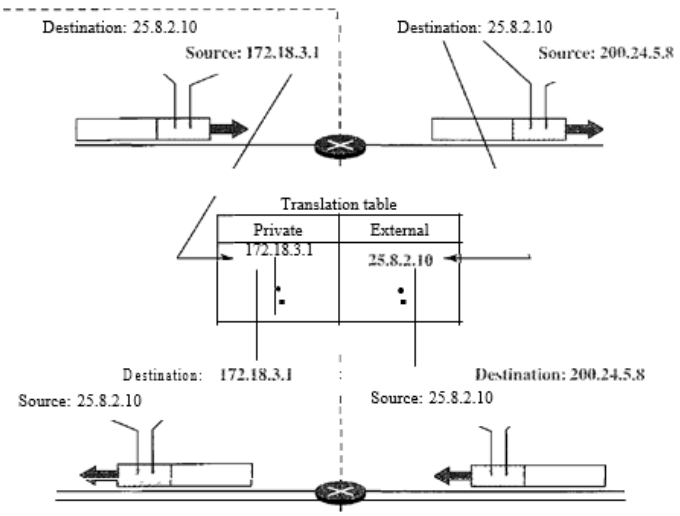


Translation Table

The reader may have noticed that translating the source addresses for outgoing packets is straightforward. But how does the NAT router know the destination address for a packet coming from the Internet? There may be tens or hundreds of private IP addresses, each belonging to one specific host. The problem is solved if the NAT router has a translation table.

Using One IP Address In its simplest form, a translation table has only two columns: the private' address and the external address (destination address of the packet). When the router translates the source address of the outgoing packet, it also makes note of the destination address-where the packet is going. When the response comes back from the destination, the router uses the source address of the packet (as the external address) to find the private address of the packet. Figure below shows the idea. Note that the addresses that are changed (translated) are shown in color.

NAT address translation



In this strategy, communication must always be initiated by the private network. The NAT mechanism described requires that the private network start the communication. As we will see, NAT is used mostly by ISPs which assign one single address to a customer. The customer, however, may be a member of a private network that has many private addresses. In this case, communication with the Internet is always initiated from the customer site, using a client program such as HTTP, TELNET, or FTP to access the corresponding server program. For example, when e-mail that originates from a non-customer site is received by the ISP e-mail server, the e-mail is stored in the mailbox of the. customer until retrieved. A private network cannot run a server program for clients outside of its network if it is using NAT technology.

Using a Pool of IP Addresses Since the NAT router has only one global address, only one private network host can access the same external host. To remove this restriction, the NAT router uses a pool of global addresses. For example, instead of using only one global address (200.24.5.8), the NAT router can use four addresses (200.24.5.8, 200.24.5.9, 200.24.5.10, and 200.24.5.11). In this case, four private network hosts can communicate with the same external host at the same time because each pair of addresses defines a connection. However, there are still some drawbacks. In this example, no more than four connections can be made to the same destination. Also, no private-network host can access two external server programs (e.g., HTTP and FTP) at the same time.

Using Both IP Addresses and Port Numbers To allow a many-to-many relationship between private-network hosts and external server programs, we need more information in the translation table. For example, suppose two hosts with addresses 172.18.3.1 and 172.18.3.2 inside a private network need to access the HTTP server on external host 25.8.3.2. If the translation table has five columns, instead of two, that include the source and destination port numbers of the transport layer protocol, the ambiguity is eliminated. Table below shows an example of such a table.

Five-column translation table

Private Address	**Private Port**	**External Address**	**External Port**	**Transport Protocol**
172.18.3.1	1400	25.8.3.2	80	TCP

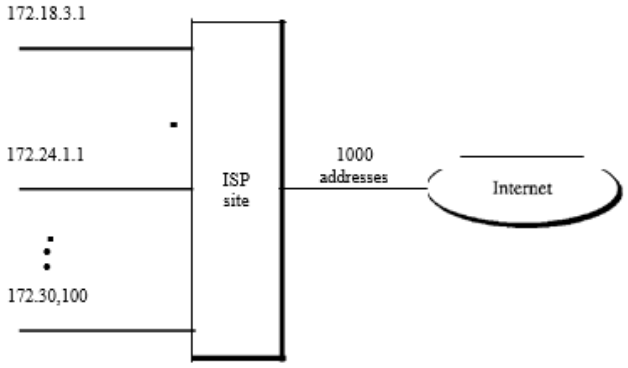
172.18.3.2	1401	25.8.3.2	80	TCP
.. .	.. .	. ..	.. .	...

Note that when the response from HTTP comes back, the combination of source address (25.8.3.2) and destination port number (1400) defines the-private network host to which the response should be directed. Note also that for this translation to work, the temporary port numbers (1400 and 1401) must be unique.

NAT and ISP

An ISP that serves dial-up customers can use NAT technology to conserve addresses. For example, suppose an ISP is granted 1000 addresses, but has 100,000 customers. Each of the customers is assigned a private network address. The ISP translates each of the 100,000 source addresses in outgoing packets to one of the 1000 global addresses; it translates the global destination address in incoming packets to the corresponding private address. Figure 19.13 shows this concept.

An ISP and NAT



ADDRESS MAPPING

An internet is made of a combination of physical networks connected by internetworking devices such as routers. A packet starting from a source host may pass through several different physical networks before finally reaching the destination host. The hosts and routers are recognized at the network level by their logical (IP) addresses.

However, packets pass through physical networks to reach these hosts and routers. At the physical level, the hosts and routers are recognized by their physical addresses.

A physical address is a local address. Its jurisdiction is a local network. It must be unique locally, but is not necessarily unique universally. It is called a physical address because it is usually (but not always) implemented in hardware. An example of a physical address is the 48-bit MAC address in the Ethernet protocol, which is imprinted on the NIC installed in the host or router.

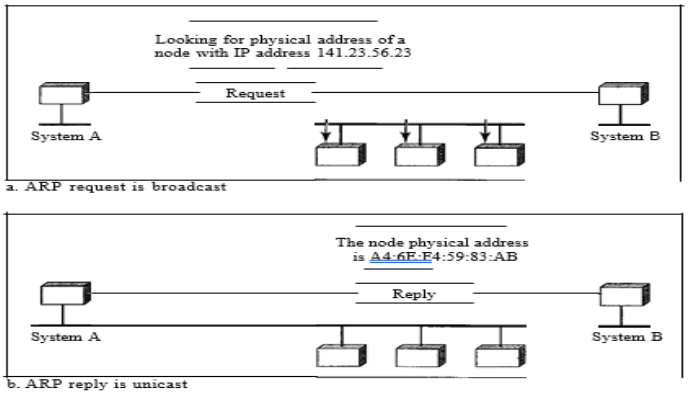
The physical address and the logical address are two different identifiers. We need both because a physical network such as Ethernet can have two different protocols at the network layer such as IP and IPX (Novell) at the same time. Likewise, a packet at a network layer such as IP may pass through different physical networks such as Ethernet and LocalTalk (Apple). This means that delivery of a packet to a host or a router requires two levels of addressing: logical and physical. We need to be able to map a logical address to its corresponding physical address and vice versa. These can be done by using either static or dynamic mapping. Static mapping involves in the creation of a table that associates a logical address with a physical address. This table is stored in each machine on the network. Each machine that

knows, for example, the IP address of another machine but not its physical address can look it up in the table. This has some limitations because physical addresses may change in the following ways:
A machine could change its NIC, resulting in a new physical address.
In some LANs, such as LocalTalk, the physical address changes every time the computer is turned on.
A mobile computer can move from one physical network to another, resulting in a change in its physical address
To implement these changes, a static mapping table must be updated periodically. This overhead could affect network performance
In dynamic mapping each time a machine knows one of the two addresses (logical or physical), it can use a protocol to find the other one.

Mapping Logical to Physical Address: ARP

Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver. The logical (IP) address is obtained from the DNS (see Chapter 25) if the sender is the host or it is found in a routing table (see Chapter 22) if the sender is a router. But the IP datagram must be encapsulated in a frame to be able to pass through the physical network. This means that the sender needs the physical address of the receiver. The host or the router sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network
Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and physical addresses. The packet is unicast directly to the inquirer by using the physical address received in the query packet.

ARP operation



In Figure (a) above, the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address 141.23.56.23. System A needs to pass the packet to its data link layer for the actual delivery, but it does not know the physical address of the recipient. It uses the services of ARP by asking the ARP protocol to send a broad• cast ARP request packet to ask for the physical address of a system with an IF address of 141.23.56.23. This packet is received by every system on the physical network, but only system B will answer it, as shown in Figure (b) above. System B sends an ARP reply packet that includes its physical address. Now system A can send all the packets it has for this destination by using the physical address it received.

Cache Memory

Using ARP is inefficient if system A needs to broadcast an ARP request for each IP packet it needs to send to system B. It could have broadcast the IP packet itself. ARP can be useful if

the ARP reply is cached (kept in cache memory for a while) because a system normally sends several packets to the same destination. A system that receives an ARP reply stores the mapping in the cache memory and keeps it for 20 to 30 minutes unless the space in the cache is exhausted. Before sending an ARP request, the system first checks its cache to see if it can find the mapping.

RARP

Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine. To create an IP datagram, a host or a router needs to know its own IP address or addresses. The IP address of a machine is usually read from its configuration file stored on a disk file.

However, a diskless machine is usually booted from ROM, which has minimum booting information. The ROM is installed by the manufacturer. It cannot include the IP address because the IP addresses on a network are assigned by the network administrator.

The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol. A RARP request is created and broadcast on the local network. Another machine on the local network that knows all the IP addresses will respond with a RARP reply. The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program.

There is a serious problem with RARP: Broadcasting is done at the data link layer. The physical broadcast address, allis in the case of Ethernet, does not pass the boundaries of a network. This means that if an administrator has several networks or several subnets, it needs to assign a RARP server for each network or subnet. This is the reason that RARP is almost obsolete. Two protocols, BOOTP and DHCP, are replacing RARP.

PORT ADDRESS TRANSLATION:

Port Address Translation (PAT), also known as Network Address Port Translation (NAPT), is a technique used in computer networking to map multiple private IP addresses to a single public IP address. It is commonly implemented in network address translation (NAT) devices, such as routers or firewalls, to conserve IPv4 addresses and enable multiple devices on a private network to access the internet using a single public IP address. Here are some key points about PAT:

Purpose: PAT allows multiple devices with private IP addresses to share a single public IP address when communicating with external networks, such as the internet

Port Mapping: In addition to translating IP addresses, PAT also translates the transport layer port numbers. Each outgoing connection from a device on the private network is assigned a unique port number, which is then mapped to the public IP address of the NAT device.

Port Multiplexing: PAT leverages port multiplexing to establish multiple concurrent connections using the same public IP address. By assigning different port numbers for each connection, the NAT device can differentiate between incoming packets and route them to the appropriate internal device.

Port Range: PAT typically uses a range of port numbers for translation. For example, a router may reserve a range of ports (e.g., 1024-65535) for PAT translations. As outgoing connections are established, the router dynamically assigns a port number from this range to each connection.

Session Tracking: The NAT device maintains a session table that tracks the translations between private IP addresses and port numbers and their corresponding public IP address and

port numbers. This table allows the device to correctly forward incoming packets to the appropriate internal device.
Overcoming IP Address Limitations: PAT helps overcome the limited availability of public IPv4 addresses by allowing multiple devices to share a single public IP address. It enables many devices within a private network to access the internet using a single public IP, facilitating efficient use of IPv4 address space.
Security Implications: PAT provides a level of security by hiding the internal IP addresses from external networks. It acts as a form of firewall by not exposing the private IP addresses directly to the internet, making it harder for external entities to target specific devices on the private network.
It's worth noting that with the increasing adoption of IPv6, which has a significantly larger address space, the need for PAT is reduced. However, PAT remains relevant in IPv4 networks where conservation of public IP addresses is necessary.
Port address translation (PAT), also known as NAT overloading, is a technique that allows multiple devices on a private network to share a single public IP address. PAT works by translating the source port of a packet when it is sent from the private network to the public network. This allows the destination device to distinguish between packets from different devices on the private network
PAT is commonly used in home and small business networks where there are more devices than there are public IP addresses available. For example, a home network with a single public IP address might have a dozen or more devices connected to it, including computers, smartphones, tablets, and gaming consoles. Without PAT, each device would need its own public IP address, which would be both expensive and impractical
PAT works by using a single public IP address and a range of source ports. When a device on the private network sends a packet to the public network, the PAT device translates the source port of the packet to a number within the range of source ports. The destination device then uses the translated source port to send a response packet back to the private network
The range of source ports that can be used for PAT is typically 1024 to 65535. This range is large enough to support a large number of devices on a private network
PAT is a useful technique that can be used to conserve public IP addresses and simplify network configuration. However, it is important to note that PAT can also introduce some security risks. For example, if a device on the private network is compromised, an attacker might be able to use PAT to access other devices on the network.
To mitigate these risks, it is important to implement strong security measures on all devices on the private network, including firewalls, antivirus software, and strong passwords.

Here are some of the benefits of using PAT:
Conserves public IP addresses: PAT can be used to conserve public IP addresses by allowing multiple devices on a private network to share a single public IP address.
Simplify network configuration: PAT can simplify network configuration by allowing devices on a private network to be accessed using a single public IP address.
Improve performance: PAT can improve performance by reducing the number of packets that need to be sent to the Internet.
Here are some of the challenges of using PAT:
Security risks: PAT can introduce some security risks, such as the possibility of an attacker gaining access to other devices on the private network.
Complexity: PAT can be complex to configure and manage, especially for large networks.
Performance: PAT can reduce the performance of the network, especially for networks with a high volume of traffic.

SAQ's-Self Assessment Questions

1. Which of the following is not a purpose of NAT?
   a. Enable private IP address usage
   b. Provide security for the network
   c. Facilitate communication between different networks
   d. Translate domain names to IP addresses
Answer: d

2. Which device is commonly used to perform NAT?
   a. Hub
   b. Switch
   c. Router
   d. Firewall
Answer: c

3. ARP is used to resolve which type of address?
   a. MAC address to IP address
   b. IP address to MAC address
   c. IP address to domain name
   d. Domain name to IP address
Answer: b

4. RARP is used to resolve which type of address?
   a. MAC address to IP address
   b. IP address to MAC address
   c. IP address to domain name
   d. Domain name to IP address
Answer: a
5. Which layer of the OSI model does NAT operate on?
   a. Physical layer
   b. Network layer
   c. Transport layer
   d. Application layer
Answer: b

6. Which of the following is a limitation of NAT?
   a. Increased network security
   b. Simultaneous use of multiple public IP addresses
   c. Complex configuration and management
   d. Transparent communication between networks
Answer: c

7. PAT (Port Address Translation) is primarily used to conserve which type of addresses?
   a. MAC addresses
   b. Private IP addresses
   c. Public IP addresses
   d. Domain names
Answer: c

8. Which of the following is true about PAT?
   a. Each device gets its own public IP address
   b. Multiple devices share a single public IP address
   c. PAT is only used for outbound connections
   d. PAT does not involve port mapping
Answer: b

9. Which protocol is responsible for dynamically assigning IP addresses in a network?
   a. ARP
   b. RARP
   c. DHCP
   d. NAT
Answer: c

10. Which of the following is not a benefit of NAT?
   a. Increased network scalability
   b. Improved network security
   c. Conservation of public IP addresses
   d. Simplified network management
Answer: a

11.The _____ protocol is the transmission mechanism used by the TCP/IP suite?
   a. ARP
   b. IP
   c. RARP
   d. None of the above
Answer: b

12. What connects IP address to the physical address of devices?
   a. ARP
   b. FTP
   c. UDP
   d. TCP
Answer: a

13. _____ translates address consisting 32 bits into 48 and vice-versa?
   a. ARP
   b. FTP
   c. UDP
   d. TCP
Answer: a

14. What is the necessity of Address Resolution protocol?
   a. Translate address bits
   b. Finds MAC address
   c. Matches IP address to MAC address
   d. All of the above
Answer: d

15. ARP cache is_____?
   a. static
   b. dynamic
   c. constant
   d. fixed
Answer: b

16. How long is the IP address?
   a. 32
   b. 48
   c. 64
   d. 128
Answer: a

17. without _____ , it is impossible to detect MAC address of other hosts ?
   a. ARP
   b. FTP
   c. UDP
   d. TCP
Answer: a

18. _____ creates entries of addresses on fly?
   a. FTP
   b. ARP
   c. UDP
   d. TCP
Answer: b

19. If _____ goes unsupported, entries in the directory made manually?
   a. FTP
   b. ARP
   c. UDP
   d. TCP
Answer: b

20. ARP requests get ignored in what field?
   a. Hardware type
   b. Target Hardware address
   c. Hardware length
   d. Protocol length
Answer: b

Terminal Questions

1) What is the purpose of NAT?
2) How does NAT conserve IP addresses?
3) Explain the process of address translation in NAT.
4) What is the role of ARP in a local network?
5) How does ARP resolve IP addresses to MAC addresses?
6) What happens if an ARP request does not receive a response?

7) What is the purpose of RARP?

Topic 8: Access Control List

Access-list (ACL)
Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.
ACL features –
The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd, and so on.
The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
There is an implicit denial at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

ACCESS CONTROL LIST
Once the access-list is built, then it should be applied to inbound or outbound of the interface:
Inbound access lists –
When an access list is applied on inbound packets of the interface then first the packets will be processed according to the access list and then routed to the outbound interface.
Outbound access lists –
When an access list is applied on outbound packets of the interface then first the packet will be routed and then processed at the outbound interface.

Guidelines for creating and implementing access list

There are some general access-list guidelines that you should keep in mind when creating and implementing access lists on a router:

You can assign only one access list per interface per protocol per direction. This means that when applying IP access lists, you can have only one inbound access list and one outbound access list per interface.

Organize your access lists so that the more specific tests are at the top.

Anytime a new entry is added to the access list, it will be placed at the bottom of the list, which is why I highly recommend using a text editor for access lists.

You can't remove one line from an access list. If you try to do this, you will remove the entire list. This is why it's best to copy the access list to a text editor before trying to edit the list. The only exception is when you're using named access lists.

Unless your access list ends with a permit any command, all packets will be discarded if they do

not meet any of the list's tests. This means every list should have at least one permit statement or it will deny all traffic.

Create access lists and then apply them to an interface. Any access list applied to an interface without access-list test statements present will not filter traffic.

Access lists are designed to filter traffic going through the router. They will not filter traffic that has originated from the router.

Place IP standard access lists as close to the destination as possible. This is the reason we don't really want to use standard access lists in our networks. You can't put a standard access list close to the source host or network because you can only filter based on source address and all destinations would be affected as a result.

Place IP extended access lists as close to the source as possible. Since extended access lists can filter on very specific addresses and protocols, you don't want your traffic to traverse the entire network just to be denied. By placing this list as close to the source address as possible, you can filter traffic before it uses up precious bandwidth.

Types of ACL –

There are two main different types of Access-list namely:

Standard Access-list –

These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.

Extended Access-list –

These are the ACL that uses source IP, Destination IP, source port, and Destination port. These types of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

Wildcard Masking

Wildcards are used with access lists to specify an individual host, a network, or a specific range of a network or networks.

The block sizes used to specify a range of addresses are key to understanding wildcards. Different block sizes available are 64, 32, 16, 8, and 4. When you need to specify a range of addresses, you choose the next-largest block size for your needs. So if you need to specify 34 networks, you need a block size of 64. If you want to specify 18 hosts, you need a block size of 32. If you specify only 2 networks, then go with a block size of 4.

Wildcards are used with the host or network address to tell the router a range of available addresses to filter. To specify a host, the address would look like this:
172.16.30.5 0.0.0.0
The four zeros represent each octet of the address. Whenever a zero is present, it indicates that the octet in the address must match the corresponding reference octet exactly. To specify that an
octet can be any value, use the value 255. Here's an example of how a /24 subnet is specified with
a wildcard mask:
172.16.30.0 0.0.0.255
This tells the router to match up the first three octets exactly, but the fourth octet can be any value.
You can only specify the exact amount that the block size value allows. This means that the range would have to be either 16 or 32, but not 20. Let's take that we want to block access to the part of the network that ranges from 172.16.8.0 through 172.16.15.0. To do that, you would go with a block size of 8, the network number would be 172.16.8.0, and the wildcard would be 0.0.7.255. The 7.255 equals the value the router will use to determine the block size. So together, the network number and the wildcard tell the router to begin at 172.16.8.0 and go up a block size of eight addresses to network 172.16.15.0.

Also, there are two categories of access-list:
Numbered access-list – These are the access list that cannot be deleted specifically once created i.e if we want to remove any rule from an Access-list then this is not permitted in the case of the numbered access list. If we try to delete a rule from the access list then the whole access list will be deleted. The numbered access-list can be used with both standard and extended access lists.

Named access list – In this type of access list, a name is assigned to identify an access list. It is allowed to delete a named access list, unlike numbered access list. Like numbered access lists, these can be used with both standards and extended access lists.

1. What is the main purpose of an Access Control List (ACL)?
a) To control access to network devices
b) To filter network traffic based on defined criteria
c) To secure wireless network connections
d) To manage IP addresses in a DHCP server

2. In networking, where are Access Control Lists commonly used?
a) Routers
b) Switches
c) Firewalls
d) All of the above

3. What is the basic unit used in an ACL to define traffic filtering rules?
a) Rules
b) Entries
c) Statements
d) Conditions

4. Which of the following is true regarding the order of ACL entries?

a) Entries are processed in a top-down order.
b) Entries are processed randomly.
c) Entries are processed simultaneously.
d) Entries are processed in a bottom-up order.

5. Which type of ACL allows both source and destination IP addresses to be matched in a single statement?
a) Standard ACL
b) Extended ACL
c) Named ACL
d) Reflexive ACL

6. Which type of ACL is based on the source IP address only?
a) Standard ACL
b) Extended ACL
c) Named ACL
d) Reflexive ACL

7. Which of the following is true regarding wildcard masks in ACLs?
a) Wildcard masks are used to specify the range of port numbers.
b) Wildcard masks are used to define the network portion of an IP address.
c) Wildcard masks are used to specify the size of the subnet mask.
d) Wildcard masks are used to perform bitwise matching in an ACL.

8. How can an ACL be applied to a specific interface on a router?
a) Using inbound or outbound direction
b) Using VLAN tagging
c) Using a specific IP address range
d) Using a DHCP server lease

9. Which of the following actions can be performed on a packet matched by an ACL entry?
a) Permit
b) Deny
c) Both permit and deny
d) Modify

10. Which protocol is commonly used for managing ACLs in a network?
a) ICMP
b) SNMP
c) FTP
d) ARP

In applying an ACL to a router interface, which traffic is designated as outbound?
traffic that is coming from the source IP address into the router
traffic that is going from the destination IP address into the router
traffic that is leaving the router and going toward the destination host
traffic for which the router can find no routing table entry

What is the quickest way to remove a single ACE from a named ACL?
Use the no access-list command to remove the entire ACL, then recreate it without the ACE.
Copy the ACL into a text editor, remove the ACE, then copy the ACL back into the router.

Use the no keyword and the sequence number of the ACE to be removed.
Create a new ACL with a different number and apply the new ACL to the router interface.
Which ICMP message type should be stopped inbound?
echo-reply
echo
source quench
unreachable
Which two statements describe appropriate general guidelines for configuring and applying ACLs? (Choose two.)
Standard ACLS are placed closest to the source, whereas extended ACLS are placed closest to the destination.
If an ACL contains no permit statements, all traffic is denied by default.
The most specific ACL statements should be entered first because of the top-down sequential nature of ACLs.
If a single ACL is to be applied to multiple interfaces, it must be configured with a unique number for each interface.
Multiple ACLS per protocol and per direction can be applied to an interface.
What wild card mask will match networks 172.16.0.0 through 172.19.0.0?
0.0.3.255
0.252.255.255
0.3.255.255
0.0.255.255
What method is used to apply an IPv6 ACL to a router interface?
the use of the access-class command
the use of the ipv6 traffic-filter command
the use of the ip access-group command
the use of the ipv6 access-list command

What type of ACL offers greater flexibility and control over network access?
named standard
numbered standard
flexible
extended

Which operator is used in an ACL statement to match packets of a specific application?
established
gt
lt
eq

Which two keywords can be used in an access control list to replace a wildcard mask or address and wildcard mask pair? (Choose two.)
some
any
gt
most
all
host
What single access list statement matches all of the following networks?
192.168.16.0

192.168.17.0
192.168.18.0
192.168.19.0
access-list 10 permit 192.168.16.0 0.0.0.255
access-list 10 permit 192.168.16.0 0.0.15.255
access-list 10 permit 192.168.0.0 0.0.15.255
access-list 10 permit 192.168.16.0 0.0.3.255

Answer Keys:
b
d
a
a
b
a
d
a
c
b
c
c
b
b,c
c
b
d
d
b,f
d

Summary
Access Control Lists (ACLs) are an integral part of security frameworks and play a vital role in managing access to resources. They enable administrators to define granular permissions and restrictions for users, groups, or network entities, ensuring that only authorized actions are allowed while protecting against unauthorized access or misuse.

Topic 9: DHCP, IP TUNNNELING

Dynamic Host Configuration Protocol (DHCP)
DHCP is a network protocol used to dynamically assign IP addresses and provide configuration information to devices on a network. It automates the process of IP address allocation and simplifies network administration.

Components of DHCP
DHCP Server:
The DHCP server is a network device or software that is responsible for assigning IP addresses and configuring network parameters to DHCP clients. It maintains a pool of available IP addresses that can be assigned to clients. The server responds to DHCP client requests by offering IP addresses and other configuration parameters.

DHCP Client:
The DHCP client is a network device or software that requests and receives IP address configuration information from the DHCP server. When a client connects to a network, it sends a DHCP Discover message to discover available DHCP servers and request IP address

assignment. The client receives DHCP Offer, Request, and Acknowledge messages from the server during the IP address acquisition process.

DHCP Messages:

DHCP messages are used for communication between DHCP clients and servers. DHCP messages include DHCP Discover, DHCP Offer, DHCP Request, DHCP Acknowledge, and DHCP Release messages. These messages carry information about IP address assignment, lease renewal, and configuration parameters.

DHCP Lease:

A DHCP lease is a time-limited assignment of an IP address to a client. When a DHCP server assigns an IP address to a client, it also specifies a lease duration. The client can use the IP address for the lease duration, and before the lease expires, it can request a lease renewal from the server.

IP Address Pool:

The IP address pool is a range of available IP addresses that the DHCP server can assign to clients. The DHCP server maintains this pool and ensures that IP addresses are not assigned to multiple clients simultaneously.

DHCP Relay Agent:

The DHCP relay agent is a network device or software that forwards DHCP messages between DHCP clients and servers when they are on different network segments. It listens for DHCP Discover messages sent by clients, encapsulates them, and forwards them to DHCP servers. The relay agent also relays DHCP Offer, Request, and Acknowledge messages back to the client.

DHCP Configuration Parameters:

In addition to IP addresses, DHCP can provide various configuration parameters to clients. These parameters include subnet mask, default gateway, DNS server addresses, NTP server addresses, and other network settings. The DHCP server includes these parameters in the DHCP Offer message, and the client uses them to configure its network connection.

DHCP Reservation:

DHCP reservation is a mechanism that allows the DHCP server to assign a specific IP address to a client based on its MAC address. The DHCP server maintains a list of reserved IP addresses and their corresponding MAC addresses, ensuring that specific devices receive the same IP address each time they connect to the network.

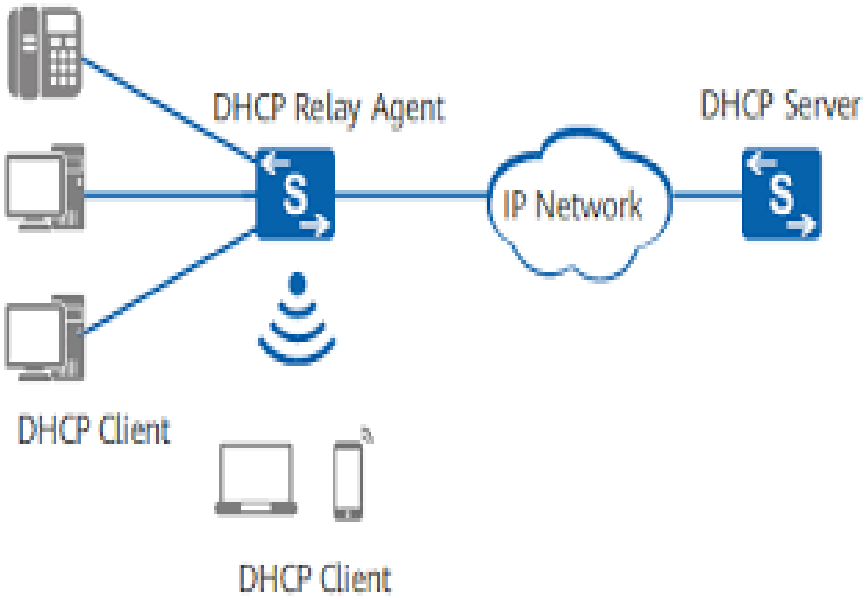


Figure 18.1 Components of DHCP

Working of DHCP

DHCP works on the Application layer of the TCP/IP Protocol. The main task of DHCP is to dynamically assigns IP Addresses to the Clients and allocate information on TCP/IP configuration to Clients. The DHCP port number for the server is 67 and for the client is 68. It is a client-server protocol that uses UDP services. An IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called the DORA process, but there are 8 DHCP messages in the process.

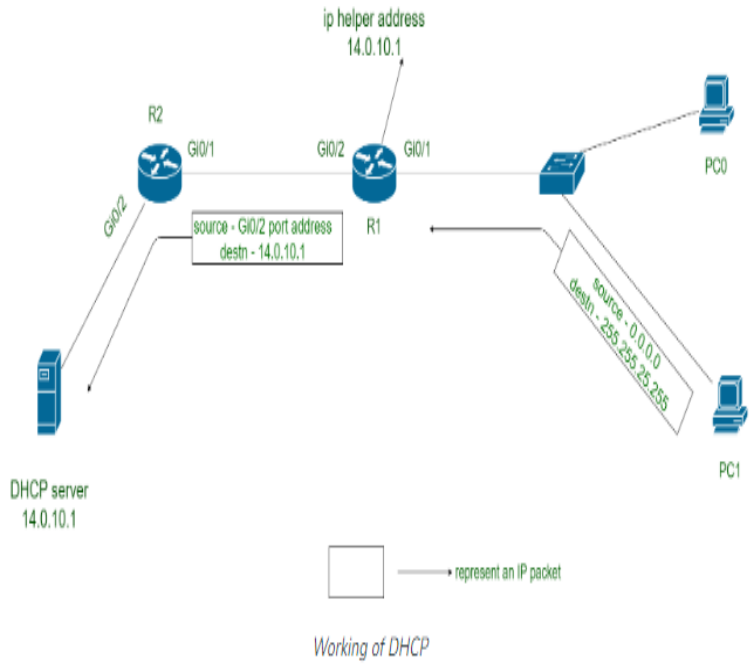


Figure 18.2 Working of DHCP

DHCP Discover (Client to Server):
The DHCP Discover message is sent by a DHCP client to discover available DHCP servers on the network. The client broadcasts this message to the local network using the destination IP address of 255.255.255.255 and the MAC address set as the source. The message includes options like the client's hardware (MAC) address, the DHCP message type (set to Discover), and optionally, any specific configuration options the client is requesting. DHCP servers receive this message and respond with DHCP Offer messages.

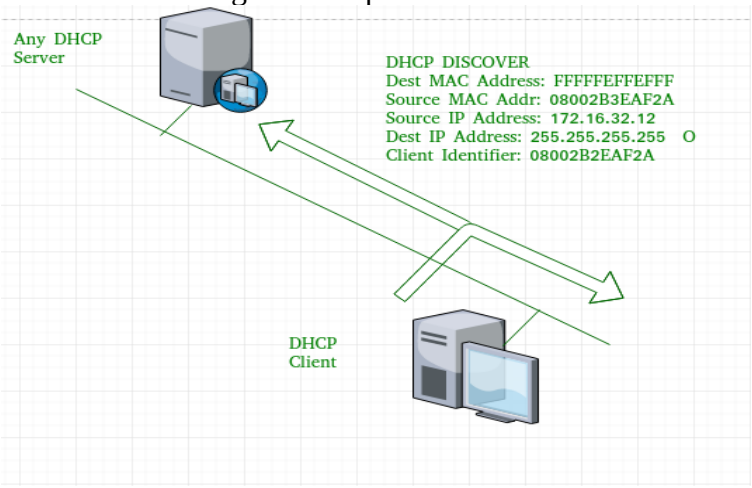


Figure 18.3 DHCP Discover Message

DHCP Offer (Server to Client):
When a DHCP server receives a DHCP Discover message, it responds with a DHCP Offer message. The DHCP Offer message is sent by the server as a unicast message to the client's IP address (or broadcast if the client's IP address is not yet known). The message includes options like the offered IP address, lease duration, subnet mask, default gateway, DNS server addresses, and any other requested configuration options. The server may include multiple IP addresses in the DHCP Offer if it has a range of available addresses. The client receives multiple DHCP Offer messages from different servers (if available) and selects one offer to accept.

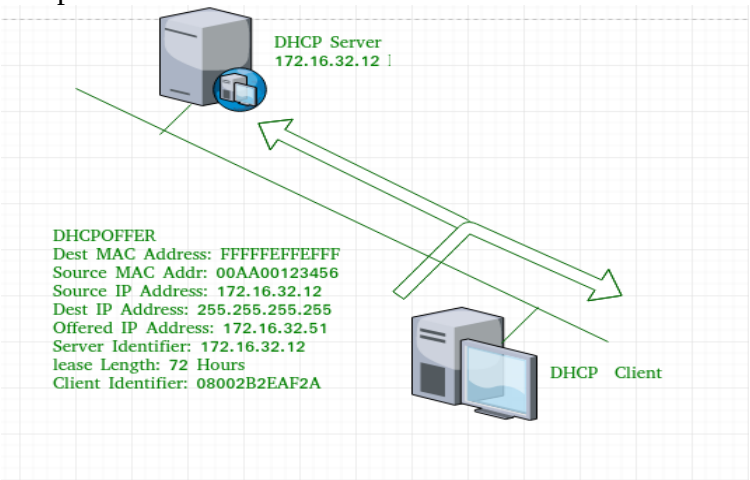


Figure 18.4 DHCP Offer Message

DHCP Request (Client to Server):
Upon receiving one or more DHCP Offer messages, the client selects an IP address lease and sends a DHCP Request message. The DHCP Request message is sent by the client as a

unicast message to the DHCP server that made the selected offer. The message includes options like the requested IP address (typically the one offered by the chosen server), DHCP message type (set to Request), and optionally, any requested configuration options. This message informs the server that the client has accepted the offered IP address and requests the server to confirm the lease.

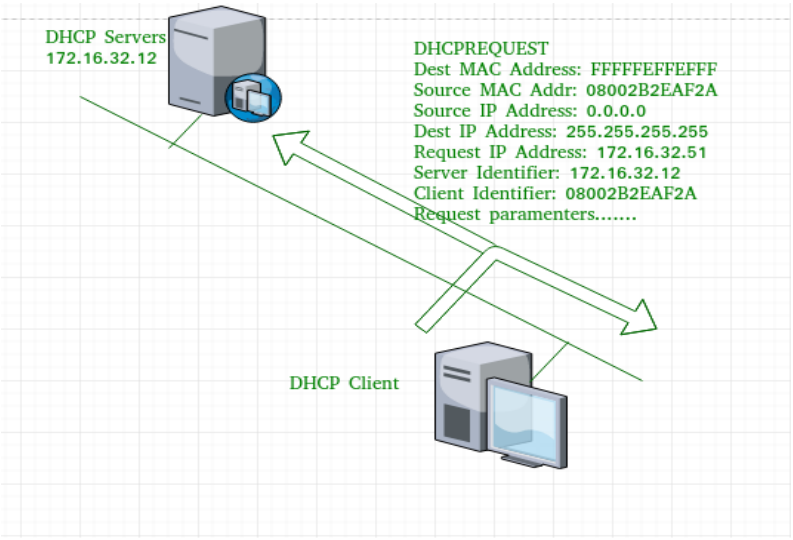


Figure 18.5 DHCP Request Message

DHCP Acknowledge (Server to Client):

In response to the DHCP Request message, the DHCP server sends a DHCP Acknowledge message to the client. The DHCP Acknowledge message is sent as a unicast message from the server to the client's IP address. The message includes options like the assigned IP address, lease duration, subnet mask, default gateway, DNS server addresses, and any other configuration options.

It confirms the IP address lease to the client and provides all necessary configuration information. Upon receiving this message, the client completes the IP address configuration process and starts using the assigned IP address.

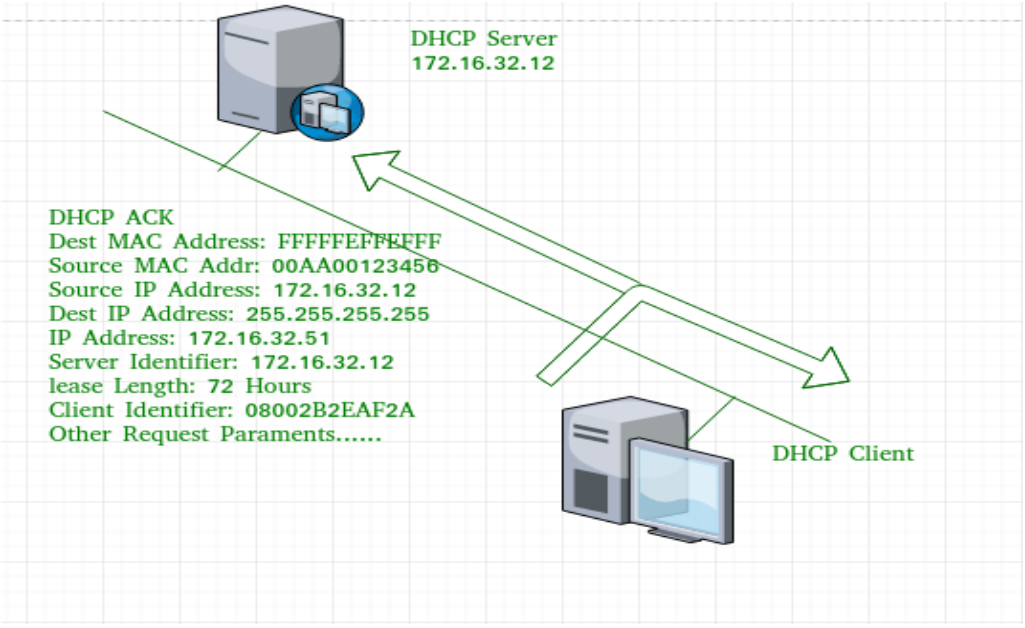


Figure 18.6 DHCP Acknowledgement Message

DHCP negative acknowledgment message:

Whenever a DHCP server receives a request for an IP address that is invalid according to the scopes that are configured, it sends a DHCP Nak message to the client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to the client.

DHCP decline:

If the DHCP client determines the offered configuration parameters are different or invalid, it sends a DHCP decline message to the server. When there is a reply to the gratuitous ARP by any host to the client, the client sends a DHCP decline message to the server showing the offered IP address is already in use

DHCP Release (Client to Server):

A DHCP client can send a DHCP Release message to the DHCP server when it no longer needs the assigned IP address. The DHCP Release message is sent as a unicast message from the client to the DHCP server's IP address. This message notifies the server that the IP address lease can be reclaimed and made available for other clients. It is typically sent by the client when disconnecting from the network or shutting down.

DHCP inform:

If a client address has obtained an IP address manually then the client uses DHCP information to obtain other local configuration parameters, such as domain name. In reply to the DHCP inform message, the DHCP server generates a DHCP ack message with a local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

IP Tunneling

IP tunneling is a technique used in computer networking to encapsulate or carry IP (Internet Protocol) packets within another IP network. It allows for the transmission of IP traffic over an intermediate network that may not natively support IP. Tunneling is commonly used in situations where there is a need to connect two networks that are physically separated or have incompatible network protocols.

Here's a high-level overview of how IP tunneling works:

Encapsulation: In IP tunneling, the original IP packet is encapsulated within a new IP packet, effectively creating a "tunnel" for the packet to traverse across the intermediate network. The original packet becomes the payload of the new packet.

Tunneling Protocol: A tunneling protocol defines the format and rules for encapsulating and decapsulating the packets. Some commonly used tunneling protocols include Generic Routing Encapsulation (GRE), IP in IP (IPIP), Layer 2 Tunneling Protocol (L2TP), and IPsec (Internet Protocol Security).

Tunnel Endpoints: To establish a tunnel, two endpoints are required: the tunnel source and the tunnel destination. The tunnel source is typically a device at the edge of the original network, and the tunnel destination is the corresponding device at the other end of the tunnel.

Intermediate Network: The encapsulated packets are then transmitted over the intermediate network, which could be a public network such as the Internet or a private network.

Decapsulation: At the tunnel destination, the encapsulated packets are received and then decapsulated to extract the original IP packets. The decapsulated packets can then be delivered to their final destination within the destination network.

IP tunneling can be used for various purposes, including:

Virtual Private Networks (VPNs): VPNs use IP tunneling to create secure, encrypted connections over public networks, allowing remote users to access private networks securely.

IPv6 Transition: IP tunneling can be used to transmit IPv6 packets over an IPv4 network, enabling the coexistence of both IP versions during the transition period.

Network Extension: Tunneling allows for the extension of a network over a different network infrastructure, enabling connectivity between geographically dispersed locations.
Traffic Engineering: Tunneling can be used for traffic engineering purposes, allowing network operators to direct traffic through specific paths to optimize performance or implement specific policies.

8. Activities/ Case studies/related to the session: NA
DHCP Server Configuration Description: In this activity, participants will configure a DHCP server to automatically assign IP addresses to client devices on a network. They will set up IP address ranges, lease durations, and DHCP options. Participants will also troubleshoot common DHCP configuration issues, such as IP address conflicts and misconfigurations.
Case Study: IP Tunneling for IPv6 Transition Description: This case study focuses on the implementation of IP tunneling to facilitate the transition from IPv4 to IPv6. Participants will configure an IPv6 tunnel between two networks, enabling communication between IPv6-enabled devices over an IPv4 infrastructure. They will address challenges such as tunneling protocols, encapsulation, and routing.

9. Examples & contemporary extracts of articles/ practices to convey the idea of the session
DHCP Example: Let's say you have a network with a DHCP server and multiple client devices. When a new client device connects to the network, it sends a DHCP Discover message to discover available DHCP servers. The DHCP server receives the message and responds with a DHCP Offer, offering an IP address, subnet mask, default gateway, DNS server, and other configuration parameters. The client device then sends a DHCP Request to accept the offer, and the server sends a DHCP Acknowledgment to confirm the assignment of the IP address. The client device can now use the assigned IP address to communicate on the network.
IP Tunneling Example: Imagine you have two remote networks, Network A and Network B, separated by the internet. To establish communication between these networks, you can create an IP tunnel. Let's say you decide to use IPsec tunneling for secure transmission. You configure IPsec policies on the routers at each network, specifying the encryption and authentication algorithms. The routers encapsulate the original IP packets with IPsec headers and encrypt the data. The encrypted packets are then sent over the internet, and upon reaching the destination router, the IPsec headers are removed, and the original packets are forwarded to the appropriate network. This allows devices in Network A and Network B to communicate securely over the IP tunnel.

10. Self Assessment Questions
1. Which of the following best describes the role of a DHCP server?
a) Assigning static IP addresses to client devices
b) Providing DNS lookup services
c) Dynamically assigning IP addresses to client devices
d) Configuring firewalls and security settings
Answer: c) Dynamically assigning IP addresses to client devices
2. What is the purpose of the DHCP Offer message in the DHCP process?
a) Confirming the IP address assignment
b) Discovering available DHCP servers
c) Requesting IP configuration parameters
d) Providing a lease duration for the IP address

Answer: b) Discovering available DHCP servers
3. Which DHCP message confirms the acceptance of an IP address offer by a client device?
a) DHCP Discover
b) DHCP Request
c) DHCP Acknowledgment
d) DHCP Release
Answer: c) DHCP Acknowledgment
4. Which DHCP option provides the IP address of the default gateway to client devices?
a) Option 66 b) Option 150 c) Option 82 d) Option 3
Answer: d) Option 3
5. What is the default lease duration for an IP address assigned by DHCP? a) 1 hour b) 6 hours c) 24 hours d) 7 days
Answer: c) 24 hours
6. DHCP stands for _____.
Answer: Dynamic Host Configuration Protocol.
7. The DHCP _____ message is used by a client device to discover available DHCP servers on the network.
Answer: Discover.
8. The DHCP _____ message is sent by a DHCP server to offer an IP address to a client device.
Answer: Offer.
9. The DHCP _____ message is sent by a client device to formally request an offered IP address from a DHCP server.
Answer: Request.
10. The DHCP _____ message is sent by a DHCP server to acknowledge the acceptance of the IP address by a client device.
Answer: Acknowledgment.
11. What is IP tunneling?
a) A technique for transmitting data packets over Wi-Fi networks
b) A method for encapsulating one network protocol within another network protocol
c) A mechanism for routing packets between different VLANs
d) A security protocol used for encrypting network traffic
Answer: b) A method for encapsulating one network protocol within another network protocol
12. Which of the following protocols is commonly used for IP tunneling?
a) IPX/SPX b) SMTP c) GRE d) FTP
Answer: c) GRE (Generic Routing Encapsulation)
13. IP tunneling is often used for which of the following purposes?
a) Encrypting network traffic
b) Enhancing wireless network performance
c) Enabling communication between IPv6 and IPv4 networks
d) Facilitating load balancing in a network
Answer: c) Enabling communication between IPv6 and IPv4 networks
14. What is the purpose of encapsulation in IP tunneling?
a) To encrypt the data packets
b) To compress the data packets
c) To add additional headers to the original packets
d) To route the packets to their destination
Answer: c) To add additional headers to the original packets
15. Which of the following is an example of an IP tunneling protocol used for secure

communication over the internet?
a) L2TP b) ICMP c) SNMP d) POP3
Answer: a) L2TP (Layer 2 Tunneling Protocol)
16. IPsec is commonly used in IP tunneling to provide which of the following?
a) Authentication and encryption
b) Bandwidth optimization
c) Quality of Service (QoS) guarantees
d) Network address translation (NAT)
Answer: a) Authentication and encryption
17. Which of the following is a disadvantage of IP tunneling?
a) Increased network latency
b) Inability to route packets between different VLANs
c) Limited compatibility with legacy network protocols
d) Difficulty in managing network security
Answer: a) Increased network latency
18. P tunneling is a technique used to encapsulate one _____ within another _____.
Answer: network protocol, network protocol.
19. The process of encapsulating the original packets with new headers is known as _____.
Answer: encapsulation.
20. _____ is a commonly used protocol for IP tunneling, allowing the encapsulation of a wide variety of network layer protocols within IP packets.
Answer: GRE (Generic Routing Encapsulation).
21. IP tunneling is often used to enable communication between _____ and _____ networks.
Answer: IPv6, IPv4.
22. In IP tunneling, the encapsulated packets are transmitted through a virtual "tunnel" created by the _____ protocol.
Answer: transport protocol.
23. IPsec (IP Security) is a suite of protocols commonly used for _____ in IP tunneling. Answer: security.
24. IP tunneling can be used to establish secure connections for _____ access over untrusted networks.
Answer: remote.
25. The additional headers added during encapsulation are compatible with the _____ protocol used in the tunnel.
Answer: transport.
26. One disadvantage of IP tunneling is the potential increase in _____ due to the additional encapsulation and decapsulation processes.
Answer: network latency.
27. IP tunneling protocols, such as _____, provide mechanisms for the creation and management of virtual private networks (VPNs).
Answer: L2TP (Layer 2 Tunneling Protocol).

Summary

Overall, DHCP simplifies the management of IP addresses and network configuration by automating the assignment process and ensuring efficient utilization of available addresses within a network. These components work together to enable the dynamic assignment of IP addresses and configuration parameters in computer networks, simplifying network

administration and management. It's important to note that IP tunneling introduces additional overhead due to the encapsulation and decapsulation process, which can impact network performance. Therefore, it's essential to consider the specific requirements and limitations of your network environment when implementing IP tunneling.

Terminal Questions

Summarize Dynamic Host Configuration Protocol.
Demonstrate the working principle of DHCP?
What are the advantages of DHCP?
What is IP tunneling?
What are the common use cases for IP tunneling?
What are some commonly used protocols for IP tunneling?
What is the purpose of the DHCP Discover message in the DHCP process?

Chapter 3: Transport layer, Session Layer, Presentation Layer and Application Layer

Topic 1: Transport Layer Process to Process Delivery

Transport layer process to process delivery is one of the techniques for lANA Ranges. When too many process are present in the network it causes process flow which degrades the performance of the system.

Process to Process Delivery:

The data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called node-to-node delivery. The network layer is responsible for delivery of datagrams between two hosts. This is called host-to-host delivery. Real communication takes place between two processes (application programs). We need process-to-process delivery. The transport layer is responsible for process-to-process delivery-the delivery of a packet, part of a message, from one process to another. Figure 4.1 shows these three types of deliveries and their domains

The transport layer is responsible for process-to-process delivery.

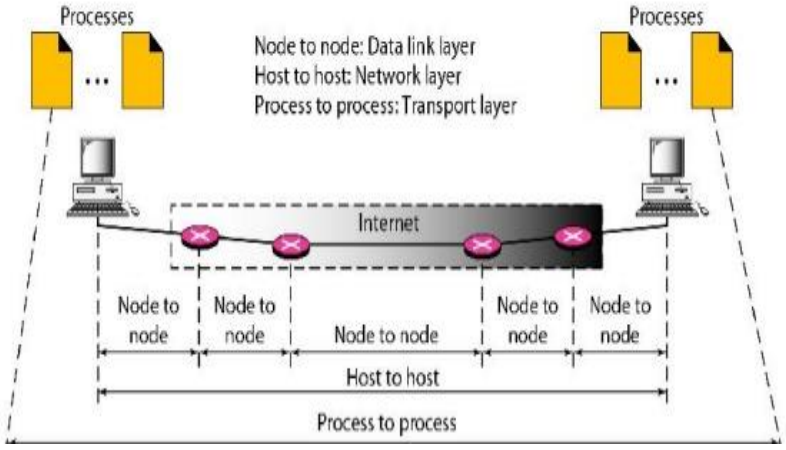


FIG :TYPES OF DATA DELIVERIES

Client/Server Paradigm

Although there are several ways to achieve process-to-process communication, the most common one is through the client/server paradigm. A process on the local host, called a client, needs services from a process usually on the remote host, called a server. Both processes (client and server) have the same name. For example, to get the day and time from a remote machine, we need a Daytime client process running on the local host and a Daytime server process running on a remote machine. For communication, we must define the following:

1. Local host
2. Local process
3. Remote host
4. Remote process

ii. **Addressing**

Whenever we need to deliver something to one specific destination among many, we need an address. At the data link layer, we need a MAC address to choose one node among several nodes if the connection is not point-to-point. A frame in the data link layer needs a Destination MAC address for delivery and a source address for the next node's reply.

Figure 4.2 shows this concept.

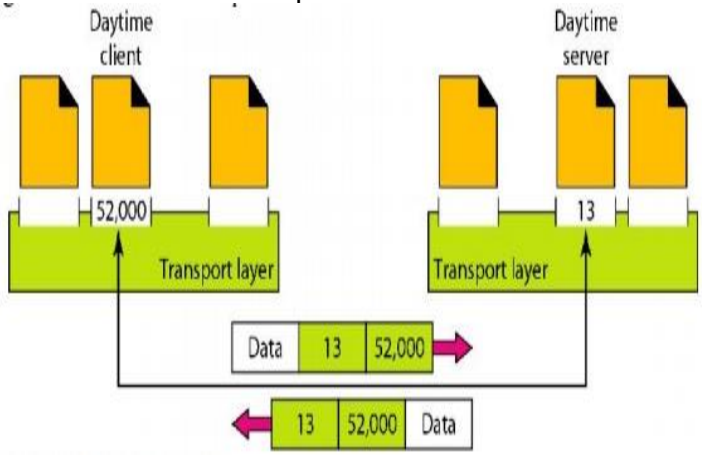


Fig 2: PORT NUMBER

The IP addresses and port numbers play different roles in selecting the final destination of data. The destination IP address defines the host among the different hosts in the world. After the host has been selected, the port number defines one of the processes on this particular host

(see Figure 3).

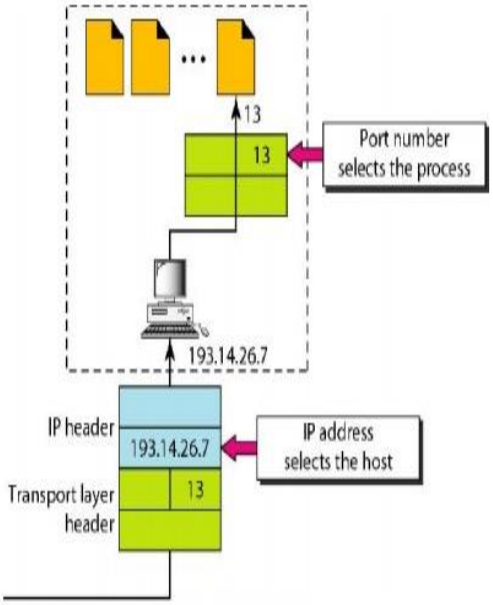


FIG 3:IP ADDRES VERSIS PORT NUMBERS

iii.lANA Ranges

The lANA (Internet Assigned Number Authority) has divided the port numbers into three ranges: well known, registered, and dynamic (or private), as shown in Figure 4.

· **Well-known ports**. The ports ranging from 0 to 1023 are assigned and controlledby lANA. These are the well-known ports.

· **Registered ports.** The ports ranging from 1024 to 49,151 are not assigned orcontrolled by lANA. They can only be registered with lANA to prevent duplication.

· **Dynamic ports**. The ports ranging from 49,152 to 65,535 are neither controllednor registered. They can be used by any process. These are the ephemeral ports.

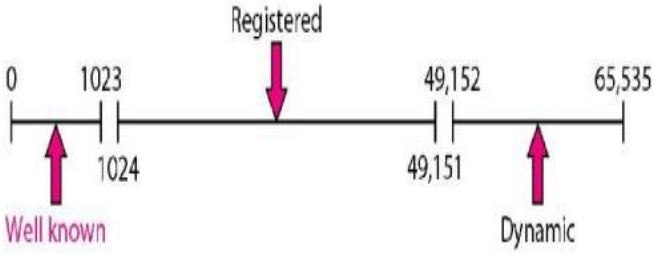


FIG 4:.IANA RANGES

iv.**Socket Addresses**

Process-to-process delivery needs two identifiers, IP address and the port number, at each end to make a connection. The combination of an IP address and a port number is called a socket address. The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely (see Figure 5).

UDP or TCP header contains the port numbers.

FIG 5.SOCKET ADDRESS

v. Multiplexing and Demultiplexing

The addressing mechanism allows multiplexing and demultiplexing by the transport layer, as shown in Figure 6.

Multiplexing

At the sender site, there may be several processes that need to send packets. However, there is only one transport layer protocol at any time. This is a many-to-one relationship and requires multiplexing.

Demultiplexing

At the receiver site, the relationship is one-to-many and requires demultiplexing. The transport layer receives datagrams from the network layer. After error checking and dropping of the header, the transport layer delivers each message to the appropriate process based on the port number.

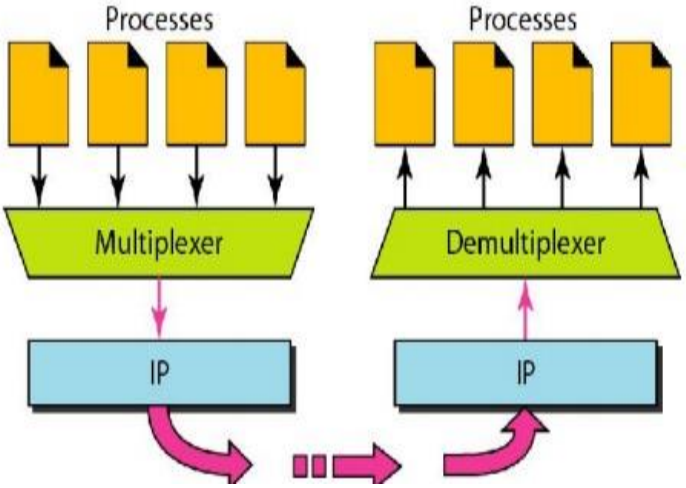


FIG 6>MULTIPLEXING AND DEMULTIPLEXING

vi. Connectionless Versus Connection-Oriented Service

A transport layer protocol can either be connectionless or connection-oriented.

Connectionless Service

In a connectionless service, the packets are sent from one party to another with no need for connection establishment or connection release. The packets are not numbered; they may be delayed or lost or may arrive out of sequence. There is no acknowledgment either.

Connection~Oriented Service

In a connection-oriented service, a connection is first established between the sender and the receiver. Data are transferred. At the end, the connection is released.

vii. Reliable Versus Unreliable

The transport layer service can be reliable or unreliable. If the application layer program needs reliability, we use a reliable transport layer protocol by implementing flow and error control at the transport layer. This means a slower and more complex service.

In the Internet, there are three common different transport layer protocols. UDP is connectionless and unreliable; TCP and SCTP are connection oriented and reliable. These three can respond to the demands of the application layer programs.

The network layer in the Internet is unreliable (best-effort delivery), we need to implement reliability at the transport layer.

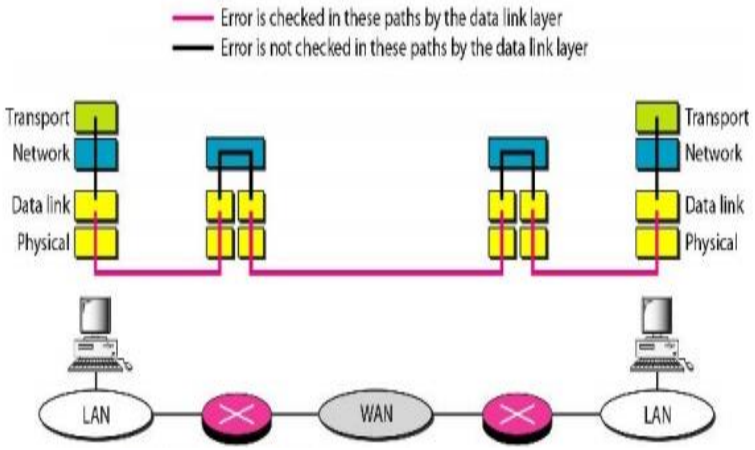


FIG 7.ERROR CONTROL

viii. Three Protocols

The original TCP/IP protocol suite specifies two protocols for the transport layer: UDP and TCP. We first focus on UDP, the simpler of the two, before discussing TCP. A new transport layer protocol, SCTP, has been designed. Figure 4.8 shows the position of these protocols in the TCP/IP protocol suite.

SAQ's Self-Assessment Questions

1. Which layer of the OSI model is responsible for process-to-process delivery?
   a. Transport Layer
   b. Network Layer
   c. Data Link Layer
   d. Physical Layer
   Answer: a. Transport Layer
2. Which transport layer protocol provides reliable, connection-oriented delivery?
   a. TCP
   b. UDP
   c. IP
   d. ICMP
   Answer: a. TCP
3. What is the primary function of sequence numbers in TCP?
   a. Identifying the source and destination IP addresses
   b. Ensuring ordered delivery of packets
   c. Detecting errors in the received data
   d. Providing flow control mechanism
   Answer: b. Ensuring ordered delivery of packets
4. Which transport layer protocol is connectionless and unreliable?
   a. TCP
   b. UDP
   c. IP
   d. ICMP
   Answer: b. UDP
5. What is the purpose of port numbers in the transport layer?
   a. Identifying the source and destination IP addresses
   b. Ensuring ordered delivery of packets
   c. Providing addressing for different applications or services
   d. Detecting errors in the received data
   Answer: c. Providing addressing for different applications or services
6. Which transport layer protocol is commonly used for web browsing?
   a. TCP
   b. UDP

c. IP
d. ICMP
Answer: a. TCP

7. Which transport layer protocol is suitable for real-time applications such as video streaming?
a. TCP
b. UDP
c. IP
d. ICMP
Answer: b. UDP

8. What is the purpose of the TCP three-way handshake?
a. Establishing a reliable connection between two hosts
b. Negotiating the maximum segment size for data transmission
c. Detecting errors in the received data
d. Providing flow control mechanism
Answer: a. Establishing a reliable connection between two hosts

9. Which mechanism is used by TCP to handle congestion control?
a. Sliding window
b. Sequence numbers
c. SYN-ACK packets
d. Slow start and congestion avoidance
Answer: d. Slow start and congestion avoidance

10. Which transport layer protocol provides error detection through checksums?
a. TCP
b. UDP
c. IP
d. ICMP
Answer: a. TCP

11. Which transport layer protocol is commonly used for voice-over-IP (VoIP) applications?
a. TCP
b. UDP
c. IP
d. ICMP
Answer: b. UDP

12. What is the purpose of flow control in TCP?
a. Ensuring ordered delivery of packets
b. Detecting errors in the received data
c. Preventing the sender from overwhelming the receiver with data
d. Providing addressing for different applications or services
Answer: c. Preventing the sender from overwhelming the receiver with data

13. Which transport layer protocol is responsible for fragmentation and reassembly of packets?
a. TCP
b. UDP
c. IP
d. ICMP
Answer: c. IP

14. What is the role of the transport layer in handling packet loss and retransmission?
a. TCP performs error correction through forward error correction codes.
b. UDP discards lost packets and relies on higher layers to handle retransmission.
c. TCP detects packet loss through sequence numbers and triggers retransmission
.
d. UDP relies on network layer protocols to handle packet loss and retransmission.
Answer: c. TCP detects packet loss through sequence numbers and triggers retransmission.

15. Which transport layer protocol is commonly used for email delivery?
a. TCP

b. UDP
c. IP
d. SMTP
Answer: a. TCP

16. Which transport layer protocol is responsible for delivering web pages over HTTP?
a. TCP
b. UDP
c. IP
d. HTTP
Answer: a. TCP

17. Which transport layer protocol is responsible for file transfer over FTP?
a. TCP
b. UDP
c. IP
d. FTP
Answer: a. TCP

18. Which transport layer protocol is commonly used for DNS (Domain Name System) queries?
a. TCP
b. UDP
c. IP
d. DNS
Answer: b. UDP

19. What is the main advantage of using UDP over TCP?
a. Reliable delivery of packets
b. Error detection through checksums
c. Flow control and congestion control mechanisms
d. Lower overhead and reduced latency
Answer: d. Lower overhead and reduced latency

20. Which transport layer protocol is responsible for sending error and control messages?
a. TCP
b. UDP
c. IP
d. ICMP
Answer: d. ICMP

Summary

The transport layer plays a crucial role in ensuring process-to-process delivery of data in a network. It operates above the network layer and provides services to the applications running on the source and destination hosts. The primary protocols used at the transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

TCP is a reliable, connection-oriented protocol that guarantees the ordered and error-free delivery of data. It achieves this through mechanisms such as sequence numbers, acknowledgement numbers, and the three-way handshake process. TCP also implements flow control and congestion control mechanisms to prevent data loss and network congestion.

UDP, on the other hand, is a connectionless and unreliable protocol that offers low overhead and reduced latency. It does not provide guarantees for data delivery or reliability but is commonly used for real-time applications such as voice and video streaming, where a small amount of data loss is acceptable.

The transport layer uses port numbers to identify specific applications or services running on the hosts. These port numbers, combined with IP addresses, enable the transport layer to deliver data to the correct process on the destination host.

In TCP, the three-way handshake process is used to establish a reliable connection between two hosts. This involves a series of messages exchanged between the client and server to synchronize sequence numbers and establish the initial parameters for communication.

Flow control in TCP prevents the sender from overwhelming the receiver with data by using

techniques like sliding window and acknowledgement-based flow control. Congestion control mechanisms, such as slow start and congestion avoidance, regulate the amount of data sent into the network to prevent congestion and maintain optimal performance.
The transport layer also handles error detection through checksums, fragmentation, and reassembly of packets, and handles retransmission in case of packet loss or errors.
Different applications utilize specific transport layer protocols. For example, HTTP (Hypertext Transfer Protocol) uses TCP for web browsing, FTP (File Transfer Protocol) uses TCP for file transfer, and DNS (Domain Name System) queries use UDP.

Terminal Questions
1. Explain the concept of reliable data delivery in TCP. How does TCP ensure reliable delivery of data packets?
2. What is the purpose of sequence numbers and acknowledgement numbers in TCP? How do they contribute to reliable data transfer?
3. Describe the TCP three-way handshake process in detail. What are the steps involved, and what purpose does each step serve?
4. How does flow control work in TCP? Explain the mechanisms employed by TCP to regulate the rate of data transmission.
5. What is congestion control, and why is it important in transport layer protocols? Explain the techniques used by TCP to control congestion.
6. Discuss the differences between TCP and UDP. In what scenarios would you choose one over the other?
7. Explain the concept of port numbers in the transport layer. How are they used to facilitate process-to-process communication?

Topic 2: Transmission Control Protocol(TCP), User Datagram Protocol

TCP:
It is a transport layer protocol.
TCP, like UDP, is a process-to-process (program-to-program) protocol.
TCP, therefore, like UDP, uses port numbers.
Unlike UDP, TCP is a connectionoriented protocol; it creates a virtual connection between two TCPs to send data.
In addition, TCP uses flow and error control mechanisms at the transport level.

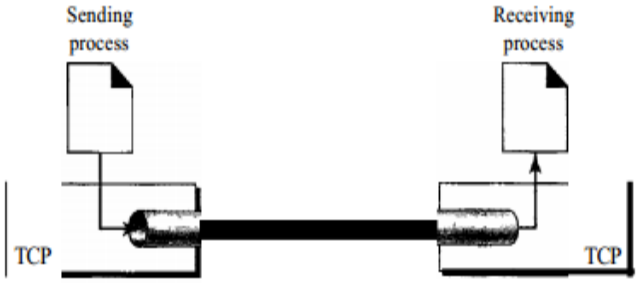
In brief, TCP is called a *connection-oriented, reliable* transport protocol. It adds connection-oriented and reliability features to the services of IP.
TCP Services
Process-to-Process Communication
Like UDP, TCP provides process-to-process communication using port numbers.

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FIP, Data	File Transfer Protocol (data connection)
21	FIP, Control	File Transfer Protocol (control connection)
23	TELNET	Tenninal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

Well known ports used by TCP

Stream Delivery Service

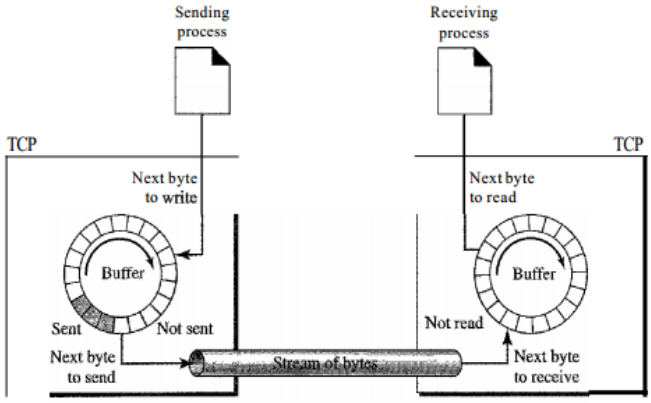
TCP allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes. TCP creates an environment in which the two processes seem to be connected by an imaginary "tube" that carries their data across the Internet.



Stream Delivery

Sending and Receiving Buffers

Because the sending and the receiving processes may not write or read data at the same speed, TCP needs buffers for storage. There are two buffers, the sending buffer and the receiving buffer, one for each direction.



Sending and receiving buffers

Full-Duplex Communication

TCP offers full-duplex service, in which data can flow in both directions at the same time. Each TCP then has a sending and receiving buffer, and segments move in both directions.

Connection-Oriented Service

TCP, unlik

e UDP, is a connection-oriented protocol. When a process at site A wants to send and receive data from another process at site B, the following occurs:

The two TCPs establish a connection between them.

Data are exchanged in both directions.

The connection is terminated.
Note that this is a virtual connection, not a physical connection. The TCP segment is encapsulated in an IP datagram and can be sent out of order, or lost, or corrupted, and then
resent. Each may use a different path to reach the destination. There is no physical connection.
Reliable Service

TCP is a reliable transport protocol. It uses an acknowledgment mechanism to check the safe and sound arrival of data. We will discuss this feature further in the section on error control.

Session Description

TCP Features

Numbering System
Although the TCP software keeps track of the segments being transmitted or received, there is no field for a segment number value in the segment header. Instead, there are two fields called the sequence number and the acknowledgment number. These two fields refer to the byte number and not the segment number.

Byte Number
TCP numbers all data bytes that are transmitted in a connection. Numbering is independent in each direction. When TCP receives bytes of data from a process, it stores them in the sending buffer and numbers them. The numbering does not necessarily start from 0. Instead, TCP generates a random number between 0 and $2^{32}-1$ for the number of the first byte. For example, if the random number happens to be 1057 and the total data to be sent are 6000 bytes, the bytes are numbered from 1057 to 7056.

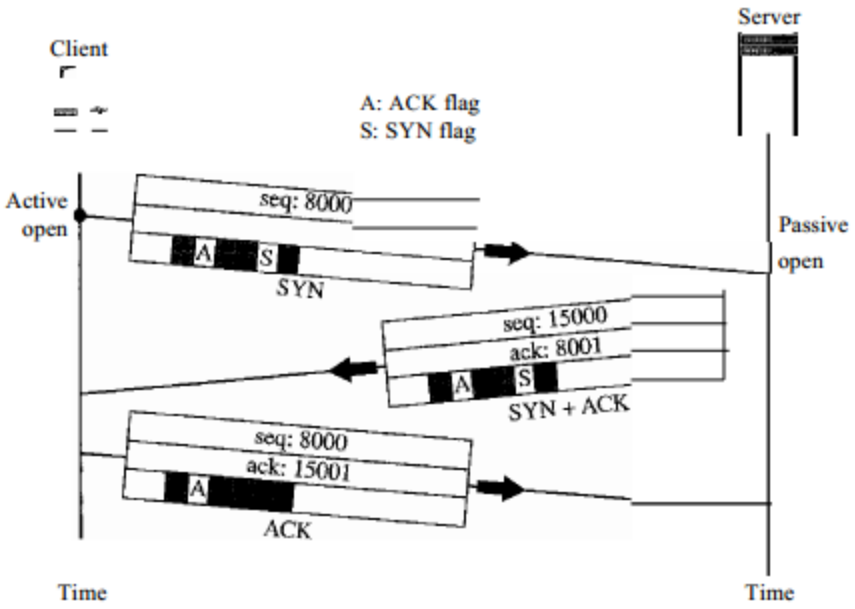
Sequence Number
After the bytes have been numbered, TCP assigns a sequence number to each segment that is being sent. The sequence number for each segment is the number of the first byte carried in that segment.

Acknowledgment Number
As TCP is full duplex; when a connection is established, both parties can send and receive data at the same time. The sequence number in each direction shows the number of the first byte carried by the segment. Each party also uses an acknowledgment number to confirm the bytes it has received. However, the acknowledgment number defines the number of the next byte that the party expects to receive.

Flow Control
TCP, unlike UDP, provides *flow control*. The receiver of the data controls the amount of data that are to be sent by the sender. This is done to prevent the receiver from being overwhelmed with data. The numbering system allows TCP to use a byte-oriented flow control.
Error Control
To provide reliable service, TCP implements an error control mechanism. Although
error control considers a segment as the unit of data for error detection (loss or corrupted segments).
Congestion Control
TCP, unlike UDP, takes into account congestion in the network. The amount of data sent by a sender is not only controlled by the receiver (flow control), but is also determined by the level of congestion in the network.
A TCP Connection

Connection Establishment
The three-way handshake is a process used by the TCP (Transmission Control Protocol) to establish a reliable connection between a client and a server. It involves a series of three messages exchanged between the client and server to synchronize and negotiate parameters before data transmission begins.

Here's a detailed explanation of the three-way handshake for connection establishment in TCP:
Step 1: SYN (Synchronize)
The client initiates the connection by sending a TCP segment with the SYN (synchronize) flag set to the server.
The client selects an initial sequence number (ISN) for the connection, which is a randomly chosen value to ensure uniqueness.
The SYN segment also includes the client's initial TCP window size, which indicates the number of bytes the client is willing to receive.
Step 2: SYN-ACK (Synchronize-Acknowledge)
Upon receiving the SYN segment from the client, the server responds with a TCP segment containing the SYN and ACK (acknowledge) flags set.
The server selects its own initial sequence number (ISN) for the connection.
The SYN-ACK segment also includes the server's initial TCP window size, acknowledging the client's window size from the previous step.
Additionally, the SYN-ACK segment may include other optional parameters negotiated between the client and server, such as maximum segment size (MSS) or TCP options.
Step 3: ACK (Acknowledge)
Finally, the client acknowledges the server's SYN-ACK segment by sending an ACK segment.
The ACK segment has the ACK flag set and contains the acknowledgment number, which is the server's initial sequence number incremented by one.
The client also confirms the server's TCP window size, indicating the number of bytes it is willing to receive from the server.
At this point, the connection is established, and both the client and server can begin transmitting data.
The three-way handshake ensures that both the client and server agree on initial sequence numbers, window sizes, and other connection parameters before data transmission begins. It establishes a reliable and synchronized connection that allows for efficient and error-free communication between the two endpoints.
It's important to note that the three-way handshake is a crucial part of TCP's connection-oriented communication, providing reliability and ensuring that both parties are ready to exchange data.



Connection establishment using three-way handshaking

Connection Termination

The TCP (Transmission Control Protocol) connection termination, often referred to as the "three-way handshake for connection termination," involves a series of steps to gracefully close a TCP connection