1. **Describe routing in a network? Explain the shortest path routing protocol**

**Routing:**

It is a process by which packets are efficiently transported from source to destination.

The algorithms that make the routing decisiosn are called Routing Algorithms.

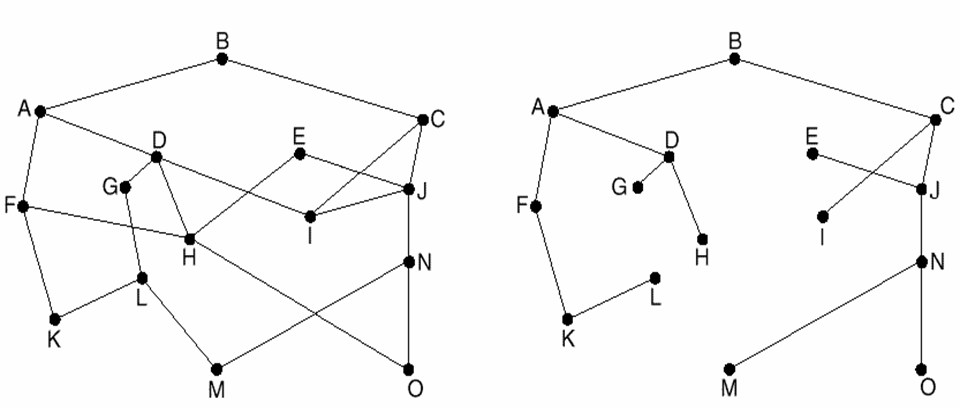
Desired properties for a routing algorithm:

* correctness
* simplicity
* robustness with respect to failures and changing conditions
* stability of the routing decisions
* fairness of the resource allocation
* optimality of the packet travel times

**The Optimality Principle**

The optimality principle states that if router *J* is on the optimal path from router *I* to router *K*, then the routes from *I* to *J* and from *J* to *K* are also optimal.

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.



A sink tree for router B

**Types of routing Algorithms:**

* Non Adaptive or Static Routing: In this type of routing decisions are not dependent on the present condition of traffic and topology of the network. As this type of routing does not depend on the present condition of traffic in the network, it has poor performance during heavy traffic. Even if traffic increases the routing decisions do not change.

Eg. Shortest Path Routing, Flooding

* Adaptive or Dynamic Routing: In this type of routing algorithm the routing decisions are made depending on the present condition of traffic and topology of the network. As this type of routing depends on the present condition of traffic in the network, the performance is good during heavy traffic.

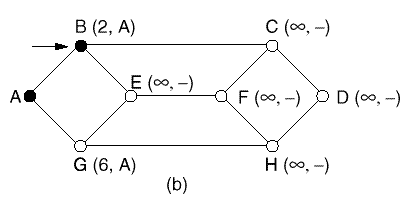
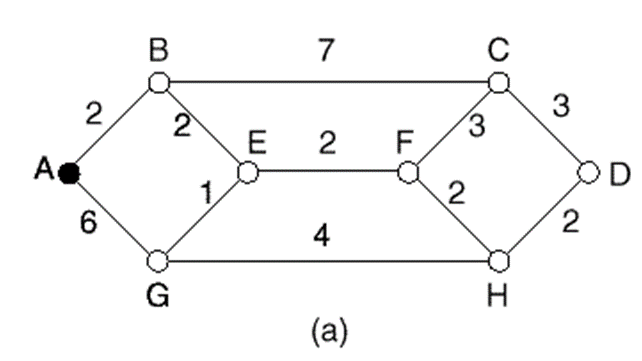
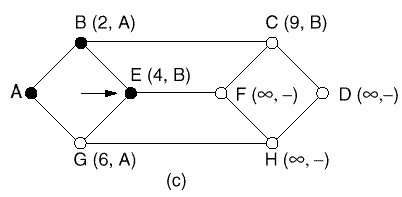
Eg. Distance Vector Routing, Hierarchical Routing.

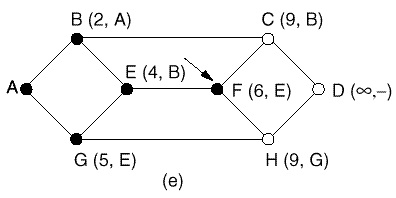
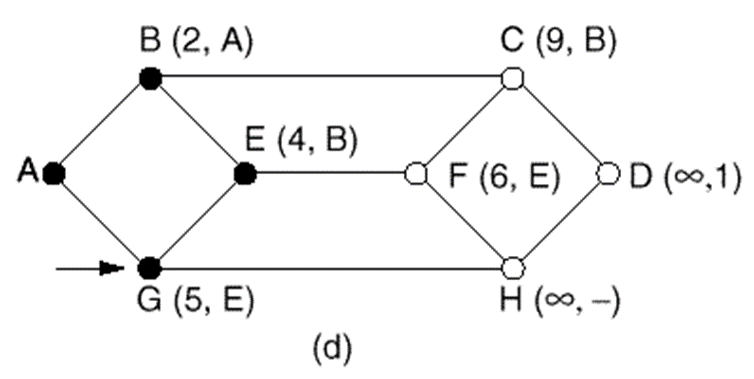
**Routing Algorithms:**

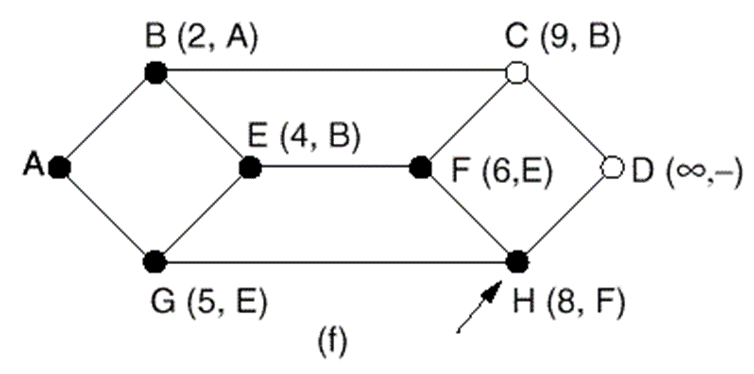
* Shortest Path Routing:

This is the same as the Dijkstras Algorithm for finding shortest path between two nodes. This is used to calculate the shortest route from source router to destination router.

To compute the shortest path from A to D





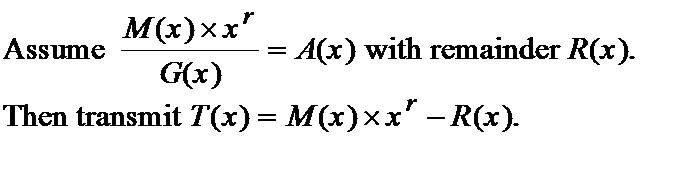
1. **In a data transmission system the received string of bits is 110011001100. Analyze whether it acceptable? If so, calculate the data bit sequence? Consider the divisor is 10101.**

**Already solved during sessions**

**Basic Idea**

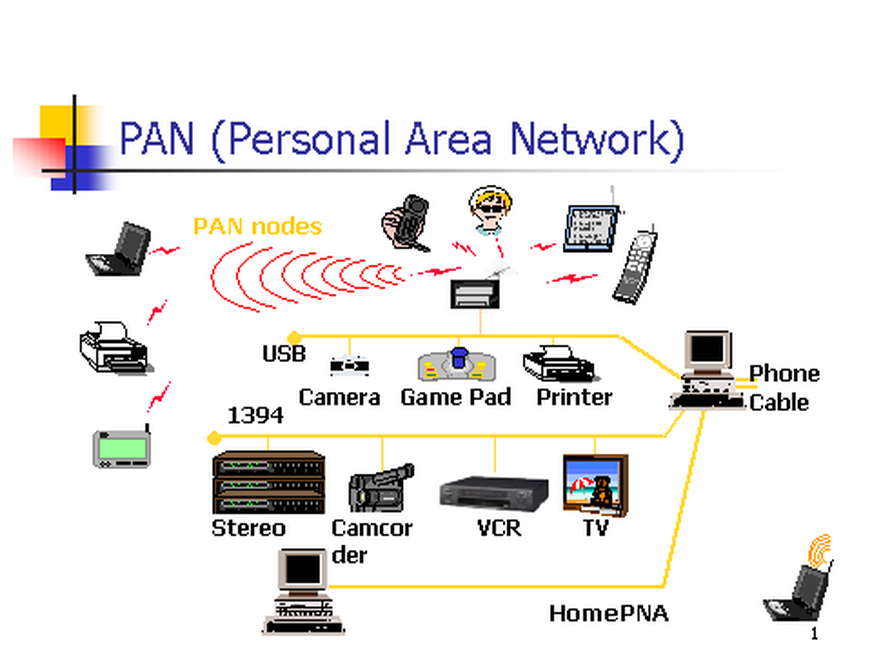
Sender and receiver agree upon a polynomial of degree *r*.

(the generating polynomial, *G*(*x*))



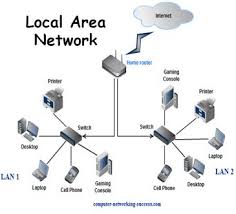
When receiver receives *T*(*x*), it divides it by *G*(*x*). If there is a remainder, then an error has occurred.

1. **What are the various types of networks? Compare and contrast LAN, MAN and WAN.**
2. **Types of Networks:**
3. Personal Area Network (PAN)
4. Local Area Network (LAN)
5. Campus Area Network (CAN)
6. Metropolitan Area Network (MAN)
7. Wide Area Network (WAN)
8. Storage-Area Network (SAN)
9. Virtual Private Network (VPN)
10. Client Server Network
11. Peer to Peer Network (P2P)
12. **Personal Area Network (PAN):**
13. Personal Area Network (PAN) is a computer network used for data transmission amongst devices such as computers, telephones, tablets and personal digital assistants.
14. Also Known as HAN (Home Area Network).
15. PANs can be used for communication amongst the personal devices themselves (interpersonal communication), or for connecting to a higher level network and the Internet (an uplink) where one "master" device takes up the role as internet router.



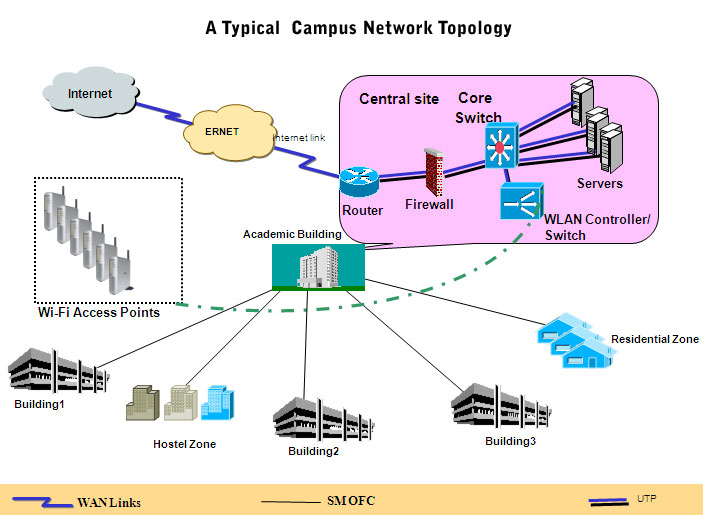
**b) Local Area Network (LAN)**:

* Xerox Corporation worked in collaboration with DEC and Intel to create Ethernet, which is the most pervasive LAN architecture used today.
* Ethernet has evolved and has seen significant improvements in regard to speed and efficiency.
* An upside of a LAN is fast data transfer with data speed that can reach up to 10Gbps.
* Other significant LAN technologies are Fiber Distributed Data Interface (FDDI) and token ring.



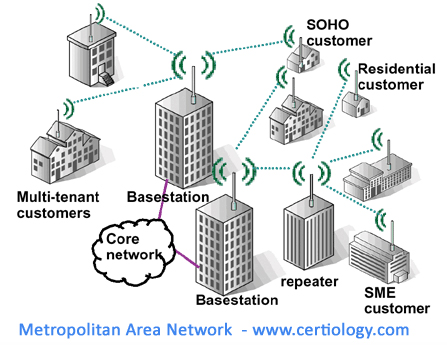
**c) Campus Area Network (CAN):**

* Larger than LANs, but smaller than metropolitan area networks these types of networks are typically seen in universities, large K-12 school districts or small businesses
* They can be spread across several buildings that are fairly close to each other so users can share resources



**d) Metropolitan Area Network:**

* A MAN is larger than a LAN but smaller than or equal in size to a WAN.
* The size range anywhere from 5 to 50km in diameter.
* MANs are typically owned and managed by a single entity.
* This could be an ISP or telecommunications company that sells its services to end-users in that metropolitan area.
* For all intents and purposes, a MAN has the same characteristics as a WAN with distance constraints.



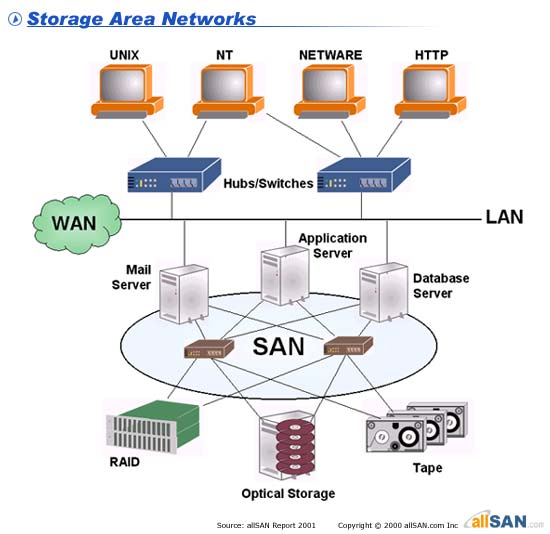
**e) Wide Area Network (WAN):**

* A Wide Area Network exist over a large area
* Data travels through telephone or cable lines
* Usually requires a Modem
* The world’s largest Wide Area Network in the Internet

[](http://images.google.com/imgres?imgurl=http://www.computernetworks.com/Images/WAN.jpg&imgrefurl=http://www.computernetworks.com/WAN.cfm&h=216&w=260&sz=32&hl=en&start=1&um=1&tbnid=FtShEV6853INCM:&tbnh=93&tbnw=112&prev=/images?q%3Dwide%2Barea%2Bnetworks%26svnum%3D10%26um%3D1%26hl%3Den)

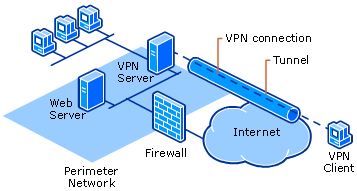
**f)Storage Area Network:**

* SAN may be referred to as a Sub network or special purpose network.
* Its special purpose is to allow users on a larger network to connect various data storage devices with clusters of data servers.
* SANs can be accessed in the same fashion as a drive attached to a server.



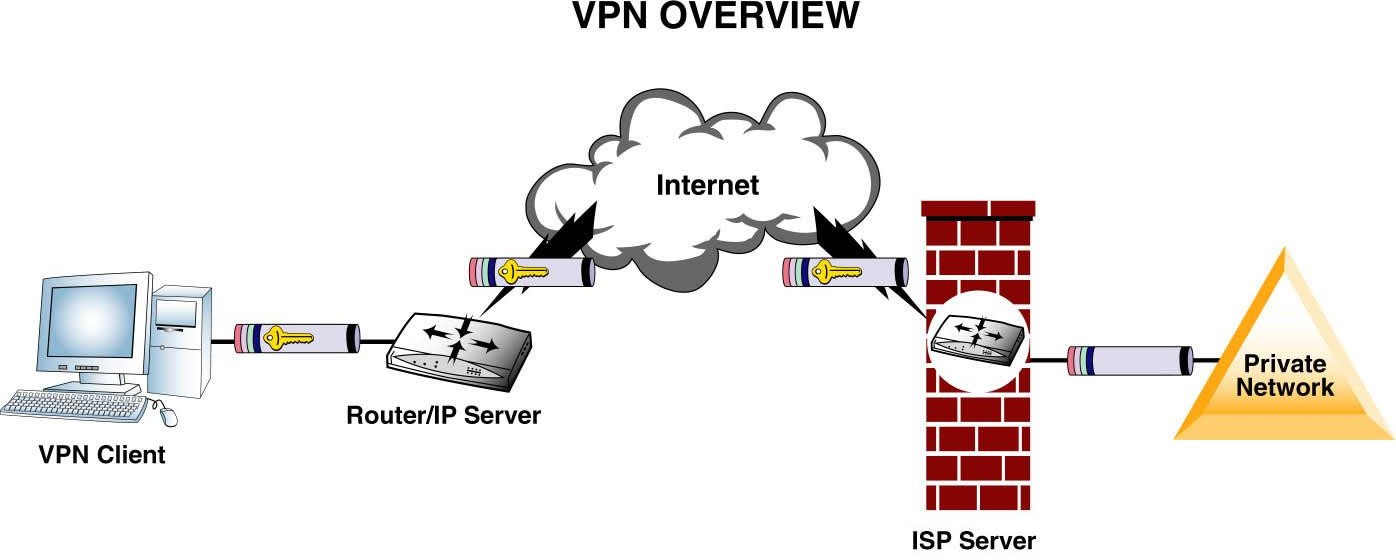
**g) Virtual Private Network:**

* VPN is a private network that can access public networks remotely. VPN uses encryption and security protocols to retain privacy while it accesses outside resources.
* When employed on a network, VPN enables an end user to create a virtual tunnel to a remote location. Typically, telecommuters use VPN to log in to their company networks from home.
* Authentication is provided to validate the identities of the two peers.
* Confidentiality provides encryption of the data to keep it private from prying eyes.
* Integrityis used to ensure that the data sent between the two devices or sites has not been tampered with.



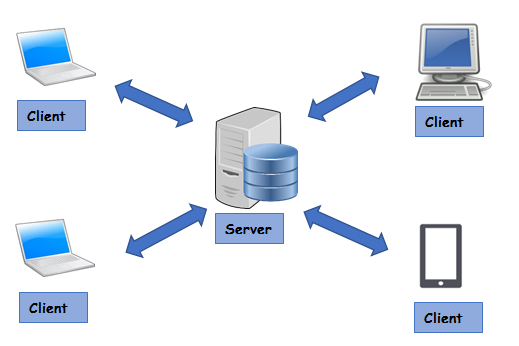
**Virtual Private Network (VPN)**

* Uses the internet as a backbone to transmit encrypted data from one site to another.
* Uses tunnelling to facilitate data encryption and to enable connections to carry protocols other than IP



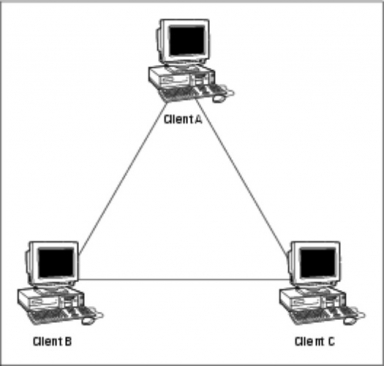
**h) Client/Server Network:**

* In a client/server arrangement, network services are located on a dedicated computer called a server.
* The server responds to the requests of clients.
* The server is a central computer that is continuously available to respond to requests from clients for file, print, application, and other services.
* Most network operating systems adopt the form of a client/server relationship.
* Typically, desktop computers function as clients, and one or more computers with additional processing power, memory, and specialized software function as servers.



**i) Peer to Peer Network:**

* Usually very small networks
* Each workstation has equivalent capabilities and responsibilities
* Does not require a switch or a hub.
* These types of networks do not perform well under heavy data loads.



1. **Explain how a typical circuit route for a medium-distance call is established in PSTN.**

## **PSTN? (Public Switched Telephone Network)**

PSTN stands for Public Switched Telephone Network, or the traditional circuit-switched telephone network. This is the system that has been in general use since the late 1800s.

Using underground copper wires, this legacy platform has provided businesses and households alike with a reliable means to communicate with anyone around the world for generations.

The phones themselves are known by several names, such as PSTN, landlines, Plain Old Telephone Service (POTS), or fixed-line telephones.

PSTN phones are widely used and generally still accepted as a standard form of communication. However, they have seen a steady decline over the last decade.

## **How Do PSTN Phone Lines Work?**

Think of a Public Switched Telephone Network (PSTN) as a combination of telephone networks used worldwide, including telephone lines, fiber optic cables, switching centers, cellular networks, as well as satellites and cable systems. These help telephones communicate with each other.

Put simply, when you dial a phone number your call moves through the network to reach its destination – and two phones get connected. To fully understand how a [**POTS**](https://www.nextiva.com/blog/what-is-pots.html) actually works, consider what happens when you dial a number from your own phone.

**Step #1 -** Your telephone set converts sound waves into electrical signals. These signals are then transmitted to a terminal via a cable.

**Step #2 -**The terminal collects the electrical signals and transmits these to the central office (CO).

**Step #3 -** The central office routes the calls in the form of electrical signals through fiber optic cable. The fiber optic conduit then carries these signals in the form of light pulses to their final destination.

**Step #4 -** Your call is routed to a tandem office (a regional hub responsible for transmitting calls to distant central offices) or a central office (for local calls).

**Step #5 -** When your call reaches the right office, the signal is converted back to an electrical signal and is then routed to a terminal.

**step #6 -** The terminal routes the call to the appropriate telephone number. Upon receiving the call, the telephone set converts the electrical signals back to sound waves.

## **PSTN - Understanding The Art of Switching**

You could say that PSTNs are all about switching, which forms the backbone of traditional phone networks. When a call is made, switches create a wire circuit between two telephones, with this particular connection lasting as long as the duration of the call.

Now, let’s have a look at each of the four types of switching which take place at different levels.

### **1. The Local Exchange**

A local exchange - which may consist of one or more exchanges - hooks up subscribers to a PSTN line. Also known as a central office or a switching exchange, a telephone exchange may have as many as 10,000 lines.

All telephones are connected to the local exchange in a specific area. Interestingly, if you were to dial the number of your supplier located in the building next to yours, the call won't leave your local exchange and will be routed to the supplier as soon as it reaches the exchange.

The exchange then identifies the number dialed so it can route the call towards the correct end destination. This process works as follows:

The first three digits of a phone number represent the exchange (the local switch), while the last four digits identify the individual subscriber within that exchange.

This means that when you dial a number and it reaches your local exchange, your call is immediately linked to the subscriber without the need for any further routing.

### **2. The Tandem Office**

Also known as a junction network, a tandem office serves a large geographical area comprising several local exchanges while managing switches between local exchanges.

Let’s say you dialed the number of a client who lives in the same city but in another suburb. In this case your call will be routed to a tandem office from your local exchange, and the tandem office will route the signal on to the local exchange near your client’s location.

### **3. The Toll Office**

This is where any national long-distance switching takes place.

A toll office is connected to all the tandem offices. For instance, if you have an office in another city you’ll find that, whenever you dial that branch’s number, your call will be switched through a toll office.

### **4. The International Gateway**

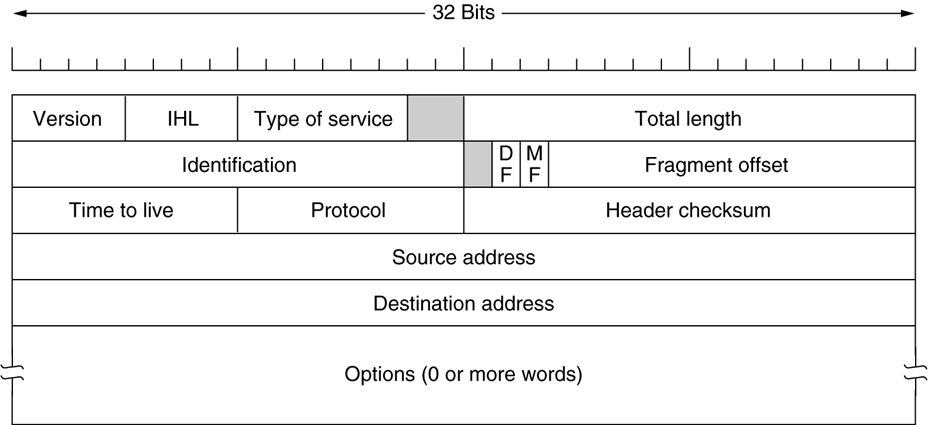
International gateways manage international call switching, routing domestic calls to the appropriate countries.

1. **Explain IP header format in detail with a diagram. Analyze the role of the field TTL in DOS attacks.**

The Internet is an interconnected collection of many networks.

* IP address: a unique numeric string that identifies the client as a unique member of a specific network.
* Logical network addressing( MAC address is the physical address embedded in the NIC)
* All TCP/IP clients must have an IP address.

The IP Protocol: IP header has a 20 byte fixed part followed by a variable length optional part.



Version (Length 4 bytes) – This field indicates the IP version used for this packet. Typically 4.

IHL: Internet Header Length (Length 4 bits) – This indicates the length of the header. Minimum length of header = 20 bytes

Type of Service – Length 8 bits. these are rarely used. If one or more of these bits are set, they indicate how routers should handle this packet.

Total length of packet (Length 16 bits) – It gives the total length of the packet,including the header and including the data sent.

Identification (Length 16 bits) – A number identifying the packet. Numbering packets is useful when fragmenting packets. All the fragments of the same packet have the same identification number.

Flags (Length 3 bits)

Fragmentation Offset: (Length 13 bits) – If the total length of the packet is too large for a network to handle, it is divided into smaller fragments.

Time to Live ( Length 8 bits) – This is used to make sure no packet will wander through the Internet for eternity.

Protocol ( Length 8 bits) – The protocol used in the packet. Typically 06 for TCP or 17 for UDP.

Header Checksum (Length 16 bits) – To identify the damaged packets.

Source Address (Length 32 bits) – The IP address of the sender of this packet.

Destination ( Length 32 bits) – The IP address of the intended receiver.

Options – If required, routers or gateways can define the custom options here

1. **What is framing? Discuss the role of Data Link Layer in encapsulating and decapsulating a packet in a frame.**

**Data Link Layer**

* Ensures that messages are delivered to the proper device.
* Translates messages from the network layer into bits for the physical layer to transmit.
* It formats the message into data frames and adds a customized header containing the hardware destination and source address.
* The IEEE ethernet data link layer has two sub layers:-
* MAC (Media Access Control) defines how packets are placed on the media and LLC (Logical Link Control) is responsible for identifying network layer protocols and then encapsulating them.
* Switch and Bridge are the examples of data link layer devices. Both filter and forward frames using hardware (MAC) addresses.

The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmit the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.

**REFER: PPT for frame structure**

1. **www is a distributed system running on the internet where the clients send their request through the web browser to the webserver, Web server takes this request, processes it and then sends back processed data to the client. In the above statement establish the importance of a domain name and IP address to the webserver.**

The domain name system (DNS) is a naming database in which internet domain names are located and translated into Internet Protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate that website.

For example, if someone types "example.com" into a web browser, a server behind the scenes maps that name to the corresponding IP address. An IP address is similar in structure to 203.0.113.72.

Web browsing and most other internet activities rely on DNS to quickly provide the information necessary to connect users to remote hosts. DNS mapping is distributed throughout the internet in a hierarchy of authority. Access providers and enterprises, as well as governments, universities and other organizations, typically have their own assigned ranges of IP addresses and an assigned domain name. They also typically run DNS servers to manage the mapping of those names to those addresses. Most Uniform Resource Locators (URLs) are built around the domain name of the web server that takes client requests.

How DNS works

DNS servers convert URLs and domain names into IP addresses that computers can understand and use. They translate what a user types into a browser into something the machine can use to find a webpage. This process of translation and lookup is called DNS resolution.

The basic process of a DNS resolution follows these steps:

The user enters a web address or domain name into a browser.

The browser sends a message, called a recursive DNS query, to the network to find out which IP or network address the domain corresponds to.

The query goes to a recursive DNS server, which is also called a recursive resolver, and is usually managed by the internet service provider (ISP). If the recursive resolver has the address, it will return the address to the user, and the webpage will load.

If the recursive DNS server does not have an answer, it will query a series of other servers in the following order: DNS root name servers, top-level domain (TLD) name servers and authoritative name servers.

The three server types work together and continue redirecting until they retrieve a DNS record that contains the queried IP address. It sends this information to the recursive DNS server, and the webpage the user is looking for loads. DNS root name servers and TLD servers primarily redirect queries and rarely provide the resolution themselves.

The recursive server stores, or caches, the A record for the domain name, which contains the IP address. The next time it receives a request for that domain name, it can respond directly to the user instead of querying other servers.

If the query reaches the authoritative server and it cannot find the information, it returns an error message.

The entire process querying the various servers takes a fraction of a second and is usually imperceptible to the user.

DNS servers answer questions from both inside and outside their own domains. When a server receives a request from outside the domain for information about a name or address inside the domain, it provides the authoritative answer.

When a server gets a request from within its domain for a name or address outside that domain, it forwards the request to another server, usually one managed by its ISP.

1. Generate the CRC for the data word of 1 1 0 0 1 0 1 0 1. The divisor is 1 0 1 0 1.

**Refer Q 2**

1. A seven bit Hamming code is received as 1 1 1 0 1 0 1. What is the correct code word?

**Sample Problem:**

Find Hamming Code for 1001101.

***Soln.***

Step 1: Parity Bit Positions: \_ \_ 1 \_0 0 1 \_1 0 1

Step 2: For bit 1 : Check positions 3=1, 5=0, 7=1, 9=1, 11=1

Even, therefore bit 1 =0

Step 3: For bit 2: Check postions 3= 1, 6= 0, 7=1, 10=0, 11=1

Odd, therefore bit 2=1

Step 4: For bit 4: Check positions 5=0, 6=0, 7=1. Odd, therefore bit 4=1

Step 5: For bit 8: Check positions 9=1, 10=0, 11=1. Even therefore bit 8=1

Hamming Code: 0 1 1 1 0 0 1 1 1 0 1

1. **1 Gbps CSMA/CD LAN is to be designed over 1km cable without repeater. The cable supports the signal speed of 200,000km/sec. What is the minimum frame size that Data Link layer should consider?**

A network with CSMA/CD protocol in the MAC layer is running at 1Gbps over a 1km cable with no repeaters. The signal speed in the cable is 2×108m/sec. The minimum frame size for this network should be: **10000bits**.

1. Explain the DNS hijacking concept along with a solution & example in detail

DNS hijacking is **a malicious exploit in which a hacker or other party redirects users through the use of a rogue DNS server or other strategy that changes the IP address to which an Internet user is redirected**.

1. Write about the stateless address autoconfiguration (SLAAC) concept is DHCP.

SLAAC stands for Stateless Address Autoconfiguration and the name pretty much explains what it does. It is **a mechanism that enables each host on the network to auto-configure a unique IPv6 address without any device keeping track of which address is assigned to which node**.

1. Discuss the operation of VPN in detail with an example.

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

### **How does a virtual private network (VPN) work?**

A VPN extends a corporate network through encrypted connections made over the Internet. Because the traffic is encrypted between the device and the network, traffic remains private as it travels. An employee can work outside the office and still securely connect to the corporate network. Even smartphones and tablets can connect through a VPN.

### **What is secure remote access?**

Secure remote access provides a safe, secure way to connect users and devices remotely to a corporate network. It includes VPN technology that uses strong ways to authenticate the user or device. VPN technology is available to check whether a device meets certain requirements, also called a device’s posture, before it is allowed to connect remotely.

### **Is VPN traffic encrypted?**

Yes, traffic on the virtual network is sent securely by establishing an encrypted connection across the Internet known as a tunnel. VPN traffic from a device such as a computer, tablet, or smartphone is encrypted as it travels through this tunnel. Offsite employees can then use the virtual network to access the corporate network.

1. State the importance of using a firewall in the network. Explain its types with neat diagrams.

**Firewalls**

A firewall is a device that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network. Usually a firewall runs on a dedicated device; because it is a single point through which traffic is channeled, performance is important, which means nonfirewall functions should not be done on the same machine. Because a firewall is executable code, an attacker could compromise that code and execute from the firewall's device. Thus, the fewer pieces of code on the device, the fewer tools the attacker would have by compromising the firewall. Firewall code usually runs on a proprietary or carefully minimized operating system

#### Types of Firewalls

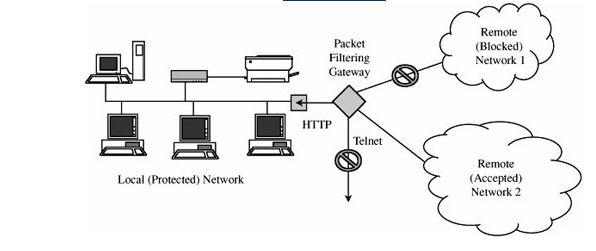
Firewalls have a wide range of capabilities. Types of firewalls include

* packet filtering gateways or screening routers
* stateful inspection firewalls
* application proxies
* guards
* personal firewalls

Each type does different things; no one is necessarily "right" and the others "wrong." In this section, we examine each type to see what it is, how it works, and what its strengths and weaknesses are. In general, screening routers tend to implement rather simplistic security policies, whereas guards and proxy gateways have a richer set of choices for security policy. Simplicity in a security policy is not a bad thing; the important question to ask when choosing a type of firewall is what threats an installation needs to counter.

##### Packet Filtering Gateway

A packet filtering gateway or screening router is the simplest, and in some situations, the most effective type of firewall. A packet filtering gateway controls access to packets on the basis of packet address (source or destination) or specific transport protocol type (such as HTTP web traffic). As described earlier in this chapter, putting ACLs on routers may severely impede their performance. But a separate firewall behind (on the local side) of the router can screen traffic before it gets to the protected network.



[Figure](mk:@MSITStore:C:\Documents%20and%20Settings\hod-%20it\Desktop\Complete%202010-Folder\DEC-2010\INS%20Module\Security%20in%20Computing,%20Fourth%20Edition.chm::/0132390779/ch07lev1sec2.html#ch07fig11) 16 Packet Filter Blocking Addresses and Protocols.

##### Stateful Inspection Firewall

Filtering firewalls work on packets one at a time, accepting or rejecting each packet and moving on to the next. They have no concept of "state" or "context" from one packet to the next. A **stateful inspection firewall** maintains state information from one packet to another in the input stream.

One classic approach used by attackers is to break an attack into multiple packets by forcing some packets to have very short lengths so that a firewall cannot detect the signature of an attack split across two or more packets. (Remember that with the TCP protocols, packets can arrive in any order, and the protocol suite is responsible for reassembling the packet stream in proper order before passing it along to the application.) A stateful inspection firewall would track the sequence of packets and conditions from one packet to another to thwart such an attack.

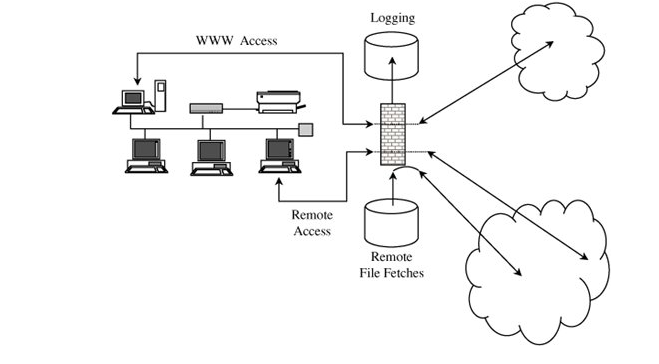
##### Application Proxy

Packet filters look only at the headers of packets, not at the data inside the packets. Therefore, a packet filter would pass anything to port 25, assuming its screening rules allow inbound connections to that port. But applications are complex and sometimes contain errors. Worse, applications (such as the e-mail delivery agent) often act on behalf of all users, so they require privileges of all users (for example, to store incoming mail messages so that inside users can read them). A flawed application, running with all users' privileges, can cause much damage.

An **application proxy gateway**, also called a **bastion host**, is a firewall that simulates the (proper) effects of an application so that the application receives only requests to act properly. A proxy gateway is a two-headed device: It looks to the inside as if it is the outside (destination) connection, while to the outside it responds just as the insider would.

An application proxy runs pseudoapplications. For instance, when electronic mail is transferred to a location, a sending process at one site and a receiving process at the destination communicate by a protocol that establishes the legitimacy of a mail transfer and then actually transfers the mail message. The protocol between sender and destination is carefully defined. A proxy gateway essentially intrudes in the middle of this protocol exchange, seeming like a destination in communication with the sender that is outside the firewall, and seeming like the sender in communication with the real destination on the inside. The proxy in the middle has the opportunity to screen the mail transfer, ensuring that only acceptable e-mail protocol commands are sent to the destination.

As an example of application proxying, consider the FTP (file transfer) protocol. Specific protocol commands fetch (get) files from a remote location, store (put) files onto a remote host, list files (ls) in a directory on a remote host, and position the process (cd) at a particular point in a directory tree on a remote host. Some administrators might want to permit gets but block puts, and to list only certain files or prohibit changing out of a particular directory (so that an outsider could retrieve only files from a prespecified directory). The proxy would simulate both sides of this protocol exchange. For example, the proxy might accept get commands, reject put commands, and filter the local response to a request to list files.



[Figure](mk:@MSITStore:C:\Documents%20and%20Settings\hod-%20it\Desktop\Complete%202010-Folder\DEC-2010\INS%20Module\Security%20in%20Computing,%20Fourth%20Edition.chm::/0132390779/ch07lev1sec2.html#ch07fig11) 17

The proxies on the firewall can be tailored to specific requirements, such as logging details about accesses. They can even present a common user interface to what may be dissimilar internal functions. Suppose the internal network has a mixture of operating system types, none of which support strong authentication through a challengeresponse token. The proxy can demand strong authentication (name, password, and challengeresponse), validate the challengeresponse itself, and then pass on only simple name and password authentication details in the form required by a specific internal host's operating system.

##### Guard

A guard is a sophisticated firewall. Like a proxy firewall, it receives protocol data units, interprets them, and passes through the same or different protocol data units that achieve either the same result or a modified result. The guard decides what services to perform on the user's behalf in accordance with its available knowledge, such as whatever it can reliably know of the (outside) user's identity, previous interactions, and so forth. The degree of control a guard can provide is limited only by what is computable. But guards and proxy firewalls are similar enough that the distinction between them is sometimes fuzzy. That is, we can add functionality to a proxy firewall until it starts to look a lot like a guard.

#### Personal Firewalls

Firewalls typically protect a (sub)network of multiple hosts. University students and employees in offices are behind a real firewall. Increasingly, home users, individual workers, and small businesses use cable modems or DSL connections with unlimited, always-on access. These people need a firewall, but a separate firewall computer to protect a single workstation can seem too complex and expensive. These people need a firewall's capabilities at a lower price.

A **personal firewall** is an application program that runs on a workstation to block unwanted traffic, usually from the network. A personal firewall can complement the work of a conventional firewall by screening the kind of data a single host will accept, or it can compensate for the lack of a regular firewall, as in a private DSL or cable modem connection.