Note : if you found any mistake on solution then please send us a message .

(You don’t need to write long answer. Some of our answer is very long for better understanding so summarize yourself)

Tribhuwan University

Institute of Science and Technology

2069

Full Marks : 60

Internet Technology **Pass Marks :24**

Time : 3 hours

New Course

Candidates are required to give their answers in their own words as far as practicable. The figures in the margin indicate full marks.

Attempt any five questions.

- **a. Explain the internet Domain and Domain Name System. <8>**
  Answer:
  Internet Domain:
  A domain name is an identification string that defines a realm of administrative autonomy, authority, or control on the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS). A domain name represents an Internet Protocol (IP) resource, such as a personal computer used to access the Internet, a server computer hosting a web site, or the web site itself or any other service communicated via the Internet. Domain names serve as humanly-memorable names for Internet participants, like computers, networks, and services. A domain name represents an Internet Protocol (IP) resource. Individual Internet host computers use domain names as host identifiers, or hostnames. Hostnames are the leaf labels in the domain name system usually without further subordinate domain name space. Hostnames appear as a component in Uniform Resource Locators (URLs) for Internet resources such as web sites.

  Structure:
  A domain name consists of one or more parts, technically called labels that are conventionally concatenated, and delimited by dots, such as example.com. The right-most label conveys the toplevel domain; for example, the domain name

www.example.combelongs to the top-level domain com.The hierarchy of domains descends from the right to the left label in the name; each label to the left specifies a subdivision, or subdomain of the domain to the right. For example: the label example specifies a node example.com as a subdomain of the com domain, and www is a label to create www.example.com, a subdomain of example.com. A hostname is a domain name that has at least one associated IP address. For example, the domain names www.example.com and example.com are also hostnames, whereas the com domain is not. However, other top-level domains, particularly country code top-level domains, may indeed have an IP address, and if so, they are also hostnames.

Subdomain:

In the Domain Name System (DNS) hierarchy, a subdomain is a domain that is part of a larger domain. The only domain that is not also a subdomain is the root domain. For example, mail.google.com and support.google.com are subdomains of the google.com domain, which in turn is a subdomain of the com top-level domain (TLD). A "subdomain" expresses relative dependence, not absolute dependence: for example, google.com comprises a subdomain of the .com domain, and mail.google.com comprises a subdomain of the domain google..com .

Reserved Domain Names:

- example: reserved for use in examples
- invalid: reserved for use in obviously invalid domain names
- localhost: reserved to avoid conflict with the traditional use of localhost as a hostname
- test: reserved for use in tests

Domain Name System:

The essence of DNS is the invention of a hierarchical, domain-based naming scheme and a distributed database system for implementing this naming scheme. It is primarily used for mapping host names to IP addresses but can also be used for other purposes. A Domain Name Service resolves queries for these names into IP addresses for the purpose of locating computer services and devices worldwide. A DNS name server is a server that stores the DNS records for a domain name, such as address (A) records, name server (NS) records, and mail exchanger (MX) records; a DNS name server responds with answers to queries against its database The way DNS is used is as follows;

Client Lookup:

When an application makes a request that requires a domain name lookup, such programs send a resolution request to the DNS resolver in the local operating system, which in turn handles the communications required. The DNS resolver will almost invariably have a cache containing recent lookups. If the cache can provide the answer to the request, the resolver will return the value in the cache to the program that made the request. If the cache does not contain the answer, the resolver will send the request to one or more designated DNS servers.

Reverse Lookup:

Computer networks use the Domain Name System to determine the IP address associated with a domain name. This process is also known as forward DNS resolution.

A reverse lookup is a query of the DNS for domain names when the IP address is known. Multiple domain names may be associated with an IP address. For IPv4, the domain is inaddr.arpa. For IPv6, the reverse lookup domain is ip6.arpa. The IP address is represented as a name in reverse-ordered octet representation for IPv4, and reverse-ordered nibble representation for IPv6.

When performing a reverse lookup, the DNS client converts the address into these formats, and then queries the name for a PTR record following the delegation chain as for any DNS query. For example, assume the IPv4 address 208.80.152.2 is assigned to Wikimedia. It is represented as a DNS name in reverse order like this: 2.152.80.208.in-addr.arpa. When the DNS resolver gets a PTR (reverse-lookup) request, it begins by querying the root servers (which point to ARIN's servers for the 208.in-addr.arpa zone). On ARIN's servers, 152.80.208.in-addr.arpa is assigned to Wikimedia, so the resolver sends another query to the Wikimedia nameserver for 2.152.80.208.in-addr.arpa, which results in an authoritative response.

b. What do you mean by Teleports and terrestrial links? Explain. <4>

Teleports:

Teleports are the ground-based side of the global satellite network – gateways that provide terrestrial networks with access to orbiting satellite transponders. But they are more than simple gateways. Teleports bridge incompatible systems and protocols, host and distribute content, and act as the hubs of broadband B2B networks. These companies range from small entrepreneurial operations with one to three facilities to large, publicly-traded companies with teleports in multiple geographic markets.

Terrestrial Link:

A communications line that travels on, near or below ground is terrestrial link. terrestrial is a ground station, or earth terminal designed for extraplanetary telecommunication with spacecraft, or reception of radio waves from an astronomical radio source. Ground stations are located either on the surface of the Earth or in its atmosphere. Earth stations communicate with spacecraft by transmitting and receiving radio waves in the super high frequency or extremely high frequency bands (e.g., microwaves). When a ground station successfully transmits radio waves to a spacecraft (or vice versa), it establishes a telecommunications link. A principal telecommunications device of the ground station is the parabolic antenna.

2. a. Define TCP/IP. Differentiate between IPV4 and IPV6. <2+6>

It's important to understand that IPv6 is much more than an extension of IPv4 addressing. IPv6, first defined in RFC 2460, is a complete implementation of the network layer of the TCP/IP protocol stack and it covers a lot more than simple address space extension from 32 to 128 bits (the mechanism that increases IPv6's ability to allocate almost unlimited addresses to all the devices in the world for years to come). IPv6 offers many improvements over IPv4, and Table 1 compares IPv4 and IPv6 operation at a glance.

Following are the list of differences between IPV4 and IPV6

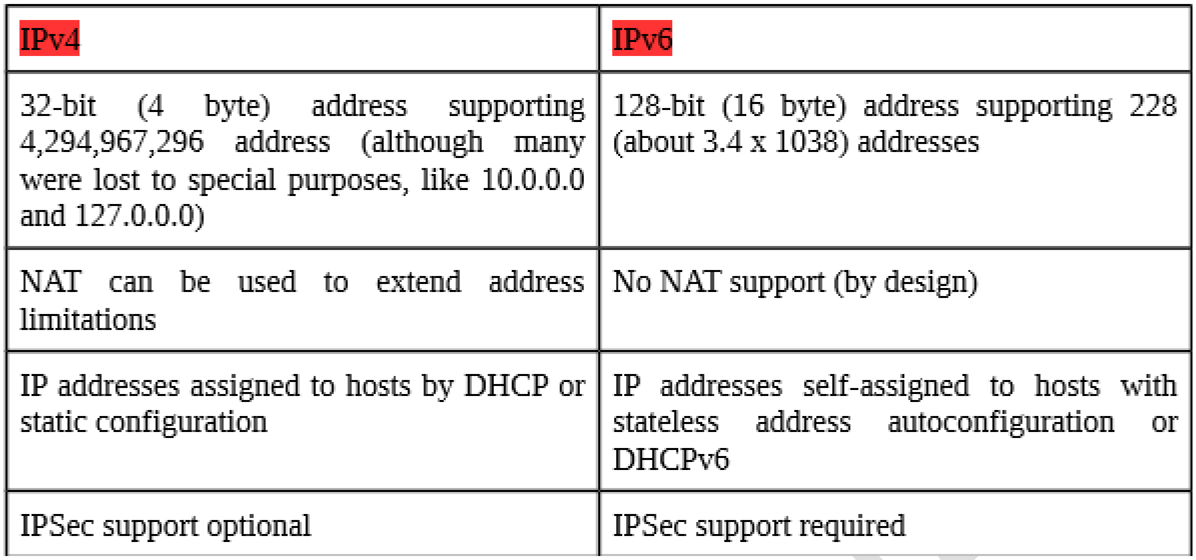
1. More efficient routing. IPv6 routers no longer have to fragment packets, an overhead-intensive process that just slows a network down.

2. Quality of service (QoS) built-in. IPv4 has no way to distinguish delay-sensitive packets from bulk data transfers, requiring extensive workarounds, but IPv6 does.

3. Elimination of NAT to extend address spaces. IPv6 increases the IPv4 address size from 32 bits (about 4 billion) to 128 bits (enough for every molecule in the solar system).

4. Network layer security built-in (IPsec). Security, always a challenge in IPv4, is an integral part of IPv6. Stateless address autoconfiguration for easier network administration. Many IPv4 „ installs were complicated by manual default router and address assignment. IPv6 handles this in an automated fashion.

5. Improved header structure with less processing overhead. Many of the fields in the IPv4 header were optional and used infrequently. IPv6 eliminates these fields (options are handled differently).



IPv4	IPv6
32-bit (4 byte) address supporting 4,294,967,296 address (although many were lost to special purposes, like 10.0.0.0 and 127.0.0.0)	128-bit (16 byte) address supporting 228 (about 3.4 x 1038) addresses
NAT can be used to extend address limitations	No NAT support (by design)
IP addresses assigned to hosts by DHCP or static configuration	IP addresses self-assigned to hosts with stateless address autoconfiguration or DHCPv6
IPSec support optional	IPSec support required

b. Explain internet RFCS. **<4>**

In computer network engineering, a Request for Comments (RFC) is a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems. They cover many aspects of computer networking, including protocols, procedures, programs, and concepts, as well as meeting notes, opinions, and sometimes humor. It began in 1969 as a set of working notes about ARPAnet research and development.

RFCs are numbered (roughly) consecutively, and these numbers provide a single unique label space for all RFCs. RFCs are published online through a number of repositories, and there is an online index of RFCs.

The most common meaning for the word standard on the Internet is probably 'current (i.e. nonobsoleted) RFC'. This isn't quite as rigorous a concept as it may sound. An Internet standard has, in addition to an RFC number, an STD number, which does not change even if the RFC number is changed; for example, the IP protocol is defined by STD 5 which is currently RFC 791. e.g.

RFC 792 — Internet Control Message Protocol

RFC 768 — User Datagram Protocol

RFC 793 — Transmission Control Protocol

RFC 959 — File Transfer Updated by RFC 2228,

RFC 2640 RFC 821 — Simple Mail Transfer Protocol

RFC 1034 — Domain names - concepts and facilities, Updated by RFC 2535, RFC 2308, RFC 2181, RFC 1982,RFC 1876, RFC 1348, RFC 1183, RFC 1101

RFC 974 — Mail routing and the domain system

RFC 1661 — The Point-to-Point Protocol

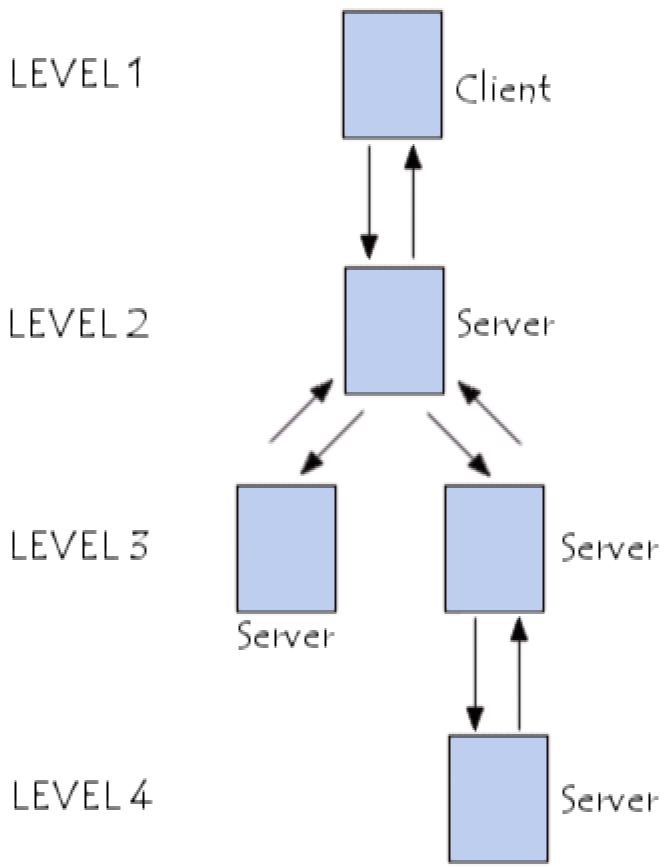
RFC 1939 — Post Office Protocol

Each RFC has a "category" or "status" designation. The possible categories are:

- STANDARD, DRAFT STANDARD, PROPOSED STANDARD:These are standardstrack documents, official specifications of the Internet protocol suite defined by the Internet Engineering Task Force (IETF) and its steering group the IESG.
- BEST CURRENT PRACTICE : These are official guidelines and recommendations, but not standards, from the IETF.
- INFORMATIONAL, EXPERIMENTAL :These non-standards documents may originate in the IETF or may be independent submissions.
- HISTORIC :These are former standards that have been actively deprecated

3.a. Explain the N-Tired Client/Server Architecture. <8>

N-tier architecture (with N more than 3) is really 3 tier architectures in which the middle tier is split up into new tiers. The application tier is broken down into separate parts. What these parts are differs from system to system. The following picture shows it:



The primary advantage of N-tier architectures is that they make load balancing possible. Since the application logic is distributed between several servers, processing can then be more evenly distributed among those servers. N-tiered architectures are also more easily scalable, since only servers experiencing high demand, such as the application server, need be upgraded. The primary disadvantage of N-tier architectures is that it is also more difficult to program and test an N-tier architecture due to its increased complexity.

b. Define the terms PGP and POP. **<4>**

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of email communications.

PGP is a public key encryption package to protect e-mail and data files. It lets you communicate securely with people you've never met, with no secure channels needed for prior exchange of keys. It's well featured and fast, with sophisticated key management, digital signatures, data compression, and good economic design . The actual operation of PGP is based on five services: authentication, confidentiality, compression, e-mail compatibility, and segmentation.

The Post Office Protocol (POP) is an application-layer Internet standard protocol used by local email clients to retrieve mail from a remote server over a TCP/IP connection. POP and IMAP (Internet Message Access Protocol) are the two most prevalent Internet standard protocols for email retrieval. Virtually all modern e-mail clients and servers support both. The POP protocol has been developed through several versions, with version 3 (POP3) being the current standard. Most webmail service providers such as Hotmail, Gmail and Yahoo! Mail also provide IMAP and POP3 service.

Like it seems everything on the internet, mail retrieval is a client-server application. The Post Office Protocol defines how your email client should talk to the POP server. The POP is a very simple protocol. This makes it easy to implement, has earned the Post Office Protocol widespread adoption and makes it very robust, but it also means the Post Office Protocol provides only basic functionality.

4. a. Define HTTP. Differentiate between HTML and DHTML. <2+6>

HTTP is the protocol to exchange or transfer hypertext. HyperText Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. HTTP is the framework for how browsers will display and use file formats. When you enter in a URL with HTTP at the beginning, you are requesting a web page which can contain other elements (such as pictures) and links to other resources. HTTP utilizes TCP port 80 by default, though other ports such as 8080 can alternatively be used.

HTML stands for HyperText Markup Language. It is a well known mark up language used to develop web pages. It has been around for a long time and is commonly used in webpage design. DHTML is essentially Dynamic HTML. It is a new way of looking at and controlling the standard HTML codes and commands. DHTML is a collection of technologies that are used to create interactive and animated web sites.

HTML

HTML stands for hypertext markup language. It is not a programming language. A markup language specifies the layout and style of a document. A markup language consists of a set of markup tags. HTML uses markup tags to describe web pages. HTML tags are keywords surrounded by angle brackets like <html>. Most HTML tags normally come in pairs like <b> and </b>. The first tag is called the start tag (or opening tag) and the second tag is called the end tag (or closing tag). HTML documents describe Web pages. HTML documents contain HTML tags and plain text. HTML documents are also called Web pages. A web browser read HTML documents and displays them as Web pages. The browser does not display the HTML tags, but uses the tags to interpret the content of the page.

DHTML:

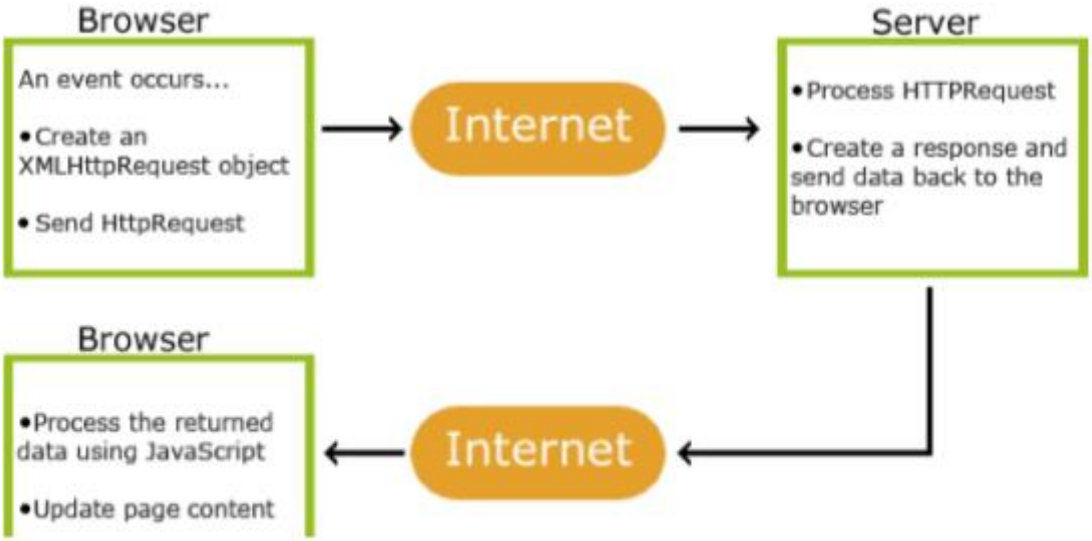
DHTML stands for Dynamic HTML. DHTML is the art of combining HTML, JavaScript, DOM, and CSS and is NOT a language or a web standard. According to the World Wide Web Consortium (W3C): "Dynamic HTML is a term used by some vendors to describe the combination of HTML, style sheets and scripts that allows documents to be animated."

DHTML is about using these features, to create dynamic and interactive web pages. DHTML allows authors to add effects to their pages without the overhead of server-side programs or complicated sets of controls to achieve special effects.For example, DHTML allows the page author to:

- Animate text and images in their document, independently moving each element from any starting point to any ending point, following a predetermined path or one chosen by the user.
- Embed a ticker that automatically refreshes its content with the latest news, stock quotes, or other data.

b. What do you mean by AJAX? **<4>**

Ajax (Asynchronous JavaScript and XML) is a group of interrelated web development techniques used on the client-side to create asynchronous web applications. With Ajax, web applications can send data to, and retrieve data from, a server asynchronously (in the background) without interfering with the display and behavior of the existing page. Data can be retrieved using the XMLHttpRequest object.


Browser
An event occurs...
•Create an XMLHttpRequest object
•Send HttpRequest
Internet
Server
•Process HTTPRequest
•Create a response and send data back to the browser
Browser
•Process the returned data using JavaScript
•Update page content
Internet

Ajax is not a single technology, but a group of technologies. HTML and CSS can be used in combination to markup and style information. The DOM is accessed with JavaScript to dynamically display, and to allow the user to interact with the information presented. JavaScript and the XMLHttpRequest object provide a method for exchanging data asynchronously between browser and server to avoid full page reloads.

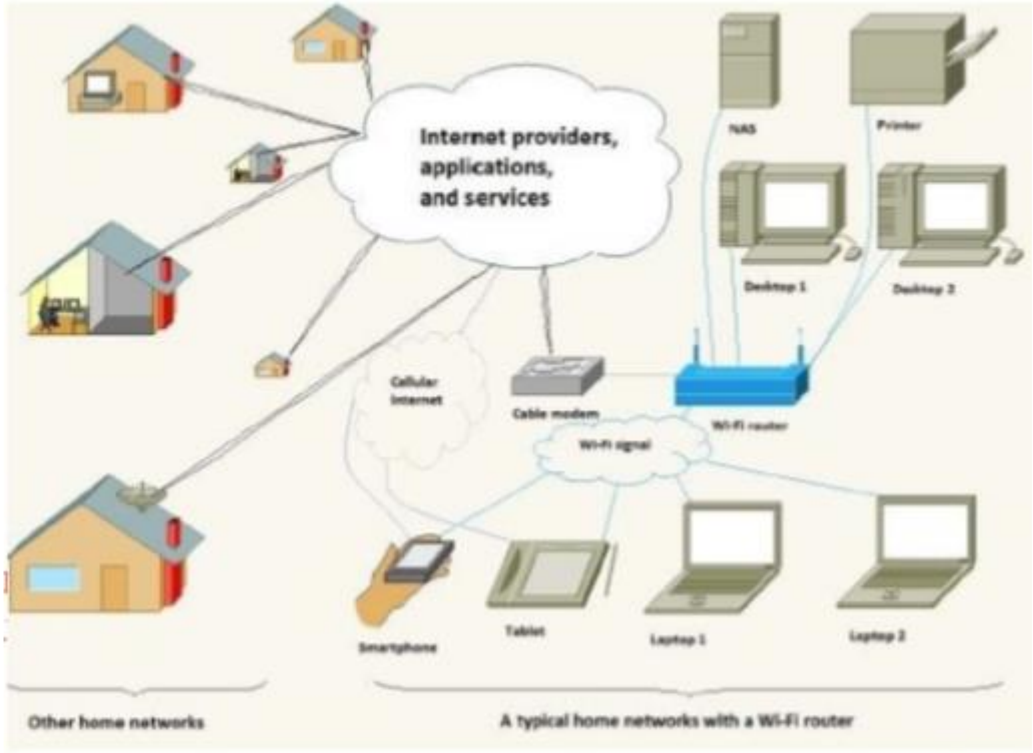
5. a. Explain the designing of Internet System network architecture. <8>

Internet architecture is by definition a meta-network, a constantly changing collection of thousands of individual networks intercommunicating with a common protocol. The Internet's architecture is described in its name, a short from of the compound word "inter-networking". Network Architecture is the complete framework of an organization's computer network. The diagram of the network architecture provides a full picture of the established network with detailed view of all the resources accessible. It includes hardware components used for communication, cabling and device types, network layout and topologies, physical and wireless connections, implemented areas and future plans. In addition, the software rules and protocols also constitute to the network architecture. This architecture is always designed by a network manager/administrator with coordination of network engineers and other design engineers.

In practice, the Internet technical architecture looks a bit like a multi-dimensional river system, with small rivers feeding medium-sized streams feeding large rivers.

The companies running the Internet backbone operate very high bandwidth networks relied on by governments, corporations, large organizations, and other Internet service providers. Their technical infrastructure often includes global connections through underwater cables and satellite links to enable communication between countries and continents. As always, a larger scale introduces new phenomena: the number of packets flowing through the switches on the backbone is so large that it exhibits the kind of complex non-linear patterns usually found in natural, analog systems like the flow of water or development of the rings of Saturn (RFC 3439, S2.2).

Each communication packet goes up the hierarchy of Internet networks as far as necessary to get to its destination network where local routing takes over to deliver it to the addressee. In the same way, each level in the hierarchy pays the next level for the bandwidth they use, and then the large backbone companies settle up with each other. Bandwidth is priced by large Internet service providers by several methods, such as at a fixed rate for constant availability of a certain number of megabits per second, or by a variety of use methods that amount to a cost per gigabyte. Due to economies of scale and efficiencies in management, bandwidth cost drops dramatically at the higher levels of the architecture.



some goals of internet architecture

● Fundamental Goal:

Effective technique for multiplexed utilization of existing interconnected networks.

● Secondary Goals:

○ Function despite loss of networks/gateways

○ Support multiple types of services

○ Accommodate a variety of networks

○ Distributed management of resources

○ Cost effective

○ Low level of effort to add a host

○ Provide accounting of resources used.

b. What do you mean by content filtering.

<4>

6. Explain the intranet implementation guidelines. What are the benefits and drawbacks of intranets. <8+4>

When planning an intranet, there are a number of questions to be considered. These questions will set the tone for how you go about developing your intranet, help you establish guidelines.

1. What is your business case for building the intranet?
2. Who can publish to the intranet?
3. What types of content can be published?

Steps:

1. Securing senior management support and funding.

2. Business requirements analysis.

3. Identify users' information needs.

4. Installation of web server and user access network.

5. Installing required user applications on computers.

6. Creation of document framework for the content to be hosted.

7. User involvement in testing and promoting use of intranet. 8. Ongoing measurement and evaluation, including through benchmarking against other intranets.

Advantages

1. Workforce productivity

2. Time

3. Communication

4. Web publishing

5. Business operations and management

6. Cost-effective:

7. Enhance collaboration

8. Cross-platform capability

9. Built for one audience

10.Promote common corporate culture

11. Immediate updates

12.Supports a distributed computing architecture:

Drawbacks of intranet

1. it is an evolving technology that requires upgrades and could have software incompatibility problems

2. security features can be inadequate

3. inadequate system performance management and poor user support

4. may not scale up adequately

5. maintaining content can be time consuming

6. some employees may not have PCs at their desks

7. The aims of the organization in developing an intranet may not align with user needs

7. Write short notes on <any three> : <4*3=12>

a.IMAP

IMAP (Internet Message Access Protocol) is a standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP Version 4) is a client/server protocol in which email is received and held for you by your Internet server. You (or your e-mail client) can view just the heading and the sender of the letter and then decide whether to download the mail. You can also create and manipulate multiple folders or mailboxes on the server, delete messages, or search for certain parts or an entire note. IMAP requires continual access to the server during the time that you are working with your mail.

b.RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. Network access servers, the gateways that control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server.[3] RADIUS is often the back-end of choice for 802.1X authentication as well.

c.VPN

VPNs, or Virtual Private Networks, allow users to securely access a private network and share data remotely through public networks. Much like a firewall protects your data on your computer, VPNs protect it online.

d.IRC

Internet Relay Chat (IRC) is an application layer protocol that facilitates the transfer of messages in the form of text. The chat process works on a client/server networking model. IRC clients are computer programs that a user can install on their system. These clients communicate with chat servers to transfer messages to other clients. IRC is mainly designed for group communication in discussion forums, called channels, but also allows one-on-one communication via private messages as well as chat and data transfer, including file sharing.

e.Cloud Computing

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. Although cloud computing has changed over time, it has always been divided into three broad service categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as service (SaaS).

Tribhuwan University

Institute of Science and Technology

2070

Full Marks : 60

Internet Technology **Pass Marks :24**

Time : 3 hours

New Course

Candidates are required to give their answers in their own words as far as practicable. The figures in the margin indicate full marks.

1.) How does satellite link work? What are the advantages using satellite as communications ?

2.) What do you mean by internet protocol suite ? Discuss about the IP heads.

The Internet protocol suite is the set of communications protocols used for the Internet and similar networks, and generally the most popular protocol stack for wide area networks. It is commonly known as TCP/IP, because of its most important protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP), which were the first networking protocols defined in this standard TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. It has four abstraction layers, each with its own protocols.

IP Heads

Version Number

The version number indicates the version of IP that is in use for this packet. IP version 4 (Ipv4) is currently in widespread use.

Header Length

The header length indicates the overall length of the header. The receiving machine then knows when to stop reading the header and start reading data.

Type of Service

Mostly unused, the Type of Service field indicates the importance of the packet in a numerical value. Higher numbers result in prioritized handling.

Total Length

Total length shows the total length of the packet in bytes. The total packet length cannot exceed 65,535 bytes or it will be deemed corrupt by the receiver.

Identification

If there is more than one packet (an invariable inevitability), the identification field has an identifier that identifies its place in line, as it were. Fragmented packets retain their original ID number.

Flags

The first flag, if set, is ignored. If the DF (Do Not Fragment) flag is set, under no circumstances can the packet be fragmented. If the MF (More Fragments) bit is turned on (1), there are packet fragments to come, the last of which is set to off (0).

Offset

If the Flag field returns a 1 (on), the Offset field contains the location of the missing piece(s) indicated by a numerical offset based on the total length of the packet.

Time To Live (TTL)

Typically 15 to 30 seconds, TTL indicates the length of time that a packet is allowed to remain in transit. If a packet is discarded or lost in transit, an indicator is sent back to the sending computer that the loss occurred. The sending machine then has the option of resending that packet.

Protocol

The protocol field holds a numerical value indicating the handling protocol in use for this packet.

Checksum

The checksum value acts as a validation checksum for the header.

Source Address

The source address field indicates the address of the sending machine.

Destination Address

The destination address field indicates the address of the destination machine.

Options and Padding

The Options field is optional. If used, it contains codes that indicate the use of security, strict or loose source routing, routing records, and timestamping. If no options are used, the field is called padded and contains a 1. Padding is used to force a byte value that is rounded.

3.) What are the main services provided by PGP protocol? How those consume in mail application?

PGP provides authentication via a digital signature scheme.

- PGP provides confidentiality by encrypting messages before transmission using RSA schemes.
- PGP compresses the message after applying the signature and before encryption. The idea is to save space.
- PGP encrypts a message together with the signature (if not sent separately) resulting into a stream of arbitrary 8-bit octets. But since many e-mail systems permit only use of blocks consisting of ASCII text, PGP accommodates this by converting the raw 8-bit binary streams into streams of printable ASCII characters using a radix-64 conversion scheme. On receipt,

the block is converted back from radix-64 format to binary. To accommodate e-mail size restrictions, PGP automatically segments email messages that are too long. However, the segmentation is done after all the housekeeping is done on the message, just before transmitting it. So the session key and signature appear only once at the beginning of the first segment transmitted. At receipt, the receiving PGP strips off all e-mail headers and reassemble the original mail.

4.) What is VPN tunnel? Illustrate the principle of VPN client-server interaction with an example.

The following steps illustrate the principles of a VPN client-server interaction in simple terms; Assume a remote host with public IP address 1.2.3.4 wishes to connect to a server found inside a company network. The server has internal address 192.168.1.10 and is not reachable publicly. Before the client can reach this server, it needs to go through a VPN server / firewall device that has public IP address 5.6.7.8 and an internal address of 192.168.1.1. All data between the client and the server will need to be kept confidential; hence a secure VPN is used.

1. The VPN client connects to a VPN server via an external network interface.
2. The VPN server assigns an IP address to the VPN client from the VPN server's subnet. The client gets internal IP address 192.168.1.50, for example, and creates a virtual network interface through which it will send encrypted packets to the other tunnel endpoint (the device at the other end of the tunnel). (This interface also gets the address 192.168.1.50.)
3. When the VPN client wishes to communicate with the company server, it prepares a packet addressed to 192.168.1.10, encrypts it and encapsulates it in an outer VPN packet, say an IPSec packet. This packet is then sent to the VPN server at IP address 5.6.7.8 over the public Internet. The inner packet is encrypted so that even if someone intercepts the packet over the Internet, they cannot get any information from it. They can see that the remote host is communicating with a server/firewall, but none of the contents of the communication. The inner encrypted packet has source address 192.168.1.50 and destination

address 192.168.1.10. The outer packet has source address 1.2.3.4 and destination address 5.6.7.8.

4. When the packet reaches the VPN server from the Internet, the VPN server unencapsulates the inner packet, decrypts it, finds the destination address to be 192.168.1.10, and forwards it to the intended server at 192.168.1.10.
5. After some time, the VPN server receives a reply packet from 192.168.1.10, intended for 192.168.1.50. The VPN server consults its routing table, and sees this packet is intended for a remote host that must go through VPN.
6. The VPN server encrypts this reply packet, encapsulates it in a VPN packet and sends it out over the Internet. The inner encrypted packet has source address 192.168.1.10 and destination address 192.168.1.50. The outer VPN packet has source address 5.6.7.8 and destination address 1.2.3.4.
7. The remote host receives the packet. The VPN client encapsulates the inner packet, decrypts it, and passes it to the appropriate software at upper layers.

Overall, it is as if the remote computer and company server are on the same 192.168.1.0/24 network.

5.) Describe the XML usage in web. What an XML element can contain, show with an example.

Extensible Markup Language (XML) is used to describe data. The XML standard is a flexible way to create information formats and electronically share structured data via the public Internet, as well as via corporate networks.XML code, a formal recommendation from the World Wide Web Consortium (W3C), is similar to Hypertext Markup Language (HTML). Both XML and HTML contain markup symbols to describe page or file contents. HTML code describes Web page content (mainly text and graphic images) only in terms of how it is to be displayed and interacted with.

XML data is known as self-describing or self-defining, meaning that the structure of the data is embedded with the data, thus when the data arrives there is no need to pre-build the structure to store the data; it is dynamically understood within the XML. The XML format can be used by any individual or group of individuals or companies that want to share information in a consistent way. XML is actually a simpler and easier-to-use subset of the Standard Generalized Markup Language (SGML), which is the standard to create a document structure. XML's power resides in its simplicity. It can take large chunks of information and consolidate them into an XML document - meaningful pieces that provide structure and organization to the information.

An XML element is everything from (including) the element's start tag to (including) the element's end tag.An element can contain:

- other elements
- text
- attributes
- or a mix of all of the above...

Example:

```
<bookstore>
          <book category="CHILDREN">
              <title>Harry Potter</title>
             <author>J K. Rowling</author>
             <year>2005</year>
           <price>29.99</price>
        </book>
        <book category="WEB">
              <title>Learning XML</title>
             <author>Erik T. Ray</author>
             <year>2003</year>
              <price>39.95</price>
         </book>
</bookstore>
```

In the example above, <bookstore> and <book> have element contents, because they contain other elements. <book> also has an attribute (category="CHILDREN"). <title>, <author>, <year>, and <price> have text content because they contain text.

6.) What do you mean by universal naming conventions? Given a URL string “http:mail.google.com/?shva=index#inbox”. Now identify schema name hierarchical part, query & fragment in the string.

Universal Naming Convention or Uniform Naming Convention, specifies a common syntax to describe the location of a network resource, such as a shared file, directory, or printer. The UNC syntax for Windows systems has the generic form:\\ComputerName\SharedFolder\Resource http[s]://HostName[:Port]/SharedFolder/Resource

7.) How an AJAX program gets executed? Discuss the steps of AJAX operations. Show with eg. How can we create XML http report object?

Ajax is not a single technology, but a group of technologies. HTML and CSS can be used in combination to mark up and style information. The DOM is accessed with JavaScript to dynamically display, and to allow the user to interact with the information presented. JavaScript and the XMLHttpRequest object provide a method for exchanging data asynchronously between browser and server to avoid full page reloads.

Steps of AJAX Operation

1. A client event occurs
2. An XMLHttpRequest object is created
3. The XMLHttpRequest object is configured
4. The XMLHttpRequest object makes an asynchronous request to the Webserver.
5. Webserver returns the result containing XML document.
6. The XMLHttpRequest object calls the callback() function and processes the result.
7. The HTML DOM is updated

The XMLHttpRequest Object

All modern browsers support the XMLHttpRequest object (IE5 and IE6 use an ActiveXObject). The XMLHttpRequest object is used to exchange data with a server behind the scenes. This means that it is possible to update parts of a web page, without reloading the whole page. All modern browsers (IE7+, Firefox, Chrome, Safari, and Opera) have a built-in XMLHttpRequest object.

Syntax for creating an XMLHttpRequest object:

```
variable=new XMLHttpRequest();
```

Old versions of Internet Explorer (IE5 and IE6) uses an ActiveX Object:

```
variable=new ActiveXObject("Microsoft.XMLHTTP");
```

To handle all modern browsers, including IE5 and IE6, check if the browser supports the XMLHttpRequest object. If it does, create an XMLHttpRequest object, if not, create an ActiveXObjec

The XMLHttpRequest object is used to exchange data with a server.

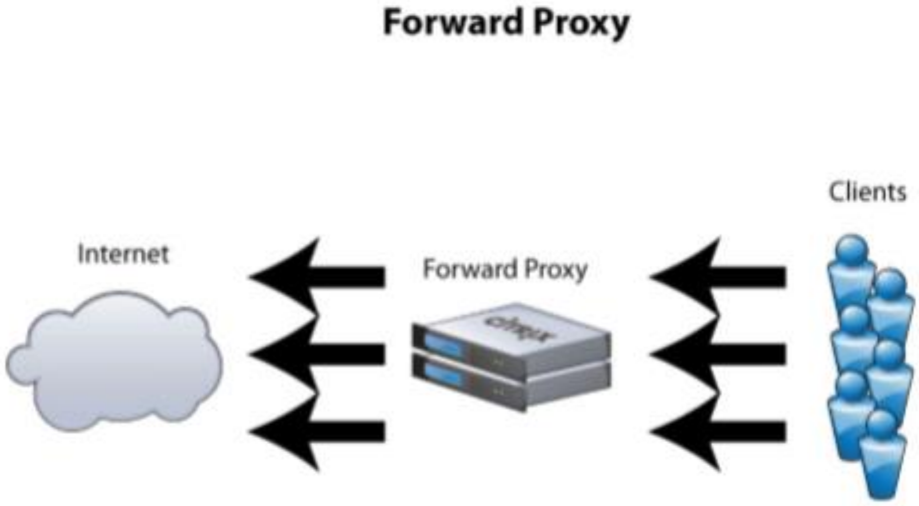
8.) What are the proxy servers? Differentiate each of open, forward and reverse proxy servers.

In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server. The proxy server evaluates the request as a way to simplify and control their complexity. Today, most proxies are web proxies, facilitating access to content on the World Wide Web.

Forward proxies

A forward proxies are those taking requests from an internal network and forwarding them to the Internet. Forward proxies are proxies where the client server names the target server to connect to. Forward proxies are able to retrieve from a wide range of sources (in most cases anywhere on the Internet).

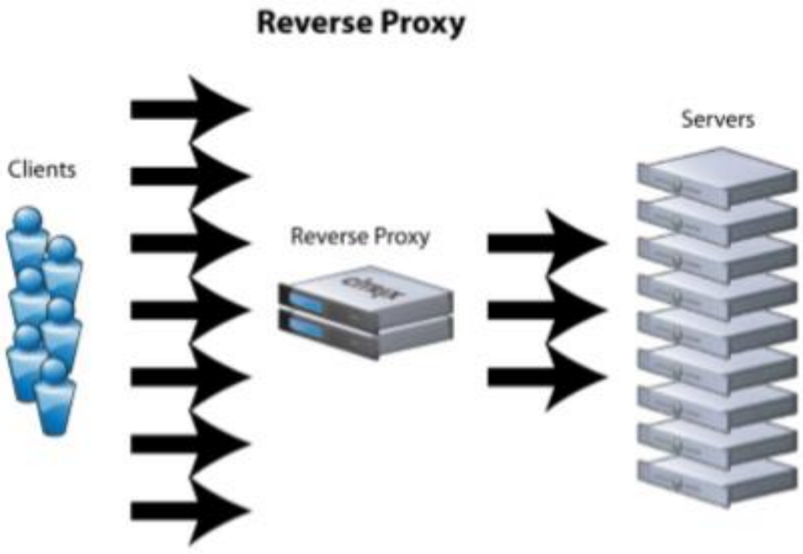
The terms "forward proxy" and "forwarding proxy" are a general description of behavior (forwarding traffic) and thus ambiguous. Except for Reverse proxy, the types of proxies described in this article are more specialized sub-types of the general forward proxy concept.



Reverse proxies

A reverse proxy is one taking requests from the Internet and forwarding them to servers in an internal network. Those making requests connect to the proxy and may not be aware of the internal network. A reverse proxy (or surrogate) is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more origin servers which handle the request. The response is returned as if it came directly from the web server.

Reverse proxies are installed in the neighborhood of one or more web servers. All traffic coming from the Internet and with a destination of one of the neighborhood's web servers goes through the proxy server. The use of "reverse" originates in its counterpart "forward proxy" since the reverse proxy sits closer to the web server and serves only a restricted set of websites.



9.) Define working mechanism of VOIP ? How undefined message benefits the communication systems?

VoIP stands for 'V'oice 'o'ver 'I'nternet 'P'rotocol. As the term says VoIP tries to let go voice (mainly human) through IP packets and, in definitive through Internet. VoIP can use accelerating hardware to achieve this purpose and can also be used in a PC environment.Many years ago we discovered that sending a signal to a remote destination could have be done also in a digital fashion: before sending it we have to digitalize it with an ADC (analog to digital converter), transmit it, and at the end transform it again in analog format with DAC (digital to analog converter) to use it. VoIP works like that, digitalizing voice in data packets, sending them and reconverting them in voice at destination.

Digital format can be better controlled: we can compress it, route it, convert it to a new better format, and so on; also we saw that digital signal is more noise tolerant than the analog one (see GSM vs TACS).

TCP/IP networks are made of IP packets containing a header (to control communication) and a payload to transport data: VoIP use it to go across the network and come to destination.

with VoIP mechanism you can talk all the time with every person you want (the needed is that other person is also connected to Internet at the same time), as far as you want (money independent) and, in addition, you can talk with many people at the same time.

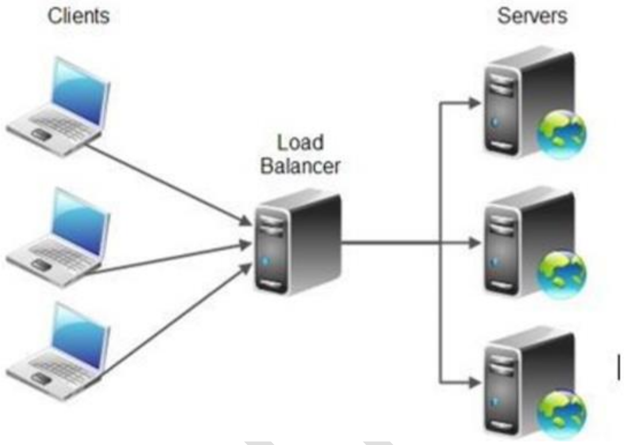
If you're still not persuaded you can consider that, at the same time, you can exchange data with people are you talking with, sending images, graphs and videos.

Then, why everybody doesn't use it yet?

Unfortunately we have to report some problem with the integration between VoIP architecture and Internet. As you can easy imagine, voice data communication must be a real time stream (you couldn't speak, wait for many seconds, then hear other side answering): this is in contrast with the Internet heterogeneous architecture that can be made of many routers (machines that route packets), about 20-30 or more and can have a very high round trip time (RTT), so we need to modify something to get it properly working.

10.) Why load balancing is needed in servers? How WRR allocation for load balancing differs from dynamic round robin allocation?

Load balancing is a method for distributing tasks onto multiple computers. For instance, distributing incoming HTTP requests (tasks) for a web application onto multiple web servers. There are a few different ways to implement load balancing. I will explain some common load balancing schemes in this text. Here is a diagram illustrating the basic principle of load balancing:



The primary purpose of load balancing is to distribute the workload of an application onto multiple computers, so the application can process a higher workload. Load balancing is a way to scale an application.

A secondary goal of load balancing is often (but not always) to provide redundancy in your application. That is, if one server in a cluster of servers fails, the load balancer can temporarily remove that server from the cluster, and divide the load onto the functioning servers. Having multiple servers help each other in this way is typically called "redundancy". When an error happens and the tasks is moved from the failing server to a functioning server, this is typically called "failover".A set of servers running the same application in cooperation is typically referred to as a "cluster" of servers. The purpose of a cluster is typically both of the above two mentioned goals: To distribute load onto different servers, and to provide redundancy / failover for each other.

Applications

Use in telecommunications

Shortest Path Bridging

Routing

Tribhuwan University

Institute of Science and Technology

2071

Full Marks : 60

Internet Technology **Pass Marks :24**

Time : 3 hours

New Course

Candidates are required to give their answers in their own words as far as practicable. The figures in the margin indicate full marks.

Attempt any five questions.

1. a. Explain the history and development of Internets and Intranets.

Answer:

1957 –USA creates the Advanced Research Projects Agency (ARPA)

1972 - Ray Tomlinson creates the first program devoted to email. 1972 - ARPA officially changes its name to DARPA 1972 - Network Control Protocol is introduced 1974 - Term Internet was introduced for the first time. 1976 – Elizabeth II, Queen of the United Kingdom, sends out an email

1983 - TCP/IP becomes the standard for internet protocol. 1984- The number of Hosts breaks 1,000 1989- The Number of hosts breaks 100 000 1989- Arpanet ceases to exist 1990- The first search engine is created, Archie Search Engine

1991 – WWW published 1992- Number of hosts breaks 1,000,000 1993- The first web browser, Mosaic 1994 - First internet ordering system created by Pizza Hut. 1994 - First internet bank opened: First Virtual. 1996 - Nokia releases first cell phone with internet access.

2001 - Blackberry releases first internet cell phone in the United States. 2001 – The spread of P2P file sharing across the Internet 2005- Estonia offers Internet Voting nationally for local elections 2005-Youtube launches 2006- There are an estimated 92 million websites online 2009 The Internet marks its 40th anniversary. 2010 China Dominates Internet Usage 2010 there are over 450 million Chinese Internet users 2012 Facebook reaches 1 billion monthly active users 2014 45% of internet users ages 18-29 in serious relationships

b. Explain the Domain Name system and its uses.

2.

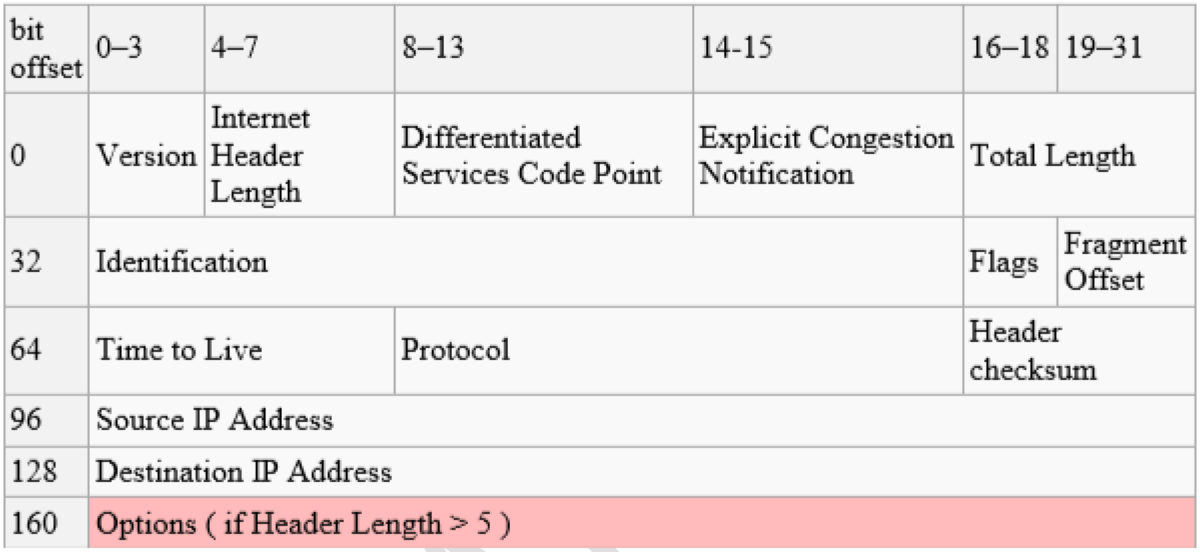
a. Discuss the IP layer and its importance.

b. Explain the IPv4 and IPv6 with header structure.

IPV4 Header Structure:

The IPv4 packet header consists of 14 fields, of which 13 are required. The 14th field is optional (red background in table) and aptly named: options. The fields in the header are packed with the most significant byte first (big endian), and for the diagram and discussion, the most significant bits are considered to come first (MSB 0 bit numbering).

The most significant bit is numbered 0, so the version field is actually found in the four most significant bits of the first byte, for example.



bit offset	0–3	4–7	8–13	14-15	16–18	19–31
0	Version	Internet Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length	
32	Identification				Flags	Fragment Offset
64	Time to Live		Protocol		Header checksum	
96	Source IP Address					
128	Destination IP Address					
160	Options (if Header Length > 5)					

Version :

The first header field in an IP packet is the four-bit version field. For IPv4, this has a value of 4 (hence the name IPv4).

Internet Header Length (IHL):

The second field (4 bits) is the Internet Header Length (IHL), which is the number of 32-bit words in the header.

Differentiated Services Code Point (DSCP):

Originally defined as the Type of Service field, this field is now defined by RFC 2474 for Differentiated services (DiffServ). New technologies are emerging that require real-time data streaming and therefore make use of the DSCP field. An example is Voice over IP (VoIP), which is used for interactive data voice exchange.

Explicit Congestion Notification (ECN): This field is defined in RFC 3168 and allows end-to-end notification of network congestion without dropping packets. ECN is an optional feature that is only used when both endpoints support it and are willing to use it. It is only effective when supported by the underlying network.

Total Length: This 16-bit field defines the entire packet (fragment) size, including header and data, in bytes. The minimum-length packet is 20 bytes (20-byte header + 0 bytes data) and the maximum is 65,535 bytes — the maximum value of a 16-bit word. The largestdatagram that any host is required to be able to reassemble is 576 bytes, but most modern hosts handle much larger packets. Sometimes subnetworks impose further restrictions on the packet size, in which case datagrams must be fragmented. Fragmentation is handled in either the host or router in IPv4.

Identification: This field is an identification field and is primarily used for uniquely identifying fragments of an original IP datagram. Some experimental work has suggested using the ID field for other purposes, such as for adding packet-tracing information to help trace datagrams with spoofed source addresses.

Flags; A three-bit field follows and is used to control or identify fragments. They are (in order, from high order to low order):

 bit 0: Reserved; must be zero. bit 1: Don't Fragment (DF) bit 2: More Fragments (MF) If the DF flag is set, and fragmentation is required to route the packet, then the packet is dropped. This can be used when sending packets to a host that does not have sufficient resources to handle fragmentation. It can also be used for Path MTU Discovery, either automatically by the host IP software, or manually using diagnostic tools such as ping or traceroute.

For unfragmented packets, the MF flag is cleared. For fragmented packets, all fragments except the last have the MF flag set. The last fragment has a non-zero Fragment Offset field, differentiating it from an unfragmented packet.

Fragment Offset: The fragment offset field, measured in units of eight-byte blocks, is 13 bits long and specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram. The first fragment has an offset of zero. This allows a maximum offset of (213 – 1) × 8 = 65,528 bytes, which would exceed the maximum IP packet length of 65,535 bytes with the header length included (65,528 + 20 = 65,548 bytes).

Time To Live (TTL): An eight-bit time to live field helps prevent datagrams from persisting (e.g. going in circles) on an internet. This field limits a datagram's lifetime. It is specified in seconds, but time intervals less than 1 second are rounded up to 1. In practice, the field has become a hop count—when the datagram arrives at a router, the router decrements the TTL field by one. When the TTL field hits zero, the router discards the packet and typically sends a ICMP Time Exceeded message to the sender.

The program traceroute uses these ICMP Time Exceeded messages to print the routers used by packets to go from the source to the destination.

Protocol: This field defines the protocol used in the data portion of the IP datagram. The Internet Assigned Numbers Authority maintains a list of IP protocol numbers which was originally defined in RFC 790.

Header Checksum: The 16-bit checksum field is used for error-checking of the header. When a packet arrives at a router, the router calculates the checksum of the header and compares it to the checksum field. If the values do not match, the router discards the packet. Errors in the data field must be handled by the encapsulated protocol. Both UDP and TCP have checksum fields. When a packet arrives at a router, the router decreases the TTL field. Consequently, the router must calculate a new checksum. RFC 1071 defines the checksum calculation:

The checksum field is the 16-bit one's complement of the one's complement sum of all 16bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero. For example, consider Hex 4500003044224000800600008c7c19acae241e2b (20 bytes IP header):

Step 1. 4500 + 0030 + 4422 + 4000 + 8006 + 0000 + 8c7c + 19ac + ae24 + 1e2b = 2BBCF (16-bit sum) Step 2. 2 + BBCF = BBD1 = 1011101111010001 (1's complement 16-bit sum) Step 3. ~BBD1 = 0100010000101110 = 442E (1's complement of 1's complement 16-bit sum)

To validate a header's checksum the same algorithm may be used - the checksum of a header which contains a correct checksum field is a word containing all zeros (value 0):

2BBCF + 442E = 2FFFD. 2 + FFFD = FFFF. the 1'S of FFFF = 0.

Source address: This field is the IPv4 address of the sender of the packet. Note that this address may be changed in transit by a network address translation device.

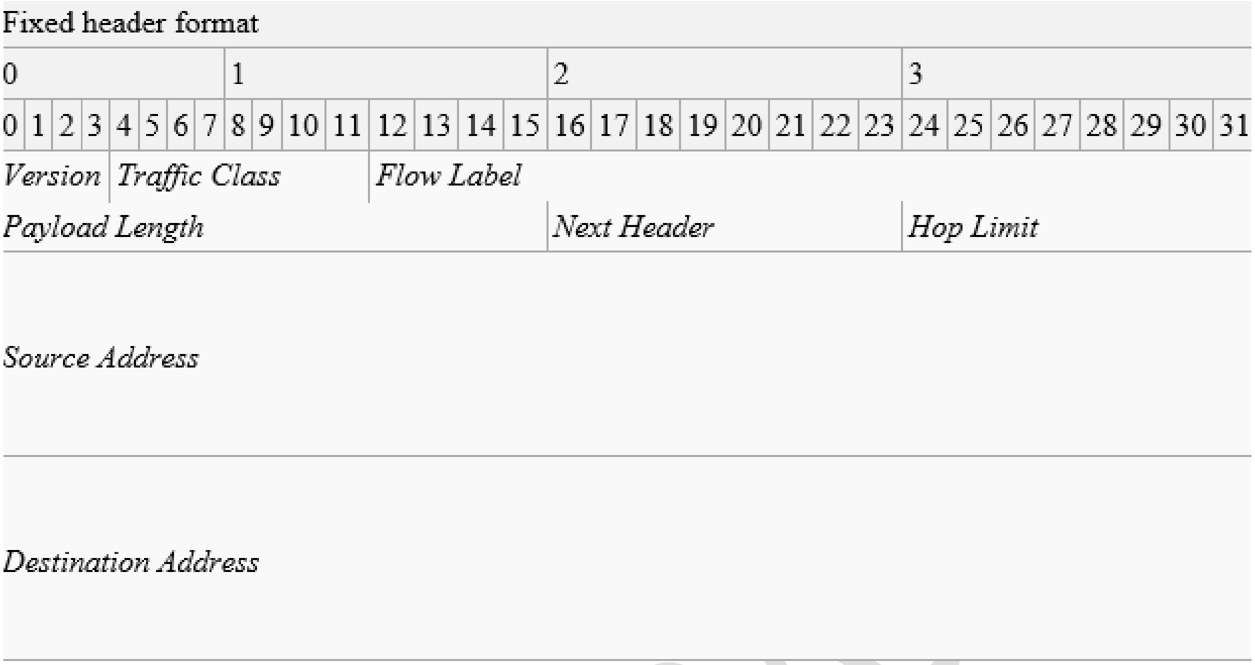
Destination address: This field is the IPv4 address of the receiver of the packet. As with the source address, this may be changed in transit by a network address translation device.

Options: The options field is not often used. Note that the value in the IHL field must include enough extra 32-bit words to hold all the options (plus any padding needed to ensure that the header contains an integral number of 32-bit words). The list of options may be terminated with an EOL (End of Options List, 0x00) option; this is only necessary if the end of the options would not otherwise coincide with the end of the header.

IPV6 Header Structure:

IPv6 specifies a new packet format, designed to minimize packet header processing by routers. Because the headers of IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable. However, in most respects, IPv6 is a conservative extension of IPv4. Most transport and application-layer protocols need little or no change to operate over IPv6; exceptions are application protocols that embed internet-layer addresses, such as FTP and NTPv3, where the new address format may cause conflicts with existing protocol syntax.

The fixed header of an IPv6 packet consists of its first 40 octets (320 bits). It has the following format:



<table>
<tr><td colspan="32">Fixed header format</td></tr>
<tr><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="4"><i>Version</i></td><td colspan="8"><i>Traffic Class</i></td><td colspan="20"><i>Flow Label</i></td></tr>
<tr><td colspan="16"><i>Payload Length</i></td><td colspan="8"><i>Next Header</i></td><td colspan="8"><i>Hop Limit</i></td></tr>
<tr><td colspan="32"><i>Source Address</i></td></tr>
<tr><td colspan="32"><i>Destination Address</i></td></tr>
</table>

Version (4 bits):

The constant 6 (bit sequence 0110).

Traffic Class (8 bits):

The bits of this field hold two values. The 6 most-significant bits are used for DSCP, which is used to classify packets. The remaining two bits are used for ECN; priority values subdivide into ranges: traffic where the source provides congestion control and non-congestion control traffic.

Flow Label (20 bits):

Originally created for giving real-time applications special service. Flow Label specifications and minimum requirements are described, and first uses of this field are emerging.

Payload Length (16 bits):

The size of the payload in octets, including any extension headers. The length is set to zero when a Hop-by-Hop extension header carries a Jumbo Payload option.

Next Header (8 bits):

Specifies the type of the next header. This field usually specifies the transport layer protocol used by a packet's payload. When extension headers are present in the packet this field indicates which extension header follows. The values are shared with those used for the IPv4 protocol field, as both fields have the same function

Hop Limit (8 bits):

Replaces the time to live field of IPv4. This value is decremented by one at each intermediate node visited by the packet. When the counter reaches 0 the packet is discarded.

Source Address (128 bits):

The IPv6 address of the sending node.

Destination Address (128 bits):

The IPv6 address of the destination node(s).

3.

a. Explain the Universal Internet Browsing.

b. Mention the different types of protocols and compare them.

4. a. Differentiate between WML and XML.

XML and WML both use the same markup / language. If you know XML, you know WML - and vice versa. However, XML is intentionally developed for computers, or other devices with larger screens. WML is developed for smaller-screened devices, such as PDA's and cell phones. Regardless, most devices, small or large screen'ed, now accept both formats of the XML language without complaining - but users may notice a difference in layout. On the technical side of things, WML standards branch off XML standards (which determine how things should be layed out on a screen or other display) - making the standards relatively different. WML is placed in WML-type documents ("file.wml"), as XML is placed in XML-type documents ("file.xml"). WML documents should have a Document Type Declaration pointing to an WML standard, as XML documents should have a Document Type Declaration pointing to an XML standard.

XML is designed to transport and store data. XML stands for EXtensible Markup Language and is much like HTML. XML was designed to carry data, not to display data. XML tags are not predefined. we must define your own tags. XML is designed to be self-descriptive. Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

XML is not a replacement for HTML OR WML . XML and HTML were designed with different goal. XML was designed to transport and store data, with focus on what data is.

b. Explain the WYS/WYG Authoring tools.

The somehow cryptic abbreviation WYSIWYG stands for “What You See Is What You Get”. In such editors you edit not directly the source code of your documents, but its presentation as it (hopefully) will appear in the final document. So instead of writing blocks of code manually (as you e.g. would do it in Word or Latex), you manipulate with design components using an editor window. This means that you view something very similar to the end result while the document or image is being created. Many of these editors do not require any knowledge of the programming languages generated by the software., generally simpler WYSIWYG editors are designed to work directly with HTML files. Exported files tend to be larger than hand-coded pages (those produced with a text-based HTML editor or a plain text editor). WYSIWYG generators tend to be better than word processors at producing highly graphical and interactive pages. Some of the WYS/WYG tools are

- ASP.NET Web Matrix
- Adobe Dreamweaver (formerly Macromedia Dreamweaver)
- Amaya - Microsoft Visual Studio
- Microsoft Visual Web Developer Express

5. a. Explain the load balancing and its applications.

Load balancing is a method for distributing tasks onto multiple computers. For instance, distributing incoming HTTP requests (tasks) for a web application onto multiple web servers. There are a few different ways to implement load balancing. I will explain some common load balancing schemes in this text. Here is a diagram illustrating the basic principle of load balancing:

The primary purpose of load balancing is to distribute the workload of an application onto multiple computers, so the application can process a higher workload. Load balancing is a way to scale an application.

A secondary goal of load balancing is often (but not always) to provide redundancy in your application. That is, if one server in a cluster of servers fails, the load balancer can temporarily remove that server from the cluster, and divide the load onto the functioning servers. Having multiple servers help each other in this way is typically called "redundancy". When an error happens and the tasks is moved from the failing server to a functioning server, this is typically called "failover".A set of servers running the same application in cooperation is typically referred to as a "cluster" of servers. The purpose of a cluster is typically both of the above two mentioned goals: To distribute load onto different servers, and to provide redundancy / failover for each other.

Applications

Use in telecommunications

Shortest Path Bridging

Routing

b. Define the cookies.

A cookie, also known as an HTTP cookie, web cookie, or browser cookie, is usually a small piece of data sent from a website and stored in a user's web browser while a user is browsing a website. When the user browses the same website in the future, the data stored in the cookie can be retrieved by the website to notify the website of the user's previous activity. Cookies were designed to be a reliable mechanism for websites to remember the state of the website or activity the user had taken in the past. This can include clicking particular buttons, logging in, or a record of which pages were visited by the user even months or years ago.

Perhaps most importantly, authentication cookies are the most common method used by web servers to know whether the user is logged in or not, and which account they are logged in under. Without such a mechanism, the site would not know whether to send a page containing sensitive information, or require the user to authenticate himself by logging-in. The security of an authentication cookie generally depends on the security of the issuing website and the user's web browser. If not implemented correctly, a cookie's data can be intercepted by a hacker to gain unapproved access to the user's data and possibly to the originating website.

Cookies are arbitrary pieces of data chosen by the Web server and sent to the browser. The browser returns them unchanged to the server, introducing a state (memory of previous events) into otherwise stateless HTTP transactions. Without cookies, each retrieval of a Web page or component of a Web page is an isolated event, mostly unrelated to all other views of the pages of the same site. Other than being set by a web server, cookies can also be set by a script in a language such as JavaScript, if supported and enabled by the Web browser. The cookies consist of several values;

Types of cookie

1. Session cookie

2. Persistent cookie

3. Secure cookie

4. HttpOnly cookie

5. Third-party cookie

6. Supercookie

7. Zombie cookie

6. a. Explain the tunneling protocols with example.

A tunneling protocol is the one utilized by computer networks in cases where the network protocol or the delivery protocol encapsulates an unsuited payload protocol at a peer level or lower than it. The protocol is termed as such because this appears as if it makes its way through the various types of packets. It is sometimes recognized with the name “encapsulation protocol" but this label is very vague for the reason that there are other network protocols which are also designed to perform the process of encapsulation.

Tunneling protocol is widely used in transmitting large amounts of protocols through the typical networks. In addition, it may serve as a medium for transferring virtual private networks (VPNs) that are already encrypted.This protocol comes as an advantage since tunneling may be employed in transporting a payload over the mismatched delivery-network. Tunneling protocol is also helpful when it comes to presentation of a safe passageway over a suspicious-looking network.

In common cases, tunneling may differ with some other forms of layered protocol including TCP/IP and OSI. There are times when a delivery protocol functions at a more advanced level in the model compared to that of a payload protocol. Rarely, however, does both the delivery and payload protocol work at similar level.

b. What are the benefits and drawbacks of internet?

The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (often called TCP/IP, although not all applications use TCP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies.

Advantages

1. Workforce productivity

2. Time

3. Communication

4. Web publishing

5. Business operations and management

6. Cost-effective:

7. Enhance collaboration

8. Cross-platform capability

9. Built for one audience

10.Promote common corporate culture

11. Immediate updates

12.Supports a distributed computing architecture:

Drawbacks of intranet

1. it is an evolving technology that requires upgrades and could have software incompatibility problems

2. security features can be inadequate

3. inadequate system performance management and poor user support

4. may not scale up adequately

5. maintaining content can be time consuming

6. some employees may not have PCs at their desks

7. The aims of the organization in developing an intranet may not align with user needs

7. Write short notes on <any three> :

a.Tele ports

Teleports are the ground-based side of the global satellite network – gateways that provide terrestrial networks with access to orbiting satellite transponders. But they are more than simple gateways. Teleports bridge incompatible systems and protocols, host and distribute content, and act as the hubs of broadband B2B networks. These companies range from small entrepreneurial operations with one to three facilities to large, publicly-traded companies with teleports in multiple geographic markets.

b.Internet RFCs

A Request for Comments (RFC) is a publication of the Internet Engineering Task Force (IETF) and the Internet Society, the principal technical development and standards-setting bodies for the Internet. An RFC is authored by engineers and computer scientists in the form of a memorandum describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems. It is submitted either for peer review or simply to convey new concepts, information, or (occasionally) engineering humor.

c.Multi Protocol Support

Multi-protocol support lets you use Connection Manager as a protocol conversion service allowing clients using one network protocol to connect to a database server using a different network protocol. Figure 1 shows Connection Manager being used to enable clients running SPX to connect to a database server over TCP/IP. Notice that connection concentration can be applied even when converting between protocols.

d.NET application

e.Data centers

A data center (sometimes spelled datacenter) is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business.

Tribhuwan University

Institute of Science and Technology

2072

Full Marks : 60

Internet Technology **Pass Marks :24**

Time : 3 hours

New Course

Candidates are required to give their answers in their own words as far as practicable. The figures in the margin indicate full marks.

1) What do you mean by internet number? Describe the role of Regional Internet Registry(RIR) and National Internet Registry(NIR) in the intetnet systems.

The role of Regional Internet Registry(RIR)

RIRs provide services for the administration, management, distribution and registration of Internet number resources; specifically IPv4 addresses, IPv6 addresses, and Autonomous System numbers. Services are based, in part, upon policies that the communities of each RIR develop in a multi-stakeholder, bottom up approach that is open to all interested parties. The Policy Development Process within each RIR region defines the way these policies are developed and adopted.

The key services the RIRs provide are administration of the Internet number resources to help ensure uniqueness, responsible distribution, ensuring that resources go to those with a demonstrated need for them, and global publication of all allocations and assignments.

NIR:

A National Internet Registry (or NIR) is an organization under the umbrella of a Regional Internet Registry with the task of coordinating IP address allocations and other Internet resource management functions at a national level within a country or economic unit.

NIRs operate primarily in the Asia Pacific region, under the authority of APNIC, the Regional Internet Registry for that region.

2) How structure of a domain name looks like, describe with an example. How forward DNS resolution works?

A domain name consists of one or more parts, technically called labels that are conventionally concatenated, and delimited by dots, such as example.com. The right-most label conveys the top-level domain; for example, the domain name https://www.rajanaryal.com.np/ belongs to the top-level domain com.

The hierarchy of domains descends from the right to the left label in the name; each label to the left specifies a subdivision, or subdomain of the domain to the right. For example: the label example specifies a node example.com as a subdomain of the com domain, and www is a label to create www.example.com, a subdomain of example.com. This tree of labels may consist of 127 levels. Each label may contain from 1 to 63 octets. The empty label is reserved for the root node. The full domain name may not exceed a total length of 255 characters. In practice, some domain registries may have shorter limits.

A hostname is a domain name that has at least one associated IP address. For example, the domain names www.example.com and example.com are also hostnames, whereas the com domain is not. However, other top-level domains, particularly country code top-level domains, may indeed have an IP address, and if so, they are also hostnames.

Reverse Lookup(forward DNS resolution):

Computer networks use the Domain Name System to determine the IP address associated with a domain name. This process is also known as forward DNS resolution. Reverse DNS lookup is the inverse process, the resolution of an IP address to its designated domain name.

The process of reverse resolving an IP address uses the pointer DNS record type (PTR record). A reverse lookup is a query of the DNS for domain names when the IP address is known. Multiple domain names may be associated with an IP address. The DNS stores IP addresses in the form of domain names as specially formatted names in pointer (PTR) records within the infrastructure top-level domain arpa. For IPv4, the domain is in-addr.arpa. For IPv6, the reverse lookup domain is ip6.arpa.

When performing a reverse lookup, the DNS client converts the address into these formats, and then queries the name for a PTR record following the delegation chain as for any DNS query.

For example,

assume the IPv4 address 208.80.152.2 is assigned to Wikimedia. It is represented as a DNS name in reverse order like this: 2.152.80.208.in-addr.arpa. When the DNS resolver gets a PTR (reverse-lookup) request, it begins by querying the root servers (which point to ARIN's servers for the 208.in-addr.arpa zone). On ARIN's servers, 152.80.208.in-addr.arpa is assigned to Wikimedia, so the resolver sends another query to the Wikimedia nameserver for 2.152.80.208.in-addr.arpa, which results in an authoritative response.

3) How IPv6 addresses can be classified? Discuss about IPv6 header structure.

IPv6 addresses are classified by the primary addressing and routing methodologies common in networking:

- unicast addressing,
- anycast addressing, and
- multicast addressing.

Unicast addressing

- A unicast address identifies a single network interface. The Internet Protocol delivers packets sent to a unicast address to that specific interface. - An anycast address is assigned to a group of interfaces, usually belonging to different nodes. A packet sent to an anycast address is delivered to just one of the member interfaces, typically the nearest host, according to the routing protocol's definition of distance.

Anycast addresses

-Anycast addresses cannot be identified easily, they have the same format as unicast addresses, and differ only by their presence in the network at multiple points. Almost any unicast address can be employed as an anycast address.

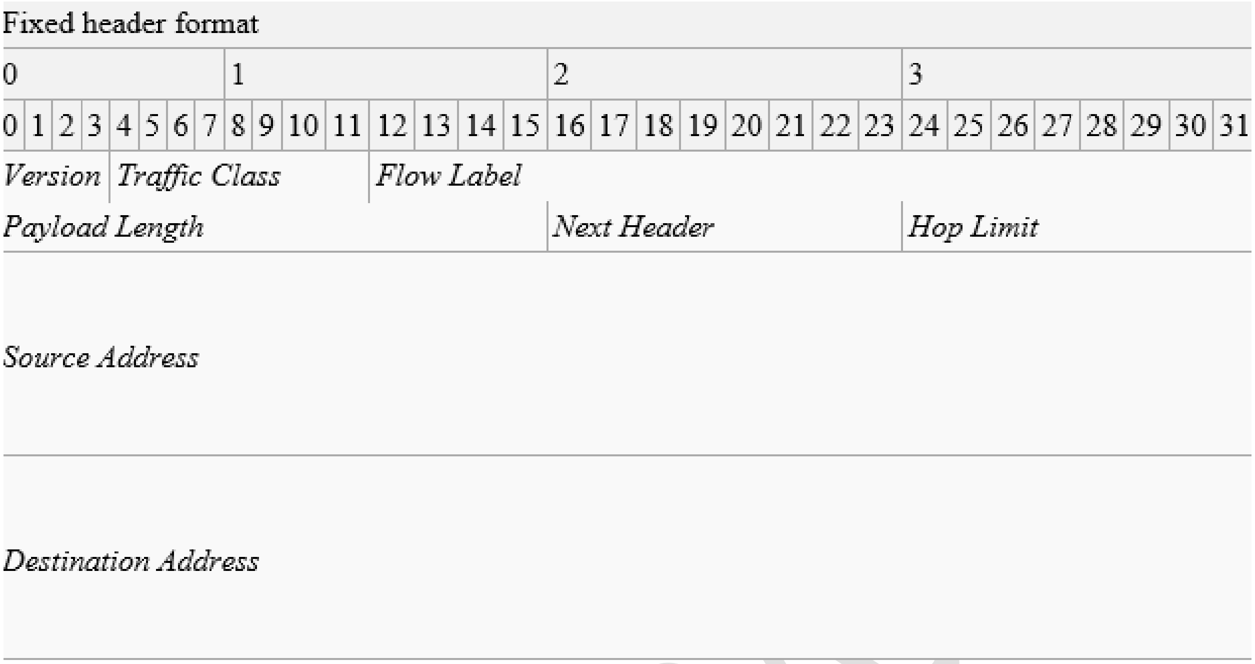
Multicast address

- A multicast address is also used by multiple hosts, which acquire the multicast address destination by participating in the multicast distribution protocol among the network routers. A packet that is sent to a multicast address is delivered to all interfaces that have joined the corresponding multicast group.

IPV6 Header Structure:

IPv6 specifies a new packet format, designed to minimize packet header processing by routers. Because the headers of IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable. However, in most respects, IPv6 is a conservative extension of IPv4. Most transport and application-layer protocols need little or no change to operate over IPv6; exceptions are application protocols that embed internet-layer addresses, such as FTP and NTPv3, where the new address format may cause conflicts with existing protocol syntax.

The fixed header of an IPv6 packet consists of its first 40 octets (320 bits). It has the following format:



<table>
<tr><td colspan="32">Fixed header format</td></tr>
<tr><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="4"><i>Version</i></td><td colspan="8"><i>Traffic Class</i></td><td colspan="20"><i>Flow Label</i></td></tr>
<tr><td colspan="16"><i>Payload Length</i></td><td colspan="8"><i>Next Header</i></td><td colspan="8"><i>Hop Limit</i></td></tr>
<tr><td colspan="32"><i>Source Address</i></td></tr>
<tr><td colspan="32"><i>Destination Address</i></td></tr>
</table>

Version (4 bits):

The constant 6 (bit sequence 0110).

Traffic Class (8 bits):

The bits of this field hold two values. The 6 most-significant bits are used for DSCP, which is used to classify packets. The remaining two bits are used for ECN; priority values subdivide into ranges: traffic where the source provides congestion control and non-congestion control traffic.

Flow Label (20 bits):

Originally created for giving real-time applications special service. Flow Label specifications and minimum requirements are described, and first uses of this field are emerging.

Payload Length (16 bits):

The size of the payload in octets, including any extension headers. The length is set to zero when a Hop-by-Hop extension header carries a Jumbo Payload option.

Next Header (8 bits):

Specifies the type of the next header. This field usually specifies the transport layer protocol used by a packet's payload. When extension headers are present in the packet this field indicates which extension header follows. The values are shared with those used for the IPv4 protocol field, as both fields have the same function

Hop Limit (8 bits):

Replaces the time to live field of IPv4. This value is decremented by one at each intermediate node visited by the packet. When the counter reaches 0 the packet is discarded.

Source Address (128 bits):

The IPv6 address of the sending node.

Destination Address (128 bits):

The IPv6 address of the destination node(s).

4) How SMTP differs from POP? What are the reasons for multiple protocols in internet systems?

Difference between SMTP and POP

1.SMTP (Simple Mail Transfer Protocol) and POP (Post Office Protocol) are both standards used for emailing.
2.Simply put, SMTP is used when receiving and sending emails (like your very own mailman who picks up and delivers your mail to different locations), while POP is the protocol used for storing emails (like your very own Post Office Box for mail storage).
3.SMTP is the protocol in general use at the moment.
4.POP gives a basic, standardized way for people to use their own mailboxes and be able to download messages to their own computers.

BASIS FOR COMPARISON	SMTP	POP
Basic	It is message transfer agent.	It is message access agent.
Full form	Simple Mail Transfer Protocol.	Post Office Protocol version 3.
Implied	Between sender and sender mail server and between sender mail server and receiver mail server.	Between receiver and receiver mail server.
work	It transfers the mail from senders computer to the mail box present on receiver's mail server.	It allows to retrieve and organize mails from mailbox on receiver mail server to receiver's computer.

5) Define WML Deck and Card. Write a simple WML code showing deck and card with some piece of text inside it.

A WML file can contain multiple cards and they form a deck.

When a WML page is accessed from a mobile phone, all the cards in the page are downloaded from the WAP server. So if the user goes to another card of the same deck, the mobile browser does not have to send any requests to the server since the file that contains the deck is already stored in the wireless device.

You can put links, text, images, input fields, option boxes and many other elements in a card.

6)What possible factors can be considered while filtering the content in web? How SMTP proxies can be used to filter mails?

7)What is the purpose of using XML? Why XML elements are said to be extensible? Support your answer with an example.

XML is used in many aspects of web development, often to simplify data storage and sharing.

1.XML Separates Data from HTML:

If you need to display dynamic data in your HTML document, it will take a lot of work to edit the HTML each time the data changes. With XML, data can be stored in separate XML files. This way you can concentrate on using HTML for layout and display, and be sure that changes in the underlying data will not require any changes to the HTML. With a few lines of JavaScript code, you can read an external XML file and update the data content of your web page.

2.XML Simplifies Data Sharing:

In the real world, computer systems and databases contain data in incompatible formats. XML data is stored in plain text format. This provides a software- and hardware-independent way of storing data. This makes it much easier to create data that can be shared by different applications.

3.XML Simplifies Data Transport:

One of the most time-consuming challenges for developers is to exchange data between incompatible systems over the Internet. Exchanging data as XML greatly reduces this complexity, since the data can be read by different incompatible applications.

4.XML Simplifies Platform Changes:

Upgrading to new systems (hardware or software platforms), is always time consuming. Large amounts of data must be converted and incompatible data is often lost. XML data is stored in text format. This makes it easier to expand or upgrade to new operating systems, new applications, or new browsers, without losing data.

5.XML Makes Your Data More Available:

Different applications can access your data, not only in HTML pages, but also from XML data sources. With XML, your data can be available to all kinds of "reading machines" (Handheld computers, voice machines, news feeds, etc), and make it more available for blind people, or people with other disabilities.

6.XML Used to Create New Internet Languages:

A lot of new Internet languages are created with XML. Here are some examples:

- XHTML
- WSDL (Web Services Description Language) for describing available web services

XML is the Extensible Markup Language. It improves the functionality of the Web by letting you identify your information in a more accurate, flexible, and adaptable way. It is extensible because it is not a fixed format like HTML (which is a single, predefined **markup language**). Instead, XML is a **metalanguage** — a language for describing other languages — which lets you design your own markup languages for limitless different types of documents. XML can do this because it's written in SGML, the international standard metalanguage for text document markup

8)What do you mean by audio broadcasting? Discuss the basic components of IRC protocol.

Digital audio broadcasting (DAB), also known as digital radio and high-definition radio, is audio broadcasting in which analog audio is converted into a digital signal and transmitted on an assigned channel in the AM or (more usually) FM frequency range. DAB is said to offer compact disc (CD)- quality audio on the FM (frequency modulation) broadcast band and to offer FM-quality audio on the AM (amplitude modulation) broadcast band.

IRC protocol

Internet Relay Chat is a method to broadcast and receive live, synchronous, messages. Internet Relay Chat (IRC) is a protocol for real-time Internet text messaging (chat) or synchronous conferencing.

Components of IRC:

Servers:

The server forms the backbone of IRC as it is the only component of the protocol which is able to link all the other components together: it provides a point to which clients may connect to talk to each other, and a point for other servers to connect to. The server is also responsible for providing the basic services defined by the IRC protocol.

Clients:

A client is anything connecting to a server that is not another server. There are two types of clients which both serve a different purpose.

User Clients:

User clients are generally programs providing a text based interface that is used to communicate interactively via IRC. This particular type of clients is often referred as "users".

Service Clients:

Unlike users, service clients are not intended to be used manually nor for talking. They have a more limited access to the chat functions of the protocol, while optionally having access to more private data from the servers. Services are typically automatons used to provide some kind of service (not necessarily related to IRC itself) to users. An example is a service collecting statistics about the origin of users connected on the IRC network.

9)Describe the building blocks that need to be considered while desigining Internet System Network Architecture.

10)Discuss possible types of VPN Tunneling. How VPN client server interaction occurs, discuss with an example.

A tunneling protocol is the one utilized by computer networks in cases where the network protocol or the delivery protocol encapsulates an unsuited payload protocol at a peer level or lower than it.

Two types of tunneling include voluntary and compulsory.

- Voluntary VPN tunneling:
  In this particular tunneling type, the VPN client sets up the connection. At first, the client establishes a connection with the network provider or the ISP. Later on, utilizing this live connection, it creates a tunnel to a particular VPN server.

- Compulsory VPN tunneling:
  The carrier network provider is responsible for managing the set up for VPN connection in this type of tunneling. It is quicker than its voluntary counterpart and can be established in just a single step as compared to the two-step process of the other one. This network device is known with varied other names as well such as Network Access Server (NAS), VPN Front End Processor (FEP) and Point of Presence Server (POS).

Five prominent tunneling protocols are readily used to establish successful VPN connection that includes PPTP VPN, L2TP VPN, IPSec, SSH VPN and SSTP VPN. Let us discuss them in brief.

- Point-to-Point Tunneling Protocol (PPTP):
  It is among the most widely preferred tunneling protocols and is available as a built in facility in almost all the windows OS versions. It utilizes a control channel over TCP to encapsulate PPP data packets. It itself does not provide authentication or encryption features but is dependent on the Point-to-Point Protocol (PPP). Still, it is the best to provide high security level and remote access during a VPN connection.

- Layer 2 Tunneling Protocol (L2TP):
  It is also a capable tunneling protocol that supports VPN connection. Like PPTP, it also does not offer confidentiality and encryption on its own but depends on an encryption protocol for the same that it leverages to assure privacy within the tunnel. It has been developed out of the combination of L2F and PPTP taking their best features and exists at the data link layer in the OSI model, same as PPTP.

- IP Security (IPSec):
  It is better known as an assemblage of varied protocols instead of being a single one. When combines with PPTP or L2TP, it provides accomplished encryption solutions and secures the data transfer within a VPN tunnel. It exists at the Layer 3, i.e. Network Layer of the OSI model.

- Secure Shell (SSH):
  This is a new protocol as compared all the rest ones and seeks assistance of an encrypted channel to transfer the unencrypted data via a secure network efficiently. In locations where VPN is blocked, SSH somehow manages to hide the identity of users and prevents their IP address from being blocked.

- Secure Socket Tunneling Protocol:
  This is yet another effective protocol that makes way for secure data transfer from network server to a remote terminal and vice versa, thereby bypassing all the firewalls and web proxies coming in its way. To accomplish such a successful data transaction, it utilizes HTTPs protocol and is very useful at places where PPTP or L2TP/IPSec cease to perform as per expected.

Tribhuwan University

Institute of Science and Technology

2073

Full Marks : 60

Internet Technology **Pass Marks :24**

Time : 3 hours

New Course

Candidates are required to give their answers in their own words as far as practicable. The figures in the margin indicate full marks.

Attempt all Questions

1. What are the roles of internet registrars? Define the generic top level domains . (3+3)

An Internet Registry (IR) is an organization that is responsible for distributing IP address space to its members or customers and for registering those distributions.

Generic top level domains

Domain names are organized in subordinate levels (subdomains) of the DNS root domain, which is nameless. The first-level set of domain names are the top-level domains (TLDs), including the generic top-level domains (gTLDs), such as the prominent domains .com, .net and .org, and the country code top-level domains (ccTLDs). Below these top-level domains in the DNS hierarchy are the second-level and third-level domain names that are typically open for reservation by end-users who wish to connect local area networks to the Internet, create other publicly accessible Internet resources or run web sites. The registration of these domain names is usually administered by domain name registrars who sell their services to the public.

A top-level domain (TLD) is one of the domains at the highest level in the hierarchical Domain Name System of the Internet. The top-level domain names are installed in the root zone of the name space. For all domains in lower levels, it is the last part of the domain name, that is, the last label of a fully qualified domain name. For example, in the domain name www.example.com, the top-level domain is .com (or .COM, as domain names are not case-sensitive). Management of most toplevel domains is done by ICANN.

A generic top-level domain (gTLD) is one of the categories of top-level domains (TLDs) maintained by the IANA for use in the Domain Name System of the Internet. The core group of generic top-level domains consists of the com, info, net, and org domains. In addition, the domains biz, name, and pro are also considered generic; however, these are designated as restricted, because registrations within them require proof of eligibility within the guidelines set for each.

2. What are RFCs? How IPV6 addressing scheme differs from IPv4? (3+3)

In computer network engineering, a Request for Comments (RFC) is a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems. It began in 1969 as a set of working notes about ARPAnet research and development.

Memos in the Requests for Comments (RFC) document series contain technical and organizational notes about the Internet. They cover many aspects of computer networking, including protocols, procedures, programs, and concepts, as well as meeting notes, opinions, and sometimes humor.

RFCs are numbered (roughly) consecutively, and these numbers provide a single unique label space for all RFCs. RFCs are published online through a number of repositories, and there is an online index of RFCs.

IPV6 addressing scheme differs from IPv4

(Refer 2069 Q no 2)

3. HTTP protocol is often called connectionless, justify the statement. How FTP can be run in passive and active mode? (3+3)

Client (browser) is using the HTTP Protocol to get some information from the Server by requesting to it. First, we should understand how the HTTP works over the Web…

- When a user tries to access a website using a client with HTTP protocol
- The client first tries to establish a connection with the server.
- Then it requests the server to display the information which was asked by the user to show.
- For this connection, the Server gives a response and display the requested information.
- When the server completes the response to the client, the connection will be destroyed.

Now, when the same client requests the same information to that server, it starts the connection again and after displaying the information the connection will be closed.

This connection Open and Close process happens on each single client-server request over the web.

If there are 10000 clients, which request the same information from the Server, the server cannot allocate a specific time to that individual client, each single connection will be open and closed after the completion of that request from the server.

This is the reason; HTTP protocol is called as a Connectionless Protocol.

FTP(Active and passive)

Active and passive are the two modes that FTP can run in.

For background, FTP actually uses *two* channels between client and server, the command and data channels, which are actually *separate* TCP connections.
The command channel is for commands and responses while the data channel is for actually transferring files.

This separation of command information and data into separate channels a nifty way of being able to send commands to the server without having to wait for the current data transfer to finish. As per the RFC, this is only mandated for a subset of commands, such as quitting, aborting the current transfer, and getting the status.

In *active* mode, the client establishes the command channel but the *server* is responsible for establishing the data channel. This can actually be a problem if, for example, the client machine is protected by firewalls and will not allow unauthorized session requests from external parties.

In *passive* mode, the client establishes *both* channels. We already know it establishes the command channel in active mode and it does the same here. However, it then requests the server (on the command channel) to start *listening* on a port (at the servers discretion) rather than trying to establish a connection back to the client.
As part of this, the server also returns to the client the port number it has selected to listen on, so that the client knows how to connect to it.

4. What is the role of rendering engines in web browsers? How browser renders contents like text and images? (3+3)

Answer:

(Web browser engine, sometimes called layout engine or rendering engine)

A **rendering engine** is software that draws text and images on the screen. The engine draws structured text from a document (often HTML), and formats it properly based on the given style declarations (often given in CSS). and displays the formatted content on the screen. It "paints" on the content area of a window, which is displayed on a monitor or a printer. A web browser engine is typically embedded in web browsers, email clients, on-line help systems or other applications that require the displaying (and editing) of web content. Engines may wait for all data to be received before rendering a page, or may begin rendering before all data is received. This can result in pages changing as more data is received, such as images being filled in or a flash of unstyled content if rendering begins before formatting information is received

5. What do you mean by proxy server? Describe the uses of proxy servers. (1+5)

In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server. The proxy server evaluates the request as a way to simplify and control their complexity. Today, most proxies are web proxies, facilitating access to content on the World Wide Web.

a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

A proxy server receives a request for an Internet service (such as a Web page request) from a user. If it passes filtering requirements, the proxy server, assuming it is also a cache server, looks in its local cache of previously downloaded Web pages. If it finds the page, it returns it to the user without needing to forward the request to the Internet. If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from the server out on the Internet. When the page is returned, the proxy server relates it to the original request and forwards it on to the user.

A proxy server has a variety of potential purposes, including:

- To keep machines behind it anonymous, mainly for security.
- To speed up access to resources (using caching). Web proxies are commonly used to cache web pages from a web server.
- To apply access policy to network services or content, e.g. to block undesired sites.
- To access sites prohibited or filtered by your ISP or institution.
- To log / audit usage, i.e. to provide company employee Internet usage reporting.
- To bypass security / parental controls.
- To circumvent Internet filtering to access content otherwise blocked by governments.
- To scan transmitted content for malware before delivery.
- To scan outbound content, e.g., for data loss prevention.
- To allow a web site to make web requests to externally hosted resources (e.g. images, music files, etc.) when cross-domain restrictions prohibit the web site from linking directly to the outside domains.

Proxy server can be placed in the user's local computer or at various points between the user and the destination servers on the Internet.

6. Describe how RADIUS server provides Authentication, Authorization and Accounting services. (6)

Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security.

Authentication

As the first process, authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials are at variance, authentication fails and network access is denied.

Authorization

Following authentication, a user must gain authorization for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.

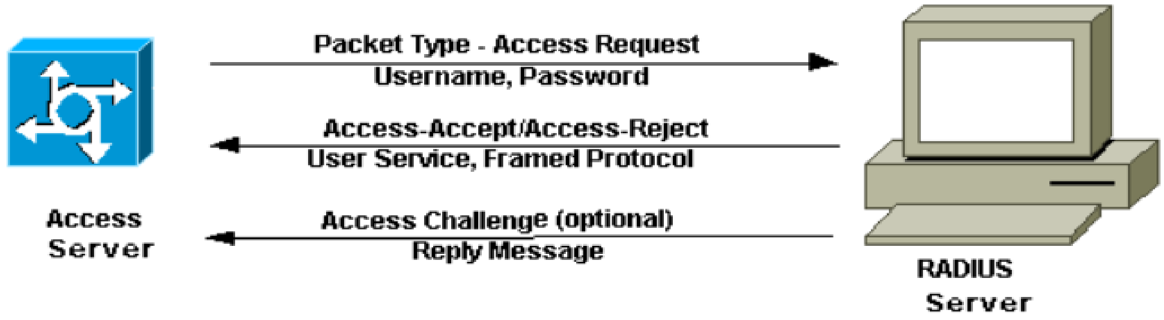

Packet Type - Access Request
Username, Password
Access-Accept/Access-Reject
User Service, Framed Protocol
Access Challenge (optional)
Reply Message
Access Server
RADIUS Server

Fig : Authentication and Authorization

Accounting

The final plank in the AAA framework is accounting, which measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

7. Describe the different fields of cookie. How session cookie differs from persistent cookie.

(3+3)

There are 2 different types of cookies: Session cookies and persistent cookies .session cookie differs from persistent cookie. difference are as below:

- If a cookie does not contain an expiration date, it is considered a session cookie. Session cookies are stored in memory and never written to disk. When the brewers closes the cookie is permanently lost from this point on.

- If the cookie contains an expiration date, it is considered a persistent cookie. On the date specified in the expiration, the cookie will be removed from the disk.

8. How use of firewalls ensures security of a network? Discuss about different types of firewalls. (3+3)

Firewall is hardware device or software applications that act as filters between a company's private network and the internet. It protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service by enforcing an access control policy between two networks.

The main purpose of a firewall system is to control access to or from a protected network (i.e., a site). It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated. A firewall system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnet. A firewall system is usually located at a higher level gateway, such as a site's connection to the Internet, however firewall systems can be located at lower-level gateways to provide protection for some smaller collection of hosts or subnets. The main function of a firewall is to centralize access control. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks. The earliest firewalls were simply routers.

Firewalls provide several types of protection:

- They can block unwanted traffic.

- They can direct incoming traffic to more trustworthy internal systems.

- They hide vulnerable systems, which can't easily be secured from the Internet.

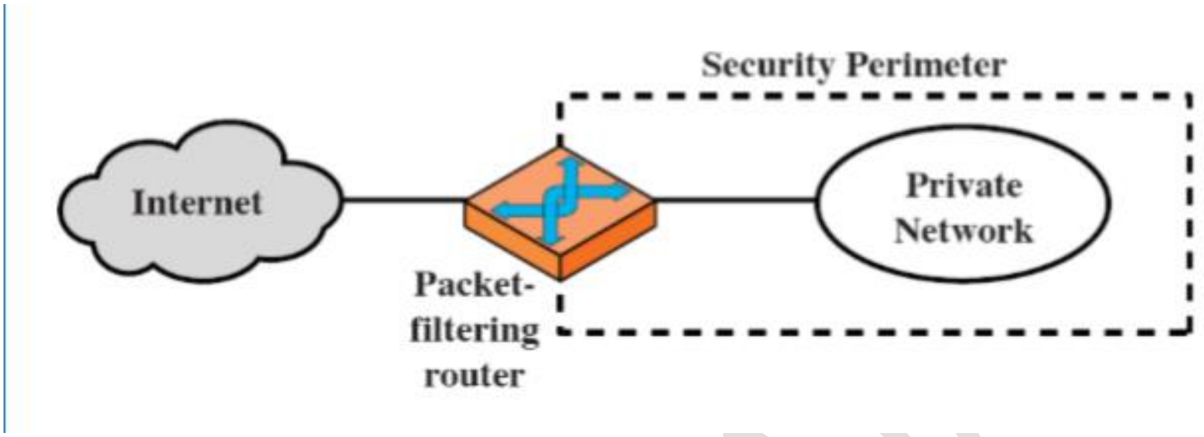
- They can log traffic to and from the private network.

- They can hide information like system names, network topology, network device types, and internal user ID's from the Internet. - They can provide more robust authentication than standard applications might be able to do.

different types of firewalls

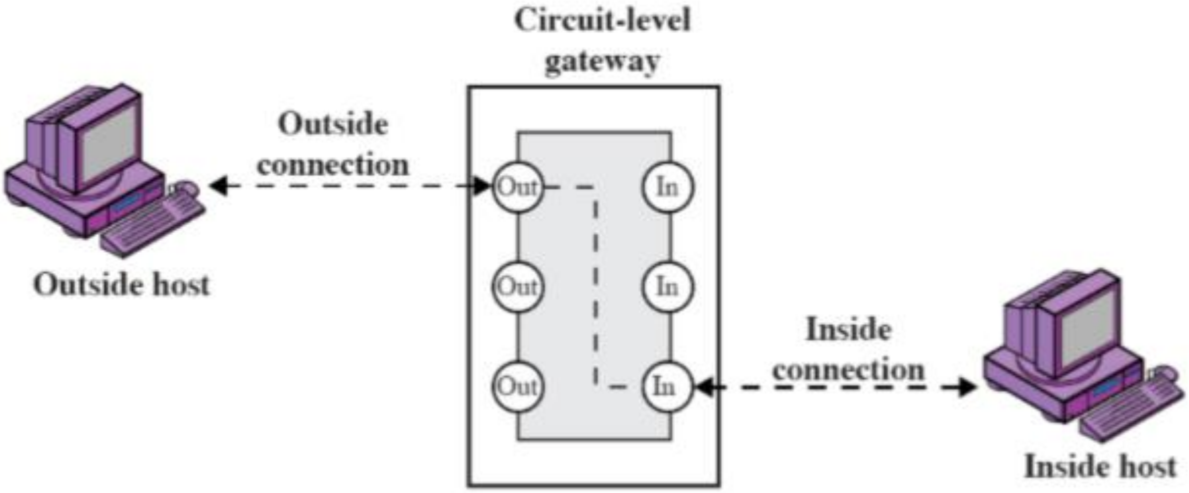
1.Packet Filters:

Packet filtering firewalls work at the network layer (OSI model), or the IP layer (TCP/IP). In this each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop, forward the packet or send a message to the originator. Rules can be source and destination IP address, source and destination port number and protocol used. The advantages of packet filtering firewalls is their low cost and low impact on network performance



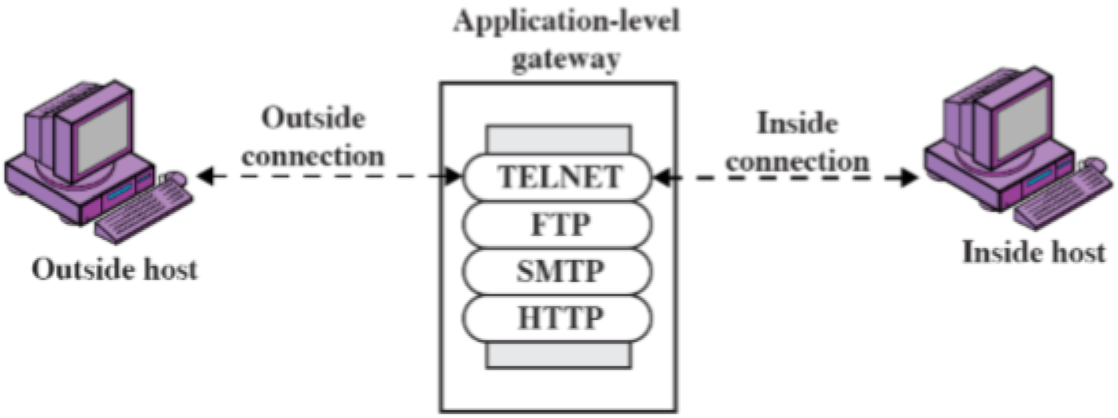
2.Circuit Level Gateways:

It work at the session layer (OSI model), or the TCP layer (TCP/IP). They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to a remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks. Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.



3.Application Gateways:

Application level gateways, also called proxies, are similar to circuit-level gateways except that they are application specific. They can filter packets at the application layer of the OSI model. Incoming or outgoing packets cannot access services for which there is no proxy. In plain terms, an application level gateway that is configured to be a web proxy acts as the server to the internal network and client to the external network. Because they examine packets at application layer, they can filter application specific commands such as http: post and get, etc. Application level gateways can also be used to log user activity and logins. They offer a high level of security, but have a significant impact on network performance.



4.Stateful Multilayer Inspection Firewall:

It combines the aspects of the other three types of firewalls. They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer. They rely on algorithms to recognize and process application layer data instead of running application specific proxies. Stateful multilayer inspection firewalls offer a high level of security, good performance and transparency to end users. They are expensive however, and due to their complexity are potentially less secure than simpler types of firewalls if not administered by highly competent personnel.

5.Content Filtering:

Content filtering is the technique whereby content is blocked or allowed based on analysis of its content, rather than its source or other criteria. It is most widely used on the internet to filter email and web access.

9. What is cloud computing? Mention the features of cloud computing. (2+4)

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation.

There are many types of public cloud computing: Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Storage as a service (STaaS), Security as a service (SECaaS), Data as a service (DaaS), Test environment as a service (TEaaS), Desktop as a service (DaaS), API as a service (APIaaS).

Characteristics:

Cloud computing exhibits the following key characteristics:

- **Agility** improves with users' ability to re-provision technological infrastructure resources.

- **Application programming interface (API)** accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers.

- **Cost** is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure.[26] This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house)

- **Device and location independence** enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.

- Virtualization technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.

- **Multitenancy** enables sharing of resources and costs across a large pool of users thus allowing for:

o **Centralization** of infrastructure in locations with lower costs (such as real estate,

electricity, etc.)

o **Peak-load capacity** increases (users need not engineer for highest possible load-levels)

o **Utilisation and efficiency**

- Reliability is improved if multiple redundant sites are used, which makes welldesigned cloud computing suitable for business continuity and disaster recovery.

- **Scalability and elasticity** via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads.

- Performance is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface.

- Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels.

- Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

10. What are benefits of intranets? What network infrastructure need to be established for intranets?

Answer: **(3+3)**

Intranets are extremely useful as a business tool. Few of the key intranet benefits include:

- **Better internal communications**
  - intranets can act as communication hubs for staff. You can store corporate information such as memos, staff news and announcements centrally and access at any time.

- **Sharing of resources and best practice**

- you can create a virtual workspace and community to facilitate information storing, sharing and collaborative working. An intranet can also act as a training platform when providing online training content to staff.

- **Improved customer service**
  - better access to accurate and consistent information by your staff can lead to enhanced levels of customer service.

Intranet Network Infrastructure:

A network infrastructure is an interconnected group of computer systems linked by the various parts of a telecommunications architecture. Specifically, this infrastructure refers to the organization of its various parts and their configuration — from individual networked computers to routers, cables, wireless access points, switches, backbones, network protocols, and network access methodologies. Infrastructures can be either open or closed, such as the open architecture of the Internet or the closed architecture of a private intranet. They can operate over wired or wireless network connections, or a combination of both.

The simplest form of network infrastructure typically consists of one or more computers, a network or Internet connection, and a hub to both link the computers to the network connection and tie the various systems to each other. The hub merely links the computers, but does not limit data flow to or from any one system. To control or limit access between systems and regulate information flow, a switch replaces the hub to create network protocols that define how the systems communicate with each other. To allow the network created by these systems to communicate to others, via the network connection, requires a router, which bridges the networks and basically provides a common language for data exchange, according to the rules of each network.

Why Is the Network Infrastructure Important to Your Intranet?

An intranet is made up of two parts: the applications (software / protocols) and the network infrastructure on which the applications run. Applications— the visible part of an intranet — provide the functionality to improve productivity and lower costs. A wide spectrum of Internet/intranet applications is available from many vendors. The network infrastructure includes the hardware—network interface cards (NICs), hubs, routers, switches, and servers—over which the applications run. All network hardware is not the same, and an intranet is only as usable, reliable, and cost-effective as the hardware on which it runs. Crucial considerations in choosing appropriate hardware include:

- Bandwidth availability
- Reliability
- Value, in terms of both initial cost and ease of use and management -
Scalability, to ensure that present and future needs can be met

So as a part of network infrastructure, go through the above highlighted portions. I think you have studied those in data communication as well.