Some old q answers (IT)

Q) History of internet and intranet. (071 a)

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

INTERNET TIMELINE (in detail)

1957 – USSR launches Sputnik into space. In response, the USA creates the Advanced Research Projects Agency (ARPA) with the mission of becoming the leading force in science and new technologies.

1962 – J.C.R. Licklider of MIT proposes the concept of a “Galactic Network.” For the first time ideas about a global network of computers are introduced. J.C.R. Licklider is later chosen to head ARPA's research efforts.

1962 - Paul Baran, a member of the RAND Corporation, determines a way for the Air Force to control bombers and missiles in case of a nuclear event. His results call for a decentralized network comprised of packet switches.

1969 – RPANET created - BBN creates the first switched network by linking four different nodes in California and Utah; one at the University of Utah, one at the University of California at Santa Barbara, one at Stanford and one at the University of California at Los Angeles.

1972 - Ray Tomlinson working for BBN creates the first program devoted to email.
1972 - ARPA officially changes its name to DARPA Defense Advanced Research Projects Agency.
1972 - Network Control Protocol is introduced to allow computers running on the same network to communicate with each other.

1973 - Vinton Cerf working from Stanford and Bob Kahn from DARPA begin work developing TCP/IP to allow computers on different networks to communicate with each other.

1974 - Kahn and Cerf refer to the system as the Internet for the first time.

1976 - Ethernet is developed by Dr. Robert M. Metcalfe.
1976 – Elizabeth II, Queen of the United Kingdom, sends out an email on 26 March from the Royal Signals and Radar Establishment (RSRE) in Malvern.
1976 - AT& T Bell Labs develops UUCP and UNIX.

1979 - USENET, the first news group network is developed by Tom Truscott, Jim Ellis and Steve Bellovin.
1979 - IBM introduces BITNET to work on emails and listserv systems.

1981 - The National Science Foundation releases CSNET 56 to allow computers to network without being connected to the government networks.

1983 - Internet Activities Board released.
1983 - TCP/IP becomes the standard for internet protocol.
1983 - Domain Name System introduced to allow domain names to automatically be assigned an IP number.

1984 - MCI creates T1 lines to allow for faster transportation of information over the internet.
1984- The number of Hosts breaks 1,000

1989- The Number of hosts breaks 100 000
1989- Arpanet ceases to exist

1990 - Advanced Network & Services (ANS) forms to research new ways to make internet speeds even faster. The group develops the T3 line and installs in on a number of networks.
1990 - A hypertext system is created and implemented by Tim Berners-Lee while working for CERN.
1990- The first search engine is created by McGill University, called the Archie Search Engine

1991- U.S green-light for commercial enterprise to take place on the Internet
1991 - CERN releases the World Wide Web publicly on August 6th, 1991

1992 – The Internet Society (ISOC) is chartered
1992- Number of hosts breaks 1,000,000

1993 - InterNIC released to provide general services, a database and internet directory.
1993- The first web browser, Mosaic (created by NCSA),

1994 - New networks added frequently.
1994 - First internet ordering system created by Pizza Hut.
1994 - First internet bank opened: First Virtual.
1995 - NSF contracts out their access to four internet providers.

1995 - NSF sells domains for a $50 annual fee.
1995 – Netscape goes public with 3rd largest ever NASDAQ IPO share value
1995- Registration of domains is no longer free.

1996- The WWW browser wars are waged mainly between Microsoft and Netscape.
1996 – Internet2 project is initiated by 34 universities
1996 - Nokia releases first cell phone with internet access.

1997- (Arin) is established to handle administration and registration of
IP numbers, now handled by Network Solutions (IinterNic)

1999 - A wireless technology called 802.11b, more commonly referred to as Wi-Fi, is standardized.
2000- The dot com bubble bursts, numerically, on March 10, 2000, when the technology heavy NASDAQ composite index peaked at 5,048.62

2001 - Blackberry releases first internet cell phone in the United States.
2001 – The spread of P2P file sharing across the Internet

2002 -Internet2 now has 200 university, 60 corporate and 40 affiliate members

2004 – The Term Web 2.0 rises in popularity when O'Reilly and MediaLive host the first Web 2.0 conference.

2004- Mydoom, the fastest ever spreading email computer worm is released. Estimated 1 in 12 emails are infected.

2005- Estonia offers Internet Voting nationally for local elections
2005-Youtube launches

2006- There are an estimated 92 million websites online
2006- Internet2 announced a partnership with Level 3 Communications to launch a brand new nationwide network, boosting its capacity from **10Gbps to 100Gbps**

2008- Google index reaches 1 Trillion URLs
2008 – NASA successfully tests the first deep space communications network modeled on the Internet from **a NASA science spacecraft located about more than 32 million kilometers from Earth**

2009 The Internet marks its 40th anniversary.

2010- Facebook announces in February that it has 400 million active users.

2010 China Dominates Internet Usage

2010 there are over 450 million Chinese Internet users

2012 Facebook reaches 1 billion monthly active users, making it the dominant social network worldwide. Some analysts start calling it "Facebookistan."

2012 South Korean music star PSY's "Gangnam Style" video surpasses as the most viewed video ever, with over 800 million views.

2013 51% of U.S. adults bank online.

2013 Former CIA employee and NSA contractor Edward Snowden turns over thousands of classified documents to media organizations, exposing a top-secret government data surveillance program.

2014 45% of internet users ages 18-29 in serious relationships say the internet has had an impact on their relationship.

Q) Explain the Internet Domain and Domain Name System (DNS) and its use. (069,71)

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 top-level 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. *Reverse* DNS lookup is the

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 in-addr.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.

Q 069) Explain internet RFCs.

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. non-obsoleted) 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 *standards-track* 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.

069 1 b) What do you mean by Teleports and terrestrial links? Explain

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.

069 2 a.) Define TCP/IP. Differentiate between IPV4 and IPV6.

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).

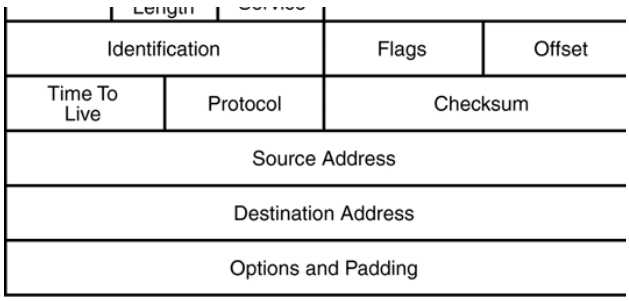
IPv4	IPv6
32-bit (4 byte) address supporting 4,294,967,296 address (although many were lost to special purposes, like 10.0.0.0 and 127.0.0.0)	128-bit (16 byte) address supporting 228 (about 3.4 x 1038) addresses
NAT can be used to extend address limitations	No NAT support (by design)
IP addresses assigned 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

070 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

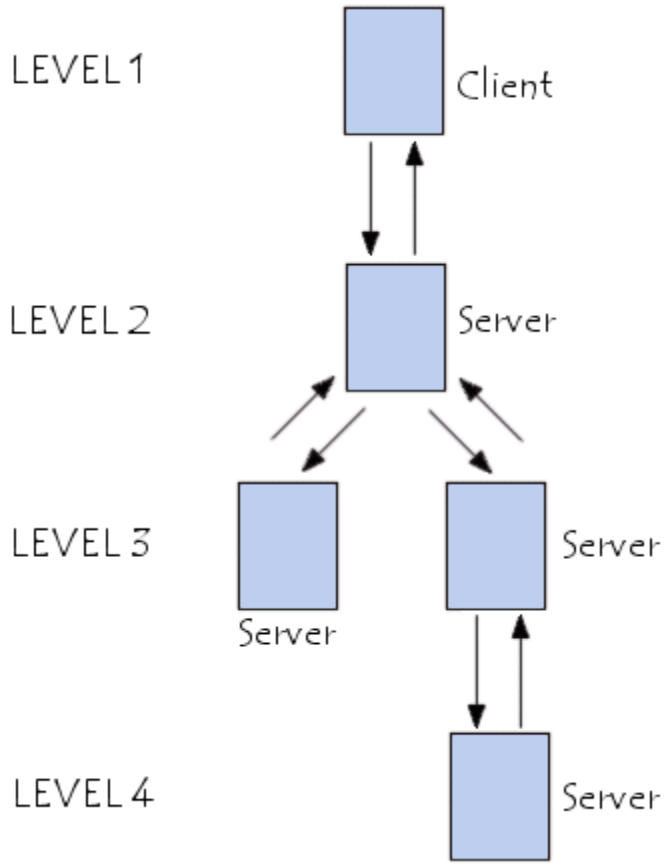
The destination address field indicates the address of the destination machine.

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.

069 3. a. Explain the N-Tired Client/Server Architecture.

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.

069 3 b. Define the terms PGP and POP.

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 e-mail 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 e-mail 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.

070 3)what are 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.

069 4. a. Define HTTP. Differentiate between HTML and DHTML.

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 and . 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.

- Use a form to capture user input, and then process and respond to that data without having to send data back to the server.
- Include rollover buttons or drop-down menus.

070 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:

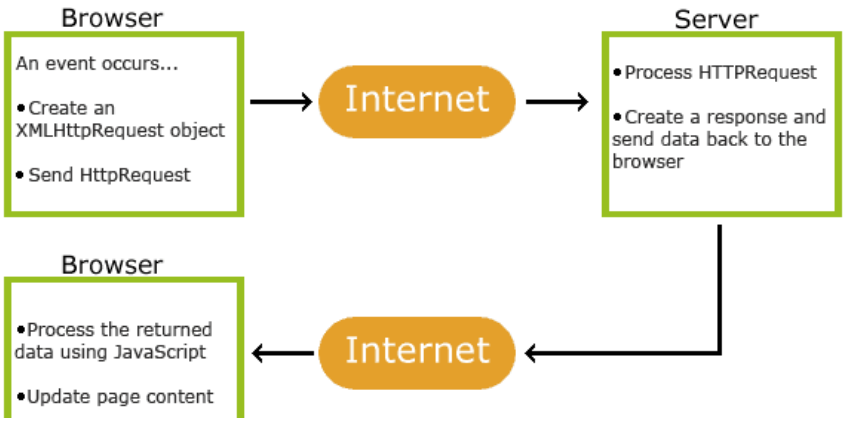
```
<bookstore>
  <book category="CHILDREN">
    <title>Harry Potter</title>
    <author>J K. Rowling</author>
    <year>2005</year>
    <price>29.99</price>
  </book>
  <book category="WEB">
    <title>Learning XML</title>
    <author>Erik T. Ray</author>
    <year>2003</year>
    <price>39.95</price>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

070 6) what do you mean by Universal Naming Conventions ? given the URL 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

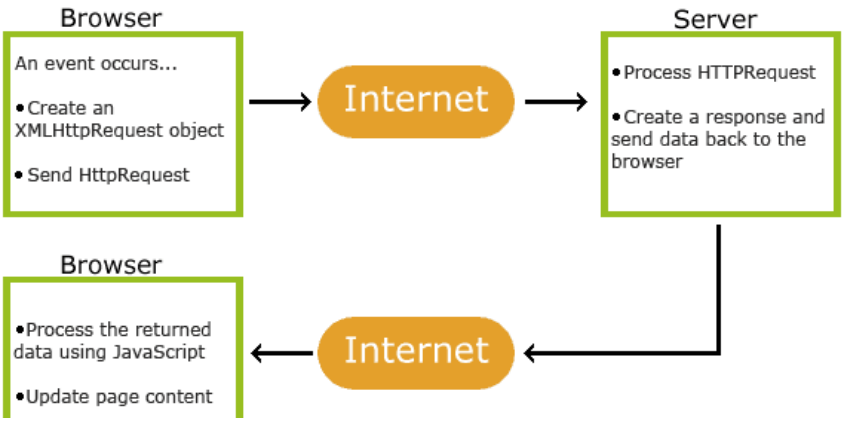
069 4 b. What do you mean by AJAX?



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.

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.

070 7) How an AJAX program gets executed ? Discuss the steps of AJAX operations.Show with example how we can 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.

071 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.

071 4(b) Explain 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 WYSIWYG tools are

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

A given HTML document will have an inconsistent appearance on various platforms and computers for several reasons

==========

Different protocols & languages

- **DNS (Domain Name System)**A service that resolves easy-to-remember host names into IP addresses.
- **DNS (Domain Name System)**A hierarchical name service that matches up Internet host names with IP addresses.
- **FTP (File Transfer Protocol)**A utility for transferring files between hosts on the Internet or any TCP/IP network.
- **HTML (Hypertext Markup Language)**The markup and tagging language used to create Web pages.
- **HTTP (HyperText Transfer Protocol)**The file transfer protocol that is the basis of the World Wide Web.
- **IMAP (Internet Message Access Protocol)** An Internet e-mail post office protocol that expands on the features of POP.
- **IPSec (IP Security)** A set of protocols that support secure and encrypted data exchange at the network layer. IPSec supports VPNs.
- **POP (Post Office Protocol)** A protocol that stores mail for users on a server and forwards that mail to them when they log on.
- **PGP (Pretty Good Privacy)** is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.
- **PPP (Point-to-Point Protocol)**A protocol for transmitting IP datagrams and other protocols over telephone links or serial lines.
- **SMTP (Simple Mail Transfer Protocol)** The primary protocol for exchanging email messages across TCP/IP networks. Works with POP and IMAP.

069 5(a) Explain the designing of internet system network architecture. (8)

[Fortunately, nobody owns the Internet, there is no centralized control, and nobody can turn it off. Its evolution depends on rough consensus about technical proposals, and on running code. Engineering feed-back from real implementations is more important than any architectural principles.-RFC 1958; B. Carpenter; Architectural Principles of the Internet; June, 1996.]

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.

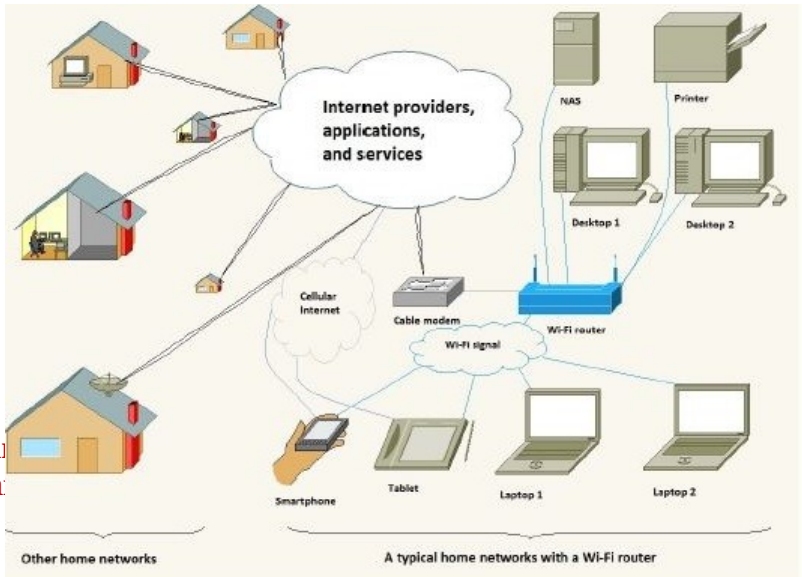
In practice, the Internet technical architecture looks a bit like a multi-dimensional river system, with small rivers feeding medium-sized streams feeding large rivers.

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



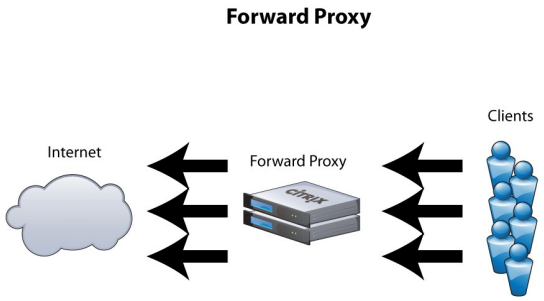
- Cost effective
- Low level of effort to add a host
- Provide accounting of resources used.

070 8) What are proxy servers? Differentiate each 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

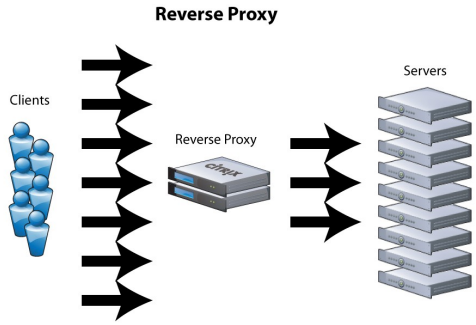
A forward proxies are those taking requests from an internal network and forwarding them to the Internet. Forward proxies are proxies where the client server names the target server to connect to. Forward proxies are able to retrieve from a wide range of sources (in most cases anywhere on the Internet).



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

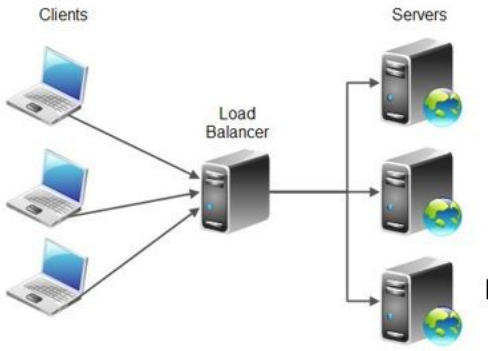
A reverse proxy is one taking requests from the Internet and forwarding them to servers in an internal network. Those making requests connect to the proxy and may not be aware of the internal network. A reverse proxy (or surrogate) is a proxy server that appears to clients to be an ordinary server. Requests 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.

070 (10) 071(5a) load balancing and its appilication . Difference between WWR and dinamic WRR.



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

071 5(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;

[optional] **Types of cookie**

1. **Session cookie**
2. **Persistent cookie**
3. **Secure cookie**
4. **HttpOnly cookie**
5. **Third-party cookie**
6. **Supercookie**
7. **Zombie cookie**

069 (6) 071 6(b) Explain the intranet implementation guidelines. what are 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

071 6(a) Explain the tunneling protocols with examples. 8

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.

070 4) Example of VPN Tunneling

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.

-

070(9) Define working mechanism of VOIP . what are its advantages.

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.

Short Notes

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 e-mail 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.

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.

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.

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.

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).

Teleports

a regional telecommunications network that provides access to communications satellites and other long distance media; telecommunications hub.

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.

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.

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.