3. TCP 56-87

Chapter

3 TCP

3.1 TCP

The Transmission Control Protocol (TCP) is a core protocol of the **Internet Protocol Suite.** It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides **reliable,** ordered and **error checked** delivery of a stream of **octets** between applications running on hosts communication over an IP network.

TCP is a protocol that major internet applications such as the **WWW, email, remote administration & file transfer** rely on applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a **connectionless datagram** service that emphasizes reduced **latency** over reliability.

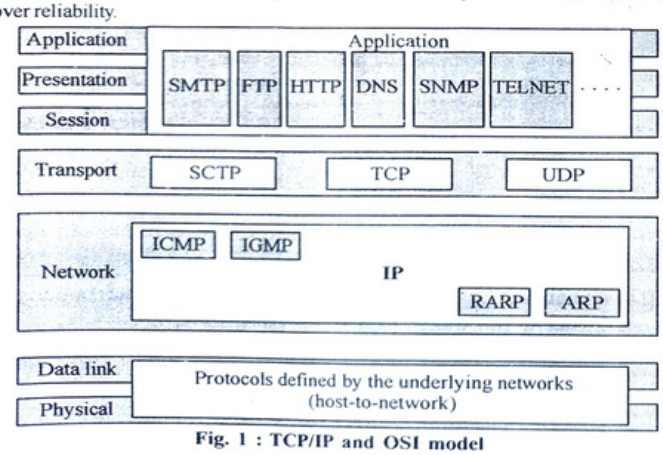


Fig. 1 : TCP/IP and OSI model

Historical & modification

In may 1974, **the institute of Electrical and Electronic Engineers (IEEE)** published a paper titled "A protocol for packet Network Inter Communication". The paper's authors, **Vint cerf** and **Bob kahn,** described an internet working protocol for sharing resources using **packet switching** among the nodes. A central control component of this model was the transmission control program that incorporatd both connection oriented links and **data gram** services between hosts.

The monolithic transmission control program was later divided into a modular architecture consisting of the TCP at the **connection oriented layer** and the internet Protocol at the internetworking (data gram) layer. The model became known informally as TCP/IP, although formally it uses hence forth called the Internet Protocol Suite.

Physical, Data link layers

At the physical and data ling layer, TCP/IP does not define any specific protocol. It support all the specific standard and proprietery protocols. A network in a TCP/IP internetwork can be a local-area network or a wide area network.

Network layer

At the network layer (or, more accurately, the internetworking protocol. IP, in turn, uses four supporting protocols protocols : ARP, RARP, ICMP and IGMP. Each of these protocols is described in greater details in later chapters.

Internetworking Protocol (IP)

The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol-a best-effort delivery service. The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track ofthe routes and has no facility for reordering datagrams once they arrive at their destination.

The limited functionality of IP should not be considered a weakness, however. IP provides bare-bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency.

3.2 Address Resolution protocol

The **Address Resolution Protocol (ARP)** is used to associate a logical address with a physical address. On a typical physical network, such as a LAN,

each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known.

Reverse Address Resolution Protocol

The **Reverse Address Resolution Protocol (RARP)** allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is conected to a network for the first time or when a diskless computer is booted.

Internet Control Message Protocol

The **Internet Control Message Protocol (ICMP)** is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

Internet Group Message Protocol

The **Internet Group Message Protocol (IGMP)** is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer

Traditionally the transport layer was represented in TCP/IP by two protocols; TCP and UDP. IP is a **host-to-host protocol,** meaning that it can deliver a packet from one physical device to another. UDP and TCP are **transport level protocols** responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

User Datagram Protocol

The **User Datagram Protocol (UDP)** is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

Transmission Control Protocol

The **Transmission Control Protocol (TCP)** provides full transport-layer services to applications. TCP in a reliable stream transport protocol. The term stream, in this context, means connection-oriented; A connection must be established between both ends of a transmission before either can transmit data.

At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgement number ofr the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collect each datagram as it comes in and recorders the transmission based on sequence numbers.

Stream Control Transmission Protocol

The **Stream Control Transmission Protocol (SCTP)** provides support for newer application such as voice over the Internet. It is a tranport layer protocol that combines the best features of UDP and TCP.

3.3 Application Layer

The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model. Many protocols are defined at this layer. We cover many of the standard protocols in later chapters.

Addressing

Four levels of addresses are used in an internet employing the TCP/IP protocols : physical (link) addresses, Logical (IP) addresses, port addresses, and specific addresses.

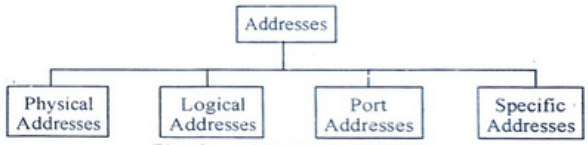


Fig. 2 : Addresses in TCP/IP

Each address is related to a specific layer in the TCP/IP architecture, as show in Figure 3.

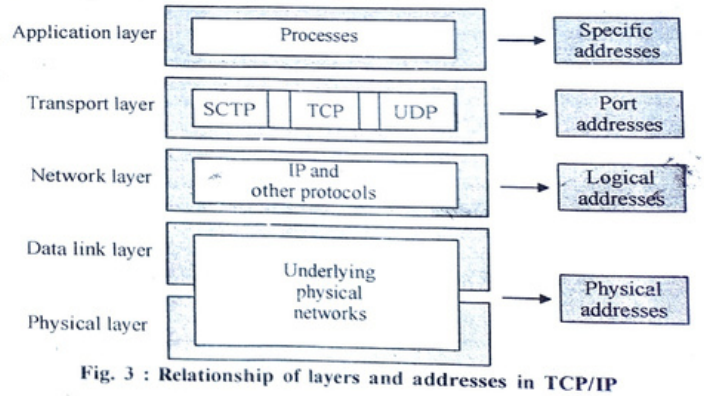


Fig. 3 : Relationship of layers and addresses in TCP/IP

Physical Addresses

The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address.

The physical addresses have authority over the network (LAN or WAN). The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC). Local Talk (Apple), however, has a 1-byte dynamic address that changes each time the station comes up.

Example 1 : In Figure 4 a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). At the data link layer, this frame conains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection. As the figure shows, the computer with physical address 10 is the sender, and the computer with physical adress 87 is the receiver. he data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The header, among other pieces of information, carries the receiver and the sender physical (link) addresses. Note that in most data link protocols, the destination address, 87 in this case, comes before the source address (10 in this case).

We have shown a bus topology for an isolated LAN. In a bus topology, the frame is propagated in both directions (left and right). The frame propagated to the left dies when it reaches the end of the cable if the cable end is terminated appropriately. The frame propagated to the right is sent to every station on the network. Each station with a physical address other than 87 drops the frame because the destination address in the frame does not match its own physical address. The intended destination computer, however, finds a match between the destintion address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is decapsulated and delivered to the upper layer.

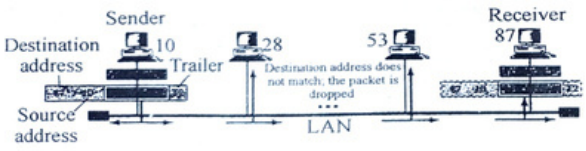


Fig. 4 : Physical addresses

Example 2.2 : Local-area networks use a 48-bit (6-byte) physical address written as 12 headecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below :

Logical Addresses

Logical addresses are necessary for universal communications that are independent of underling physical network. Physical addresses are not adequate in an internetwork environment where different network can have different address formates. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.

The logical address are designed for this purpose. A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

Example 2 : Figure 5 shows a part of an internet with two routes connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection. Although it may obvious that each router must have a separate physical address for each connection, it may not be obvious why it needs a logical address for each connection. We discuss these issues in Chapter 22 when we discuss routing.

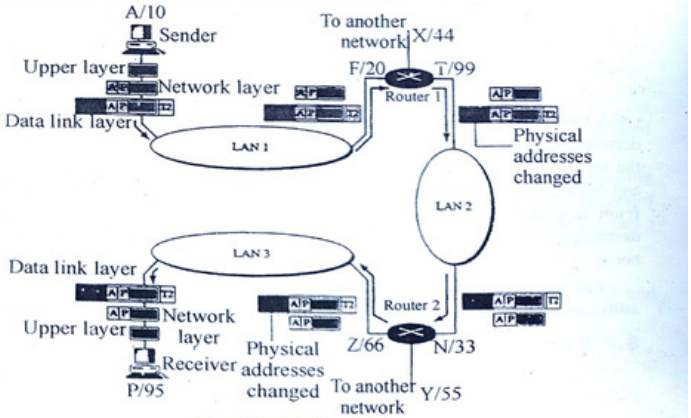


Fig. 5 : IP Addresses

The computer with logical address A and physical address 10 needs to send a packet to the computer with logical address P and physical address 95. We used letters to show the logical addresses and numbers for physical addresses, but not that both are actually numbers.

The sender encapsulates its data in a packet at the network layer and adds two logical addresses (A and P). Note that in most protocols, the logical source address comes before the logical destination address (contrary to the order of physical addresses). The network layer, however, needs to find the physical address of the next hop before the packet can be delivered. The network layer consults its routing table and find the logical address of the next hop (router 1) to be F. The ARP discussed previously finds the physical address of router 1 that corresponds to the logical address of 20. Now the network layer passes this address to the data link layer which in turn, encapsulates the packet with physical destination address 20 and physical source address 10.

The frame is received by every device on LAN 1, but is discarded by all except router 1, which finds that the destination physical address in the frame matches with its own physical address. The router decapsulates the packet from the frame to read the logical destination address P. Since the logical destination address does not match the router's logical address, the router knows that the packet needs to be forwarded. The router consults its routing table and ARP to find the physical destination address of the next hop (router 2), creates a new frame, encapsulates the packet, and sends it to router 2.

Note the physical addresses in the frame. The source physical address changes from 10 to 99. The destination physical address changes from 20 (router 1 physical address) to 33 (router 2 physical address). The logical source and destination addresses must remain the same; otherwise the packet will be lost.

At router 2 we have a similar scenario. The physical addresses are changed and a new frame is sent to the destination computer. When the frame reaches the destination, the packet is decapsulated. The destination logical address P matches the logical address of the computer. The data are decapsulated from the packet and delivered to the upper layer. Note that although **physical address will change from hop to hop, logical addresses remain the same** from the source to destination. There are some exceptions to this rule that we discover later in the book.

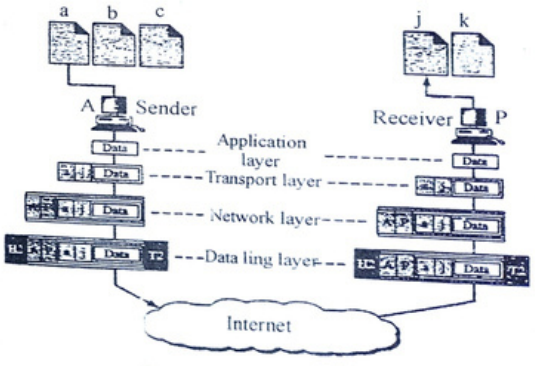
The physical addresses will change from hop to hop, but the logical addresses usually remain the same.

3.4 Port Addresses

The IP address and the physical address are necessary for a quantity of data to travel from a surce to the destination host. However, arrival at the destination

host is not the final objectie of data communications on the Internet. A system that sends nothing but data from one computer to another is not complete. Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, e need a method to label the different processes. In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port addresss in TCP/IP is 16 bits in length.

Example 3 : Figure 6 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although both computers are using the same application, FTP, for example, the port addresses are different because one is a client program and the other is a server program. To show that data from process a need to be dlivered to process j, and not k, the transport layer encapsulates data from the application layer in a packet and adds two port addresses (a and j), source and destination. The packet from the transport layer is then encapsulated in another packet at the network layer with logical source and destination addresses (A and P). Finally, this packet is encapsulated in a frame with the physical source and destination addresses of the next hop. We hae not shown the Internet. Note that although physical addresses change from hop to hop logical and port addresses remain the same from the source to destination. There are some exceptions to this rule that we discuss later in the book.



The physical addresses change from hop to hop, but the logical and port address usually remain the same.

Example 2.5 : a port address is a 16-bit address represented by one decimal number as shown.

753

A 16-bt port address represented as one single number

Specific Addresses

Some applications have user-friendly addresses that are designed for that specific address. Examples include the e-mail address (for example, forouzan @ fhda. edu) and the Universal Resource Locator (URL) (for example, www.mhhe.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.

3.5 Network function

The TCP provides a communication service at an intermediate level between an application program and the Internet Protocol. It provides **host to host** connectivity at the **transport layer** of the Internet model. An application doesn't need to know the particular mechanism for sending data via a link to another host, such as the required packet fragmentation on the transmission medium. At the transport layer, the protocol handles all hand shaking and transmission details and presents an abstraction of the network connection to the application.

At the lower levels of the protocol stack, due to network congestion, traffic load balancing or other unpredictable network behaviour, IP packets may be **lost,** duplicated, or **delivered out of order.** TCP detects these problems, requests **retransmission** of lost data, rearranges out of order data, and even helps minimize network congestion to reduce the occurrence of other problems. If the data still remains undelivered, its source is notified of this failure. Once the TCP receiver has reassembled the sequence of **octets** originally transmitted, it passes them to the receiving application. Thus, TCP abstracts the application's communication from the underlying networking details.

TCP is utilized extensively by many popular applications carried on the internet, including the **World Wide Web (WWW), E-mail, File transfer protocol, Secure shell, peer-to-peer file sharing,** and many **streaming media** application.

TCP is optimized for accurate delivery rather than timely delivery, and therefore, TCP sometimes incurs relatively long delays (on the order of seconds) while waiting for out of order messages or retransmissions of lost message. It is not particularly suitable for real time application such as **voice over IP.** For such applications,

protocols like the **Real time Transport protocol (RTP)** running over the **user datagram protocopl (UDP)** are usually recommended instead (2).

TCP is a retiable stearm delivery servjce that guarantees that all bytes received will be indentical with bytes sent and in the correct order. Since packet transfer over many networks is not reliable, a technique know as positive acknowledgment with retransmission is used to guarantee reliability of Packet transfers. This fundamental technique requires the receiver to respond with and acknowledgment message as it receives the data. The sender keeps a record of each packet it sends. The sender also maintains a timer from when the packet was sent, and retransmits a packet if the timer expires before the message has been acknowledged. The timer is needed in case a packet gets lost or corrupted. (2)

While IP handles actual delivery of the data, TCP keeps track of the individual units of data transmission, called segments, that a message is divided into for efficient routing through the network. For example, when an HTML file is sent from a web server, the TCP software layer of that server divides the sequence of octets of the file into seqments and forwards them individually to the IP software layer **(Internet layer).** The internet layer encapsulate each ICP segment into an IP packet by adding a header that includes (among other data) the destination **IP address.** When the client program on the destination computer receives them the TCP layer **(Transport layer)** reassembles the individual segments, and ensures they are correctly orderded and error free as it streams then to an application.

Protocol Operation

A simplified TCP state diagram. See **TCP EFSM diagram** for a more detailed state diagram including the states inside the ESTABLISHED state.

TCP protocol operations may be divided into three phase connections must be properly established in a multi-step hand shake process (connection establishment) before entering the data transfer phase. After data transmission is completed, the connection termination closes established virtual circuits and releases all allocated resources.

The TCP connection is managed by an operating system through a programming interface that represents the local end point for communications, the **Internet socket.** During the litetime of a TCP connection the local end point undergoes a series of **state** changes. (11)

LISTEN

(Server) represents waiting for a connection request for any remote TCP and port.

SYN-SENT

(Client) represents waiting for a matching connection request after having sent a connection request.

SYN-RECEIVED

(Server) represent waiting for a confirming connection request acknowledgment after having both received and sent a connection request.

ESTABLISHED

(both server and client) represent an open connection, data received can be delivered to user. The normal state for the data transfer phase of the connection.

FIN-WAIT-1

(both server and client) represents waiting for a connection termination request from the remote TCP or an acknowledgment o the connection termination request previously saint.

FIN-WAIT-2

(both server and client) represents waiting for a connection termination request from the remote TCP.

CLOSE-WAIT

(both server and client) represent waiting for a connection termination request from the local user.

CLOSING

(both server and client) represents waiting for a connection termination request acknowledgment from the remote TCP.

LAST-ACK

(both serve and client) represents waiting for an acknowledgement of the connection termination request previously sent to the remote TCP (which includes an acknowledgment of its connection termination request).

TIME-WAIT

(either server or client) represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request. [According to **RFC 793** a connection can stay in TIME-WAIT for a maximum of four minutes known as two **MSL** (maximum segment lifetime).]

CLOSED

(both server and client) represents no connection state at all.

Connection establishment

To establish a connection, TCP uses a three way **hand shake.** Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections : this is called a passive open. Once the passive open once the passive open is established, a client may initiate an active open. To establish a connection, the three way (or 3 steps) handshake occures :

1. **SYN :** The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A.

2. **SYN-ACK :** In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number i.e. A + 1, and the sequence number that the server chooses for the packet is another random number B.
3. **ACK :** finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgment value i.e. A + 1, and the acknowledgment number is set t one more tan the received sequence number i.e. B + 1.

At this point, both the client and server have received an acknowledgment of the connection. The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledgment. The step 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged with these, a full-duplex communication is established.

Comparison TCP/IP to the open system connection refrence model :

The internet protocol suite is the **computer networking** model and set of **communication protocols** used on the **Internet** an similar computer networks. It is commonly known as TCP/IP, because its most important protocols, the **Transmission Control Protocol (TCP)** and the **Internet Protocol (IP)** were the first networking protocols defined in this standard. It is occasionally. Known as DOD model, because the development of the networking model was funded by **DARPA,** an agency o the **united states department of Defence.**

TCP/IP provides end to end connectivity specifying how data should be packetized, addressed, transmitted, **routed** and received at the destination. This functionality is arganized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved. (1) (2) from lowest to highest, the layers are the **link layer,** containing communication methods for data that remains within a single network segment (link); the **internet layer,** connecting independent networks, thus establishing **internet working;** the **transport layer** handling host to host communication; and the **application layer,** which provides process to process data exchange for application.

The TCP/IP model and many of its protocols are maintained by the **Internet Engineering Task Force.**

FTP

The file transfer protocol (FTP) is a standard network protocol used to transfer computer files between a client and server an a computer network.

FTP is built on a client server model architecture and uses separate control and data connection between the client and the server. FTP users may authenticate themreluer with a clear text sign in protocol, normally in the form of a username

and password but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password and encrypt the content FTP is often secured with SSL/TLS (FTPs). SSH file transfer protocol (SFTP) is sometimes also used instead but is technologically different.

The first FTP client applications were command line program developed before operating systems had graphical user interfaces and are still shipped with most windows Unix and Linux operating systems. Many FTP clients and automation utilities have since been developed for deshtops, servers, mobile devices and hardware, and FTP has been incorporated into productivity application such a web page editors.

Telnet

Telnet is an application layer protocol used on the internet text oriented communication facility using a virtual terminal connection. User data is interspersed in ban with telnet control information in an 8 bit byte oriented data connection over the transmission control protocol (TCP).

Telnet was developed in 1969 beginning with RFC 854, and tenderized as internal. Engineering task force (IETF) internet standard STD 8, one of the first internet standards.

Historically, telnet provided access to a connect line interface (usually, of an operating system) on a remote host, including most network equipment and operating system with a configuration utility (including systems based on windows NT). However, because of serious security concers when using telnet over an open network such as the internet, its use for this purpose has wahed significantly in favor of SSH.

The term telnet is also used to refer to the software that implements the client part of the protocol. Telnet client application are available for virtually all computer platforms. Telnet is also used as a verb. To telnet means to establish a connection with the telnet protocol either with command line client or with a programmatic interface. For example, a command directive might be, "To change your password telnet to the server, log in and run the password command. "Most often, a user will be telnetting to a Unix-like server system or a network device (such as a rouer) and obtaining a login prompt to a command line text interface or a character based full screen manager.

History and Standards

Telnet is a client server protocol based on a reliable connection oriented transport. Tropically this protocol in used to establish a connection to transmission control protocol (TCP) port number 23, where a telnet server application (telneted) is listening. Telnet, however, predetes TCP/IP and was originally run over network control program (NCP) protocols.

Before March 5, 1973, Telnet was an ad hoc protocol with no offical definition. (1) Essentially, it used an 8 bit channel to exchange 7-bit ASCII data. They byte with the high bit set was a special telnet character. On march 5, 1973. Telnet protocol stendard was defined at UCLA 2. With the publication of two N/C documants : Telnet protocol specification NIC # 15372, and Telnet option specification. NIC # 15373.

Because of negotiable options protocol architecture, many extensions were for it, some of which have been adopted as internet standards. IETF documents STD 27 through STD 32. Some extensions have been widely implemented and others are proposed standards on the IETF standards track.

When telnet was initially developed in 1969, most users of networked computers were in the computer departments of academic institutions or at large private and government research. In this environment security was not nearly as much a concern the as it become after the handwidth explosion of the 1990 s. The rise in the number of people with access to the internet and by extension the number of people ettempting to lock other people's servers made chcrypted alternatives necessary.

Experts in computer security, such as SANS institute, recommend that the use of telnet for remote logins should be discontinued under all normal circumrtances for the following reasons.

Telnet by deteult does not encrypt any data sent over the connection cincluding passwords, and so it is often feasible to eavesdrop on the communications and use the password later for malicious purpose; anybody who has access to a router, it switch, hub or gateway located on the network between to the two hosts where telnet is being used can intercept the packets passing by an obtain login password and watever else is typed with a packet analyzer.

Most implementations of telnet have no authentication that would ensure communication is carried out between the two desired hosts and not intercepted in the middle.

Several vulnerabilities have been discovered over the years in commonly used telnet doemons.

These security. related shortcoming have seen the usage of the telnet protocol drop rapidly especially on the public internet in favor of the secure shell (SSH) protocol, first released in 1995. SSH provides much of the functionality of the telnet with the addition of strong encryption to prevent sensitive data such as password from being intercepted and public key authentication to ensure that the remote computer is actually who it claims to be as has happened with other early internet protocols extension to the telnet protocol provide transport layer security (TLS) security and simple authentication and security layer (SASL) authentication that address the above concerhs. However, most telnet implementations do not support these extension; and others has been relatively little interest in implementing these as SSH is adequate for most purpose.

If is of note that there are a large number of industrial and scientific devices which have only telnet available as a communication option. Some are built with only a standard RS 232 part and use a serial server hardware appliance to provide the translation between the TCP/Telnet data and the RS-232 serial data. In such cases, SSH is not an option unless the interface app applliance can be configured for SSH.

Domain Name System

The domain name system (DNS) is a hierarchical decentralized naming system for computers services, ar any resource connected to the internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently. It translates more readily memorized domain names to the numorical if addresses needed for the purpose of locating and identifying computer services and devices with the underlying network protocols by providing a worldwide, distributed dirictary service the domain name system is an essential component of the functionality of the internet.

The domain name system deligates the responsibility of assigning domain names and mapping these names to internat resources by designating authoritective name serves for each domain network administrators may delegate authority over sub domains of their allocated name space to other name services. This mecanism provides distroibuted and fault tolerant service and was designed to avoid a single large control database.

The domain name system alsc specifies the technical functionality of the database service which is at its care it defines the DNS protocol a detailed specification of the data structures and data communication exchanges used in the DNA, as pact of the internet protocol suite. Historical other directory services preceding DNS were not scalable to large are global directories as they were originally based on text files. Prominently the hosts. TXT resolver te domain name system has been in use since the 1980s.

The internet maintains two principal namespaces, the domain name hierarchy and the internet protocol (IP) address spaces. The domain name system maintains the domain name hierarchy and provides translation services between it and the address spaces. Internet name servers and a communication protocol implement the domain name system. A DNS name server is a server that stores the DNS records for a domain a DNS name server responds with answers to queries against its database.

The most common types of records stored in the DNS database are for DNS zone authority (SOA), IP addresses (A and AAA), SMTP mail exchangess (MX), name servers (NS), pointers for reverse DNS lookups (PTR), and domain name ariases (CNAME). Although not interded to be a general purpose database, DNS

can store records for other types of data for either automatic lookups such as DNSSEC records, or for human queries such as responsible prson (RP) records. As a general purpose database, the DNS has also been used in compating unsolicited email (spam) by storing a real time blackhole list. The DNS database is traditionally stored in a structured zone file.

An often used analogy to explain the domain name system is that it serves as the phon book for the internet by translating human friendly computer hostnames into. IP addresses. For example, the domain name www. example. com translates to the addresses 93.184.216. 119 (IPr4) and 2606 : 2800 : 220 : 6d : 26 bf : 1447 : 1097 : 997 (IPV6) unlike a phone book DNS can be quickly updates allowing a service's location on the network to change without offecting the end risers who continue to use the same host name users take advantage of this when they use meaningful uniform resource locators (URLS), and email address without having to know now the computer actually locates the services.

Additionally DNS reflects administrative partitioxing. For ionesoprated by a registry, also known as public suffix lones administrative information is often complemented by the registry RDAP and WHOIS services. That data can be used to gain insight an: and track responsibility for, a given host on time internet. An important and ubiquitors function of DNS is its control role in distributed internet services such as cloud services and context delivery networks. When a user accesses a distributed internet services using a URL the domain name of the URL is translated to the IP address of a server that is proximal to the users. The key functionalaty of DNS exploited there is that different users can simultaneously receive different translations for the same domain name, a key point of divergence from a tranditional "phone boo" view of DNS. This process of using DNS to assign proximal servers to users is key to providing foster response times on the internet and is widely used by most major internet services today.

Domain name Space

The domain name spaces consists of a tree data structure. Each made or leaf in the tree has a label and zero or more resource records (RR), which hald infarmation associated with the doamin name. The domain name itself consists of the label, possibly concatenated with the name of its parent node on the right. Separrated by dot. The tree sub-divides into zones beginening at the roat zone. A DNS zone may consist of only one domain or may consist of many domains and sub domains depending on the administrative choices of the zone manager. DNS can also be partitioned according to class; the separate classes can be thought of as an array of parallel namespace trees.

Administractive responsibility over any zone may be divided by creating additional zones authority over the new zone is said to be delegated to a designeted name server the parent zone causes to be authoritive for the new zone.

Domain name syntax

The definitive descriptions of the rules for forming domain names appear in RFC 1035 RFC 1123 and RFC 2181. A domain name consists of one or more parts technically called lables that are conventionally concatenated and delimited by dats, such as example com.

The right most label conveys the top level domain; for example the domain name www. example com belongs to the top level domain com.

The hiererchy of domains descends from right to left; each label to the left specifies a subdivision ar subdomain of the domain to the right. For example the label example specifies a subdomain of the comdomain and www is a subdomain of example com. this tree of subdivisions may have up to 127 levels.

A label may contain zero to 63 cheracters the null label of length zero, is reserved for the roat zone. The full domain name may not exceed the length of 253 characters in its textual representation. In the internal binary representation of the DNS the maximum length requires 255 octets of storage, since it also stores the length o the name.

Although domain names may theoratically consist of any character representable in an actet host names use a preferred format and character set. The characters allowed in their labels are a subset of the ASCII character set, consisting of characters a through Z, digits O through 9, and hyphen. This rule is known as the LDH rule (letters, digits, hyphen) Domain names are interpreted in case independent manner. Labels may not start or end with a hyphen. An additional rule requirs that top level domain name should not be all numeric.

Dynamic host configuration protocol (DHCP)

The dynamic host configuration protocol (DHCP) is a standardized network protocol used on internet protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services with DHCP computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these seffings manually computers use the dynamic host configuration protocol to request internet protocol parameters such as an IP address from a network server. The protocol operates based on the client server model as of 2011, modern networks ranging in size from name networks to large campus networks and regional interact service provider networks commonaly used DHCP most

residential networks routers receive a globally reique IP address within the provider network within a local network DHCP assigns a local IP address to devices connected to the local network.

When a computer or other networked device connects to a networked device connects to a network, the DHCP client software sends a broadcast query requesting necessary information any DHCP server on the network may service the request the DHCP server manages a poal of IP addresses and information about client configuation parameters such as defeult gateway domain name name the name servers and time servers on receiving a request the server may respond with specific inforation for each client, as previously configured by an administrator ar with a specific address and any other information valid for the entire network and for the time period for which the allocation (lease) is valid. A client typically queries for this information immediately after booting and periodically thereafter before the expiration of the information. When a DHCP client refrishes an assignment it initially request the same parameter values, but the DHCP server may assign a new address based on the assignment plalici set by administors.

On large netweok that consist of multiple links, a single DHCP server may service the entire network when aided by DHCP relay agents located on the interconnecting routers. Such agents relay massages between DHCP clients and DHCP servers located on different subnets. Depending on implemaxtation the DHCP server may have three methods of allocating IP addresses.

Dynamic allocation : a network administrator reserves a range of IP addresses for DHCP and each DHCP client of on the LAN is configured to request an IP address from the DHCP server during network initialization. The request and grast process uses a lease concept with a controllable time period, allowing the DHCP server to reclaim (and than reallocate) IP addresses that are not renewed.

Autometic allocatien : The DHCP server permanexty assigns an IP address to a requesting client from the range defined by the administrator. This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments so that it can preferentially assign to a client the same IP address that the client previously had.

Manual allocation : Commonly called static allocation the DHCP server alocates an IP address based on a preconfigured mapping to each client's MCA address. THis feature is variously called static DHCP assignment y DD-WRI, fixed address by the dncpd documantation, address reservation by metgear, DHCP reservation or static DHCP by cisco and linksys, and IP address reservation of MCA/IP address binding by various other roonter manufactures.

DHCP is used for internet protocol version 4(IPV4) as well as for IPV6. While both versions serve the same purpose, the details of the protocol for IPV6 differ sufficiently that tey may be considered separate protocols. For the IPV6 operation

devices may alternatively use stateless address autoconfiguration. IPV6 hosts may also use link local addressing to achieve operations restricted the local network link.

In computing looking (or booting up) is the utialization of computerized system. The system can be computer of a computer appliance. The booting process be "lard" after electrical power to the CPU is switched from oof to on (in order to diaghose particular hardware errors or "soft". when tose power on self tests (post) can be avoided soft booting can be initiated by hardware such as a button press, or by software command. Booting is complete when the normal operative runtime environment is attained.

Boot

A boot loader is a computer program that loads an operating system or some other system software for the computer after completion of the power on self tests, it is the loader for the operating system inself within the hard reboot process, it runs after completion of the self tests then loads and runds the software. A tests than loads and runs the software. A boot loader is loaded into main memory from persistext memory, such as a hard disk drive or in some order computers, from a medium such as punched cords, punched tape or magnetic tape. The boot loader than loads and executes the processes that finalize the boot, like post processes, the boot loader codes come from a "hard wired" and presistext location if that location is too limited for some reason, that primary boot loader calls a second stage boot loader or secondary program loader.

On modern general purpose computers, the boat up process can take tens of seconds and typically ivalves performing a power on serf-text, locating and inilializing peripheral devices, and then finding leading and starting an operating system. The process of hibernating or sleeping does not involve boating minimally, some embedded system do not require a noticeable boat sequence to begin functioning and when turned on may simply run operational progress that are stored in ROM. All computing systems are state machines and a reboot may be the only method to return to a designated zero state from an uninstalled clocked state.

Boot is start for bootstrap are bootstrap load and derives from the phrase to pull oneself up by one's bootstrayss. The calls attention to the requirement threat, if most software is loaded onto a computer by other software already runing on the computer, some mechanism must exit to load the initial software onto the computer. Early computers used a variety of ad-hoc methos to get a small program into memory to solve this problem the invention of read only memory (ROM) of various types solved this paradox by allowing computers to be shipped with a start up program that could not be erased growth in the capacity of ROM has allowed even more elaborate start up procedures to be implemented.

Connection less Communication

Connection less internet working

Connection less communication often referred to is CL-mode communication, is a data transmission method used in packet switching networks by which each data unit is individualy addressed and routed based on information carried in each unit rather than in the setup information of a prearranged, fixed data channel as in connection oriented communication.

Under connectionless communication between two network end points a massage can be sent from one end point to another without prior arrangement. The device at one of at the communication transmits data addressed to the other, without first ensuring that the recipient is available and ready to receive that data. Some protocols allow for error correction by reqursted retransmission. Internet protocol (IP) and user datagram protocol (UDP) are connectionless protocols.

A packet transmitted in a connectionless mode is frequently called a datagram.

Connectionless protocols are usually described us stateless protocolex because the end points have no protocol defined way to remember where tey are in d " conversation " of message exchanges.

In connection oriented communication the communicating peers must first establish a logical or physical data channel or connection in a dialog preceding the exchange of user data.

The connectionless communications that service provider usually cannel guarantee that there will be to less error insertion, misdelivery, duplication or out of sequence delivery of the packet. However, the effect of errors may be reduced y implemently error correction within an application protocol.

In connectionless mode no optimizations are possible when sending several data units between the same two peers. By establishing a connection at the beginning of such a data exchange the component (routers bridges) along the network path would be able to pre-computer (and hence cache) routing related information, avoiding re-computation for every pocket. Network components could also reserve capacity for the transfer o the subsequent data units of a video download for example.

Distinction between connectionless and connection oriented transmission may take place at several layers of the OSI reference model.

Transport layer : TCP is a connection oriented transport protocol UDP is connectionless.

Network layer.

Data link layer : The IEEE 802.2 protocol at the logicalk link control sublayer of the data link layer may provide both connectionless and connection oriented services. In fact some network protocols (such as SNA s path control in its early stages) require a connection oriented data link connectionless data link service ds well.

Notable connectionless protocols
- Internet protocol (IP)
- User Datagram Protocoal (UDP)
- Internet Control Message protocol (ICMP)
- Internetwork packet exchange (IPX)
- TIPC
- Net BEUI

3.6 Internet protocol (IP)

The Internet protocol suite is the computer networking model and set of communications protocols used on the Internet and similar computer networks. It is commonly known as TCP/IP, because its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP) were the first networking protocols defined in this standard. It is occasionally known as the 000 model, because the development of the networking model was funded by DARPA, an agency of the United States Department of Defense.

TCP/IP provides end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed and received at the destination. This functionality is organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved. [1][2] From lowest to highest, the layers are the link layer, containing communication methods for data that remains within a single network segment (link); the internet layer, connecting independent networks, thus establishing internetworking; the transport layer handling host-to host communication; and the application layer, which provides process-to-process data exchange for applications.

The TCP/IP model and many of its protocols are maintained by the Internet Engineering Task Force (IETF) .

The Internet protocol suite resulted from research and development conducted by the Defense Advanced Research Projects Agency (DARPA) in the late 1968s. [3] After initiating the pioneering ARPANET in 1969, DARPA started work on a number of other data transmission technologies. In 1972, Robert E. Kahn joined the DARPA Information Processing Technology Office, where he worked on both satellite packet networks and ground-based radio packet networks, and recognized the value of being able to communicate across both. In the spring of 1973, Vinton Cerf, the developer of the existing ARPANET Network Control Program (NCP) protocol, joined Kahn to work on open-architecture interconnection models with the goal of designing the next protocol generation for the ARPANET.

By the summer of 1973, Kahn and Cerf had worked out a fundamental reformulation, in which the differences between network protocols were hidden by using a common internetwork protocol, and, instead of the network being responsible

for reliability, as in the ARPANET, the hosts became responsible. Cerf credits Hubert Zimmermann and Louis Pouzin, designer of the CYCLADES network, with important influences on this design.

The design of the network included the recognition that it should provide only the functions of efficiently transmitting and routing traffic between end nodes and that all other intelligence should be located at the edge of the network, in the end nodes. Using a simple design, it became possible to connect almost any network to the ARPANET, irrespective of the local characteristics, thereby solving Kahn's initial problem. One popular expression is that TCP/IP, the eventual product of Cerf and Kahn's work, win run over "two tin cans and a string." (Years later, as a joke, the IP over Avian Carriers formal protocol specification was created and successfully tested.)

A computer called a router is provided with an interface to each network. it forwards packets back and forth between them. [4] Originally a router was called gateway, but the term was changed to avoid confusion with other types of gateways Speci fication.

From 1973 to 1974, Cerf's networking research group at Stanford worked out details of the idea, resulting in the first TCP specification. [5] A significant technical influence was the early networking work at Xerox PARC, which produced the PARC Universal Packet protQcol suite, much of which existed around that time.

DARPA then contracted with BBN Technologies, Stanford University, and the University College London to develop operational versions of the protocol on different hardware platforms. Four versions were developed: TCP vI, TCP v2, TCP v3 and IP v3, and TCP/IP v4. The last protocol is still in use today.

In 1975, a two-network TCP/IP communications test was performed between Stanford and University College London (UCL). In November, 1977, a three-network TCP/IP test was conducted between sites in the US, the UK, and Norway. Several other TCP/IP prototypes were developed at multiple research centers between 1978 and 1983. The migration of the ARPANET to TCP/IP was officially completed on flag day January I, 1983, when the new protocols were permanently activated. [6] Adoption

In March 1982, the US Department of Defence declared TCP/IP as the standard for all military computer networking. [7] In 1985, the Internet Advisory Board (later renamed the Internet Architecture Board) held a three-day workshop on TCP/IP for the computer industry, attended by 258 vendor representatives, promoting the protocol and leading to its increasing commercial use.

In 1985, the first Interop conference focused on network interoperability by broader adoption of TCP/ IP. The conference was founded by Dan Lynch, an early Internet activist. From the beginning, large corporations, such as IBM and DEC, attended the meeting. Interoperability conferences have been held every year since

then. Every year from 1985 through 1993, the number of attendees tripled. [citation needed]

IBM, AT&T and DEC were the first major corporations to adopt TCP/IP, despite having competing internal protocols (SNA, XNS, etc.). In IBM, from 1984, Barry Appelman's group did TCP/IP development. (Appelman later moved to AOL to be the head of all its development efforts.)'They navigated the corporate politics to get a stream of TCP/IP products for various IBM systems, including MVS, VM, and OS/2. At the same time, several smaller companies began offering TCP/IP stacks for DOS and MS Windows, such as the company FTP Software, and the Wollongong Group. [8] The first VM/CMS TCP/IP stack came from the University of Wisconsin. [9].

Many of these TCP/IP stacks were written single-handedly by a few talented programmers. For example, John Romkey of FTP Software was the author of the MIT PC/IP package. [10] John Romkey's PC/IP implementation was the first IBM PC TCP/IP stack. Jay Elinsky and Oleg Vishnepolsky of IBM Research wrote TCP/IP stacks for VM/CMS and OS/2, respectively. [11]

The spread of TCP/IP was fueled further in June 1989, when AT&T agreed to place the TCP/IP code developed for UNIX into the public domain. Various vendors, including IBM, included this code in their own TCPjIP stacks. Many companies sold TCP/IP stacks for Windows until Microsoft released a native TCP/ IP stack in Windows 95. This event was a little late in the evolution of the Internet, but it cemented TCP/IP's dominance over other protocols, which began to lose ground.

Internet protocol (ipv6)

An Internet Protocol Version 6 address (IPv6 address) is a numerical label that is used to identify a network interface of a computer or other network node participating in an IPv6 computer network.

An IP address serves the purpose of uniquely identifying an individual network interface of a host, locating it on the network, and thus permitting the routing of IP packets between hosts, For routing, IP addresses are present in fields of the packet header where they indicate source and destination of the packet.

IPv6 is the successor to the first addressing infrastructure of the Internet, Internet Protocol version 4 (IPv4). In contrast to IPv4, which defined an IP address as a 32-bit value, IPv6 addresses have a size of 128 bits. Therefore, IPv6 has a vastly enlarged address space compared to IPv4.

IPv6 address classes

IPv6 addresses are classified by the primary addressing and routing methodologies common in networking: unicast addressing, anycast addressing, and multicast addressing. [1] 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 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.

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 does not implement broadcast addressing. Broadcast's traditional role is subsumed by multicast addressing to the all-nodes link-local multicast group ff02::1. However, the use of the all-nodes group is not recommended, and most IPv6 protocols use a dedicated link-local multicast group to avoid disturbing every interface in the network.

Address formats

An IPv6 address consists of 128 bits. [1] Addresses are classified into various types for applications in the major addressing and routing methodologies: unicast, multicast, and anycast networking. In each of these, various address formats are recognized by logically dividing the 128 address bits into bit groups and establishing rules for associating the values of these bit groups with special addressing features. Unicast and anycast address format

Unicast and anycast addresses are typically composed of two logical parts: a 64-bit network prefix used for routing, and a 64-bit interface identifier used to identify a host's network interface.

General unicast address format (routing prefix size varies) bits 48 (or more) 16 (or fewer) 64 field routing prefix subnet id interface identifier

The network prefix (the routing prefix combined with the subnet id) is contained in the most significant 64 bits of the address~ The size of the routing prefix may vary; "a larger prefix size means a smaller subnet id size. The bits of the subnet id(entifier) field are available to the network administrator to define subnets within the given network. The 64-bit interface identifier is either automatically generated from the interface's MAC address using the modified EU1-64 format, obtained from a DHCPv6 server, automatically established randomly, or assigned manually.

A link-local address is also based on the interface identifier, but uses a different format for the network prefix.

Link-local address format bits 10 54 64

field prefix zeroes interface identifier

The prefix field contains the binary value 1111111010. The 54 zeroes that follow make the total network prefix the same for all link-local addresses (fe80::/64 link-local address prefix), rendering them non-routable.

Multicast address format

For more details on this topic, see Multicast address § 1Pv6. Multicast addresses are formed according to several specific formatting rules, depending on the application.

General multicast address format bits 8 4 4 112

field prefix flg sc group 1D

The prefix holds the binary value 11111111 for any multicast address.

Currently, 3 of the 4 flag bits in the flg field are defined; [1] the most-significant flag bit is reserved for future use.

Multicast address flags[2] bit flag Meaning when 0

8 reserved reserved reserved

9 R (Rendezvous) [3] Rendezvous point not embedded Rendezvous point embedded

10 P (Prefix)[4] Without prefix information Addreess based on network prefix

11 T (Transient) [1] Well-known multicast address Dynamically assigned multicast address

The 4-bit scope field (sc) is used to indicate where the address is valid and unique.

There are special multicast addresses, like Solicited Node.

Solicited-Node multicast address format bits 8 4 4 79 9 24

field prefix flg sc zeroes ones unicast address

The sc(ope) field holds the binary value 0010 (link-local). Solicited-node multicast addresses are computed as a function of a node's unicast or anycast addresses. A solicited-node multicast address is created by copying the last 24 bits of a unicast or anycast address to the last 24 bits of the multicast address.

Unicast-prefix-based multicast address format[3] [4] bits 8 4 4 4 4 8 64 32

field prefix flg sc res riid plen network prefix group 1D

Link-scoped multicast addresses use a comparable format. [5]

Presentation

An 1Pv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:). An example of an 1Pv6 address is:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

The hexadecimal digits are case-insensitive, but 1ETF recommendations suggest the use of lower case letters. The full representation of eight 4-digit groups may be simplified by several techniques, eliminating parts of the representation.

Leading zeroes

Leading zeroes in a group may be omitted. [1] Thus, the example address may be written as:

2001:db8:85a3:0:0:8a2e:370:7334

Groups of zeroes

One or more consecutive groups of zero value may be replaced with a single empty group using two consecutive colons (: :). [1] Thus, the example address can be further simplified:

2001:db8:85a3: :8a2e:370:7334

The localhost (loopback) address, 0:0:0:0:0:0:0:1, and the IPv6 unspecified address, 0:0:0:0:0:0:0:0, are reduced to ::1 and::, respectively. This two-colon replacement may only"be applied once in an address, because multiple occurrences would create an ambiguous representation.

Dotted-quad notation

During the transition of the Internet from IPv4 to IPv6 it is typical to operate in a mixed addressing environment, and for this purpose a special notation has been introduced to express IPv4-mapped and IPv4-compatible IPv6 addresses by writing the final 32 bits of an address in the familiar IPv4 dottedquad notation. For example, the IPv4-mapped IPv6 address: :ffff:c000:0280 is"usually written as ::ffff:192.0.2.128, thus expressing clearly the original IPv4 address that was mapped to IPv6.

Routing protocol

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network. Although there are many types of routing protocols, three major classes are in widespread use on IP networks: Interior gateway protocols type 1, link-state routing protocols, such as OSPF and IS-IS Interior gateway protocols type 2, distance-vector routing protocols, such as Routing Information Protocol, RIPv2, IGRP.

Exterior gateway protocols are' routing protocols used on the Internet for exchanging routing information between Autonomous Systems, such as Border Gateway Protocol (BGP), Path Vector Routing Protocol. Please notice that the term "Exterior gateway protocol" has two meanings. It could mean a category of protocols used to exchange routing information between autonomous systems (see: exterior gateway protocol). It could also mean a specific RFC-described protocol (see: Exterior Gateway Protocol).

Many routing protocols are defined in documents called RFCs. [1][2] [3] [4]

Some versions of the Open System Interconnection (OSI) networking model distinguish routing protocols in a special sublayer of the Network Layer (Layer 3).

The specific characteristics of routing protocols include the manner in which they avoid routing loops, the manner in which they select preferred routes, using information about hop costs, the time they require to reach routing convergence, their scalability, and other factors.

OSI layer designation

Routing protocols, according to the OSI routing framework, are layer management protocols for the network layer, regardless of their transport mechanism: IS-IS runs on the data link layer (Layer 2) Open Shortest Path First (OSPF) is encapsulated in IP, but runs only on the IPv4 subnet, while the IPv6 version runs on the link using only link-local addressing. IGRP, and EIGRP are directly encapsulated in IP. EIGRP uses its own reliable transmission mechanism, while IGRP assumed an unreliable transport.

RIP runs over UDP

BGP runs over TCP

Interior gateway protocols

Interior gateway protocols (IGPs) exchange routing information within a single routing domain.

Examples of IGPs include:

Open Shortest Path First (OSPF)

Routing Information Protocol (RIP)

Intermediate System to Intermediate System (IS-IS)

Enhanced Interior Gateway Routing Protocol (EIGRP)[a]

Exterior gateway protocols exchange routing information between autonomous systems. Examples include:

Exterior Gateway Protocol (EGP)

Border Gateway Protocol (BGP)

Routing software

Many software implementations exist for most of the common routing protocols. Examples of open-source applications are Bird Internet routing daemon, Quagga, GNU Zebra, OpenBGPD, OpenOSPFD, and XORP.

Routed protocols

Some network certification courses distinguish between routing protocols and" routed protocols. A routed protocol is used to deliver application traffic. It provides appropriate addressing information in its Internet Layer (Network Layer) addressing to allow a packet to be forwarded from one network to another.

User Datagram Protocol (UDP)-

The User Datagram Protocol (UDP) is one of the core members of the Interpet protocol suite. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768. UDP uses a simple connectionless transmission model with a minimum of protocol mechanism. It has no handshaking dialogues, and thus exposes the user's program to any un reliability of the underlying network protocol. There is no guarantee of delivery, ordering, or duplicate protection. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.

With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. UDP is suitable for purposes where error checking and correction is either not necessary or is performed in the application, avoiding the overhead of such processing at the network interface level. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system. [1] If error correction facilities are needed at the network interface level, an application may use the Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP) which are designed for this purpose.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.

SNMP is widely used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. Overview and basic concepts Principle of SNMP Communication In typical uses of SNMP one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

An SNMP-managed network consists of three key components:

Managed device

Agent - software which runs on managed devices

Network management station (NMS) - software which runs on the manager

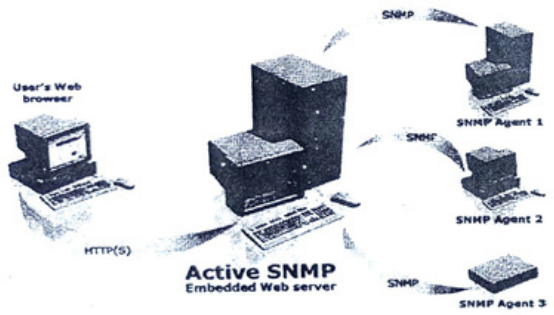
A managed device is a network node that implements an SNMP interface that allows unidirectional (readonly) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, 2witches, cable modems, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.

A network management station (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

Overview and basic concepts

In typical SNMP usage, there are a number of systems to be managed, and one or more systems managing them. A software component called an agent (see below) runs on each managed system and reports information via SNMP to the managing systems.



Essentially, SNMP agents expose management data on the managed systems as variables (such as "free memory", "system name", "number of running processes", "default route"). But the protocol also permits active management tasks, such as modifying and applying a new configuration. The managing system can

retrieve the information through the <iET, GETNEXT and GETBULK protocol operations or the agent will send data without being asked using TRAP or INFORM protocol operations. Management systems can also send configuration updates or controlling requests through the SET protocol operation to actively manage a system. Configuration and control operations are used only when changes are needed to the network infrastructure. The monitoring operations are usually performed on a regular basis. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases(MIBs). SNMP is part of the Internet network management architecture. This architecture is based on the interaction of many entities, as described in the following section.

The Internet Management Model

As specified in Internet RFCs and other documents, a network management system comprises:

- **Network elements** - Sometimes called managed devices, network elements are hardware devices such as computers, routers, and terminal servers that are connected to networks .
- **Agents-** Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Managed object-** A managed object is a characteristic of something that can be managed. For example, a list of currently active TCP circuits in a particular host computer is a managed object. Managed objects differ from variables, which are particular object instances. Using our example, an object instance is a single active TCP circuit in a particular host computer. Managed objects can be scalar (defining a single object instance) or tabular (defining multiple, related instances) .
- **Management information base (MIB)-** A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules .
- **Syntax notation -** A syntax notation is a language used to describe a MIB's managed objects in a machine-independent format. Consistent use of a syntax notation allows different types of computers to share information. Internet management systems use a subset of the International Organization for Standardization's (ISO's) Open System Interconnection (OSI) Abstract Syntax Notation (ASN.1) to define both the packets exchanged by the management protocol and the objects that are to be managed .
- **Structure of Management Information (SMI) -** The SMI defines the rules for describing management information. The SMI is defined using ASN.J .

- **Network management stations (NMSs)**- Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
  Parties - Newly defined in SNMPv2, a party is a logical SNMPv2 entity that can initiate or receive SNMPv2 communication. Each SNMPv2 party comprises a single, unique party identity, a logical network location, a single authentication protocol, and a single privacy protocol. SNMPv2 messages are communicated between two parties. An SNMPv2 entity can define multiple parties, each with different parameters. For example, different parties can use different authentication and/or privacy protocols .
- Management protocol - A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

Exercises

Very Short Questions [2 marks each]

1. What is TCP ?
2. What is IP address ?
3. What is FTP ?
4. Explain Telnet ?
5. What is UDP ?
6. What is SNMP ?
7. What is the work of IPX ?
8. Explain network.
9. How many types of network we use ?
10. What is Interior gateway protocol.

Short Questions [4 marks each]

1. Explain TCP and IP.
2. What is connection less Networking ?
3. What is protocol, explain.
4. What is Domain name space and Domain name syntax ?
5. Explain FTP and Telnet.

Long Questions [12 marks each]

1. Explain TCP and UDP? Explain how you will choosen between TCP and UDP, compare them.
2. Explain connection less network with diagram.
3. Compare TCP and UDP with diagram.
4. What is Network function and protocol operation ? Explain.
5. Explain protocols with diagram.

■■■