MINISTRY OF DEVELOPMENT OF INFORMATION TECHNOLOGIES AND COMMUNICATIONS

FERGANA BRANCH OF TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES NAMED MUHAMMAD AL - XORAZMIY

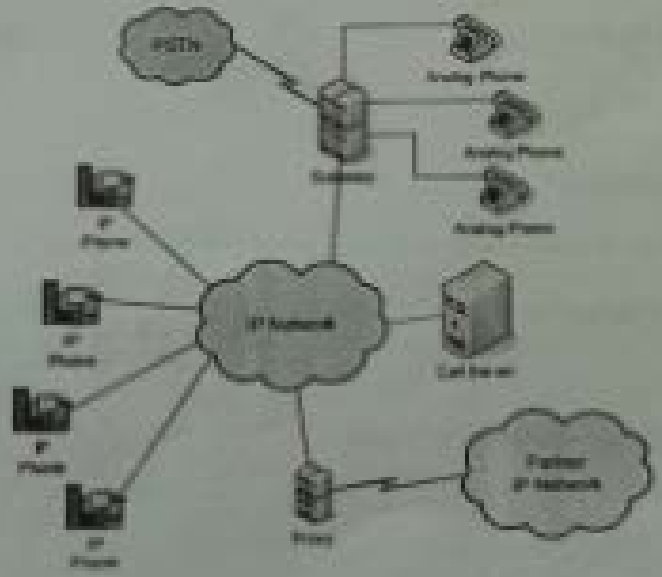
Faculty of "Telecommunication technologies and professional education"

Department of "Telecommunication inginiring"

LECTURES

by **"Internet networks and services"**

for the students of the direction of **"Telecommunication technology"**



Fergana 2017

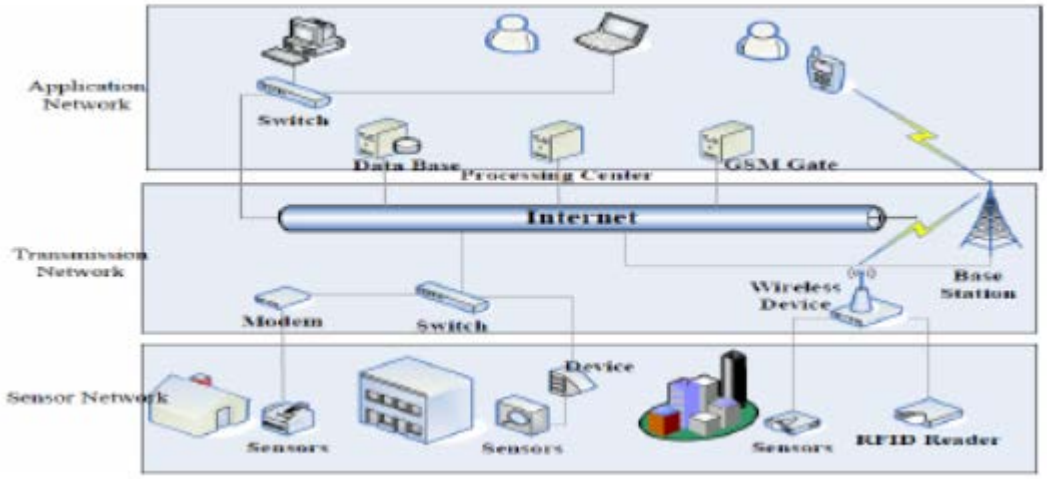
Lecture#1

Theme: Introduction. Purpose of object. Structure chart of internet network.

The Internet, also known as the "Net" is an international system where computers are linked together in a network that permits different data communication servers to operate. These include e-mail, the World Wide Web, newsgroups and FTP. In general the Internet is a means of publishing information about anything and everything. It can be said that the Internet has revolutionised the world of communications.

Introduction DURING the recent years mobile devices have been embraced by everyone, thus creating a huge market that is expected to evolve even more in the years to come. One of the many fields of their application is the medical domain [1], as they are considered to be a great means of improving provided healthcare. An increasing number of healthcare professionals utilize applications that enable remote monitoring or healthcare management. Moreover, many consumers already take advantage of m-health applications to improve and assist their own health [2]. Internet of Things (IoT) is a novel paradigm that realizes intelligent identification, location, tracking, monitoring, and management by connecting anything to the Internet [3]. The basic idea of this concept is the ability of many objects around us to interact and cooperate with each other in order to achieve common goals [4] towards pervasive healthcare. For example, according to [5], IoT uses as an approach to improve mental health problems like depression. Indeed, it is an integrated part of Future Internet with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities [6]. The obsessions and compulsions that characterize obsessive-compulsive disorder (OCD) greatly interfere with life and trap the individual in a cycle of distressing, anxiety- provoking thoughts and behaviors. The symptoms of OCD are time-consuming, irrational, and distracting, and the individual may desperately wish to stop them. The most common compulsions involve the repetition of a specific behaviour, such as washing and cleaning, counting, putting items in order, checking, or requesting assurance [7]. II. I NTERNET O F T HINGS The concept of the

Internet of Things (IoT) is to make every single ‘network enabled’ object in the world network connected, and represents a vision in which the Internet extends into the real world embracing everyday objects [8]. IoT comes from the Auto-ID Center at the Massachusetts Institute of Technology (MIT), which in 1999 started to design and propagate across-company radio frequency identification (RFID) infrastructure [9]. Internet of things directs the world into the intelligence so that collaboration these things not only improves business development of organizations but also improves managing and controlling in medical centers. Figure 1 shows the structure of the internet of things. In the sensor network level, objects will identify and information will gather from object. In the transmission network level, contain integration network of communication and internet, network management center, information center and intelligent processing centers. In the application network, contain integration of the Internet of Things with the professional industry technology and help to organizations for achieving intelligence.



In this Website I hope to explore the historical development of the Internet. The pages will contain information including the development of the World Wide Web, the ownership and structure, the media and communications, the research and commercial developments that now impact on our daily lives.

The internet impacts heavily upon the way that we live, study and work. But it hasn't always been that way. In the 1960s ARPA, a part of the American Department of Defence, funded several large computing projects. These projects were very expensive and

situated in different parts of the USA. It was unreasonable to expect research groups to travel to each of these sites, and it was far too expensive to build more of them, what was needed was a method to link them together so that information could be easily exchanged. ARPANET was created, basing communication on *packet switching*. This system of communication broke messages into chunks which were then passed to other sites using a network of interlinked computers. Due to the unreliable nature of connections, if any link in the network broke, a packet could be re-routed around the problem to reach its destination. The concept is similar to how drivers can take different routes when they meet a blocked off road.

The Internet is basically a hierarchy that allows any Internet connected device in one geographic location, talk to another Internet connected device in another geographic location. The way that the information is transmitted varies greatly, and in some countries, wireless ham radios are even used to transmit email. Keep in mind that the word "connected" is used very loosely here.

Lecture#2

Theme: Types of transmission medium in the internet network. Classification of computer networks

Transmission media is a pathway that carries the information from sender to receiver. We use different types of cables or waves to transmit data. Data is transmitted normally through electrical or electromagnetic signals.

An electrical signal is in the form of current. An electromagnetic signal is series of electromagnetic energy pulses at various frequencies. These signals can be transmitted through copper wires, optical fibers, atmosphere, water and vacuum Different Medias have different properties like bandwidth, delay, cost and ease of installation and maintenance. Transmission media is also called Communication channel.

Types of Transmission Media

Transmission media is broadly classified into two groups.

1. Wired or Guided Media or BoundTransmission Media

2. Wireless or Unguided Media or Unbound Transmission Media

Wired or Guided Media or Bound Transmission Media: Bound transmission media are the cables that are tangible or have physical existence and are limited by the physical geography. Popular bound transmission media in use are twisted pair cable, co-axial cable and fiber optical cable. Each of them has its own characteristics like transmission speed, effect of noise, physical appearance, cost etc.

Wireless or Unguided Media or Unbound Transmission Media: Unbound transmission media are the ways of transmitting data without using any cables. These media are not bounded by physical geography. This type of transmission is called Wireless **communication.** Nowadays wireless communication is becoming popular. Wireless LANs are being installed in office and college campuses. This transmission uses Microwave, Radio wave, Infra red are some of popular unbound transmission media.

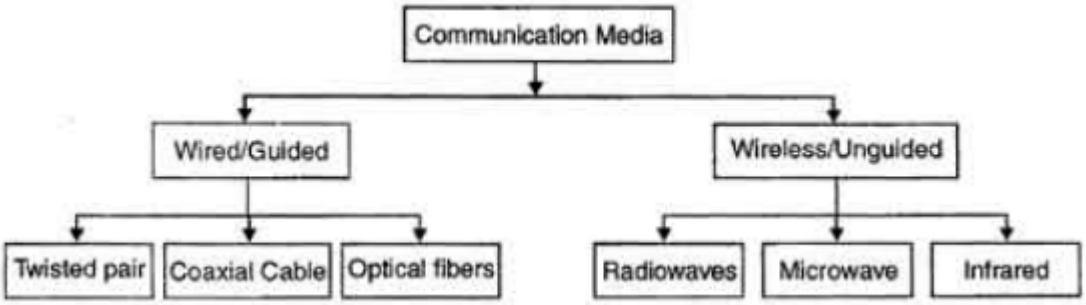


Fig. . Classification of communication media

The data transmission capabilities of various Medias vary differently depending upon the various factors. These factors are:

1. **Bandwidth**. It refers to the data carrying capacity of a channel or medium. Higher bandwidth communication channels support higher data rates.

2. **Radiation**. It refers to the leakage of signal from the medium due to undesirable electrical characteristics of the medium.

3. **Noise Absorption**. It refers to the susceptibility of the media to external electrical noise that can cause distortion of data signal.

4. **Attenuation**. It refers to loss of energy as signal propagates outwards. The amount of energy lost depends on frequency. Radiations and physical characteristics of media contribute to attenuation.

Lecture#3

Theme: Different types of internet connections. Local networks and their components.

There are many ways a personal electronic device can connect to the internet. They all use different hardware and each has a range of connection speeds. As technology changes, faster internet connections are needed to handle those changes. I thought it would be interesting to list some of the different types of internet connections that are available for home and personal use, paired with their average speeds.

Dial-Up (Analog 56K).

Dial-up access is cheap but slow. A modem (internal or external) connects to the Internet after the computer dials a phone number. This analog signal is converted to digital via the modem and sent over a land-line serviced by a public telephone network. Telephone lines are variable in quality and the connection can be poor at times. The lines regularly experience interference and this affects the speed, anywhere from 28K to 56K. Since a computer or other device shares the same line as the telephone, they can't be active at the same time.

DSL. DSL stands for Digital Subscriber Line. It is an internet connection that is always "on". This uses 2 lines so your phone is not tied up when your computer is connected. There is also no need to dial a phone number to connect. DSL uses a router to

transport data and the range of connection speed, depending on the service offered, is between 128K to 8 Mbps.

Cable. Cable provides an internet connection through a cable modem and operates over cable TV lines. There are different speeds depending on if you are uploading data transmissions or downloading. Since the coax cable provides a much greater bandwidth over dial-up or DSL telephone lines, you can get faster access. Cable speeds range from 512K to 20 Mbps.

Wireless. Wireless, or Wi-Fi, as the name suggests, does not use telephone lines or cables to connect to the internet. Instead, it uses radio frequency. Wireless is also an always on connection and it can be accessed from just about anywhere. Wireless networks are growing in coverage areas by the minute so when I mean access from just about anywhere, I really mean it. Speeds will vary, and the range is between 5 Mbps to 20 Mbps.

Satellite. Satellite accesses the internet via a satellite in Earth's orbit. The enormous distance that a signal travels from earth to satellite and back again, provides a delayed connection compared to cable and DSL. Satellite connection speeds are around 512K to 2.0 Mbps.

Cellular. Cellular technology provides wireless Internet access through cell phones. The speeds vary depending on the provider, but the most common are 3G and 4G speeds. A 3G is a term that describes a 3rd generation cellular network obtaining mobile speeds of around 2.0 Mbps. 4G is the fourth generation of cellular wireless standards. The goal of 4G is to achieve peak mobile speeds of 100 Mbps but the reality is about 21 Mbps currently.

Follow these step-by-step instructions to connect to WI-FI

Step 1: Set up your wireless router - an example of which is on the right - (see How to connect to the internet for instructions). Most internet providers now supply wireless routers as standard. When setting up one, it's important to provide appropriate security so that your computer can't be entered by anyone but you. Instructions for this should be supplied with the router, but if in doubt, consult an expert.

Step 2: Check that your computer has a built-in wireless adaptor. Up-to-date laptops generally have one, but most desktop computers don't.

To check whether there’s a built-in adaptor you can search for **'Device manager'** on your computer. Then find **'Display adaptors'.**

If there is a wifi adaptor, a wifi icon should also appear in the system tray in the bottom right-hand corner of the screen. In Windows 10,

If you don’t have a wireless adaptor, you’ll need to buy one to plug into one of your computer’s USB ports. The adaptor should be supplied complete with instructions on how to use it to connect to a wireless network.

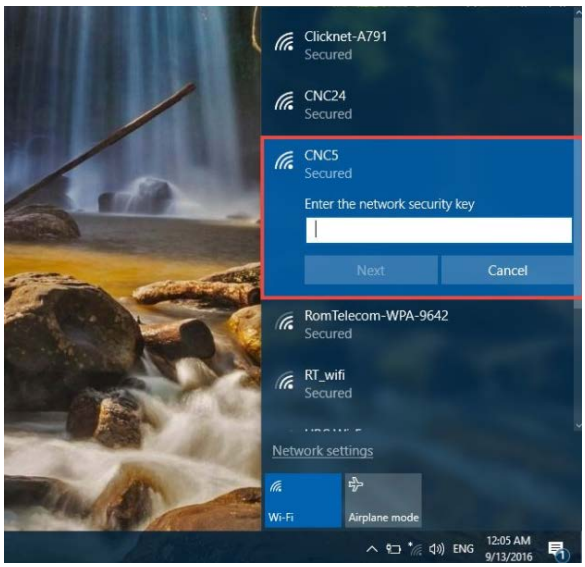
For laptops select the Network icon on the system tray. The icon that appears depends on your current connection state. If you don’t see one of the network icons below or a similar one, select Up arrow icon to see if it appears there.

Step 3: To connect to a wireless network, click the wifi icon. You should now see a list of available networks

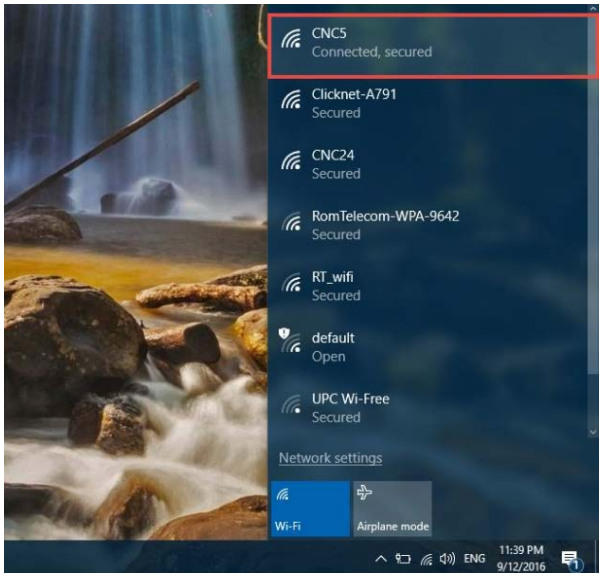
Step 4: To connect to a network, just click on its name. If it’s a secure network and it’s the first time you’ve used it, you’ll need a password. If it’s your home network, your internet provider will have given you a password – sometimes it’s printed on a sticker attached to the router.

If you’ll be using the same connection regularly, you can tick the box to connect automatically.

Step 5: Once you establish a connecion, your Windows 10 PC will ask you whether you want to set its location as private or as public. If you choose Yes , you will “allow your PC to be discoverable by other PCs and devices on this network” , and it’s what you should do if you are connecting to your home or work wireless network. If you are connecting to a public wireless network, choose No. If you don’t choose anything and simply close this dialog, you should know that Windows 10 will set this new network as public, by default.



Once you have done this your device is finally connected to the internet.



Warning: Be very careful if you connect to unsecured wireless networks such as WI-FI ‘hotspots’ in public places. While on them, it’s important not to use websites that require you to enter personal or financial details as other users of the network could gain access to these details.

Lecture#4

Theme: Main devices and their functions of internet network, Transmission principle of packet data. Main types of the routing methods.

Networking hardware, also known as network equipment or computer networking devices, are physical devices which are required for communication and interaction between devices on a computer network. Specifically, they mediate data in a computer

network.[1] Units which are the last receiver or generate data are called hosts or data terminal equipment.

Hub is one of the basic icons of networking devices which works at physical layer and hence connect networking devices physically together. Hubs are fundamentally used in networks that use twisted pair cabling to connect devices. They are designed to transmit the packets to the other appended devices without altering any of the transmitted packets received. They act as pathways to direct electrical signals to travel along. They transmit the information regardless of the fact if data packet is destined for the device connected or not.

Hub falls in two categories:

Active Hub: They are smarter than the passive hubs. They not only provide the path for the data signals infact they regenerate, concentrate and strengthen the signals before sending them to their destinations. Active hubs are also termed as ‘repeaters’.

Passive Hub: They are more like point contact for the wires to built in the physical network. They have nothing to do with modifying the signals.

Ethernet Hubs

It is a device connecting multiple Ethernet devices together and makes them perform the functions as a single unit. They vary in speed in terms of data transfer rate. Ether utilizes Carrier Sense Multiple Access with Collision Detect (CSMA/CD) to control Media access. Ethernet hub communicates in half-duplex mode where the chances of data collision are inevitable at most of the times.

Switches

Switches are the linkage points of an Ethernet network. Just as in hub, devices in switches are connected to them through twisted pair cabling. But the difference shows up in the manner both the devices; hub and a switch treat the data they receive. Hub works by sending the data to all the ports on the device whereas a switch transfers it only to that port which is connected to the destination device. A switch does so by having an in-built learning of the MAC address of the devices connected to it. Since the transmission of data signals are well defined in a switch hence the network performance is consequently enhanced. Switches operate in full-duplex mode where devices can send and receive data from the switch at the simultaneously unlike in half-duplex mode. The transmission speed in switches is double than in Ethernet hub transferring a 20Mbps connection into 30Mbps and a 200Mbps connection to become 300Mbps. Performance improvements are observed in networking with the extensive usage of switches in the modern days.

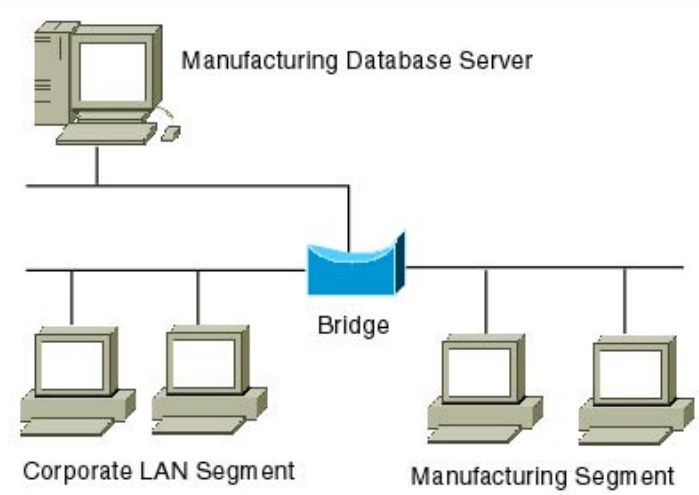
The following method will elucidate further how data transmission takes place via switches:

- Cut-through transmission: It allows the packets to be forwarded as soon as they are received. The method is prompt and quick but the possibility of error checking gets overlooked in such kind of packet data transmission.
- Store and forward: In this switching environment the entire packet are received and ‘checked’ before being forwarded ahead. The errors are thus eliminated before being propagated further. The downside of this process is that error checking takes relatively longer time consequently making it a bit slower in processing and delivering.
- Fragment Free: In a fragment free switching environment, a greater part of the packet is examined so that the switch can determine whether the packet has been

caught up in a collision. After the collision status is determined, the packet is forwarded.

Bridges

A bridge is a computer networking device that builds the connection with the other bridge networks which use the same protocol. It works at the Data Link layer of the OSI Model and connects the different networks together and develops communication between them. It connects two local-area networks; two physical LANs into larger logical LAN or two segments of the same LAN that use the same protocol.



Apart from building up larger networks, bridges are also used to segment larger networks into smaller portions. The bridge does so by placing itself between the two portions of two physical networks and controlling the flow of the data between them. Bridges nominate to forward the data after inspecting into the MAC address of the devices connected to every segment. The forwarding of the data is dependent on the acknowledgement of the fact that the destination address resides on some other interface. It has the capacity to block the incoming flow of data as well. Today Learning bridges have been introduced that build a list of the MAC addresses on the interface by observing the traffic on the network. This is a leap in the development field of manually recording of MAC addresses.

Routers

Routers are network layer devices and are particularly identified as Layer- 3 devices of the OSI Model. They process logical addressing information in the Network header of a packet such as IP Addresses. Router is used to create larger complex networks by complex traffic routing. It has the ability to connect dissimilar LANs on the same protocol. It also has the ability to limit the flow of broadcasts. A router primarily comprises of a hardware

device or a system of the computer which has more than one network interface and routing software.

Functionality:

When a router receives the data, it determines the destination address by reading the header of the packet. Once the address is determined, it searches in its **routing table** to get know how to reach the destination and then forwards the packet to the higher hop on the route. The hop could be the final destination or another router.

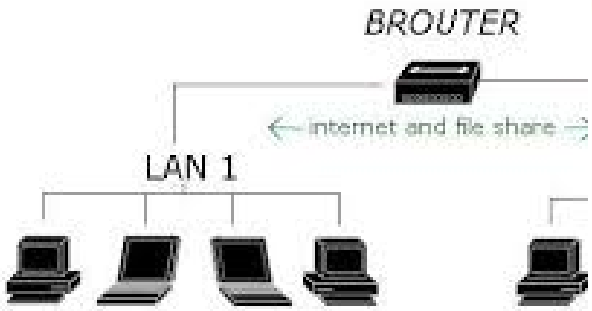
Routing tables play a very pivotal role in letting the router makes a decision. Thus a routing table is ought to be updated and complete. The two ways through which a router can receive information are:

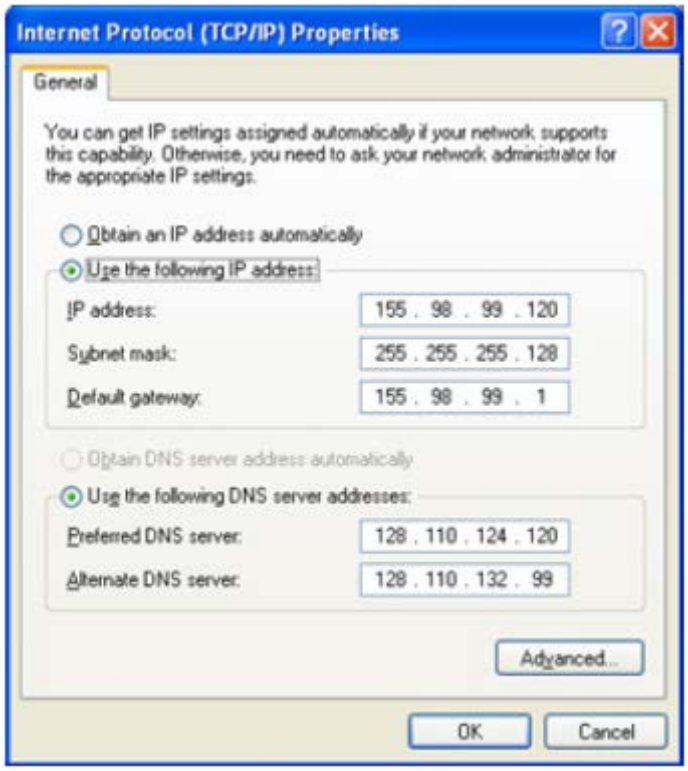
- **Static Routing**: In static routing, the routing information is fed into the routing tables manually. It does not only become a time-taking task but gets prone to errors as well. The manual updating is also required in case of statically configured routers when change in the topology of the network or in the layout takes place. Thus static routing is feasible for tinniest environments with minimum of one or two routers.

- **Dynamic Routing**: For larger environment dynamic routing proves to be the practical solution. The process involves use of peculiar routing protocols to hold communication. The purpose of these protocols is to enable the other routers to transfer information about to other routers, so that the other routers can build their own routing tables.

Brouters

Brouters are the combination of both the bridge and routers. They take up the functionality of the both networking devices serving as a bridge when forwarding data between networks, and serving as a router when routing data to individual systems. Brouter functions as a filter that allows some data into the local network and redirects unknown data to the other network.





Brouters are rare and their functionality is embedded into the routers functioned to act as bridge as well.

Lecture#5

Theme: The network TCP/IP. Main types of addressing systems.

An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.[1] An IP address serves two principal functions: host or network interface identification and location addressing.

Version 4 of the Internet Protocol (IPv4) defines an IP address as a 32-bit number.[1] However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was developed in 1995,[2] and standardized as RFC 2460 in 1998.[3] IPv6 deployment has been ongoing since the mid-2000s.

IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 in IPv4, and 2001:db8:0:1234:0:567:8:1 in IPv6.

The IP address space is managed globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries (RIR) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers. IPv4 addresses have been distributed by IANA to the RIRs in blocks of approximately 16.8 million addresses each. Each ISP or private network administrator assigns an IP address to each device connected to its network. Such assignments may be on a static (fixed or permanent) or dynamic basis, depending on its software and practices.

Function

An IP address serves two principal functions. It identifies the host, or more specifically its network interface, and it provides the location of the host in the network, and thus the capability of addressing that host. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."[4]

The header of each IP packet contains the IP address of the sending host, and that of the destination host. A host may use geolocation software to deduce the geolocation of its communicating peer.[5][6]

IP versions

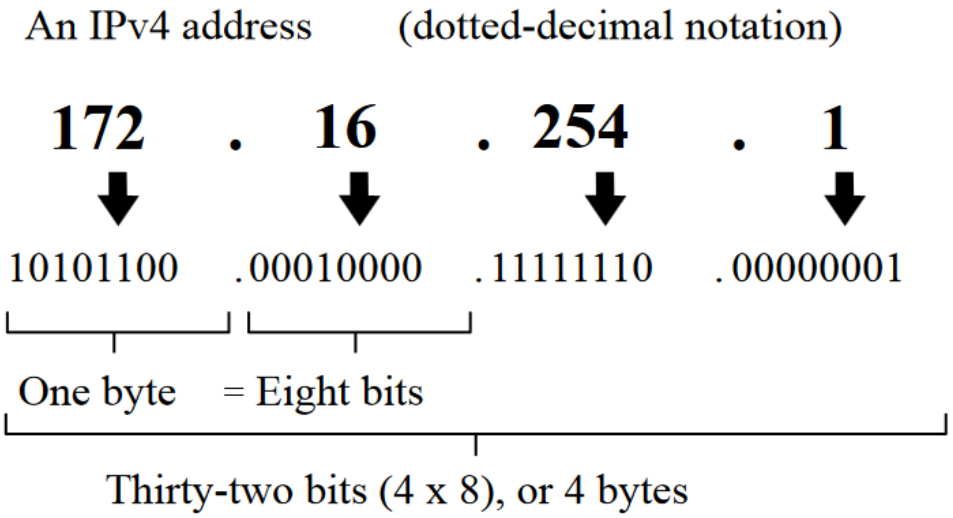
Two versions of the Internet Protocol are in common use in the Internet today. The original version of the Internet Protocol for use in the Internet is Internet Protocol version 4 (IPv4), first installed in 1983.

The rapid exhaustion of IPv4 address space available for assignment to Internet service providers and end user organizations by the early 1990s, prompted the Internet Engineering Task Force (IETF) to explore new technologies to expand the addressing capability in the Internet. The result was a redesign of the Internet Protocol which became eventually known as *Internet Protocol Version 6* (IPv6) in 1995.[2][3] IPv6 technology was in various testing stages until the mid-2000s, when commercial production deployment commenced.

IANA's primary IPv4 address pool was exhausted on 3 February 2011, when the last five blocks were allocated to the five RIRs.[7][8] APNIC was the first RIR to exhaust its regional pool on 15 April 2011, except for a small amount of address space reserved for the transition to IPv6, intended to be allocated in a restricted process.[9] Individual ISPs still had unassigned pools of IP addresses, and could recycle addresses no longer needed by their subscribers.

Today, these two versions of the Internet Protocol are in simultaneous use. Among other technical changes, each version defines the format of addresses differently. Because of the historical prevalence of IPv4, the generic term *IP address* typically still refers to the addresses defined by IPv4. The gap in version sequence between IPv4 and IPv6 resulted from the assignment of version 5 to the experimental Internet Stream Protocol in 1979, which however was never referred to as IPv5.

IPv4 addresses



Decomposition of an IPv4 address from dot-decimal notation to its binary value.

An IP address in IPv4 is 32-bits in size, which limits the address space to 4294967296 (2^{32}) IP addresses. Of this number, IPv4 reserves some addresses for special purposes such as private networks (~18 million addresses) or multicast addresses (~270 million addresses).

IPv4 addresses are usually represented in dot-decimal notation, consisting of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 172.16.254.1. Each part represents a group of 8 bits (octet) of the address. In some cases of technical writing, IPv4 addresses may be presented in various hexadecimal, octal, or binary representations.

Lecture#6

Theme: Domain name systems, distribution principles of domain names.

The **Domain Name System** (**DNS**) is a hierarchical decentralized naming system for computers, services, or other resources 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 numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality on the Internet, that has been in use since 1985.

The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain. Network administrators may delegate authority over sub-domains of their

allocated name space to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid a single large central database.

The Domain Name System also specifies the technical functionality of the database service that is at its core. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in the DNS, as part of the Internet Protocol Suite. Historically, other directory services preceding DNS were not scalable to large or global directories as they were originally based on text files, prominently the HOSTS.TXT resolver.

The Internet maintains two principal namespaces, the domain name hierarchy[1] and the Internet Protocol (IP) address spaces.[2] 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.[3] 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 Start of Authority (SOA), IP addresses (A and AAAA), SMTP mail exchangers (MX), name servers (NS), pointers for reverse DNS lookups (PTR), and domain name aliases (CNAME). Although not intended 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 person* (RP) records. As a general purpose database, the DNS has also been used in combating unsolicited email (spam) by storing a real-time blackhole list. The DNS database is traditionally stored in a structured zone file.

Function

An often-used analogy to explain the Domain Name System is that it serves as the phone 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 (IPv4) and 2606:2800:220:6d:26bf:1447:1097:aa7 (IPv6). Unlike a phone book, DNS can be quickly updated, allowing a service's location on the network to change without affecting the end users, who continue to use the same host name. Users take advantage of this when they use meaningful Uniform Resource Locators (URLs), and e-mail addresses without having to know how the computer actually locates the services.

An important and ubiquitous function of DNS is its central role in distributed Internet services such as cloud services and content delivery networks.[4] When a user accesses a distributed Internet service using a URL, the domain name of the URL is translated to the IP address of a server that is proximal to the user. The key functionality of DNS exploited here is that different users can *simultaneously* receive different translations

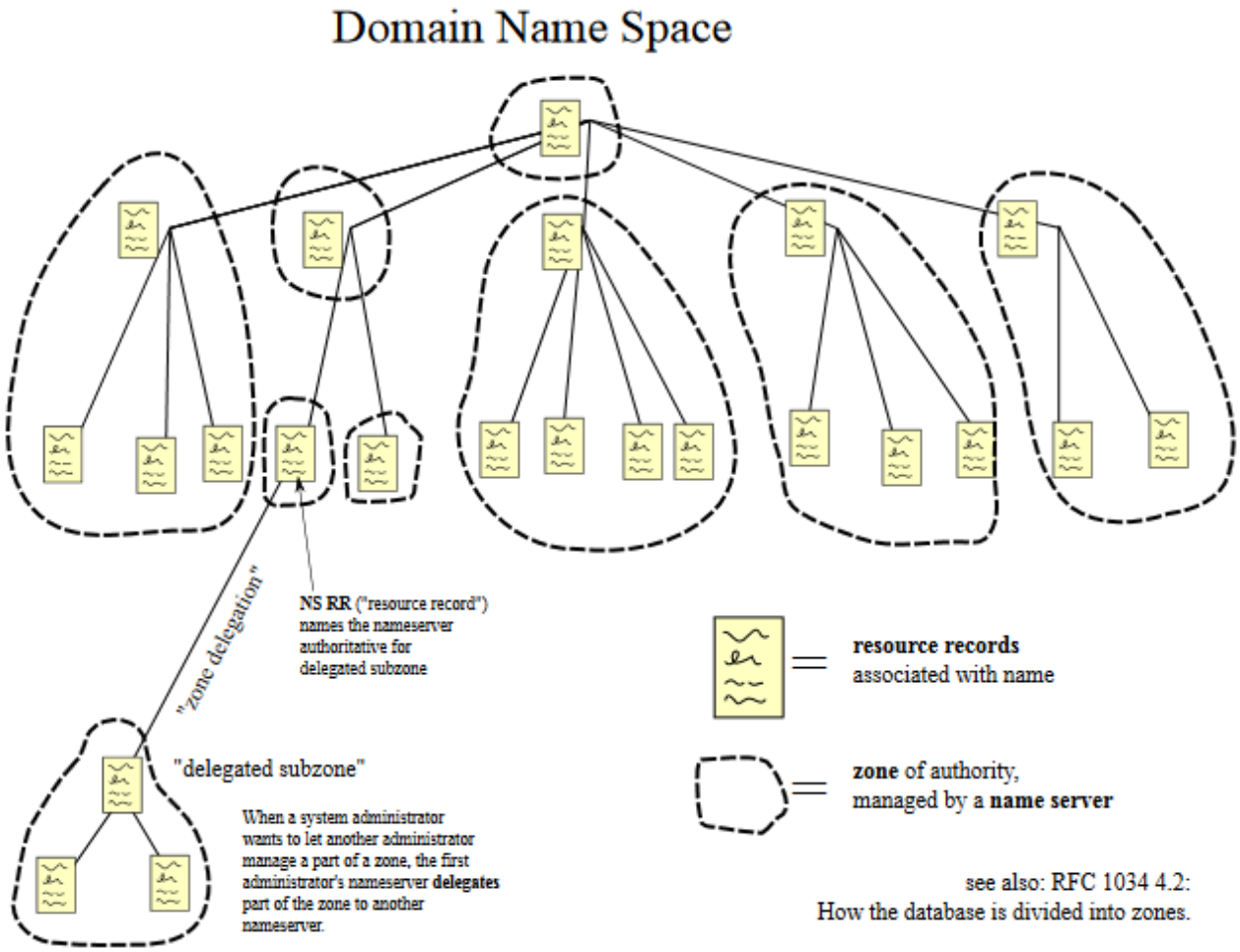
for the *same* domain name, a key point of divergence from a traditional phone-book view of the DNS. This process of using the DNS to assign proximal servers to users is key to providing faster and more reliable responses on the Internet and is widely used by most major Internet services.[5]

The DNS reflects the structure of administrative responsibility in the Internet.[6] Each subdomain is a zone of administrative autonomy delegated to a manager. For zones operated by a registry, administrative information is often complemented by the registry's RDAP and WHOIS services. That data can be used to gain insight on, and track responsibility for, a given host on the Internet.[7]

Structure

Domain name space

The domain name space consists of a tree data structure. Each node or leaf in the tree has a label and zero or more resource records (RR), which hold information associated with the domain name. The domain name itself consists of the label, possibly concatenated with the name of its parent node on the right, separated by a dot.[17] The tree sub-divides into zones beginning at the root 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.[18]



The hierarchical Domain Name System for class *Internet*, organized into zones, each served by a name server

Administrative responsibility over any zone may be divided by creating additional zones. Authority over the new zone is said to be *delegated* to a designated name server. The parent zone ceases to be authoritative 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 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.com belongs to the top-level domain com.

The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain of the domain to the right. For example: the label example specifies a subdomain of the com domain, 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 characters. The null label, of length zero, is reserved for the root zone. The full domain name may not exceed the length of 253 characters in its textual representation.[1] In the internal binary representation of the DNS the maximum length requires 255 octets of storage, since it also stores the length of the name.[3]

Although domain names may theoretically consist of any character representable in an octet, 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, A through Z, digits 0 through 9, and hyphen. This rule is known as the LDH rule (letters, digits, hyphen). Domain names are interpreted in case-independent manner.[19] Labels may not start or end with a hyphen.[20] An additional rule requires that top-level domain names should not be all-numeric.[20]

Internationalized domain names

The limited set of ASCII characters permitted in the DNS prevented the representation of names and words of many languages in their native alphabets or scripts. To make this possible, ICANN approved the Internationalizing Domain Names in Applications (IDNA) system, by which user applications, such as web browsers, map Unicode strings into the valid DNS character set using Punycode. In 2009 ICANN approved the installation of internationalized domain name country code top-level domains (ccTLDs). In addition, many registries of the existing top level domain names (TLDs) have adopted the IDNA system.

Name servers

The Domain Name System is maintained by a distributed database system, which uses the client–server model. The nodes of this database are the name servers. Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root name servers, the servers to query when looking up (resolving) a TLD.

Authoritative name server

An authoritative name server is a name server that only gives answers to DNS queries from data that has been configured by an original source, for example, the domain administrator or by dynamic DNS methods, in contrast to answers obtained via a query to another name server that only maintains a cache of data.

An authoritative name server can either be a master server or a slave server. A master server is a server that stores the original (master) copies of all zone records. A slave server uses a special automatic updating mechanism in the DNS protocol in communication with its master to maintain an identical copy of the master records.

Every DNS zone must be assigned a set of authoritative name servers. This set of servers is stored in the parent domain zone with name server (NS) records.

An authoritative server indicates its status of supplying definitive answers, deemed authoritative, by setting a protocol flag, called the Authoritative Answer (AA) bit in its

responses.[3] This flag is usually reproduced prominently in the output of DNS administration query tools, such as dig, to indicate that the responding name server is an authority for the domain name in question

Lecture#7

Theme: The internet protocol-IP is main protocol in network layer of the model OSI.

The **Internet Protocol** (**IP**) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

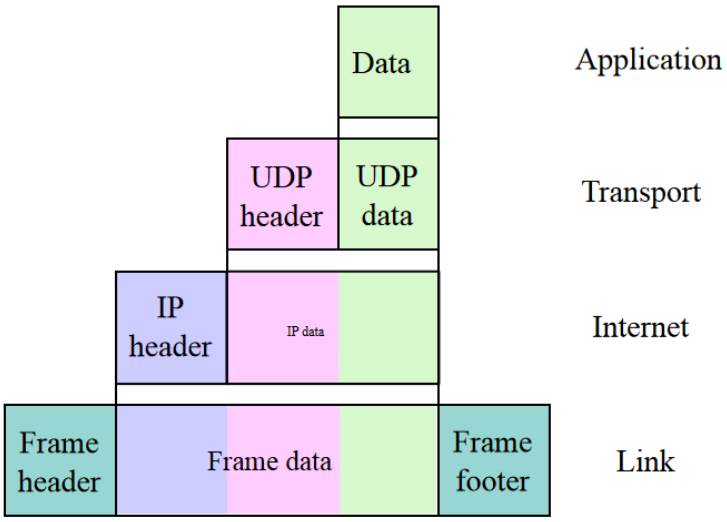
Historically, IP was the connectionless datagram service in the original *Transmission Control Program* introduced by Vint Cerf and Bob Kahn in 1974; the other being the connection-oriented Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6).

Function

Sample encapsulation of application data from UDP to a Link protocol frame

The Internet Protocol is responsible for addressing hosts, encapsulating data into datagrams (including fragmentation and reassembly) and routing datagrams from a source host to a destination host across one or more IP networks.[1] For these purposes, the Internet Protocol defines the format of packets and provides an addressing system.



Each datagram has two components: a header and a payload. The IP header includes source IP address, destination IP address, and other metadata needed to route and deliver the datagram. The payload is the data that is transported. This method of nesting the data payload in a packet with a header is called encapsulation.

IP addressing entails the assignment of IP addresses and associated parameters to host interfaces. The address space is divided into subnetworks, involving the designation of network prefixes. IP routing is performed by all hosts, as well as routers, whose main function is to transport packets across network boundaries. Routers communicate with one another via specially designed routing protocols, either interior gateway protocols or exterior gateway protocols, as needed for the topology of the network.

Version history

In May 1974, the Institute of Electrical and Electronic Engineers (IEEE) published a paper entitled "A Protocol for Packet Network Intercommunication".[2] The paper's authors, Vint Cerf and Bob Kahn, described an internetworking protocol for sharing resources using packet switching among network nodes. A central control component of this model was the "Transmission Control Program" that incorporated both connection-oriented links and datagram services between hosts. The monolithic Transmission Control Program was later divided into a modular architecture consisting of the Transmission Control Protocol and User Datagram Protocol at the transport layer and the Internet Protocol at the network layer. The model became known as the *Department of Defense (DoD) Internet Model* and *Internet protocol suite*, and informally as *TCP/IP*.

IP versions 0 to 3 were experimental versions, used between 1977 and 1979. The following Internet Experiment Note (IEN) documents describe versions of the Internet Protocol prior to the modern version of IPv4:

- IEN 2 (*Comments on Internet Protocol and TCP*), dated August 1977 describes the need to separate the TCP and Internet Protocol functionalities (which were

previously combined.) It proposes the first version of the IP header, using 0 for the version field.

- IEN 26 (*A Proposed New Internet Header Format*), dated February 1978 describes a version of the IP header that uses a 1-bit version field.
- IEN 28 (*Draft Internetwork Protocol Description Version 2*), dated February 1978 describes IPv2.
- IEN 41 (*Internetwork Protocol Specification Version 4*), dated June 1978 describes the first protocol to be called IPv4. The IP header is different from the modern IPv4 header.
- IEN 44 (*Latest Header Formats*), dated June 1978 describes another version of IPv4, also with a header different from the modern IPv4 header.
- IEN 54 (*Internetwork Protocol Specification Version 4*), dated September 1978 is the first description of IPv4 using the header that would be standardized in RFC 760.

The dominant internetworking protocol in the Internet Layer in use today is IPv4; the number 4 is the protocol version number carried in every IP datagram. IPv4 is described in RFC 791 (1981).

Version 5 was used by the Internet Stream Protocol, an experimental streaming protocol.

The successor to IPv4 is IPv6. IPv6 was a result of several years of experimentation and dialog during which various protocol models were proposed, such as TP/IX (RFC 1475), PIP (RFC 1621) and TUBA (TCP and UDP with Bigger Addresses, RFC 1347). Its most prominent difference from version 4 is the size of the addresses. While IPv4 uses 32 bits for addressing, yielding c. 4.3 billion (4.3×10^9) addresses, IPv6 uses 128-bit addresses providing ca. 340 undecillion, or 3.4×10^{38} addresses. Although adoption of IPv6 has been slow, as of June 2008, all United States government systems have demonstrated basic infrastructure support for IPv6.[3]

The assignment of the new protocol as IPv6 was uncertain until due diligence revealed that IPv6 had not yet been used previously.[4] Other protocol proposals named *IPv9* and *IPv8* briefly surfaced, but had no affiliation with any international standards body, and have had no support.[5] However, on April 1, 1994, the IETF published an April Fools' Day joke about IPv9.[6]

Reliability

The design of the Internet protocol suite adheres to the end-to-end principle, a concept adapted from the CYCLADES project. Under the end-to-end principle, the network infrastructure is considered inherently unreliable at any single network element or transmission medium and is dynamic in terms of availability of links and nodes. No central monitoring or performance measurement facility exists that tracks or maintains the

state of the network. For the benefit of reducing network complexity, the intelligence in the network is purposely located in the end nodes.

As a consequence of this design, the Internet Protocol only provides best-effort delivery and its service is characterized as unreliable. In network architectural language, it is a connectionless protocol, in contrast to connection-oriented communication. Various error conditions may occur, such as data corruption, packet loss, duplication and out-of-order delivery. Because routing is dynamic, meaning every packet is treated independently, and because the network maintains no state based on the path of prior packets, different packets may be routed to the same destination via different paths, resulting in out-of-order sequencing at the receiver.

IPv4 provides safeguards to ensure that the IP packet header is error-free. A routing node calculates a checksum for a packet. If the checksum is bad, the routing node discards the packet. Although the Internet Control Message Protocol (ICMP) allows such notification, the routing node is not required to notify either end node of these errors. By contrast, in order to increase performance, and since current link layer technology is assumed to provide sufficient error detection,[7] the IPv6 header has no checksum to protect it.[8]

All error conditions in the network must be detected and compensated by the end nodes of a transmission. The upper layer protocols of the Internet protocol suite are responsible for resolving reliability issues. For example, a host may buffer network data to ensure correct ordering before the data is delivered to an application.

Link capacity and capability

The dynamic nature of the Internet and the diversity of its components provide no guarantee that any particular path is actually capable of, or suitable for, performing the data transmission requested, even if the path is available and reliable. One of the technical constraints is the size of data packets allowed on a given link. An application must assure that it uses proper transmission characteristics. Some of this responsibility lies also in the upper layer protocols. Facilities exist to examine the maximum transmission unit (MTU) size of the local link and Path MTU Discovery can be used for the entire projected path to the destination. The IPv4 internetworking layer has the capability to automatically fragment the original datagram into smaller units for transmission. In this case, IP provides re-ordering of fragments delivered out of order.[9]

The Transmission Control Protocol (TCP) is an example of a protocol that adjusts its segment size to be smaller than the MTU. The User Datagram Protocol (UDP) and the Internet Control Message Protocol (ICMP) disregard MTU size, thereby forcing IP to fragment oversized datagrams.

An IPv6 network does not perform fragmentation or reassembly, and as per the end-to-end principle, requires end stations and higher-layer protocols to avoid exceeding the network's MTU.[11]

Security

During the design phase of the ARPANET and the early Internet, the security aspects and needs of a public, international network could not be adequately anticipated. Consequently, many Internet protocols exhibited vulnerabilities highlighted by network attacks and later security assessments. In 2008, a thorough security assessment and proposed mitigation of problems was published.[12] The Internet Engineering Task Force (IETF) has been pursuing further studies.[13]

Lecture#8

Theme: Network protocols. Address Resolution Protocol. Reverse Address Resolution Protocol

The following articles contain lists of network protocols in various formats.

- Protocol stack: List of network protocol stacks
- fiber optic protocol
- mime protocol
- Bluetooth protocol
- Fibre Channel network protocols
- Internet Protocol Suite or TCP/IP model or TCP/IP stack
- OSI protocols family of information exchange standards developed jointly by the ISO and the ITU-T
- Routing protocols
- List of IP protocol numbers, protocol numbers used in the Protocol field of the IPv4 header and the Next Header field of IPv6 header
- Yahoo! Messenger, underlying protocol used by the Yahoo messenger
- RTPS protocol, an interoperability protocol
- SSH Secure Shell
- SMB Server Message Block, one version of which was also known as CIFS (Common Internet File System)
- FTP File Transfer Protocol
- SMTP Simple Mail Transfer Protocol
- TCP Transmission Control Protocol
- Telnet Teletype Network
- HTTP Hyper Text Transfer Protocol
- HTTPs Secure Hyper Text Transfer Protocol
- POP Post Office Protocol
- HTCPCP Hyper Text Coffee Pot Control Protocol
- MTP Media Transfer Protocol
- SFTP Secure File Transfer Protocol
- SSL Secure Socket Layer
- TLS Transport Layer Security

- E6 Ethernet globalization protocols
- NTP Network time protocol
- PPP Point to Point Protocol
- NNTP Network News Transfer Protocol
- QOTD Quote Of The Day
- IMAP Internet Message Access Protocol
- Bitcoin Protocol Protocol for Bitcoin transactions and transfers on the web
- Ethereum Protocol for Ethereum transactions and smart contracts
- Steam Protocol used by steam service

Address Resolution Protocol

The **Address Resolution Protocol** (**ARP**) is a communications protocol used for discovering the link layer address associated with a given Internet layer address, a critical function in the Internet protocol suite. ARP was defined by RFC 826 in 1982,[1] and is Internet Standard STD 37. **ARP** is also the name of the program for manipulating these addresses in most operating systems.

ARP is used for mapping a network address (e.g. an IPv4 address) to a physical address like an MAC address. ARP has been implemented with many combinations of network and data link layer technologies, like IPv4, Chaosnet, DECnet and Xerox PARC Universal Packet (PUP) using IEEE 802 standards, FDDI, X.25, Frame Relay and Asynchronous Transfer Mode (ATM). IPv4 over IEEE 802.3 and IEEE 802.11 is the most common usage.

In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbor Discovery Protocol (NDP).

Operating scope

The Address Resolution Protocol is a request and response protocol whose messages are encapsulated by a link layer protocol. It is communicated within the boundaries of a single network, never routed across internetwork nodes. This property places ARP into the link layer of the Internet Protocol Suite.[2] Although ARP was not developed in the OSI model, it is often described here as residing in layer 3, being encapsulated by Layer 2 protocols.[*citation needed*]

Packet structure

The Address Resolution Protocol uses a simple message format containing one address resolution request or response. The size of the ARP message depends on the upper layer and lower layer address sizes, which are given by the type of networking protocol (usually IPv4) in use and the type of hardware or virtual link layer that the upper layer protocol is running on. The message header specifies these types, as well as the size of addresses of each. The message header is completed with the operation code for request (1) and reply (2). The payload of the packet consists of four addresses, the hardware and protocol address of the sender and receiver hosts.

The principal packet structure of ARP packets is shown in the following table which illustrates the case of IPv4 networks running on Ethernet. In this scenario, the packet has 48-bit fields for the sender hardware address (SHA) and target hardware address (THA), and 32-bit fields for the corresponding sender and target protocol addresses (SPA and TPA). Thus, the ARP packet size in this case is 28 bytes. The EtherType for ARP is 0x0806. (This appears in the Ethernet frame header when the payload is an ARP packet. Not to be confused with PTYPE below, which appears within this encapsulated ARP packet?)

Hardware type (HTYPE)

This field specifies the network protocol type. Example: Ethernet is 1.

Protocol type (PTYPE)

This field specifies the internetwork protocol for which the ARP request is intended. For IPv4, this has the value 0x0800. The permitted PTYPE values share a numbering space with those for Ether Type.

Hardware length (HLEN)

Length (in octets) of a hardware address. Ethernet addresses size is 6.

Protocol length (PLEN)

Length (in octets) of addresses used in the upper layer protocol. (The upper layer protocol specified in PTYPE.) IPv4 address size is 4.

Operation

Specifies the operation that the sender is performing: 1 for request, 2 for reply.

Sender hardware address (SHA)

Media address of the sender. In an ARP request this field is used to indicate the address of the host sending the request. In an ARP reply this field is used to indicate the address of the host that the request was looking for. (Not necessarily address of the host replying as in the case of virtual media.) Note that switches do not pay attention to this field, particularly in learning MAC addresses. The ARP PDU is encapsulated in Ethernet frame, and that is what Layer 2 devices examine.

Sender protocol address (SPA)

Internetwork address of the sender.

Target hardware address (THA)

Internet Protocol (IPv4) over Ethernet ARP packet		
octet offset	0	1
0	Hardware type (HTYPE)	
2	Protocol type (PTYPE)	
4	Hardware address length (HLEN)	Protocol address length (PLEN)
6	Operation (OPER)	
8	Sender hardware address (SHA) (first 2 bytes)	
10	(next 2 bytes)	
12	(last 2 bytes)	
14	Sender protocol address (SPA) (first 2 bytes)	
16	(last 2 bytes)	
18	Target hardware address (THA) (first 2 bytes)	
20	(next 2 bytes)	
22	(last 2 bytes)	
24	Target protocol address (TPA) (first 2 bytes)	
26	(last 2 bytes)	

Media address of the intended receiver. In an ARP request this field is ignored. In an ARP reply this field is used to indicate the address of the host that originated the ARP request.

Target protocol address (TPA)

Internetwork address of the intended receiver.

ARP protocol parameter values have been standardized and are maintained by the Internet Assigned Numbers Authority (IANA).

USED LITERATURES

1.How to Build a Computer by John Gower III

2. The STREAM TONE: The Future of Personal Computing? by T. Gilling

3. The Shallows: What the Internet is Doing to Our Brains. Growing up Wired by David Wallace Fleming

4. Personal Connections in the Digital Age by Nancy Baym

5. The Filter Bubble: What the Internet is Hiding From You by Eli Pariser

6. It's Complicated: The Social Lives of Networked Teens The Future of the Internet-And How to Stop It by Jonathan L. Zittrain