Network Basics

Theory

Hacking with

RANJITH ADLAKADI

A network is a group of two or more computer systems or other devices that are linked together to exchange data. In networks, computing devices exchange data with each other using data links between nodes. These data links are established with the help of cable media such as wires or wireless media such as WiFi.

Network Components and Functions

Server: A computer or device on a network that manages network resources. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks like accepts and responds to requests made by another program, known as a client.

Client: A client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. The client accesses the server by way of a network.

Devices: Computer devices, such as a CD-ROM drive or printer, that is not part of the essential computer. Examples of devices include disk drives, printers, and modems.

Hub: Hub is a network hardware device for connecting multiple devices and making them act as a single network segment. A hub works at the physical layer of the OSI model.

Switch: A device that filters and forwards packets between LAN segments. Switches operate at the data link layer and sometimes the network layer of the OSI Reference Model.

Router: A router is a device that is capable of forwarding data packets on a network. Routers are placed at the junction (gateway) of two or more networks connect. Routers use headers and forwarding tables to determine the best path for forwarding the packets.

Bridge: Bridge is a computer networking device that connects a local area network (LAN) to another local area network that uses the same protocol.

Access Point: A hardware device or a computer's software that acts as a communication hub for users to connect all their wireless device.

Types of Networks

Local area network (LAN)

A LAN is a network that connects computers and devices in a limited geographical area such as a home, school, office building.

Wide area network (WAN)

A WAN is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances. A WAN uses a communications channel that combines many types of media such as telephone lines, ethernet cables, optical fibers, etc.

Metropolitan Area Networks (MAN)

Metropolitan area Network covers a larger area than that of a LAN and smaller area when compared to WAN. MANs rarely extend beyond 100 KM and comprise a combination of different hardware and transmission media.

Wireless Local Area Network (WLAN)

Wireless local area networks provide wireless network communication over short distances using radio or infrared signals instead of traditional network cabling. WLANs are built by attaching a device called the access point to the edge of the wired network. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter.

Virtual private network (VPN)

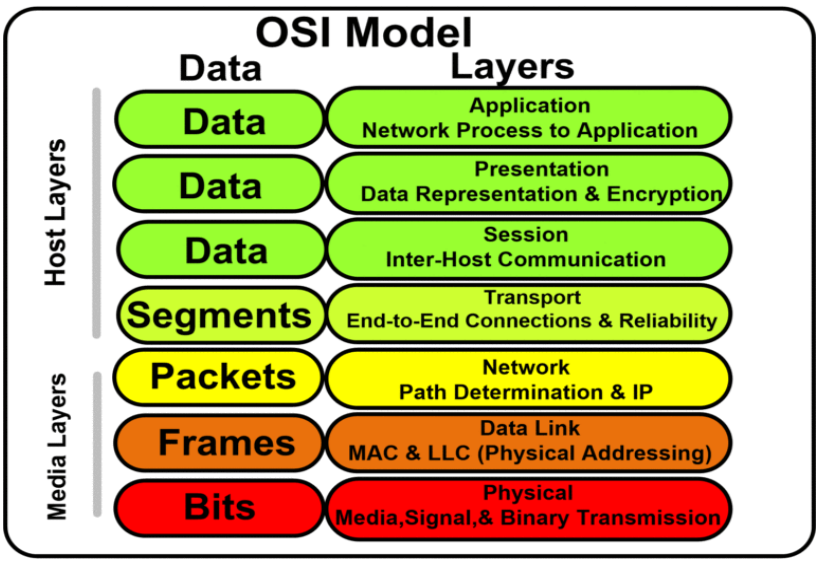
The virtual private network is an overlay network in which some of the links between nodes are carried by virtual circuits in the network instead of physical wires. The data link layer protocols of the virtual network are said to be tunneled through the network.

Personal Area Network (PAN)

A personal area network is a computer network organized around an individual. Personal area networks typically involve mobile devices. Personal area networks can be wired or wirelessly. These networks generally cover a network range of 10 meters (about 30 feet).

OSI model

OSI (Open Systems Interconnection) is a reference model for how applications communicate over a network. The main concept of OSI is that the process of communication between two endpoints in a network can be divided into seven distinct groups of related functions or layers. Each communicating user or program is on a device that can provide those seven layers of function. The seven Open Systems Interconnection layers are:



Layer 1: Physical Layer

This layer conveys the bit stream across the network either electrically, mechanically or through radio waves. The physical layer covers a variety of devices and mediums, among them cabling, connectors, receivers, transceivers, and repeaters.

Layer 2: Data Link Layer

This layer sets up links across the physical network, putting packets into network frames. This layer has two sublayers the logical link control layer and the media access control layer (MAC). MAC layer types include Ethernet and 802.11 wireless specifications.

Layer 3: Network Layer

This layer handles addressing and routing the data. To transfer it from the right source to the right destination. The IP address is part of the network layer.

Layer 4: Transport Layer

This layer manages packetization of data, then the delivery of the packets, including checking for errors in the data once it arrives. On the internet, TCP and UDP provide these services for most applications.

Layer 5: Session Layer

The session layer controls the connections between computers. It establishes, manages and terminates the connections between the local and remote application.

Layer 6: Presentation Layer

This layer is usually part of an operating system (OS) and converts incoming and outgoing data from one presentation format to another for example, from clear text to encrypted text at one end and back to clear text at the other.

Layer 7: Application Layer

The application layer of the OSI model interacts with the end user. Protocols at this layer handle the requests from different software applications. If a web browser wants to download an image, an email client wants to check the server, and a file-sharing program wants to upload a movie, the protocols in the application layer will process those requests.

IP address

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network. IP address serves two purposes, host or network interface identification and location addressing. Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number and new version of IP (IPv6), uses 128 bits for the IP address.

Private IP address: A private IP address is a non-Internet facing IP address. Private IP addresses are provided by network devices, such as routers, using network address translation (NAT).

Public IP address: A public IP address is an IP address that can be accessed over the Internet. The public IP address is a globally unique IP address assigned to a computing device.

IPv4: Internet Protocol Version 4 is the fourth revision of the Internet Protocol used to identify devices on a network. IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing a total of 2^32 addresses.

IPv6: Internet Protocol Version 6 is the newest version of the Internet Protocol reviewed in the IETF standards committees to replace the current version of IPv4. IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons. An example IPv6 address could be written like this 3ffe: 1900:4545:3:200: f8ff: fe21:67cf.

IP address classes

There are five classes of IP addresses, they are Class A, Class B, Class C, Class D and Class E, where only A, B, and C are commonly used.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

Subnetwork (Subnet)

A subnet is a logical subdivision of an IP network. Dividing a network into two or more networks is known as subnetting. Computers that belong to a subnet are addressed with a significant bit-group in their IP addresses. Subnetting results in the logical division of an IP address into two parts, the network address, and the host identifier.

Super network (Supernet)

Supernet is an Internet Protocol network that is formed, for combining two or more networks into a larger network. The benefits of supernetting are conservation of address space, gaining efficiency regarding memory storage and route information processing.

Network address translation

Network address translation (NAT) is a method of remapping one IP address space into another by modifying network address information in IP header packets while they are in transit. It has become a popular and essential tool in conserving global address space in the face of IPv4 address exhaustion.

Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP/IP networks. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so that they can communicate with other IP networks.

TCP

TCP stands for Transmission Control Protocol, which is a widely used protocol for data transmission over a network. TCP establishes a connection between two hosts before transmitting data, to ensure that data transmitted over the network reaches the destination without fail. TCP also known as a connection-oriented protocol, establishes a reliable connection between sender and receiver. TCP provides error and flow control mechanisms which help in orderly transmission of data and retransmission of lost packets.

UDP

UDP stands for User Datagram Protocol, which is connectionless protocol, mostly used for connections that can tolerate data loss. UDP is used by applications on the internet that offer voice and video communications, which can suffer some data loss without adversely affecting the quality. UDP does not provide error and flow control mechanisms because of which it does not require a connection to be established before transmitting data over the network.

ICMP

ICMP stands for Internet Control Message Protocol; this is widely used for internet communication troubleshooting or generated in response to errors in IP operations, this will send packets to the target machine and will see whether the packets are delivered or not.

Address Resolution Protocol

Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given network layer address. This mapping is a critical function in the Internet Protocol suite. It works within the boundaries of a single network never routed across internetworking nodes. ARP uses a simple message format containing one address resolution request or response. The size of the ARP message depends on the link layer and network layer address sizes.

Domain Name System

Domain Name System (DNS) is a naming system for resources connected to the Internet or a private network. The DNS is responsible for assigning domain names and mapping those names to Internet resources by designating name servers for each domain. Network administrators have authority over the subdomains of their allocated namespace to other name servers. Domain Name System is an essential component of Internet functionality.

Internet Group Management Protocol

Internet Group Management Protocol (IGMP) is a communication protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast. IGMP can be used for one-to-many networking applications such as online video streaming and gaming and allows the more efficient use of resources.

Routing

Routing is the process of selecting a path for traffic in a network or across multiple networks. In routing, network packets from their source toward their destination are routed through intermediate network nodes by specific packet forwarding mechanisms. Intermediate nodes are typically networked hardware devices such as routers, bridges, gateways, firewalls, or switches. In routing, process packets are directed on based on routing tables, which maintain a record of the routes to various network destinations. An administrator specifies the routing table.

Routing protocol

Routing protocol specifies how routers communicate with each other, distributing information, which enables them to select routes between any two nodes on a computer network. Routing algorithms determine to choose a specific route. A routing protocol shares this information first among immediate neighbors, and then throughout the network. The major types of routing protocols.

- Routing Information Protocols (RIP)

- Interior Gateway Routing Protocol (IGRP)
- Open Shortest Path First (OSPF)
- Exterior Gateway Protocol (EGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Border Gateway Protocol (BGP)
- Intermediate System-to-Intermediate System (IS-IS)

References:

1. Beal, V. (n.d.). Network Fundamentals Study Guide. Retrieved from https://www.webopedia.com/quick_ref/network-fundamentals-study-guide.html.
2. Beal, V. (n.d.). What is The Difference Between IPv6 and IPv4? Retrieved from https://www.webopedia.com/DidYouKnow/Internet/ipv6_ipv4_difference.html.
3. What is OSI model (Open Systems Interconnection)? - Definition from WhatIs.com. (n.d.). Retrieved from https://searchnetworking.techtarget.com/definition/OSI
4. Image reference: 7 Layers of OSI Model and Their Functions. (2017, November 05). Retrieved from http://electricala2z.com/cloud-computing/osi-model-layers-7-layers-osi-model/