**Networking Questions**

1. **What is Computer Networking?**

It is the process of creating and using wired or wireless networks for exchanging information, ideas, files and other electronic communication.

1. **Type of computer network**
2. Peer to Peer
3. Server Based
4. Hybrid
5. **What is backbone network?**

A backbone network is a centralized infrastructure that is designed to distribute different routes and data to various networks. It also handles management of bandwidth and various channels.

1. **Difference between Dial-up and broad band network**

A dial-up is a connection that is established using a modem. To make the dial-up connection the modem must be connected to an active phone line that is not in use. When connecting the modem will pick up the phone and dial a number that is attached to another computer. After the connection has been made the computer can check e-mail, browse the Internet, and share files.

Alternatively referred to as high-speed Internet or wideband transmission, broadband (bb) is telecommunications that provide a variety of channels of data over a single communication medium (wire). Today, there are a wide variety of broadband technologies available in most areas, below is a short listing of some of these services and companies that provide it. Keep in mind, the examples of carriers all depend on where you are in the world.

1. **What is VPN?**

VPN means Virtual Private Network, a technology that allows a secure tunnel to be created across a network such as the Internet. For example, VPNs allow you to establish a secure dial-up connection to a remote server.

1. **Ethernet & Types of Ethernet**

Ethernet is the most popular physical layer LAN technology in use today. Ethernet is an arrangement of networking technologies and systems used in local area networks (LAN), where computers are connected within a primary physical space. Systems using Ethernet communication divide data streams into packets, which are known as frames. Frames include source and destination address information, as well as mechanisms used to detect errors in transmitted data and retransmission requests.

Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits, combined with wide acceptance in the computer marketplace and the ability to support virtually all popular network protocols, make Ethernet an ideal networking technology for most computer users today.

1. **Collision Domain & Broadcast Domain**

collision domain refers to a network scenario wherein one device sends a frame out on a physical network

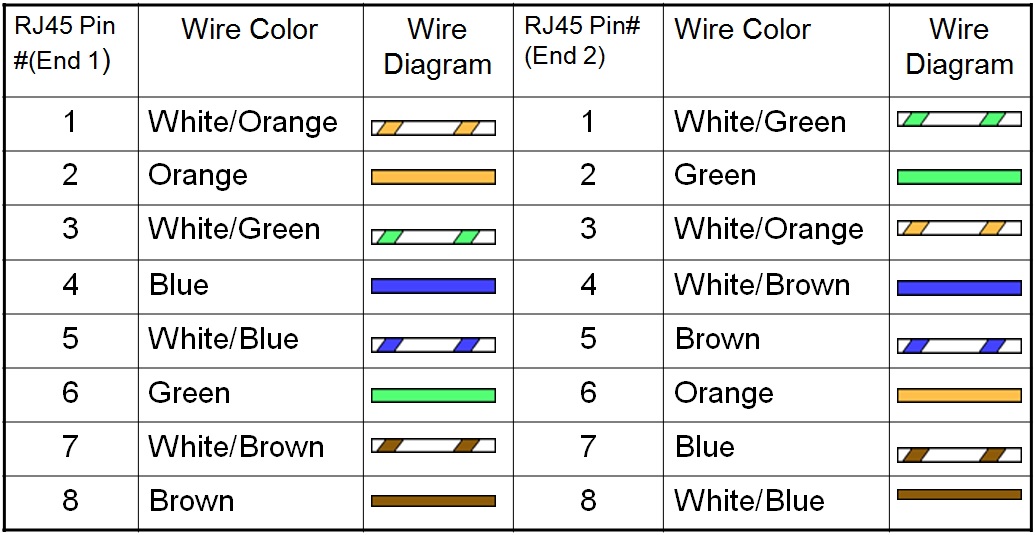
segment forcing every other device on the same segment to pay attention to it. Think of a collision event as a situation where each device’s digital signals totally interfere with one another on the wire. The hosts connected to each hub are in the same collision domain, so if one of them transmits, all the others must take the time to listen for and read the digital signal. Switch or Hub is the device for the Collision Domain.

broadcast domain refers to a group of devices on a specific network segment that hear all the broadcasts sent out on that specific network segment. But even though a broadcast domain is usually a boundary delimited by physical media like switches and routers, it can also refer to a logical division of a network segment, where all hosts can communicate via a Data Link layer, hardware address broadcast. Switches break up collision domains with each port, which is awesome, but they’re still only one broadcast domain by default! It’s also one more reason why it’s extremely important to design our networks very carefully. A router creates broadcast domain boundaries.

1. **CSMA/CD**

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is the LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is free. If the network is not free, the device waits a random amount of time before retrying. If the network is free and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and wait a random amount of time before retrying. Only switches and routers can affectively prevent a transmission from propagating throughout the entire network!

1. **Cross Cabling**



1. **Briefly describe NAT.**

NAT is Network Address Translation. This is a protocol that provides a way for multiple computers on a common network to share single connection to the Internet.

1. **What does Protocol mean?**

Protocol is defined as the rules that connect two or more devices to transfer the information from one device to another. It helps to know how data is being transferred from one network to another network for communication.

1. **What is OSI reference model?**

OSI is a reference model that tells how information and data are communicated over a network. It is a conceptual framework that understands the relationships of transmission.

1. **What are the different layers of OSI model?**

Basically, there are 7 layers of OSI model. Each layer has its own functionality in the OSI model.

They are:

Layer 1 – Physical

Layer 2 – Data Link Layer

Layer 3 – Network

Layer 4 – Transport

Layer 5 – Session

Layer 6 – Presentation

Layer 7- Application

1. **What is a Switch and why we are using Switches?**

Switch is used to receive the signal to create a frame. It forwards the packets between various LAN segments. It supports packet control when the data is sent to Data Link layer or Network layer of the OSI model. While sending packets, a signal gets enabled and gets accessed by reading the destination address and forwards the frame to appropriate frame, hence we use switches.

1. **What are Routers?**

Routing is the process to find the path on which the information or data can pass from the source to its destination. The device by which routing is done is called Routers.

1. **What is the difference between Switch, Routers, and Hub?**

Switch is used to receive the signal to create a frame. It forwards the packets between various LAN segments. It is the platform for packet control when the data is sent at a Data Link layer or Network layer of the OSI model. It supports single broadcast domain and multiple collision domains.

Routers is a networking gateway device that is used to forward data packets to the computer networks. A router is connected by at least a single LAN with its IP address or with LAN or WAN. A router supports two broadcast domains.

Hub, if anything comes in its port then it sends it out to the others. It is less expensive and least complicated. It has a single collision domain and single broadcast domain.

1. **What is Half duplex and Full duplex?**

* In half-duplex, transmission of information or communication is from one direction only.

Example: Walkie-talkie

* In full duplex, transmission of information or communication is from both the directions.

Example: Talking on the telephone.

1. **What is the difference between LAN, MAN, and WAN?**

LAN, It is a local area network where computers and network devices are connected with each other, usually within the same area or building. Connections in LAN must be of high speed.

Example: Ethernet

MAN

It is metropolitan area network where the networks are connected widely within several buildings in the same city.

Example: The IUB Network

WAN

It is a wide area network where the networks are limited to one enterprise or organization and can be accessed by the public. It connects several LANs. Connection in WAN is high speed and expensive too.

Example: Internet.

1. **Define IPv4 Address?**

Internet Protocol (IP Address) is a 32-bits to 128-bits identifier for a device on TCP/IP protocol. IP address of a device must be uniquely defined for communication.

It has 2 principal functions which include host and location address. And it has two versions which are IPv4 (32-bits) and IPv6 (128-bits).

1. **Define IPv6 Address**

An Ipv6 address uses 128 bits as opposed to 32 bits in IPv4. IPv6 addresses are written using hexadecimal, as opposed to dotted decimal in IPv4. Because an hexadecimal number uses 4 bits this means that an IPv6 address consists of 32 hexadecimal numbers. These numbers are grouped in 4’s giving 8 groups or blocks. The groups are written with a : (colon) as a separator.

1. **What is the difference between static IP addressing and dynamic IP addressing?**

Static IP addresses are reserved and they don't change over time while dynamic IP addresses can be changed each time you connect to the internet. Static IP addresses are given manually while dynamic IP addresses are provided by DHCP server.

1. **In how many ways can data be transferred in CCNA?**

Ans: Data can be transferred in 3 ways:

* Simplex
* Half-duplex
* Full-duplex

1. **What is the difference between Unicast, Multicast, Broadcast, and Anycast?**

Unicast: It is the exchange of messages between a single source and a single destination. In Unicast, while sending packets from a sender, it contains data address of the receiver so that it can go there directly.

Broadcast: It is the exchange of messages between one sender to possible multiple receivers. It works only on a local network. Broadcasting of data can’t be done on the public internet due to a massive amount of unrelated and unnecessary data.

Multicast: It is the exchange of messages between one sender and multiple receivers. In multicast, the network settings determine your receiving clients and sort of broadcasting.

Anycast: It is the exchange of messages between one host to another host. It uses TCP and UDP protocol. Copy of each data packet goes to every host that requests it.

1. **What is NIC?**

NIC is short for Network Interface Card. This is a peripheral card that is attached to a PC in order to connect to a network. Every NIC has its own MAC address that identifies the PC on the network.

1. **What are the different types of network in CCNA?**

There are two types of network:

* Server-based network
* Peer-to-Peer network

1. **What is a Network subnet?**

Ans: It is the subdivision of an IP address which is divided into two parts such as the network prefix and the host identifier.

1. **Subnetting Chart**

10000000 128

11000000 192 64

11100000 224 32

11110000 240 16

11111000 248 8

11111100 252 4

11111110 254 2

11111111 255 1

1. **Class -C , CIDR Chart**

/24 = 28 =254

/25 = 27 =126

/26 = 26 =62

/27 = 25 =30

/28 = 24 =14

/29 = 23 =6

/30 = 22 =2

1. **Can IP address be assigned to Layer 2?**

No, IP addresses cannot assign to Layer2.

1. **What is PING used for?**

PING is packet Internet groper. It is used to test the reachability of a host on an Internet protocol (IP) network. When any data is sent via the network through the IP addresses, then it will PING the receiver to receive the data from the sender.

1. **What are the different class and ranges of IP address?**

There are 5 different classes of IP address:

Class Range

A 1-126

B 127-191

C 192-223

D 224-239

E 240-254

1. **What is Private IP and Public IP? Range of Private IP address.**

Private IP used within the local LAN and Public IP used across the Internet.

* Class-A: 10.0.0.0/8 IP addresses: 10.0.0.0 – 10.255.255.255
* Class-B: 172.16.0.0/12 IP addresses: 172.16.0.0 – 172.31.255.255
* Class-C: 192.168.0.0/16 IP addresses: 192.168.0.0 – 192.168.255.255

1. **Define Network Topology.**

It is an arrangement of elements in a specific order. The various types of Topology include:

* Bus
* Star
* Mesh
* Ring
* Hybrid
* Tree

1. **Define MAC Address.**

MAC address is Media Access Control address. It is stored in ROM and is uniquely defined. It is identified as Media Access Control layer in the network architecture.

1. **What does 10Base-T mean?**

The 10 refers to the data transfer rate, in this case is 10Mbps. The word Base refers to base band, as oppose to broad band. T means twisted pair, which is the cable used for that network.

1. **What is NOS?**

NOS, or Network Operating System, is specialized software whose main task is to provide network connectivity to a computer in order for it to be able to communicate with other computers and connected devices.

1. **What is DoS?**

DoS, or Denial-of-Service attack, is an attempt to prevent users from being able to access the internet or any other network services. Such attacks may come in different forms and are done by a group of perpetuators. One common method of doing this is to overload the system server so it cannot anymore process legitimate traffic and will be forced to reset.

1. **What are firewalls?**

Firewalls serve to protect an internal network from external attacks. These external threats can be hackers who want to steal data or computer viruses that can wipe out data in an instant. It also prevents other users from external networks from gaining access to the private network.

1. **Why is VLAN used?**

It is a Virtual LAN network which is used to make a separate domain in a single switch.

1. **What are the different types of passwords that you can use in Cisco routers?**

Different types of passwords that are used in Cisco routers are enabled, enable secret, auxiliary (AUX), console and virtual terminal (VTY).

1. **How many types of memories are used in Cisco router?**

Given below are the 3 different types of memory that are used:

* Flash memory – Store system IOS. It is electronically erasable and a re-programmable memory chip.
* RAM – Store configuration file which is being executed. It loses its information when a router is restarted or shut down.
* NVRAM – Store startup configuration file and IOS reads this file when the router boots up.
* ROM – Read Only Memory. It saves the information if the router is shut down or restarted. It maintains the instructions for POST diagnostics.

1. **What is meant ARP and RARP?**

* ARP is Address Resolution Protocol which is used to map an IP address to a physical machine.
* RARP is Reverse Address Resolution Protocol which is used to map MAC address to the IP address.

1. **What are the different types of cables that are used in routing?**

Three different types of cables that are used include:

* Straight cable – (switch-router)
* Cross cable – (PC-PC, switch-switch)
* Rollover cable – (Console port to computer)

1. **Define Logical Topology.**

Logical Topology is the network from where the data packets are sent from the source to destination, which we can see as well.

1. **What is the difference between static and dynamic IP addresses?**

Static IP address won’t change over the time and is reserved statically whereas dynamic IP address changes each time when you connect to the Internet.

1. **Some Common IEEE Standards**

|  |  |
| --- | --- |
| **Standard** | **Description** |
| 802.1 | Internetworking |
| 802.2 | Logical Link Control (LLC) |
| 802.3 | Ethernet (CSMA/CD) |
| 802.4 | Token bus LAN |
| 802.5 | Token ring LAN |
| 802.6 | Metropolitan Area Network (MAN) |
| 802.7 | Broadband technical advisory |
| 802.8 | Fiber optic |
| 802.9 | Integrated voice/data |
| 802.10 | Network Security |
| 802.11 | Wireless Networks |
| 802.12 | Demand Priority (100VG-Any LAN) |
| 802.13 | Not used |
| 802.14 | Cable modem |
| 802.15 | Wireless personal area network |
| 802.16 | Broadband wireless access |
| 802.17 | Resilient packet ring |

1. **What do you understand by ‘Protocol’ in networking?**

A protocol enables two devices to connect and transmit the information or data to one another.

1. **What do you understand by PoE (Power over Ethernet)?**

It is defined by IEEE standard and it passes electric power supply to the network devices over the existing data connection.

1. **What is OSPF? Describe it.**

OSPF stands for Open Shortest Path First. It uses Dijkstra algorithm and is a link state routing protocol which is used to connect to a large number of networks without having any limitation on the number of hops.

1. **What does Multiple Access mean?**

In Multiple Access, it allows more than one devices to transmit the data at the same time. For Example, Star or Mesh Topology.

1. **Explain the difference between Collision Domain and Broadcast Domain.**

In the Broadcast Domain, all the juncture can reach each other by broadcast at the data link layer and every device is ready to receive their respective data. It can bind to the same LAN segments or the other LAN segment. Broadcast Domain uses local network for broadcasting the data packets to the receiver. While broadcasting, massive data are broadcasted, hence the speed of receiving the data is less and it also takes more time to receive the data of their address.

In the Collision Domain, data collision occurs more due to sending of more frames simultaneously. If more than two frames are sent simultaneously then the data will collide with each other in between and the information gets lost due to an occurrence of a collision and the devices will not accept the data and due to this, the communication between the sender and receiver side will collide. Hence, the sender has to send the data again and like this, it will take more time to receive the data at the receiver's side.

1. **Frame Relay Technology works on which layer of OSI model?**

It works on Data Link Layer.

1. **What does Round Trip Time mean?**

Round-trip time or round-trip delay is defined as the time taken by a signal to send the data plus the time it receives the acknowledgment from the receiver of that signal.

1. **What is MTU and what is its size for transmission?**

MTU stands for Maximum Transmission Unit and its size is 1500 bytes.

1. **What is the difference between CSMA/CD and CSMA/CA?**

Carrier Sense multiple access with Collision detection (CSMA/CD) is a media access control method which is used in local area networking. It uses early Ethernet technology to overcome collision when it happened. And Carrier sense multiple access with collision avoidance (CSMA/CA) is used in the wireless network to avoid a collision.

1. **Define Autonomous System (AS).**

It is either a single network or a group of networks that are managed by a single directive. It is defined by a unique number or code and is called as an Autonomous system number (ASN). Sometimes, it is also called as a routing domain. Communication of networks within an AS is done by using Interior Gateway Protocol (IGP).

1. **Why do you use ‘Service Password Encryption’?**

Service Password Encryption is used to encrypt plaintext password into type 7 password. Security is less and hence it can be easily decrypted.

1. **Explain DHCP scope.**

Dynamic Host Configuration Protocol (DHCP) is used to automatically assign IP host with its address to a client.

1. **Explain the difference between Tracert and Traceroute.**

You would use tracert on a PC while you would use the command traceroute on a router or switch.

1. **Why is Distributed Processing useful?**

Distributed processing is useful because of its lower cost, improved performance, reliability, and flexibility.

1. **What do you understand by Redundancy?**

Redundancy is a method which provides backup paths in case of network or path failure.

1. **What is Domain Name System (DNS)?**

DNS is an internet service that translates domain names into IP addresses. Anything connected to the internet i.e. mobile phones, laptops, websites etc. has an IP address which is uniquely defined.

1. **What is RIP?**

RIP, short for Routing Information Protocol is used by routers to send data from one network to another. It efficiently manages routing data by broadcasting its routing table to all other routers within the network. It determines the network distance in units of hops.

1. **Define Bandwidth.**

Bandwidth is defined as the amount of data that can be transmitted or carried in a fixed interval of time.

1. **Explain the basic difference between TCP/IP and OSI model.**

OSI and TCP/IP protocol are different by their layers. In OSI model, there are 7 layers whereas in TCP/IP there are 4 layers.

1. **What is the difference between ‘bit rate’ and ‘baud rate’?**

A bit rate is defined as the total number of bits transmitted in one second whereas baud rate defines the number of signal unit per second that is required to represent those bits.

Baud rate=bit rate / N,

where N = no. of bits represented by each signal shift.

1. **TCP/IP Ports and Protocols**

|  |  |  |
| --- | --- | --- |
| **SL** | **Port Number** | **Description** |
|  | 20 | [FTP](https://www.webopedia.com/TERM/F/ftp.html) -- Data |
|  | 21 | FTP -- Control |
|  | 22 | [SSH](https://www.webopedia.com/TERM/S/SSH.html) Remote Login Protocol |
|  | 23 | [Telnet](https://www.webopedia.com/TERM/T/Telnet.html) |
|  | 25 | [Simple Mail Transfer Protocol](https://www.webopedia.com/TERM/S/SMTP.html) (SMTP) |
|  | 42 | Host Name Server (Nameserv) |
|  | 53 | [Domain Name System](https://www.webopedia.com/TERM/D/DNS.html) (DNS) |
|  | 69 | [Trivial File Transfer Protocol](https://www.webopedia.com/TERM/T/TFTP.html) (TFTP) |
|  | 80 | [HTTP](http://www.webopedia.com/TERM/H/HTTP.html) |
|  | 115 | Simple File Transfer Protocol (SFTP) |
|  | 118 | SQL Services |
|  | 143 | Interim Mail Access Protocol (IMAP) |
|  | 150 | NetBIOS Session Service |
|  | 156 | [SQL Server](https://www.webopedia.com/TERM/S/SQL_Server.html) |
|  | 161 | [SNMP](https://www.webopedia.com/TERM/S/SNMP.html) |
|  | 179 | [Border Gateway Protocol](https://www.webopedia.com/TERM/B/BGP.html) (BGP) |
|  | 190 | Gateway Access Control Protocol (GACP) |
|  | 389 | [Lightweight Directory Access Protocol](https://www.webopedia.com/TERM/L/LDAP.html) (LDAP) |
|  | 443 | [HTTPS](https://www.webopedia.com/TERM/H/HTTPS.html) |
|  | 444 | Simple Network Paging Protocol (SNPP) |
|  | 546 | [DHCP](https://www.webopedia.com/TERM/D/DHCP.html) Client |
|  | 547 | DHCP Server |

1. **Abbreviation**

TCP/IP protocol suite

|  |  |  |
| --- | --- | --- |
| Name | Meaning | Function |
| TCP | Transmission Control Protocol | Enables two hosts to establish connection and exchange network data; connection-oriented; guaranteed delivery of packets |
| UDP | User Datagram Protocol | Enables two hosts to establish connection and exchange network data; connectionless, unreliable, less overhead |
| FTP | File Transfer Protocol | Downloads or uploads files between hosts; performs directory operations; also offers authentication security |
| SFTP | Secure File Transfer Protocol | Transfer of files with SSH to provide encryption, public key authentication, and file compression; similar to FTP |
| HTTP | HyperText Transfer Protocol | Transfer files or web pages from web server to client web browser; uses lesser bandwidth and supports both text and graphics |
| HTTPS | HyperText Transfer Protocol Secure | Allows browsers and servers to authenticate and encrypt network packets using SSL; secure version of HTTP |
| SMTP | Simple Mail Transfer Protocol | Uses a spooled or queued method to deliver or send emails |
| POP3 | Post Office Protocol version 3 | Used to retrieve email files from the email server; can be used with or without SMTP |
| Telnet | Telephone Network | A terminal emulation program that connects remote computers to a server; execute a commands using command prompt |
| SSH | Secure Shell | A suite of protocols used to log into another computer on the network, execute commands, and secure transfer of files |
| ICMP | Internet Control Message Protocol | Provides network layer management and control by sending datagrams and control messages; works with IP |
| ARP | Address Resolution Protocol | Resolves network addresses (IP) into hardware addresses (MAC); uses address resolution cache table built into every NIC |
| NTP | Network Time Protocol | Sets computer clock to a standard time source usually a nuclear clock |

Network services and protocols

|  |  |  |
| --- | --- | --- |
| Name | Meaning | Function |
| DNS | Domain Name System | Translates and resolves IP addresses into host names or the reverse |
| DHCP | Dynamic Host Configuration Protocol | Allows a client device to request and obtain a unique IP address and other parameters from a server automatically |
| NAT | Network Address Translation | Allows a local network to use one set of IP address for internal or in-house traffic and a different set for external or internet traffic |
| NFS | Network File System | Permits network users to access and used shared files; allows different computer platforms to share files and disk space |

Remote access protocols and services

|  |  |  |
| --- | --- | --- |
| Name | Meaning | Function |
| PPP | Point-Point Protocol | Used to establish an internet connection between serial point-to-point links; provides for dial-up connnections to networks |
| SLIP | Serial Line Internet Protocol | Used to connect to the internet via a dial-up modem; older, slower, less reliable than PPP |
| PPPoE | PPP over Ethernet | Uses PPP over Ethernet to connect an ethernet LAN user to the internet using an ADSL or cable modem; users share a broadband connection |
| PPTP | Point-Point Tunnel Protocol | A form of encryption that provides a tunnel for secure connections over the internet; used to create VPN |
| VPN | Virtual Private Network | A private, secure, point to point connection from a company LAN to the remote users and wireless nodes using the internet |

Security protocols

|  |  |  |
| --- | --- | --- |
| Name | Meaning | Function |
| IPSec | Internet Protocol Security | Provides authentication and encryption over the internet; works with IPv4 and IPv6; used to secure VPN |
| L2TP | Layer 2 Tunneling Protocol | Supports non-TCP/IP protocols VPN over the internet; combines the best features of PPTP and L2F |
| SSL | Secure Sockets Layer | Uses a private key to encrypt data that is transferred over the SSL connection; service independent and can secure different network applications |
| WEP | Wired Equivalent Privacy | Encrypts and protects data packets over radio frequencies; does not offer end-end security |
| WPA | WiFi Protected Access | Offers improved data encryption and user authentication using the wireless devices MAC address; uses TKIP encryption |
| AES | Advanced Encryption Standard | A cryptographic cipher that uses Rijndael algorithm |

Routing protocols

|  |  |  |
| --- | --- | --- |
| Name | Meaning | Function |
| RIP | Routing Information Protocol | Finds the quickest route between two computers; offers a maximum of 16 hops between routers before deciding that a packet is undeliverable |
| OSPF | Open Shortest Path First | A descendant of RIP that increases its speed and reliability; much used on the internet; accepts 256 hops between routers |
| IGRP | Interior Gateway Routing Protocol | A propriety protocol from Cisco that takes bandwidth, latency, reliability, and current traffic load into consideration |
| EGP | Exterior Gateway Protocol | A distance vector protocol that uses polling to retrieve routing information |
| BGP | Border Gateway Protocol | Used to span autonomous systems in the internet; used at the edge of networks; designed to supersede EGP |
| NLSP | Netware Link Services Protocol | A link state routing protocol that was designed to reduce wasted bandwidth associated with RIP |
| RTMP | Routing Table Maintenance Protocol | Used by Appletalk to ensure that all routers in the network have consistent routing information |

|  |  |  |
| --- | --- | --- |
| Name | Meaning | Function |
| EUI | Extended Unique Identifier | An IPv6 device will use the MAC address of its interface to generate a unique 64-bit interface ID. |
| OUI | Organizationally Unique Identifier | (OUI) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization of NIC |