

Cisco CCENT Handbook

Quick Reference Book
for All Topics of ICND1 (100-101)

Hikmat Jafarli




Table of Contents

Chapter 1: Basic Networking Concepts

Chapter 2: TCP/IP and IP Addressing

Chapter 3: IOS Basics

Chapter 4: Network Essentials

Chapter 5: IP Routing

Chapter 6: Switching

Chapter 7: VLANs

Chapter 8: Security

Chapter 9: NAT

Chapter 10: IPv6

Chapter 1: Basic Networking Concepts

Network devices

Hub is a device that connects multiple Ethernet segments and effectively makes them act as a single segment. Hubs provide basic OSI layer 1 connectivity.

Every device that is attached to a hub shares a single broadcast and a single collision domain. Hubs broadcast all received data through all their available ports.

Switch forwards data only to the devices that need to receive it, rather than broadcasting every incoming data through all its ports like the hub would do. Switches work on layer 2 of the OSI model. Switches can also perform error checking and provide many other advanced functionalities.

Bridge is similar to a switch in its function, but bridges usually have less ports than switches. Bridges are easy and inexpensive way of connecting segments.

Router is a device that determines the next network hop to which it can forward a packet towards, to allow the packet to be able to reach its ultimate destination. Routers do not forward broadcast packets by default.

Routers support different WAN technologies and work on layer 3 of the OSI model. They perform packet filtering, packet switching, path selection, and facilitate internetwork communications.

Collision domains

A collision domain is a domain where packet collisions can occur. A collision can occur when multiple devices send a packet at the same time.

Collisions do often occur in a hub environment, because each port on a hub is in the same collision domain. Each port on a bridge, a switch, and a router is in a separate collision domain.

Broadcast domains

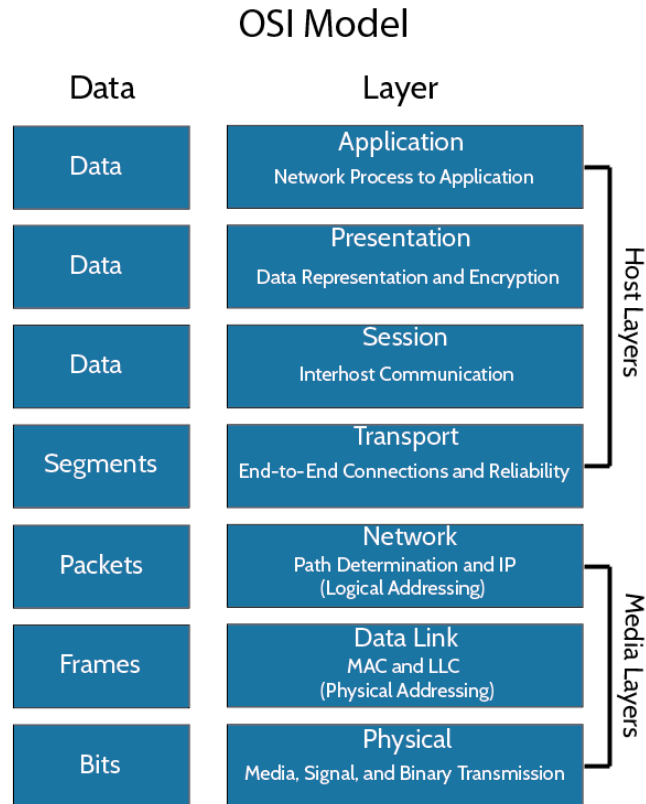
A broadcast domain is a domain in which broadcasts are forwarded. A broadcast domain contains all devices that can reach each other by using broadcast messages.

All ports on a hub or a switch are in the same broadcast domain by default. All ports on a router are in a different broadcast domain and routers do not forward broadcasts from one broadcast domain to another, unless specifically made to do so.

OSI Model

The Open Systems Interconnection (OSI) model is a standard definition that characterizes and standardizes the communication functions of the modern computer systems. It strives to allow better interoperability between different computer systems by defining standard protocols and conventions of communication.

The OSI reference model has 7 layers:



The Application Layer serves as a medium through which users and applications can access network and communication services. Examples include DNS, FTP, HTTP, NTP, DHCP, SMTP, and SNMP.

The Presentation Layer formats the data before it is presented to the Application Layer, and serves as a “translator of the network”. This layer translates data into a common format at the sending host, then translates the common format back to a format known to the Application Layer at the receiving host. It is sometimes called “the syntax layer”. Examples include MIME, and XDR.

The Session Layer establishes sessions between processes running on different stations. Examples include SOCKS, PPTP, NetBIOS, and RTP.

The Transport Layer provides transfer of data between hosts, and is responsible for error recovery and flow control. It ensures complete data transfer. Transport Layer creates logical paths, known as virtual circuits, for transmitting data from host to host. Examples include SPX, TCP, SCTP, and UDP.

The Network Layer provides switching and routing capabilities. Routing, forwarding, addressing, internetworking, error handling, congestion control, and packet sequencing are mainly handled by this layer. Examples include IP, IPsec, ICMP, IGMP, and IPX.

The Data Link Layer encodes data packets and decodes them to bits. It also handles errors of the physical layer. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a host on the network gains access to the data and the permission to transmit it. The LLC sublayer handles error checking, flow control, and frame synchronization. Examples include PPP, ARP, Frame Relay, HDLC, and L2TP.

The Physical Layer handles transmission and reception of the raw bit streams over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces of the physical medium and carries the signals for all of the higher layers. Examples include Ethernet, DSL, and USB.

TCP and UDP

TCP is a connection-oriented stream over an IP network. It guarantees that all sent packets will reach the destination in the correct order. This is achieved by the use of acknowledgement packets that are sent back to the sender.

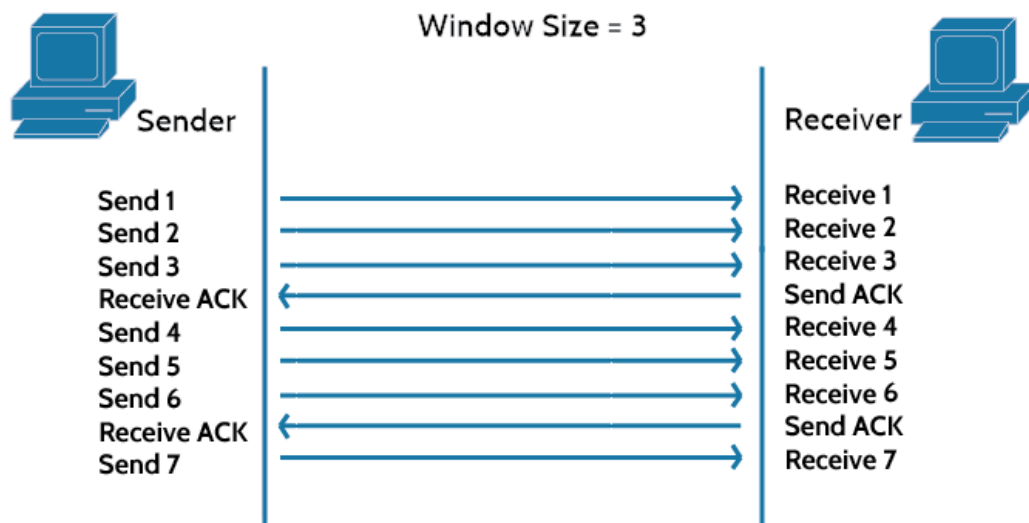
TCP usually causes additional delays and is recommended to be used only when transmission integrity is crucial.

UDP is a connection-less protocol. UDP communication are datagram-oriented. The integrity is guaranteed only on a single datagram. Datagrams can be received out of order or don't arrive to the receiving host at all.

Most real-time communications use UDP to transmit data, where packet loss is preferable to the overhead of a TCP connection.

TCP flow control and windowing

TCP uses flow control protocol to avoid having the sender send the data too fast for the receiver to receive and process it. Having a mechanism for flow control is important for connections where hosts of different speeds communicate. TCP uses sliding window flow control protocol. In each TCP segment the receiver specifies the amount of additional data that it is willing to buffer and process for the given connection. The sending host can't send more than that amount before it must wait for an acknowledgment and window update. Because of limited buffer space (where received data is temporarily stored before it is processed), TCP hosts agree to limit the amount of data that can be transmitted unacknowledged. This is called a window size.



CSMA/CD

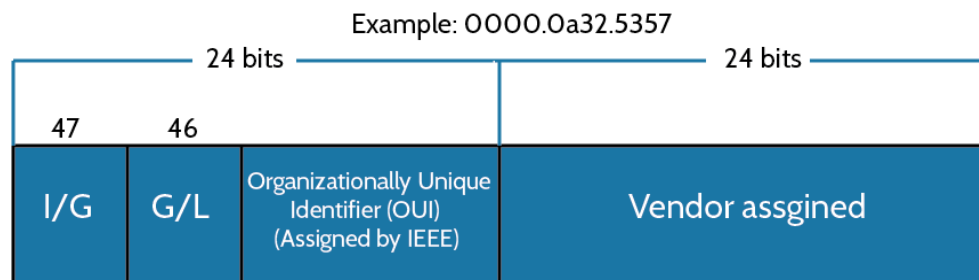
Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a protocol which helps devices share the bandwidth while preventing devices from transmitting simultaneously on the network and creating a collision. If the network is busy when a station needs to transmit, the station waits a random amount of time before attempting to transmit again. If two stations transmit their data at exactly the same time their signals will collide. Both stations will detect the collision and back off a random duration before trying again.

Half-Duplex and Full-Duplex Ethernet

A node can either transmit or receive but not perform both actions at the same time with half-duplex communication channels. A node can transmit and receive at the same time with full-duplex communication channels. Maximum of two nodes can be connected on a full-duplex link. Usually this is a host-to-switch or switch-to-switch configuration. Full duplex communication provides every host with a unique collision domain. This approach completely avoids collisions without need for CSMA/CD.

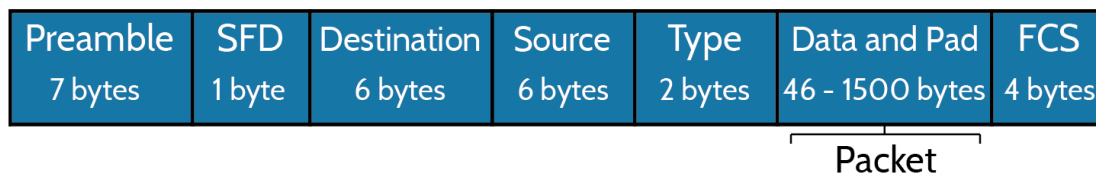
Ethernet at the Data Link Layer

Data Link Layer addressing is commonly referred to as MAC or hardware addressing. Data Link Layer frames packets received from the Network Layer and prepares them for transmission on the local network. Each and every network interface card (NIC) has a MAC address associated with them. The MAC address is a 48-bit address written in a hexadecimal format.



Ethernet frames

Bytes get combined into frames in Data Link Layer. Packets handed down from the Network Layer are encapsulated to frames in Data Link Layer for transmission. Frames provide error detection using a cyclic redundancy check (CRC). This is error detection, not error correction. An example of a typical Ethernet frame is shown below.



Ethernet at the Physical Layer

Every Ethernet cable has attenuation, which is defined as the loss of signal strength as it travels further. Crosstalk is another vector of loss of signal quality and is caused by unwanted signal interference, usually sourced from adjacent pairs of the cable.

Some of the IEEE Ethernet standards:

10Base-T (IEEE 802.3) uses category 3 unshielded twisted pair (UTP). It runs up to 100 meters. RJ45 connector is used.

100Base-TX (IEEE 802.3u) is known as Fast Ethernet, uses category 5, 5E, or 6 UTP two-pair wiring. It can run up to 100 meters long. It uses an RJ45 connector.

100Base-FX (IEEE 802.3u) uses fiber cabling 62.5/125-micron multimode fiber. It can run up to 412 meters long. It uses ST and SC connectors.

1000Base-CX (IEEE 802.3z) uses copper twisted-pair. It can run up to 25 meters. It uses a 9-pin connector known as High Speed Serial Data Connector (HSSDC).

1000Base-T (IEEE 802.3ab) is category 5, four-pair UTP wiring that can run up to 100 meters and offer speeds up to 1Gbps.

1000Base-SX (IEEE 802.3z) is a multimode fiber optic Gigabit Ethernet standard for operation over near infrared (NIR) light, 770 to 860 nanometer. The standard specifies a distance capability between 220 meters (62.5/125µm fiber with low modal bandwidth) and 550 meters (50/125µm fiber with high modal bandwidth). Offers speeds up to 1Gbps.

1000Base-LX (IEEE 802.3z) is a single-mode fiber standard. It uses 9-micron core and 1300nm laser. Maximum cable length is 10km under optimal conditions.

1000Base-ZX (Cisco standard) is a Cisco standard for Gigabit Ethernet. It operates on singlemode fiber optic links and it can run up to 70 kilometers.

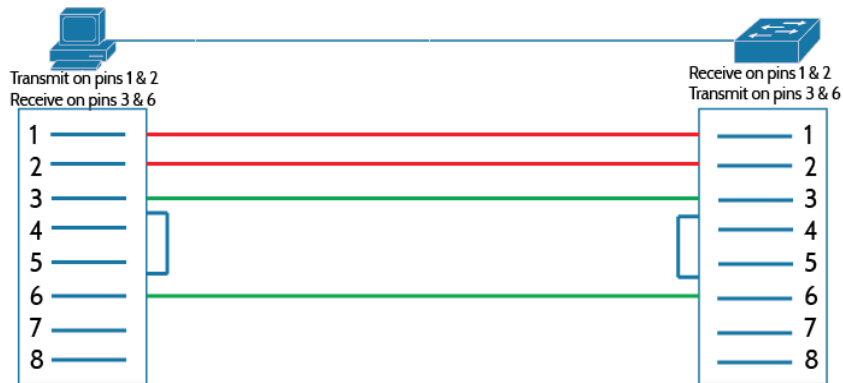
10GBase-T (802.3.an) is a standard for 10Gbps connections over UTP cables. RJ45 connector are used and cable lengths can go up to 100 meters.

Ethernet cabling

Straight-through cable uses four wires. It is used to connect the following devices:

Router to switch or hub

Host to switch or hub



Crossover cable uses four wires too but wires are connected to different ends, in crossed manner as name implies. Can be used to connect the following device types:

Host to host

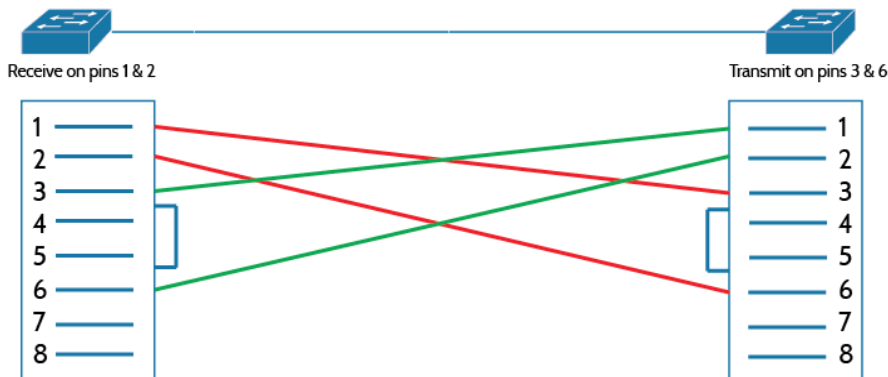
Router to host

Router to router

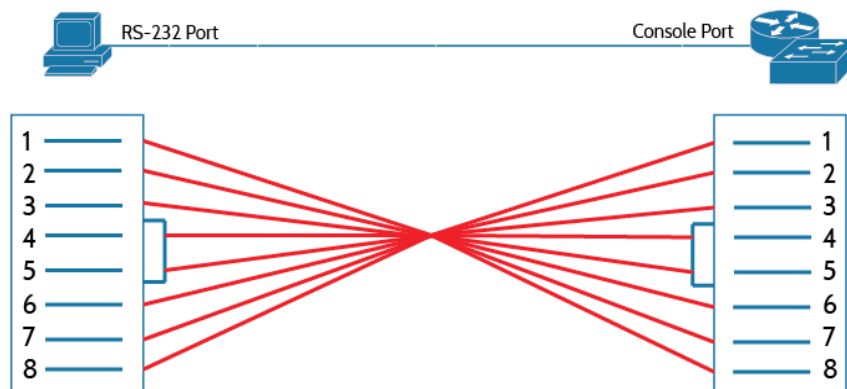
Switch to switch

Switch to hub

Hub to hub



Rolled cable uses eight wires. Rolled cable is used to connect host's EIA-TIA 232 interface to router's or switch's console port.



Fiber Optic

Fiber optic is used for fast transmission of data, is made of glass or plastic, and is thin. It works as a waveguide to transmit light between the two ends of the cable. Fiber optic can usually extend to very long distances. It is protected against interference like crosstalk. There are two types of fiber optics: singlemode and multimode. Singlemode fiber optic cable allows only one mode of light to go through. Multimode fiber optic cable allows multiple modes of light to go through.

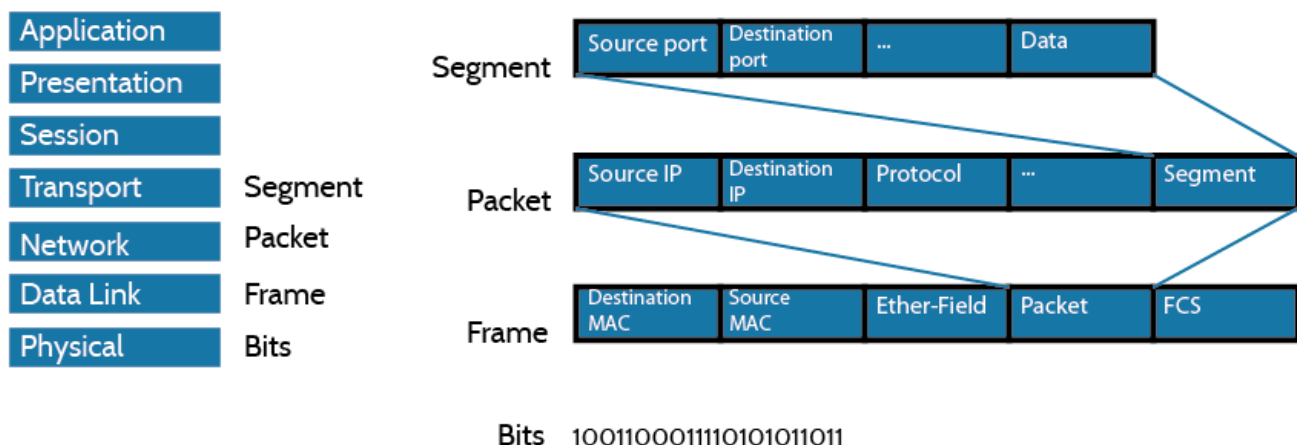
Data encapsulation

When a data is being transmitted across a network, it goes through a process called encapsulation and is encapsulated with protocol information at each layer of the OSI model.

Each layer uses protocol data units (PDUs) to communicate. PDU information is read only by the peer layer on the receiving device. After PDU is read, it gets stripped off and the information is handed to the next layer.

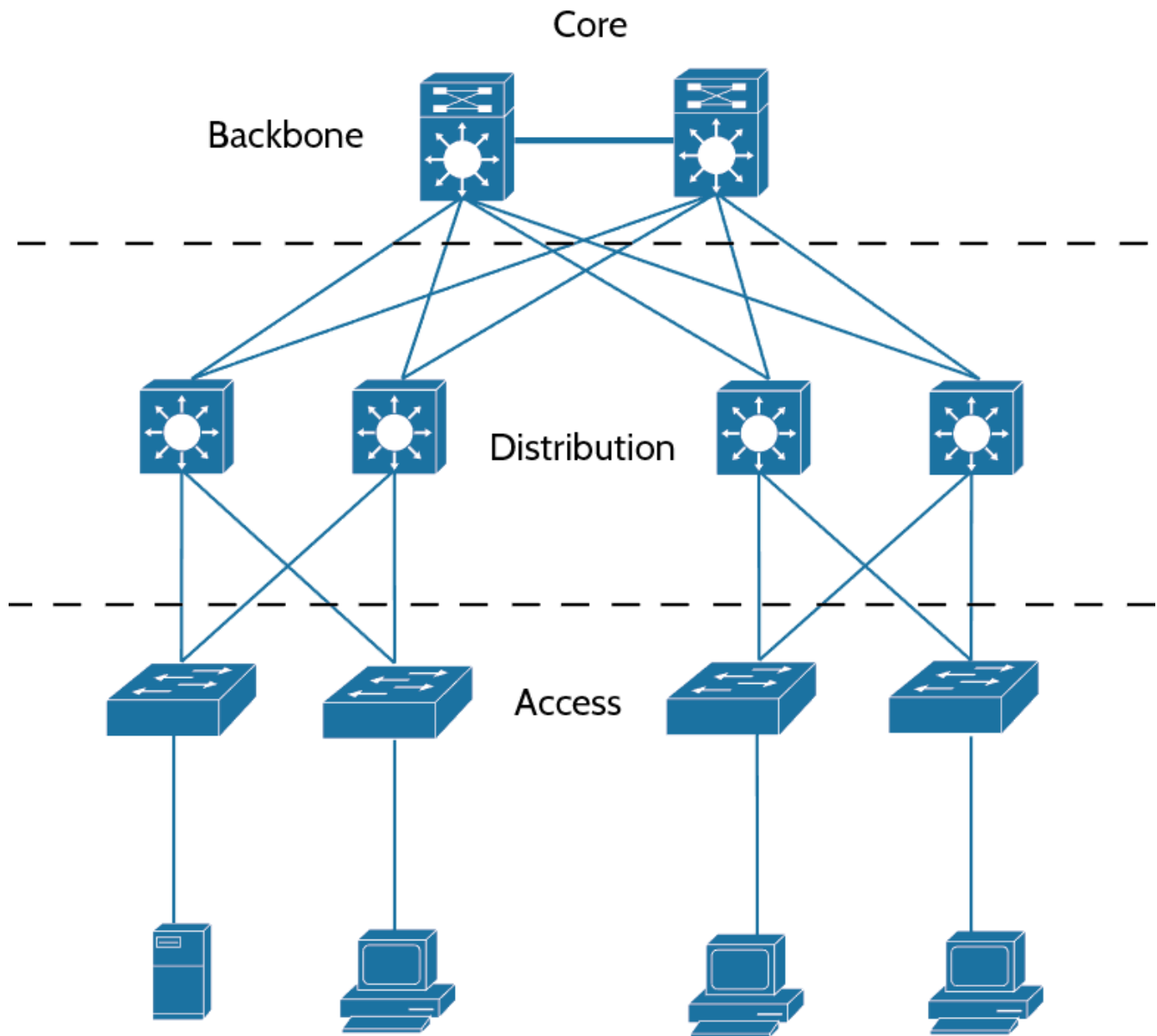
Data encapsulation works as follows in the transmitting device:

1. Information is converted to data for transmission.
2. Data is converted to segments and a connection is set up between the hosts.
3. Segments are converted to packets and a logical address is placed in the header.
4. Packets are converted to frames for transmission. Hardware addresses are used to identify hosts of a local segment.
5. Frames are converted to bits. Digital encoding and clocking schemes are used.



The Cisco three-layer hierarchical model

The Cisco hierarchical model is used to design, implement, and maintain a scalable network. Cisco hierarchical model has three layers, each with specific functions.



The Core Layer is responsible for transporting large amounts of data. Its purpose is to switch traffic as fast as possible. The Core Layer usually deals with large volumes of data. High speeds and low latency are crucial in this layer.

The Distribution Layer is a communication point between the Access Layer and the Core Layer. It exists to serve routing and filtering capabilities. The Distribution Layer is tasked with determining the fastest way of handling a request.

The Access Layer controls and provides user's access to the network. The Access Layer is also referred to as the "desktop layer".

Chapter 2: TCP/IP and IP Addressing

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language and protocol of the modern Internet. It can also be used as a communication protocol in the private networks. TCP/IP dictates how information should be packaged, sent, and received, as well as how to get to its destination.

DoD Model

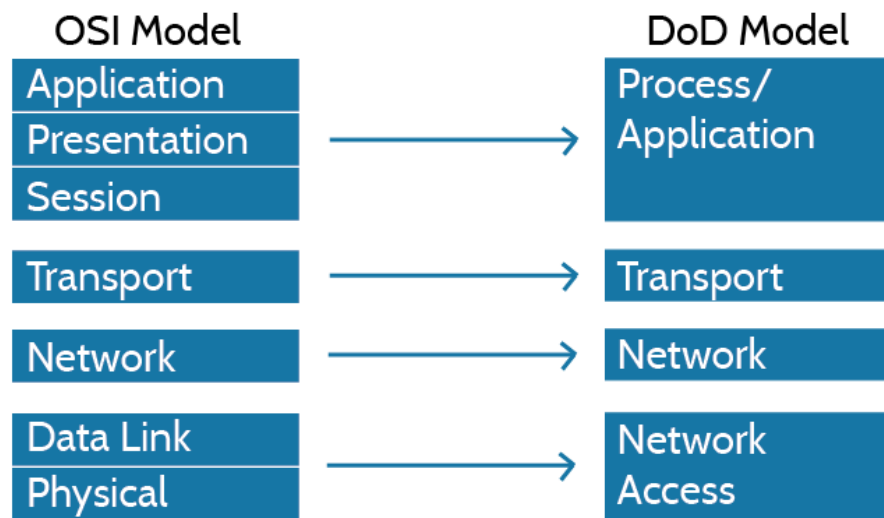
The DoD model is a condensed version of the OSI model and it has four layers:

Process Layer or Application Layer

Host-to-Host Layer or Transport Layer

Internet Layer

Network Access Layer or Link Layer



The Process/Application Layer protocols

Some of the common Application Layer protocols are described below.

Telnet allows a user of a remote client machine to access the resources of another machine, in order to access a command-line interface. Telnet sends everything in a clear text fashion and doesn't utilize any kind of encryption.

Secure Shell (SSH) is similar to Telnet in function but uses encrypted connection and can be considered a secure protocol.

File Transfer Protocol (FTP) lets users transfer files between two machines. FTP can also perform directory operations. FTP requires authentication to allow access to serving machine.

Trivial File Transfer Protocol (TFTP) is a simpler version of FTP. TFTP can only send and receive files, it does not have any directory and other such advanced capabilities.

Simple Network Management Protocol (SNMP) collects and manipulates network information. Network management station (NMS) gathers information from network devices at fixed or random intervals. In addition, network devices can inform the NMS station about the problems in the network device as they occur.

Hypertext Transfer Protocol (HTTP) is usually used as communication protocol between a web browser and a web server.

Hypertext Transfer Protocol Secure (HTTPS) is a secure version of HTTP. It utilized Secure Sockets Layer (SSL) to provide encrypted communications.

Network Time Protocol (NTP) synchronizes clocks of network devices and ensures that all devices on a given network agree on the current time and date.

Domain Name Service (DNS) resolves hostnames. DNS maintains a list of domain names and translates them to associated IP addresses.

Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to hosts. These are the information DHCP server provides when the host is requesting an IP address from the DHCP server: IP address, subnet mask, domain name, default gateway, DNS server address, WINS server address. DHCP utilized UDP protocol to exchange information with the clients.

Clients take these steps to receive an IP address from a DHCP server:

1. The client broadcasts a DHCP Discover message at port 67 that looks for a DHCP server.
2. The DHCP server that receives the Discover message sends a DHCP Offer message back to the client.
3. The client then proceeds to send a DHCP Request message that asks for the offered IP address and other information.
4. The server sends back DHCP Acknowledgment message to finalize the exchange.

Automatic Private IP Addressing (APIPA) is a feature of Windows systems. Clients can automatically self-configure an IP address and subnet mask with APIPA - when a DHCP server isn't available. The IP address range of APIPA is 169.254.0.1 through 169.254.255.254. APIPA also configures clients with the default Class B subnet mask of 255.255.0.0.

Port numbers

TCP and UDP uses port numbers to communicate with the upper layers. Port numbers are used to keep the track of the different conversations that take place at the same time. Source port numbers are usually dynamically assigned and are some number starting at 1024. Port numbers below 1023 are “well-known” port numbers.

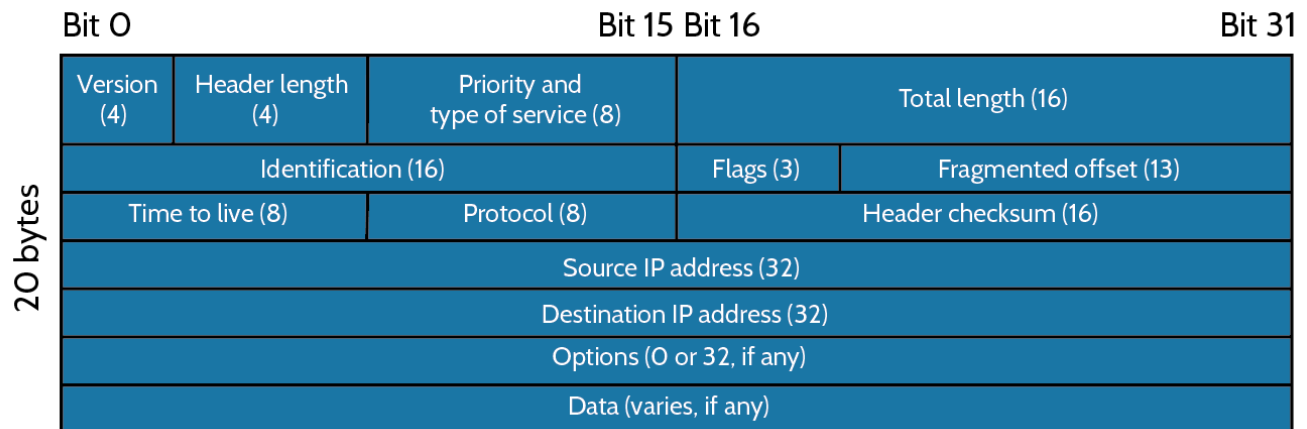
Some of the “well-known” port numbers:

TCP		UDP
Telnet - 23	POP3 - 110	SNMP - 161
SMTP - 25	NTP - 123	TFTP - 69
HTTP - 80	IMAP4 - 143	DNS - 53
FTP - 20,21		DHCP - 67
DNS - 53		
HTTPS - 443		
SSH - 22		

The Internet Layer protocols

Common Internet Layer protocols are explained below.

Internet Protocol (IP) holds the big picture and is aware of all the interconnected networks. All machines on the network have a logical address called an IP address. Internet Protocol looks at each packet's logical destination address and uses routing table to decide where to send it next. IP receives segments from the Host-to-Host Layer and fragments them into datagrams. IP then reassembles datagrams back into segments on the receiving host. Each datagram has a source and a destination address on it. Routers usually make a routing decision based on datagram's destination address. Image of IP header is given below.



Internet Control Message Protocol (ICMP) works at the Network Layer and has many uses. ICMP is a management protocol and messaging service provider. Packet Internet Groper (Ping) uses ICMP echo request and reply messages to check the connectivity of machines. Traceroute uses ICMP Time-outs to determine the path data takes to reach the destination.

Address Resolution Protocol (ARP) resolves the hardware address of a host from a known IP address. When IP sends a datagram, it must use the destination node's hardware address. If IP can't find the destination node's hardware address in the ARP cache, it uses ARP to find the destination hardware address. ARP sends out a broadcast asking the host with the specified IP address to reply with its hardware address. ARP basically translates the software/logical addresses into hardware addresses.

IP addressing

An IP address is basically an identifier assigned to each host on a network. An IP address is a software address, not a hardware address (hardware addresses are usually hard-coded into the network interface card (NIC) and is used for finding hosts on a local network). IP addressing is used to allow hosts on one network to communicate with the hosts on another network. An IPv4 address is 32 bits in length. These bits are divided into four parts, referred to as octets, each containing 8 bits. IP addresses can be shown using one of three methods outlined below:

Decimal: 10.20.5.15

Binary: 00001010.00010100.00000101.00001111

Hexadecimal: 0A.14.05.0F

Network classes are classification of network addresses based on network size.

	8 bits	8 bits	8 bits	8 bits
Class A:	Network	Host	Host	Host
Class B:	Network	Network	Host	Host
Class C:	Network	Network	Network	Host
Class D:	Multicast			
Class E:	Research			

Reserved and special IP addresses are outlined below:

Network address of all 0s – stand for “this network”.

Network address of all 1s – stands for “all networks”

127.0.0.1 – usually used as local loopback address. Allows local host to send packets to itself.

Node address of all 0s – “network address” or any host on specific network.

Node address of all 1s – means “all nodes” on specified network.

Entire IP address set to all 0s – “any network”.

Entire IP address set to all 1s – broadcast to all nodes on the current network.

10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255 – Private IP addresses

Private IP addresses can be used on a private network and they’re not routable through the Internet. This is designed for the purpose of creating a measure of security, saving IP address space, and making creation of local network easier.

Types of packets:

Unicast – is used to send packets to a single host.

Multicast – are packets sent from a single source and transmitted to many devices. Referred to as “one-to-many”.

Subnetting basics

The act of taking bits from the host portion of the address and reserving them to define the subnet address instead is called subnetting. This practice will result in fewer bits being available for defining your hosts.

Every host on a network must know which part of the host address will be used as the subnet address for subnetting to be achieved. This is done by assigning subnet mask to each host. A subnet mask is a 32 bit value that helps the device distinguish the network ID part of the IP address from the host ID part.

Classless Inter-Domain Routing (CIDR) is the method that is usually used by Internet service providers to allocate addresses to their customers. They provide addresses in a certain block size using CIDR.

When you receive a block of addresses, it will be written down with a slash notation like this: /29. This shows what your subnet mask is. The slash notation basically show how many bits are turned to 1s. For example, a Class A default subnet mask, which is 255.0.0.0, tells us that the 8 bit of the subnet mask is all 1s (11111111). You need to count all the 1-bits to figure out your mask. The 255.0.0.0 is a /8 in slash notation because it has 8 bits that are 1s. Table below lists subnet masks and equivalent CIDR slash notation:

Subnet Mask	CIDR Value	Subnet Mask	CIDR Value	Subnet Mask	CIDR Value
255.0.0.0	/8	255.255.128.0	/17	255.255.255.192	/26
255.128.0.0	/9	255.255.192.0	/18	255.255.255.224	/27
255.192.0.0	/10	255.255.224.0	/19	255.255.255.240	/28
255.224.0.0	/11	255.255.240.0	/20	255.255.255.248	/29
255.240.0.0	/12	255.255.248.0	/21	255.255.255.252	/30
255.248.0.0	/13	255.255.252.0	/22		
255.252.0.0	/14	255.255.254.0	/23		
255.254.0.0	/15	255.255.255.0	/24		
255.255.0.0	/16	255.255.255.128	/25		

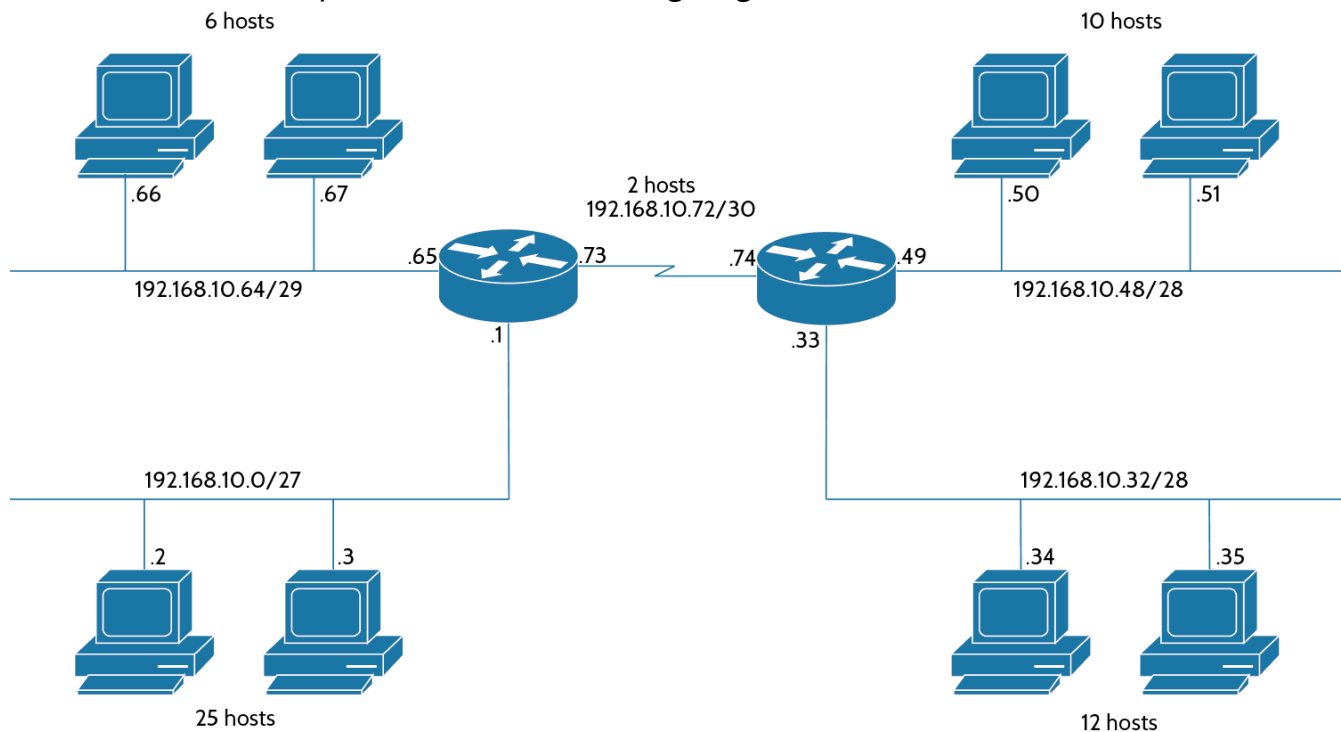
IP Subnet-Zero is a command that allows you to use the first and last subnet in your network design.

Subnetting can easily be accomplished by answering these five questions:

- How many subnets are there in chosen subnet mask? 2^x = number of subnets, where x is the number of masked bits, “the 1s”.
- How many valid hosts are there in each subnet? $2^y - 2$ = number of hosts per subnet, where y is the number of unmasked bits, “the 0s”.
- What are the valid subnets? $256 - \text{subnet mask} = \text{block size}$, “the increment number”. Lets use 255.255.255.224 mask as an example. $256 - 224 = 32$. The block size, “increment number” of the 224 mask is always 32. Start counting at zero in blocks of 32 to figure out your subnets: 0, 32, 64, 96, 128, 160, 192, 224.
- What’s the broadcast address of a given subnet? The broadcast address is always the number right before the next subnet. The 0 subnet has a broadcast address of 31 because the next subnet is 32. The 32 subnet has a broadcast address of 95 because the next subnet is 96.
- What are the valid hosts in each subnet? Valid hosts are the numbers between the subnets. If 32 is the subnet number and 63 is the broadcast address, then 33–62 range is the valid host range. Host range is between the subnet address and the broadcast address.

Variable Length Subnet Masks (VLSMs)

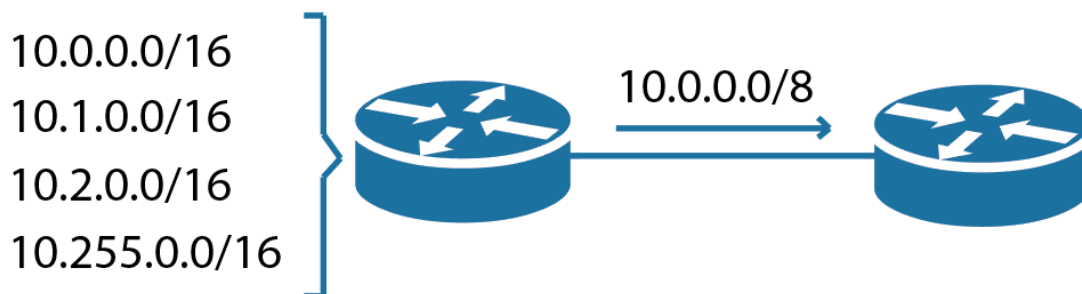
VLSMs are subnet masks with different lengths that are assigned to different router interfaces of the same device. Example of classless VLSM design is given below:



In example given above, the network is broken down to four subnets: /30, /29, /28, /27. Subnets will have 2 hosts, 6 hosts, 10 hosts, and 25 hosts respectively.

Summarization

Routing protocols can advertise many networks as one address and this practice is known as “summarization”. The main purpose of summarization is to reduce the size of routing tables.



List of useful commands

ping uses ICMP echo requests and replies to test connectivity.

tracert shows the path packet takes to a network destination.

tracert is a Microsoft Windows command that accomplishes same thing as “traceroute” of Cisco IOS.

arp -a displays IP-to-MAC address mappings on a Microsoft Windows systems.

show ip arp displays IP-to-MAC address mappings.

ipconfig /all is used on a Microsoft Windows machines to display the network configuration.

Chapter 3: IOS Basics

Cisco IOS basics

IOS is the name of operating system of the Cisco devices. The Cisco IOS provides routing, switching, internetworking, and telecommunication features.

Cisco devices are usually configured using command-line interface (CLI). You can access the CLI through the console port of a device or through Telnet and Secure Shell (SSH).

When you power up a Cisco IOS device, power-on self-test (POST) sequence is run. After POST, the device will load Cisco IOS from flash memory if an IOS file is present, then expand it into RAM. Flash memory is electronically erasable programmable read-only memory (EEPROM).

The next step is to locate and load a configuration known as the “startup-config” which is usually stored in nonvolatile RAM (NVRAM). After the IOS is loaded, the “startup-config” will be copied from NVRAM into RAM and from then on called the “running-config”. If a “startup-config” isn’t found in the NVRAM, device will enter “setup mode”, which gives the user step-by-step guide for setting up basic parameters.

Command-line interface

When you enter CLI, “Switch>” prompt will show up. This prompt signifies “user exec mode”, or simple “user mode” and it’s mostly used to view statistics.

Configuration of a Cisco device can only be changed while in “privileged exec mode”, and you can access it by using the “enable” command as shown:

```
Switch>enable
```

```
Switch#
```

The “Switch#” prompt means that you are in privileged mode where you can view and also change the device configuration.

You can go back to user mode by using the “disable” command:

```
Switch#disable
```

```
Switch>
```

You can use “logout” command from either mode to exit the console.

You can make global changes to the device by typing “configure terminal”. This command gets you into global configuration mode where you can make changes to the “running-config”.

Interfaces

Interface command is used to make changes to an interface:

```
Switch(config)#interface fastEthernet 0/1
```

```
Switch(config-if)#
```

Prompt has changed to “Switch(config-if)#”, this signifies that you’re in the interface configuration mode.

Administrative configurations and commands

Hostname “hostname” command is used to set the name of the device. Hostname is only locally significant, hostnames don't affect how a device performs name lookups or how the device works on the internet network.

```
Switch#config t
Switch(config)#hostname name
```

Banners Banners are little messages and notifications that show up when a connection is made to the device. They can be created and customized to give the users some kind of information.

Three types of banners are: exec banner, login banner and message of the day banner. Message of the day (MOTD) banners display a message to anyone connecting to the device via Telnet, auxiliary port or through a console port. You can configure MOTD banners as shown:

```
Switch(config)#banner motd message
```

Passwords There are usually five types of common passwords that can be set on Cisco device: console, auxiliary, telnet, enable password, and enable secret. The enable secret and enable password are used to secure privileged mode. Once the enable commands are set, users will be prompted for a password when they try to access privileged mode. Here's an example of setting up enable passwords:

```
Switch(config)#enable password password
Switch(config)#enable secret password
```

User-mode passwords are assigned via the line command like this:

```
Switch(config)#line console 0
Switch(config-line)#password password
Switch(config-line)#login
```

Telnet password are assigned via the line commands like this:

```
Switch(config)#line vty 0 15
Switch(config-line)#password password
Switch(config-line)#login
```

Auxiliary passwords are assigned like this:

```
Switch(config)#line aux 0
Switch(config-line)#password password
Switch(config-line)#login
```

Encrypting passwords

To manually encrypt your passwords, use the service password-encryption command. Here's how:

```
Router#config t
Router(config)#service password-encryption
```

Setting up Secure Shell (SSH)

Here are the commands for setting up SSH:

```
Router(config)#hostname name
name(config)#ip domain-name domain
name(config)#username username password password
name(config)#crypto key generate rsa
name(config)#ip ssh version 2
name(config)#line vty 0 15
name(config-line)#transport input ssh
```

Descriptions

You can set up locally significant descriptions on interfaces. Here's an example:

```
Switch#config t
Switch(config)#int fa0/1
Switch(config-if)#description description
```

Pipe command

Pipe can be used for searching through large amounts of output among many other things.

Three examples of pipe command are given below:

Router#show any-command | begin regular-expression - Shows output starting from the first line that contains the regular expression.

Router#show any-command | exclude regular-expression - Shows lines that don't contain the regular expression.

Router#show any-command | include regular-expression - Shows lines that contain regular expression.

List of useful commands

show running-config - Shows currently running configuration.

show startup-config - Shows startup configuration.

copy running-configuration startup-configuration - Saves running configuration from RAM to NVRAM.

erase startup-config - Deletes the startup configuration file.

reload - Restarts the device.

show ip interface brief - Shows brief information about all interfaces of the device.

show interface - Shows information about the specified interface.

show protocols - Shows layer 1, layer 2, and IP address information of all interfaces.

show controllers - Displays physical information about specified interface.

no shutdown - Turns on the interface.

speed - Sets the speed of an interface.

duplex - Sets the duplex mode of an interface.

clock set - Sets the clock of a device.

? - Using question mark after a command shows all the possible commands that can come after the given command.

Chapter 4: Network Essentials

Boot sequence

Boot sequence is performed when a device is powered on. Boot sequence tests the hardware and loads the software. The boot sequence is made of following steps:

1. The device performs a POST, which tests the hardware to verify that all parts of the device are operational. POST is stored in and runs from the read-only memory (ROM).
2. The bootstrap then locates and loads the Cisco IOS software. The IOS software is loaded from the flash memory as the first-order storage of the software, by default. The default order of an IOS loading is: flash memory, TFTP server, ROM.
3. IOS software looks for a configuration file in the NVRAM. This file is usually called “startup-config” and will be there only if the “running-config” have been copied into the NVRAM before. If a “startup-config” file is found in the NVRAM, then the device will copy it into the working memory - RAM, and name it the “running-config”.

After these steps are taken the device becomes operational. If no “startup-config” is found in the NVRAM, the device reacts by broadcasting out any interface that detects carrier detect (CD) to locate a TFTP server for retrieving the configuration files from. If that fails then the device will begin the “setup mode” configuration process.

DHCP (Dynamic Host Configuration Protocol)

To configure a DHCP server for your hosts, you need the following information:

- Network and mask for each Network ID. All addresses in a subnet can be leased to hosts by default.
- Reserved and excluded addresses. These addresses will not be leased to hosts and are usually reserved for printers, servers, routers, etc.
- Default gateway.
- DNS server addresses.

Here are the configuration steps:

1. Exclude the addresses you want don't want to lease.
2. Create your pool using a unique name.
3. Choose the network ID and subnet mask for the DHCP pool.
4. Specify the default gateway.
5. Provide the DNS server addresses.

Here's how DHCP can be configured using the 192.168.10.0/24 network ID:

```
Switch(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
Switch(config)#ip dhcp pool pool_name
Switch(dhcp-config)#network 192.168.10.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.10.1
Switch(dhcp-config)#dns-server 4.4.4.4
```

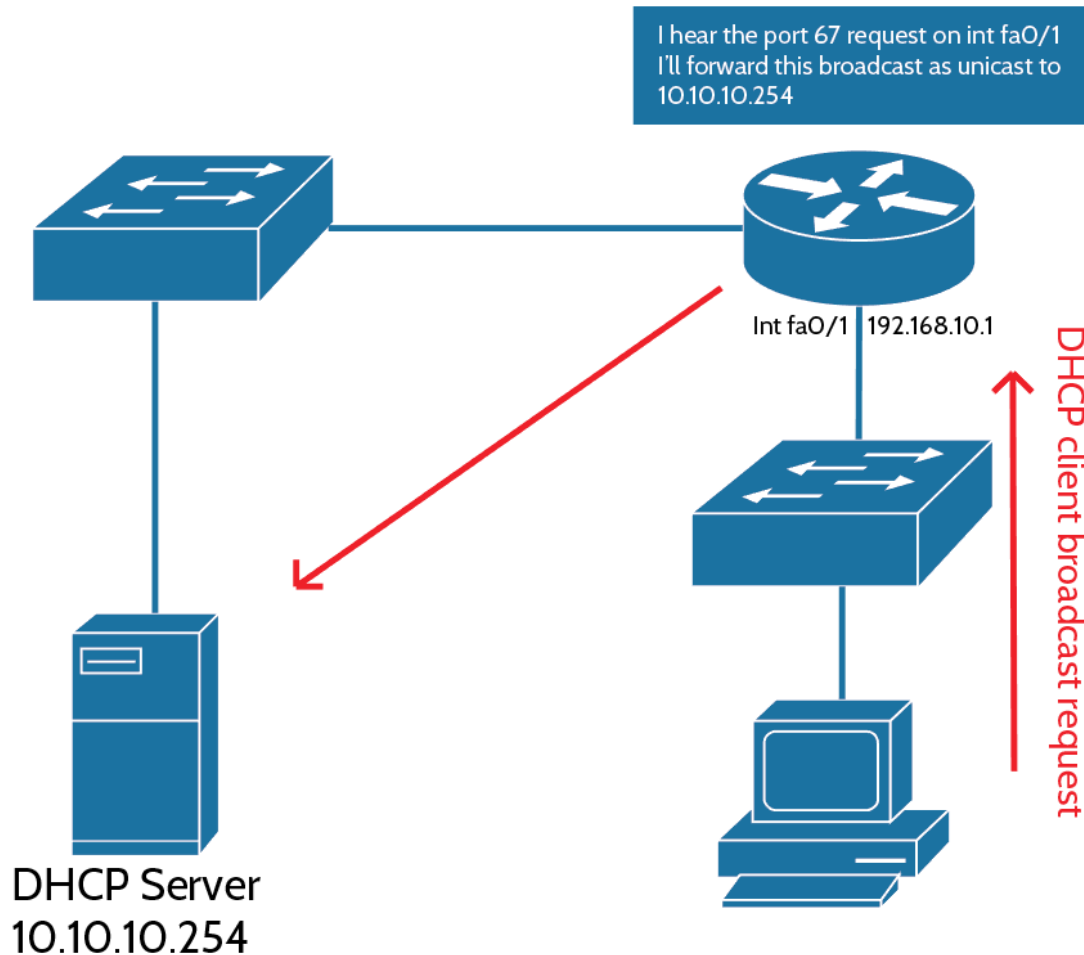
DHCP Relay

If DHCP server and DHCP clients aren't on the same LAN, router can be configured to forward the DHCP client requests to a DHCP server. Here's how FaO/1 interface of router can be configured to forward the DHCP requests to a DHCP server:

```
Router#config t
```

```
Router(config)#interface fa0/0
```

```
Router(config-if)#ip helper-address 10.10.10.254
```



List of useful DHCP commands

`show ip dhcp binding` - Lists state information about every IP address currently leased to the clients.

`show ip dhcp pool pool_name` - Displays the pool configuration and statistics.

`show ip dhcp server statistics` - Lists DHCP server statistics.

`show ip dhcp conflict` - If someone statically configures an IP address on a LAN and the DHCP server hands out the same address, you'll end up with a duplicate addresses. This command displays information about such conflicts.

Network Time Protocol (NTP)

NTP synchronizes clocks of computer systems. Typically you'll have an NTP server that connects to an atomic clock to retrieve the current time and date. Other devices learn clock information from such NTP servers.

You can specify NTP server IP address in NTP clients with the following command:

```
Router(config)#ntp server ip_address
```

Cisco Discovery Protocol (CDP)

Cisco Discovery Protocol (CDP) is a protocol that can help with collecting information about directly connected devices. The `show cdp neighbor` command delivers information about directly connected devices. By default, it is not possible to get information about remote devices with CDP, only the directly connected ones. `show cdp neighbors detail` command shows detailed information about CDP neighbors.

CDP is Cisco proprietary protocol and are not supported by the devices of other vendors.

LLDP is industry standard protocol that provides the same functionality as CDP and is supported by most devices regardless of their vendor.

List of useful commands

`telnet ip_address` - Creates telnet session to a specified IP address.

`show sessions` - Shows hosts you are connected to through telnet.

`show users` - Shows users connected to your device through telnet.

`disconnect x` - Disconnects the specified host from your device. ("x" signifies the number of an user)

`ip host hostname ip_address` - Links a hostname to an IP address.

`show hosts` - Shows table of hostname-IP bindings.

`ip domain-lookup` - Turns on DNS domain lookup service.

`no ip domain-lookup` - Turns off DNS domain lookup service.

`debug all` - Turns on all debugging messages.

`debug ip icmp` - Turns on ICMP debugging messages.

`no debug all` - Turns off all debugging messages.

`show processes` - Displays information about processes currently running on the device.

Chapter 5: IP Routing

Routing basics

Routing means taking a packet from one device and sending it through the network to another device on a different network. Routers use logical destination addresses to choose the best path to route the packets through.

Router must be aware of these things to effectively route a packet:

- Destination address
- Neighbor routers from where it can learn about remote networks
- Possible routes to all remote networks
- The best route to each remote network

There are few ways router can learn about non-directly connected networks:

Static routing method is about manually entering all routes into the router.

Dynamic routing method is about using a specific protocol that communicates with the same protocol on neighboring routers and exchanges routing information automatically. Neighboring routers running same dynamic routing protocol update each other about known networks.

Dynamic routing protocols also update all neighboring routers when change occurs on the network.

Packet-forwarding techniques

Cisco uses three types of packet-forwarding technique:

Process Switching is a process that looks up for every destination in the routing table and finds the exit interface for each packet. This process usually consumes much more processing power.

Fast Switching is a process that utilizes a cache to store the most recently used destinations, which gets rid of the need of searching through routing table for every received packet.

Cisco Express Forwarding (CEF) is a process that creates many different cache tables and is change-triggered, not packet triggered. When network topology changes, CEF caches change as well.

Static routing

Routes can be manually taught to a router and this practice is called “static routing”.

Pros:

- Usually more secure, because the administrator is the only one who can add and remove entries.
- Lower usage of router's resources.
- Minimizes bandwidth usage. Doesn't exchange updates and keepalives like dynamic routing protocols.

Cons:

- If a new network is added to the topology, new entry must be manually added to each relevant router.
- Accurate map of the network is required to be able to configure fully-functioning static routing.

Static routing can be configured as shown:

```
ip route destination_network mask next-hop_address or exit_interface  
administrative_distance permanent
```

Dissection of the command above:

- *ip route* - This command is used to create a static route.
- *destination_network* - Specifies the network you want to place into the routing table.
- *mask* - Specifies the subnet mask being used on the said network.
- *next-hop_address* - Specifies the IP address of the next-hop router - the router which will receive packets that are destined to the remote network and forward them to their destination. This router must be directly-connected.
- *exit_interface* - Specified the exit interface that connects to the next-hop router. Can be used instead of next-hop address.
- *administrative_distance* - Static routes have an administrative distance of 1 (0 if you use an exit interface instead of next hop address). You can change the default administrative distance by specifying it here. Information about administrative distances are given later in this chapter.
- *permanent* - Adding this tag to the end of command keeps the entry in routing table even if the next-hop interface shuts down or next-hop router can't be communicated with.

Default route

If a destination is not found in the routing table then a default route is used to forward the packets. It is also known as “gateway of last resort”.

Default route can be configured as shown:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 next-hop_address
```

Dynamic routing

Practice of using specific protocols called “routing protocols” to exchange routing information between the routers is called “dynamic routing”.

Two types of routing protocols are interior gateway protocols (IGPs) and exterior gateway protocols (EGPs):

Interior gateway protocols are used to exchange the routing information with routers in the same autonomous system. An autonomous system is either a single network or a collection of networks under a common administrative domain. Examples include: OSPF, RIP, and EIGRP.

Exterior gateway protocols are used to communicate between the autonomous systems. BGP is an exterior gateway protocol.

Administrative distances

The administrative distance rates the “trustworthiness” of a route. An administrative distance is a number between 0 and 255. “Most trusted routes” are rated 0 and unusable routes are rated 255. If a router receives multiple updates regarding a same network, one with lower administrative distance will be placed on the routing table and used as first-order route.

If two or more advertised routes to a same network are rated the same administrative distance then a routing protocol metric is used to determine which route is preferred. Routes with lowest metric will be placed into the routing table. If two routes have the same administrative distance as well as the same metrics then the routing protocol will load-balance between these two routes.

Default administrative distances are as follows:
Connected interface – 0
Static route – 1
EIGRP – 90
OSPF – 110
RIP – 120
External EIGRP – 170

Routing protocols

There are three classes of routing protocols.

Distance vector protocols use distance as metric to find best routes to a given network. RIP protocol uses hops to determine the best path. Each router in a way to the destination is considered a single “hop”. Routes that amount to less number of hops are considered superior to the ones that pass through more hops.

Link state, also known as “shortest path first” protocols, create and utilize three separate tables to function. First table keeps track of directly-connected neighbors, second table determines the topology of the entire network, and the third one is used as the routing table. Link state protocols usually store more information about the network than distance vector protocol. OSPF is an example of a link state protocol. These protocols send updates containing the state of their links to all other directly-connected routers. Then this information is propagated to their neighbors.

Hybrid protocols use aspects of both link state and distance vector protocols. EIGRP is an example of a hybrid routing protocol.

Routing Information Protocol (RIP)

RIP sends the complete routing table to neighbors every 30 seconds. It uses “hop” count to determine the best path to the given destination and it has a maximum allowable hop count of 15, which means that the route of 16 hops would be considered unreachable and not used at all. RIP is suitable for small networks.

RIP version 1 is a “classful” routing protocol, which means that all devices in the network must use the same subnet mask because RIP version 1 doesn't send subnet mask information in its updates. This also implies that all devices on the network must use the same subnet mask.

RIP version 2 does send subnet mask information in routing updates and therefore is called “classless” routing protocol.

Example of RIPv2 configuration is given below:

```
Router#config t
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 172.16.0.0
Router(config-router)#version 2
Router(config-router)#no auto-summary
```

We usually don't want routing protocols to auto-summarize because it's better to do that manually. Both RIP and EIGRP auto-summarize by default. We can turn this feature off with `no auto-summary` command.

Passive-interface

Most of the time you don't want RIP networks advertised everywhere on your network. In this case you can use `passive-interface` command to prevent routing updates being sent out from specified interfaces. However it should be noted that this command does not prevent the specified

interface from receiving RIP updates.

Here's an example of how Router's FastEthernet 0/1 interface can be made to act as a passive interface:

```
Router#config t
Router(config)#router rip
Router(config-router)#passive-interface FastEthernet 0/1
```

Advertising a default route

Existing default routes can be advertised to RIP neighbors using the `default-information originate` command as shown:

```
Router(config)#router rip
Router(config-router)#default-information originate
```

Open Shortest Path First (OSPF)

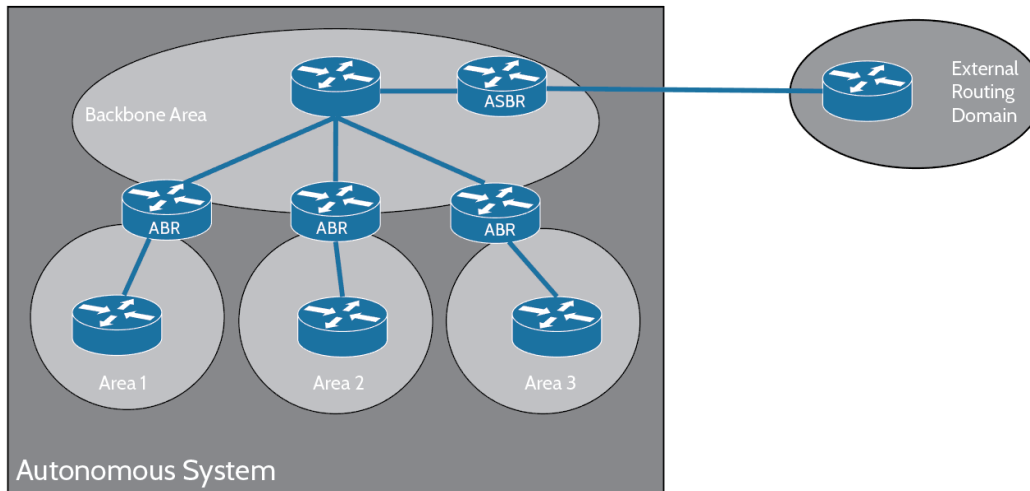
OSPF is an open-standard routing protocol and this is the key to OSPF's flexibility and popularity. OSPF utilizes the Dijkstra algorithm to construct a shortest path tree and populates the routing table according to this tree. Here's a list that summarizes some of the OSPF's best features:

- Allows creation of areas and autonomous systems
- Minimizes routing update traffic and ambient bandwidth usage
- High flexibility and scalability
- Supports VLSM/CIDR
- Is an open-standard and work flawlessly in multi-vendor deployment scenarios

Table below compares RIP to OSPF.

	RIPv1	RIPv2	OSPF
Type of protocol	Distance vector	Distance vector	Link state
Classless support	No	Yes	Yes
VLSM support	No	Yes	Yes
Auto-summarization	Yes	Yes	No
Manual summarization	No	Yes	Yes
Noncontiguous support	No	Yes	Yes
Route propagation	Periodic broadcast	Periodic multicast	Multicast on change
Path metric	Hops	Hops	Bandwidth
Hop count limit	15	15	None
Convergence	Slow	Slow	Fast
Peer authentication	No	No	Yes
Hierarchical network requirement	No	No	Yes (using areas)
Updates	Periodic	Periodic	Event triggered
Route computation	Bellman-Ford	Bellman-Ford	Dijkstra

OSPF's hierarchical design minimizes the routing table entries and keeps the updates of any topology changes contained within a single area. Hierarchical design of OSPF decreases routing overhead, speeds up convergence and confines network instability to a single area. Example of OSPF hierarchical design is shown below.



OSPF Terminology

Link is a name given to an interface added to the OSPF process. Links have up/down state information and one or more IP addresses associated with them.

Router ID is an IP address that is used to identify a router. Cisco routers choose to use the highest IP address of all the loopback interfaces as the Router ID. If no loopback interface is found then the router will choose the highest IP address of all active interfaces. Router ID is basically a name of the router in the OSPF process.

Neighbors are routers that have a interface on a common network. These configuration options must match for OSPF routers to form a neighborship:

- Area ID
- Stub area flag
- Authentication password (if using one)
- Hello and Dead intervals

Adjacency is a relationship between two routers that allows the direct exchange of routing updates. OSPF will directly share routes only with neighbors that are also considered an “established adjacency”. Not all neighbors become adjacent because of type of connection and configuration options. Routers form adjacency only with designated and backup designated routers in the multi-access networks. Routers form adjacency with the router on the other end of a link in point-to-point and point-to-multipoint networks.

Designated router is elected whenever OSPF routers are connected to a same broadcast network. It minimizes the number of adjacencies that need to be established. Elections are held based on a router's priority level. Router with highest priority becomes the designated router and Router ID is used as a tie-breaker. All routers on the network establish adjacency with the designated router (DR) and the backup designated router (BDR).

Backup designated router is considered a backup to the designated router and takes the role of designated router should it fail. Backup designated routers receive all routing updates from adjacent routers but don't send out LSA updates.

Hello protocol is a protocol that is used for dynamic neighbor discovery and for maintaining neighbor relationships. By default, hello packets are sent to multicast address of 224.0.0.5.

Neighborship database is a list of all routers from which hello packets have been received. Router ID and state information about each router are kept in the neighborship database.

Topological database is a database that contains information from all of the Link State Advertisement (LSA) packets that have been received for a given area. Information inside the topology database is used as the input to the Dijkstra algorithm that computes the shortest path to every network. Topological database is updated and maintained with LSA updates.

Link State Advertisement is a packet that contains link state and routing information that is shared among routers. There are different types of LSA packets. A router shares LSA packets only with established adjacency.

Areas are groups of contiguous networks and routers. Router can be a member of more than one area at a time, therefore area ID is associated with each interface. Routers in the same area has the same topology table (when up-to-date). All areas have to connect to area 0 which is also called a “backbone area”. Areas play a big role in establishing hierarchical network design.

OSPF metrics

OSPF's metric is called a “cost”. The cost of the entire path is the sum of the costs of the outgoing interfaces along the path. Cisco calculates the cost by using an equation of reference/bandwidth, where bandwidth is the configured bandwidth of the interface and the reference equals to 100 by default but this value can be altered to establish granular control over routes.

List of useful commands

`show ip route` – Displays the entire routing-table. Example of output is given below:

```
labb#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

R 192.168.8.0/24 [120/2] via 192.168.5.2, 00:00:24, Serial0
R 192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:03, Serial1
C 192.168.4.0/24 is directly connected, Ethernet0
C 192.168.5.0/24 is directly connected, Serial0
R 192.168.7.0/24 [120/1] via 192.168.5.2, 00:00:24, Serial0
R 192.168.1.0/24 [120/1] via 192.168.3.1, 00:00:03, Serial1
R 192.168.6.0/24 [120/1] via 192.168.5.2, 00:00:24, Serial0
C 192.168.3.0/24 is directly connected, Serial1
```

`int loopback x` – Creates a loopback interface. Can be used to specify OSPF router ID.

`network ip_address wildcard_mask area x` – Adds specified network to OSPF area x.

`show ip ospf` – Displays OSPF information for all OSPF processes running on the device.

`show ip ospf interface` – Displays all interface-related OSPF information.

`show ip ospf database` – Displays information about number of routers in AS and neighbor's Router ID.

`show ip ospf neighbor` – Displays information about neighbors and adjacency states.

`show ip protocols` – Displays information about all currently running protocols.

Chapter 6: Switching

Basic switch functions

Bridges utilize software to create and manage a Content Addressable Memory (CAM) filter table, switches however use application-specific integrated circuits (ASICs) to build and maintain their MAC filter tables. Basic function of a switch is to break up collision domains. Switches are usually faster operators than routers because they don't care about Network Layer overhead. They only take into account hardware address encoded into the frames and take one of these three actions: forward, flood, or drop. Switches create private, dedicated collision domains unlike hubs.

Here's a list of four important advantages that are gained when using Layer 2 switching:

- Hardware-based bridging (ASICs)
- Wire speed
- Low latency
- Low cost

No modification to data packet takes place and that's one of the reasons why Layer 2 switches are efficient. There are three main components to layer 2 switching: address learning, forward/filter decisions, and loop avoidance.

Address learning: Switches record the source hardware address of each frame received and record this information in the MAC table.

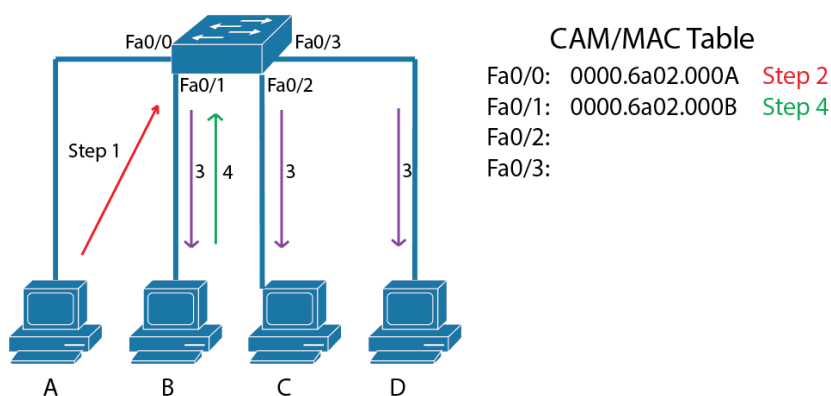
Forward/filter decisions: When a frame is received, the switch looks for destination address in the MAC table and chooses appropriate exit interface.

Loop avoidance: If multiple connections between switches are created for redundancy purposes then network loops can occur. Spanning Tree Protocol (STP) is used to prevent network loops while still allowing redundant setups.

When a switch receives a frame, it records the source address in the MAC table which allows it to identify precisely which interface the sending device can be reached through. Switch then floods this frame out all ports except the one that it was received on, given that the destination address is not found in the MAC table. If a destination device replies to the said flooded frame and sends a reply frame back, then the switch learns the source address from the reply frame and records source MAC address in its MAC table.

Alternatively, if the destination address is found in the MAC table then switch doesn't flood the frame out all its ports, it simply sends it out the interface associated with the destination address, as recorded in the MAC table.

Picture below shows how switches learn hosts' locations.



Port security

You can limit the number of MAC addresses that can be assigned dynamically to a port, set static MAC addresses, and set penalties when given policy is abused. This process is known as port security. There are three types of actions that a switch can take when port security is violated: shutdown, protect, restrict:

Shutdown mode shuts interface down and puts it into “err-disabled” state when configured policy is broken.

Protect mode simply drops the traffic received from MAC address that violates the policy.

Restrict mode takes same actions as protect mode but it also generates notification messages when a policy is broken.

Following commands can be used to allow maximum of one MAC address association with the interface and shutdown the interface in a case where the policy is broken:

```
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown
```

Sticky command can be used to automatically learn MAC addresses that are seen first on the interface, which can get rid of the burden of manually inputting each and every host's MAC address into the switch just to enforce a port security. In the example given below the first two MAC addresses coming into the port “stick” to the interface as static addresses and will be placed into the “running-config”, but when a third address tries to connect, the port will shut down:

```
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security violation shutdown
```

List of useful commands

`show mac address-table` - Shows entire content addressable memory (CAM) table.

`ip default-gateway ip_address` - Sets default gateway of a switch.

Chapter 7: VLANs

VLAN basics

VLAN is a logical grouping of hosts and network resources. When a VLAN is created, different ports of a switch can be assigned to different VLAN, in turn creating smaller broadcast domains. A VLAN is its own subnet and broadcast domain, and broadcast frames are only switched between the ports grouped within the same VLAN.

By default, nodes in the different VLANs can't communicate with each other. To implement InterVLAN communication, you need to use either a router to route between VLANs or a layer 3 switch that can act as a router.

Ways VLANs simplify network management:

- High level of security can be created for specific hosts by putting them into their own dedicated VLAN.
- Users can be logically grouped according to their function, without a regard to their physical location.
- Network changes are more simplified.
- VLANs can simplify network security.
- VLANs increase the number of broadcast domains and decrease their sizes.

There are two types of switch ports, access ports and trunk ports:

Access ports are ports that belongs to a single VLAN. They carry traffic for one VLAN only. Traffic is sent and received without any VLAN tagging information. Traffic arriving to access port is considered to belong to the VLAN that the same port is associated with. Devices that are attached to an access ports are not “aware” of their VLAN membership status, they just assume that they are part of some broadcast domain.

Voice access ports are ports that are supported by newer switches. Using voice access ports, a second VLAN can be associated with an access port, to make a way for easy traversal of the voice traffic. With voice access ports, user's PC and IP phone can be plugged into a single switch port.

Trunk ports carry traffic for multiple VLANs. They can carry traffic for VLANs 1 through 4094. Cisco devices make use of a proprietary protocol called Dynamic Trunk Protocol (DTP). DTP checks if switch is compatible with the connected switch, to be able to “agree on” a trunk port. If switches are compatible then trunk port will be configured automatically by default.

Configuring VLANs

Commands below can be used to create two different VLANs and also name them:

```
Switch(config)#vlan 2
Switch(config-vlan)#name Sales
Switch(config-vlan)#vlan 3
Switch(config-vlan)#name Marketing
```

Assigning switch ports to VLANs

Commands below can be used to associate FastEthernet 0/3 interface with VLAN 3:

```
Switch#config t
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
```

Configuring trunk ports

Commands below can be used to make the FastEthernet 0/15 interface a trunk port:

```
Switch(config)#int range f0/15
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
```

Defining the allowed VLANs on a trunk

Commands below can be used to allow only VLAN 4,6,12 and 15 through the trunk port.

```
Switch(config)#int f0/15
Switch(config-if)#switchport trunk allowed vlan 4,6,12,15
```

Modifying the trunk native VLAN

Following commands can be used to change native VLAN of a trunk port from default VLAN 1 to VLAN 4:

```
Switch(config)#int f0/15
Switch(config-if)#switchport trunk native vlan 4
```

VLAN Identification Methods

Switches use VLAN identification protocols to keep track of the frames and to determine where they belong. Two trunking protocols are given below:

Inter-Switch Link (ISL) tags VLAN information into the Ethernet frames. ISL encapsulates the entire frame to add in the VLAN information. It allows switch to identify VLAN membership status of any frame.

802.1q only inserts the VLAN field into frame instead of encapsulating whole frame, unlike ISL. 802.1q has to be used if trunking between Cisco switch and a switch of some different vendor.

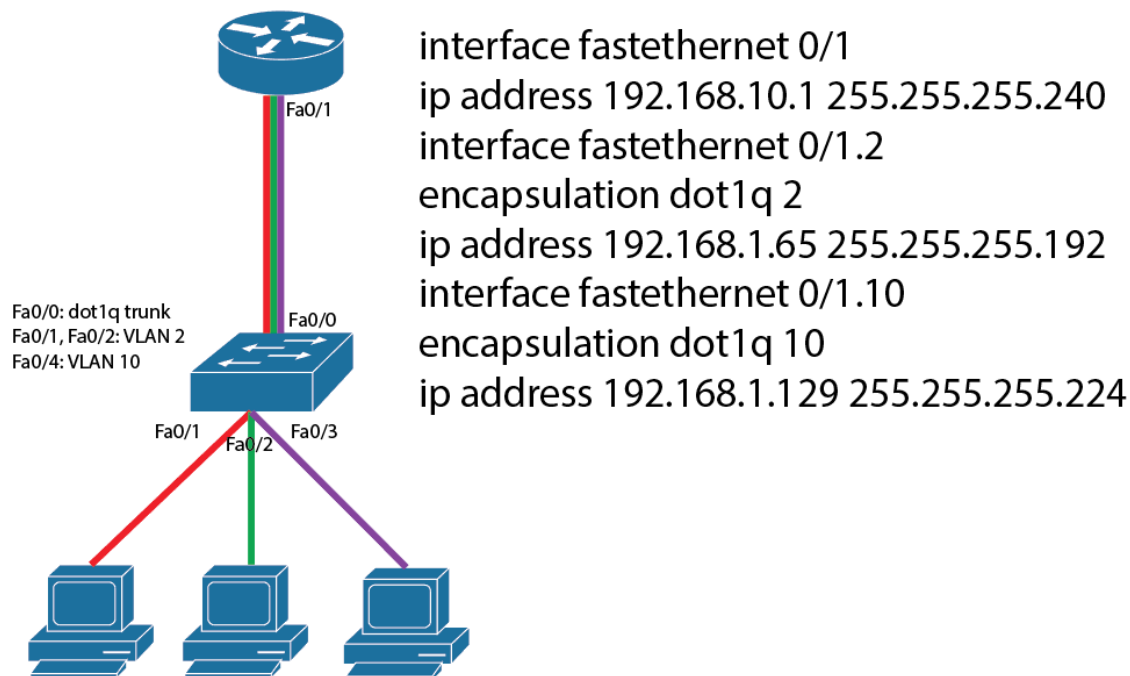
Configuring Inter-VLAN Routing

By default, only the nodes of the same VLANs can communicate. To allow InterVLAN communications, either a layer 3 switch or a router with router-on-a-stick configuration is required. To support ISL or 802.1q routing, router's interfaces have to be divided into logical interfaces – one for each VLAN. These are called “subinterfaces”.

These three things should be paid attention to when a router is being configured to act as a middle-point for InterVLAN communication:

- Router should be connected to the switch and the router must be configured with subinterfaces.
- Switch port connecting to the router must be a trunk port.
- Switch ports connecting to the hosts must be access ports.

Example of a router-on-a-stick configuration is shown below:



List of useful commands

`show vlan` – Displays VLANs and associated interfaces.

`show interfaces trunk` – Displays information about trunking interfaces.

`switchport mode access` – Puts interface into the access mode.

`switchport mode dynamic auto` – Interfaces with this command become trunk interfaces if the connected interface is set to trunk or desirable mode.

`switchport mode dynamic desirable` – Interfaces with this command actively attempt to form a trunk link. These interfaces become a trunk interface if the connected interface is set to trunk, desirable, or auto mode.

`switchport mode trunk` – Puts the interface into trunking mode.

`switchport nonegotiate` – Disables DTP on an interface.

Chapter 8: Security

Access lists

An access list is a list of conditions that categorize packets. Access lists are most commonly used to filter unwanted packets and for implementing security policies.

Packets follow three rules when being compared against an access list:

- The packet is compared with each line of the access list in sequential order.
- The packet is compared only until a match is found. Once a packet matches a condition, it is acted upon. Remaining lines are ignored.
- There is an implicit “deny” at the end of each access list. If a packet doesn't match any of the lines then it will match the implicit “deny”.

There are three types of access lists:

Standard access lists don't distinguish between protocols and make decisions based only on the source addresses. Destination address or packet type is not checked with standard access lists. With standard access lists, packet can be denied or permitted based only on its source address.

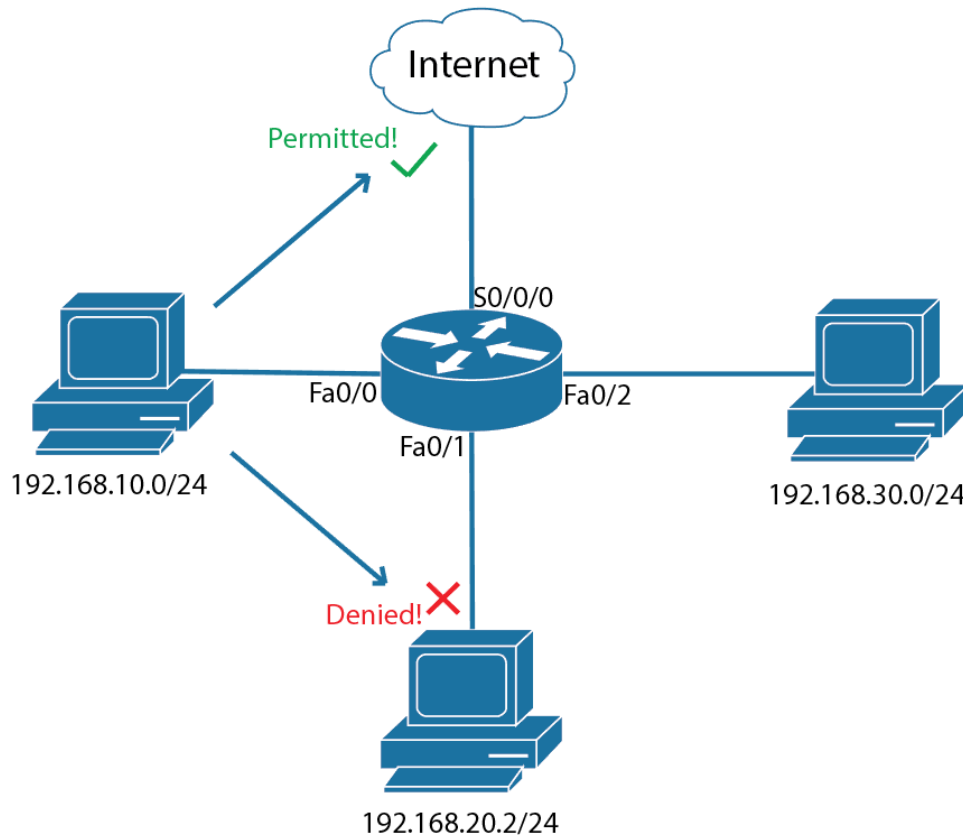
Extended access lists can evaluate many more fields of the packet than standard access lists. Extended access lists filter based on source address, destination address, protocol, and port number.

Named access lists are either standard access lists or extended lists, and are not a distinct type. They are functionally same with standard or extended access lists but only difference is the fact that an alphanumeric name can be given to them.

Access lists usually don't do anything after their initial creation, unless they are “applied”. For packet filtering, access lists must be applied to an interface. When access list is being applied, the direction of application has to be specified. When an access list is applied as “inbound”, packets are filtered when they are received on an interface. When an access list is applied as “outbound”, packets are filtered when they are being sent out of an interface.

Standard access lists

Standard access lists filter the traffic based on a source address only. Standard access list can be created by giving it a number identifier between 1 and 99 or a number in the expanded range of 1300–1999.



If you want to allow 192.168.10.0 network an access to the Internet but not allow access to the 192.168.20.2 host, you need to create a standard access list and apply it to the Fa0/1 interface of the router as an outbound access list. Here's how it's done:

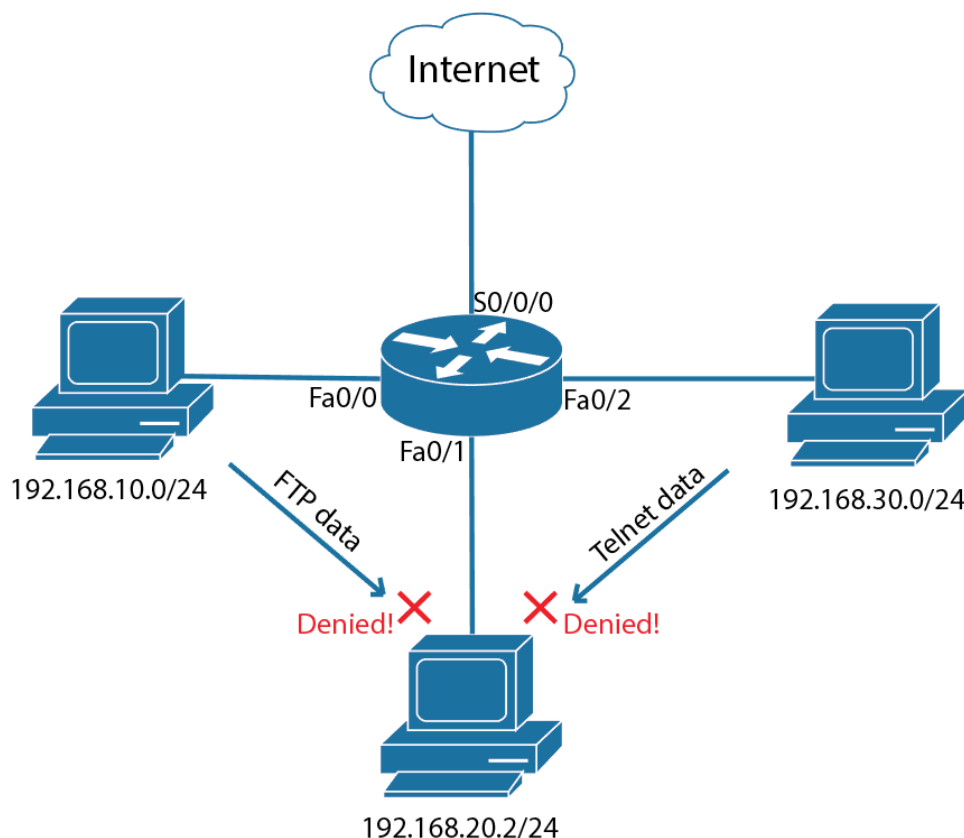
```
Router(config)#access-list 10 deny host 192.168.10.0 0.0.0.255
Router(config)#access-list 10 permit any
Router(config)#interface fastEthernet 0/1
Router(config-if)#access-group 10 out
```

0.0.0.255 at the end of the access-list command is a wildcard mask. They can be called an inverse subnet masks. Wildcard masks indicate which parts of an IP address is available for examination. 0s in first three octets means that three first octets of IP address has to match exactly "192.168.10.", 255 in the last octet means that the last octet of an IP address can be anything from 0 to 255.

"permit any" was used as the last line of the access list to permit other traffic to pass through. If said line wasn't configured then all other traffic would match the implicit deny at the end of the access list and get discarded.

Extended access lists

Extended access lists can filter traffic based on a source address, a destination address, a protocol and a port number. Extended access lists' number range is from 100 to 199 and expanded range of extended access lists are 2000-2699.



In the situation above, we had to deny FTP traffic from 192.168.10.0/24 network to 192.168.20.2 node and also deny Telnet traffic from 192.168.30.0/24 network to the 192.168.20.2 node. Here's how it was done:

```
Router(config)#access-list 110 deny tcp 192.168.10.0 0.0.0.255
192.168.20.2 0.0.0.0 eq 21
Router(config)#access-list 110 deny tcp 192.168.30.0 0.0.0.255
192.168.20.2 0.0.0.0 eq 23
Router(config)#access-list 110 permit ip any any
Router(config)#interface fastEthernet 0/1
Router(config-if)#access-group 10 out
```

Named access lists

Named ACLs are no different than standard or extended ACLs except for the fact that you can give them a name. Here's how you can create a named standard access list and give it a name of "MyACL":

```
Router(config)#ip access-list standard MyACL
```

Using access lists for filtering traffic to VTY

Access lists can be applied to a VTY line to filter Telnet and SSH traffic. These commands show how one can permit only the host of 192.168.10.5 to pass through and get everything else denied:

```
Router(config)#access-list 30 permit host 192.168.10.5
Router(config)#line vty 0 4
Router(config-line)#access-class 30 in
```


List of useful commands

`show access-list` - Displays all configured access lists and their parameters. Also displays some statistics, such as number of times a line has been “matched”.

`show ip interface` - Displays interface information along with information about the applied access lists.

`log` - Is used at the end of the access-list command and generates console messages as the packets match the said access list line.

Chapter 9: NAT

Network Address Translation (NAT)

NAT is usually used for assigning public IP addresses to local hosts. There are three types of NAT: **Static NAT** is for one-to-one mapping between local and global addresses. One global Internet address is needed for each private host when using static NAT.

Dynamic NAT allows one to map a private IP address to a global IP address from a pool of registered IP addresses. You don't have to statically configure mappings when using dynamic NAT.

PAT (Port Address Translation) or overloading is the most commonly-used type of NAT today. PAT is a type of dynamic NAT that allows multiple private hosts to use a single global address to access the Internet. Traffic is separated using unique port numbers for each connection.

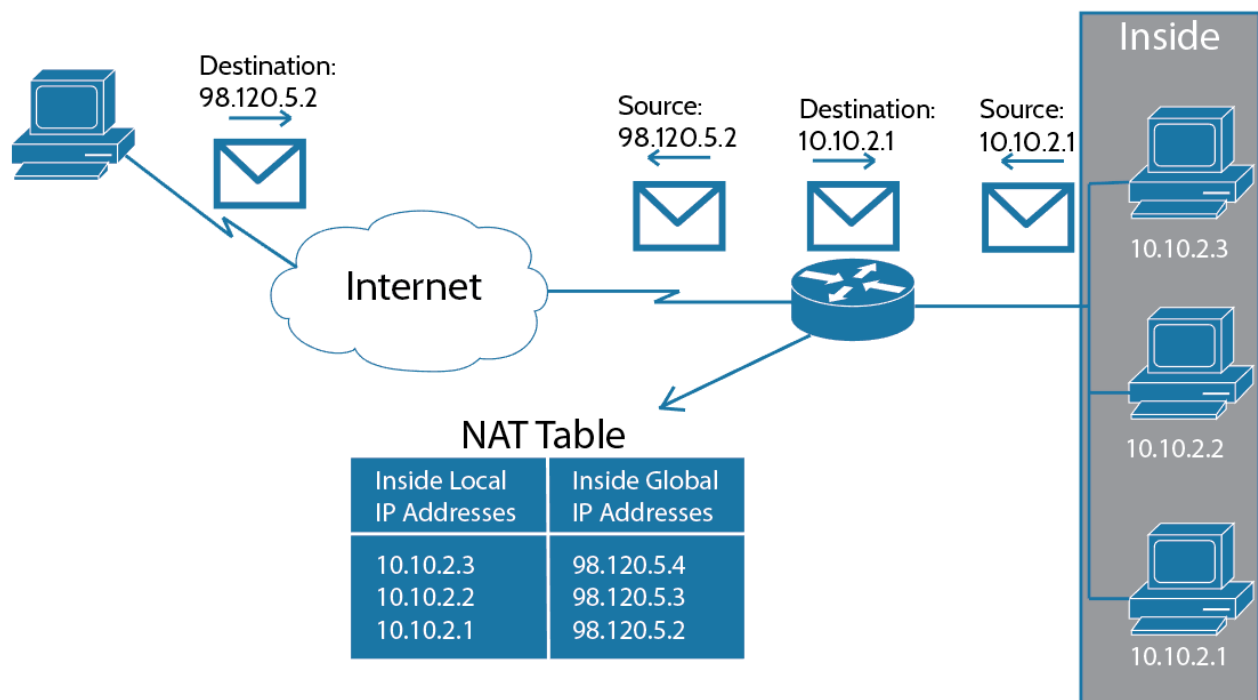
NAT configuration

Static NAT and PAT configurations are given below:

Static NAT configuration

Commands below can be used to configure static NAT:

```
Router(config)#ip nat inside source static 10.10.2.3 98.120.5.4
Router(config)#ip nat inside source static 10.10.2.2 98.120.5.3
Router(config)#ip nat inside source static 10.10.2.1 98.120.5.2
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#interface Serial 0/1
Router(config-if)#ip nat outside
```



Dynamic NAT configuration

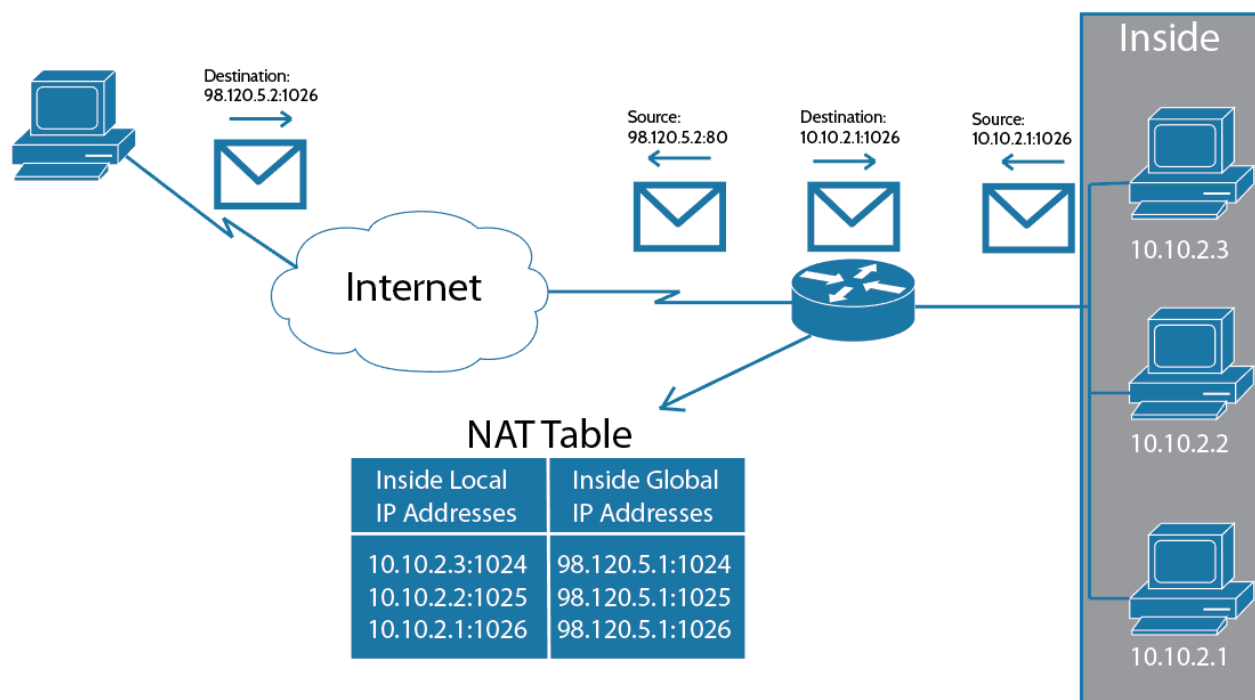
Commands below can be used to configure dynamic NAT:

```
Router(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)#ip nat pool pool_name 170.168.2.3 170.168.2.254
netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool pool_name
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#interface Serial 0/1
Router(config-if)#ip nat outside
```

PAT configuration

Commands below can be used to configure PAT:

```
Router(config)#access-list 1 permit 10.10.2.0 0.0.0.255
Router(config)#ip nat pool pool_name 98.120.5.1 98.120.5.1 netmask
255.255.255.0
Router(config)#ip nat inside source list 1 pool pool_name overload
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#interface Serial 0/1
Router(config-if)#ip nat outside
```



List of useful commands

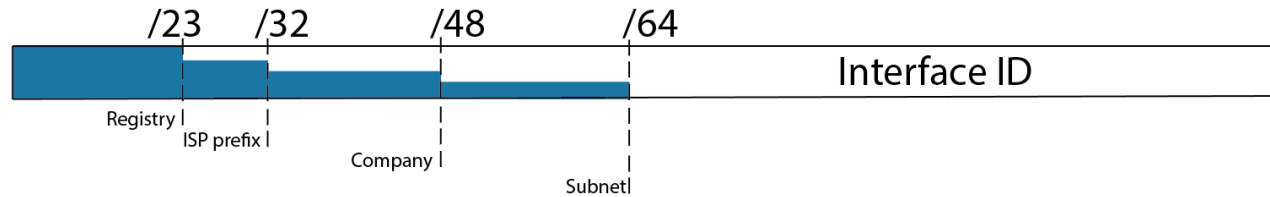
show ip nat translations - Is used to verify NAT translations on a router. Displays list of all current IP translations.

debug ip nat - Displays detailed debug messages regarding NAT.

Chapter 10: IPv6

IPv6 basics

Main advantage of IPv6 over IPv4 is the fact that it has a lot of addresses (3.4×10^{38}) available, compared to IPv4's 4.3 billion addresses. IPv6 has host of new features as well. IPv6s are 128 bits long.



Shortened expression

There are two ways of shortening IPv6 addresses:

1. Any leading zeros in each of the individual blocks can be dropped.
2. Whole section of all 0s can be replaced with a double colon. Only one contiguous block of 0s can be replaced with a double colon.

Example: 2001:0db8:0000:000b:0000:0000:0000:001A is same as 2001:db8:0:b::1A.

Address types

IPv6 standard specifies three address types:

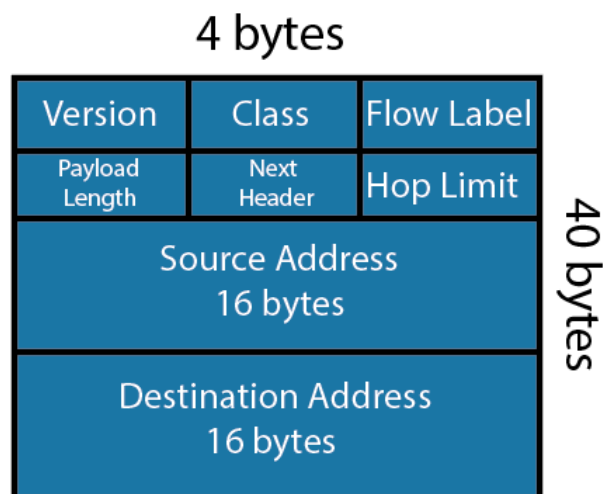
Unicast packets are sent to a single host.

Multicast packets are sent from one node to a group of nodes. Also called one-to-many.

Anycast is also called one-to-any. Anycast packets are sent to the nearest host with the destination IP address. Many nodes can share a same address and each can receive anycast packets from nearest clients.

Header

IPv6 header is shorter and much more efficient than IPv4 header. Diagram of IPv6 header is as follow:



Special addresses

List of special addresses are given below:

0:0:0:0:0:0:0:0 or simply "::" is the equivalent of IPv4's 0.0.0.0 and is typically the source address of a host before the host receives an IP address from a DHCP server.

0:0:0:0:0:0:0:1 or simply "::1" is the equivalent of 127.0.0.1.

0:0:0:0:0:0:192.168.100.1 is how an IPv4 address is shown in a mixed IPv6/IPv4 network.

2000::/3 is the global unicast address range.

FC00::/7 is the unique local unicast range.

FE80::/10 is the link-local unicast range.

FF00::/8 is the multicast range.

3FFF:FFFF::/32 is reserved for examples and documentation.

2001:0DB8::/32 is also reserved for examples and documentation.

2002::/16 is used with 6-to-4 tunneling, which is an IPv4-to-IPv6 transitioning system. The structure allows IPv6 packets to be transmitted over an IPv4 network without a need for configuration of explicit tunnels.

Address assignment

Generally there are three ways of assigning IPv6 addresses to the interfaces:

Manual address assignment: `Router(config-if)#ipv6 address ip_address`

Stateless autoconfiguration (EUI-64) uses device's MAC address to assign an IPv6 address to an interface. Interface ID in an IPv6 address is 64 bits and a MAC address is only 48 bits. Therefore 16 bits, "FFFE" is added in the middle of a MAC address to make up a 64 bit interface ID. For example, let's say that you have a device with a MAC address of 0020:a623:1127. After it gets padded with EUI64, it looks like this: 0020:a6FF:FE23:1127.

DHCPv6 (stateful autoconfiguration) offers DNS server, domain name, and some other options that stateless autoconfiguration doesn't. Client gets IPv6 address from a DHCP by sending out a DHCP solicit message, which is a multicast message with a destination address of FF02::1:2.

IPv6 protocols

Neighbor Discovery (NDP), ARP has been renamed to NDP in IPv6. Function of the NDP remains the same.

OSPFv3, IPv6 version of OSPF is called OSPFv3. All functions of OSPF remain the same, including the 32 bit router ID. A Router ID has to be manually assigned to the router because IPv6 addresses are 128 bits long and can't be used as Router ID. Here's an example of assigning a Router ID of "10.10.10.10" to the OSPF process:

```
Router(config)#ipv6 router ospf 10
```

```
Router(config-rtr)#router-id 10.10.10.10
```

Another thing that changed is the fact that you can't use network command to enable OSPF process on interfaces anymore. You have to enable interfaces into the OSPF process by using the following command under the relevant interface configuration mode:

```
Router(config-if)#ipv6 ospf 10 area 0
```

(This command sets interface to OSPF area "0" under the process ID of "10")

List of useful commands

`Router(config)#ipv6 unicast-routing` - Turns on IPv6 features of a router.

`Router#ping ipv6 ip_address` - Pings specified IPv6 address.

`Router#show ipv6 interface brief` - Displays brief information about interfaces and IPv6 configurations associated with them.

`Router#show ipv6 route` - Displays IPv6 routing table.

`Router#show ipv6 protocols` - Displays layer 1, layer 2, and IPv6 information of the interfaces.