***Day 31: Network Models, Devices and Components***

OSI and TCP/IP Models

OSI:

7 - Application

6 - Presentation

5 - Session

4 - Transport

3 - Network

2 - Data Link

1 - Physical

TCP/IP Model:

7 - Application

6 - Application

5 - Application

4 - Transport

3 - Internet

2 - Network Access

1 - Network Access

Osi Model = layers

TCP/IP model - Protocols

Application - interfaces between network and app software, including authentication services

Presentation - Defines format and organisation of data, including encryption

Session - establishes and maintains end-to-end bidirectional flows between endpoints, including managing transaction flows

Transport - services between host computers, including connection, establishment and termination, flow control, error recovery and segmentation

Network - logical addressing, routing and path determination

Data link - formats data into frames appropriate for transmission onto some physical medium. Defines rules . Defines ways to recognise transmission errors.

Physical - physical components like cables

TCP/IP Layers and protocols:

| **TCP/IP Layer** | **Function** | **Example Protocols** |
| --- | --- | --- |
| Application | Represents data to user and controls dialogue | DNS, Telnet, SMTP, POP3, IMAP, DHCP, HTTP, FTP, SNMP |
| Transport | Supports comms between diverse devices across networks | TCP, UDP |
| Internet | Determines best path through network | ICMP, ARP, IP |
| Network Access | Controls hardware devices and media that make up the network | Ethernet, Wireless |

PDUs at each layer of the OSI model:

| **OSI Layer** | **PDU** |
| --- | --- |
| Application | Data |
| Presentation | Data |
| Session | Data |
| Transport | Segment |
| Network | Packet |
| Data Link | Frame |
| Physical | Bits |

TCP/IP Transport Layer features:

| **function** | **Description** |
| --- | --- |
| Multiplexing using ports | Enables receiving hosts to choose correct app for which data is destined based on port number |
| Error recovery (reliability) | Numbering and acknowledging data with sequence and acknowledgement header fields |
| Flow control using windowing | Sliding windows size that two end devices dynamically agree upon at various points during connection. Size is represented in bites. Max amount of data the source will send before receiving an acknowledgment from dest. |
| Connection establishment and termination | Process used to initialise port numbers and sequence and acknowledgement fields |
| Ordered data transfer and data segmentation | Continuous stream of bytes that is segmented for transmission and delivered in order |

TCP Header:

Sequence Number portion (32 bits):

Source port - 16 bits

Destination Port - 16 bits

Acknowledgement number - 32 bits

Header length - 4 bits

Reserved - 6 bits

Code bits - 6 bits

Window - 16 bits

Checksum - 16 bits

Urgent - 16 bits

Options - 0 or 32 bits

Data - varies

Port numbers:

FTP data - 20 - TCP

FTP control - 21 - TCP

SSH - 22 - TCP

Telnet - 23 - TCP

SMTP - 25 - TCP

HTTP - 80 - TCP

POP3 - 110 - TCP

HTTPS - 443 - TCP

DHCP - 67, 68 - UDP

TFTP - 69 - UDP

SNMP - 161 - UDP

DNS - 53 - UDP/TCP

TCP acknowledgement with Errors:

2000 = never got segment with sequence number, resend it

TCP connection establishment:

SYN (seq 200) → SYN ACK (seq 1450, 201) → ACK (seq 201, 1451)

TCP and UDP headers:

TCP:

| 2 | 2 | 4 | 4 | 4 | 6 | 6 | 2 | 2 | 2 | 3 | 1 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Source port | Dest. port | Seq. number | Ack number | offset | reserved | flags | Window size | checksum | urgent | options | PAD |

UDP:

| 2 | 2 | 2 | 2 |
| --- | --- | --- | --- |
| Source port | Dest. port | length | checksum |

Ethernet cables:

Single mode goes up to 2km long and 10gbps speed

Multimode goes to 550 metres at 10gbps

10base is slowest, then 100base, then 1000base, then 10Gbase

Physical Topologies:

Ring

Point to point

Star

Mesh

Partial mesh

Bus

Extended star

Hierarchical Campus Design:

Access Layer - local and remote user access

Distribution Layer - controls flow of data between access and core layers

Core layer - Acts as high speed redundant back bones

***Day 31: Ethernet Switching***

STANDARD FOR ETHERNET = 802.3

Logical Link Control (LLC) = 802.2

Media Access Control (MAC) = 802.3

MAC sublayer:

Data encapsulation, Media Access Control

Organisationally Unique identifier (OUI):

24 bits, 6 hex digits, e.g. 00 60 2F

Broadcast address value: FFFF.FFFF.FFFF

Ethernet Frame:

| Preamble (7) | SFD (1) | Destination (6) | Source 96) | Length (2) | Data (46 - 1500) | FCS (4) |
| --- | --- | --- | --- | --- | --- | --- |

Preamble - synchronisation

SFD (Start Frame Delimeter) - next byte begins destination MAC field

Dest MAC - recipient of frame

Source MAC - sender of frame

Length - length of data field of frame

Type - type of protocol listed inside frame

Data - holds data from higher layer, typically, layer 3 PDU and IP packert

FCS (Frame check sequence) - method for receiving NIC to determine whether frame experienced transmission errors

Ethernet types:

Ethernet - 10mbps - 10BASE T - 802.3 - 100m

Fast Ethernet - 100mbps - 100BASE TX - 802.3u - 100m

Gigabit ethernet - 1000mbps - 1000BASE LX - 802.3z (fibre), ab (copper) - 550m, 100m

10GigE - 10gbps - 10GBASE T - 802.3ae (fibre), an (copper), 400m, 100m

***Day 29: Switch Configuration Basics***

Cisco device Configuration:

Console terminal - RJ45 rollover cable or Mini USB cable and console port

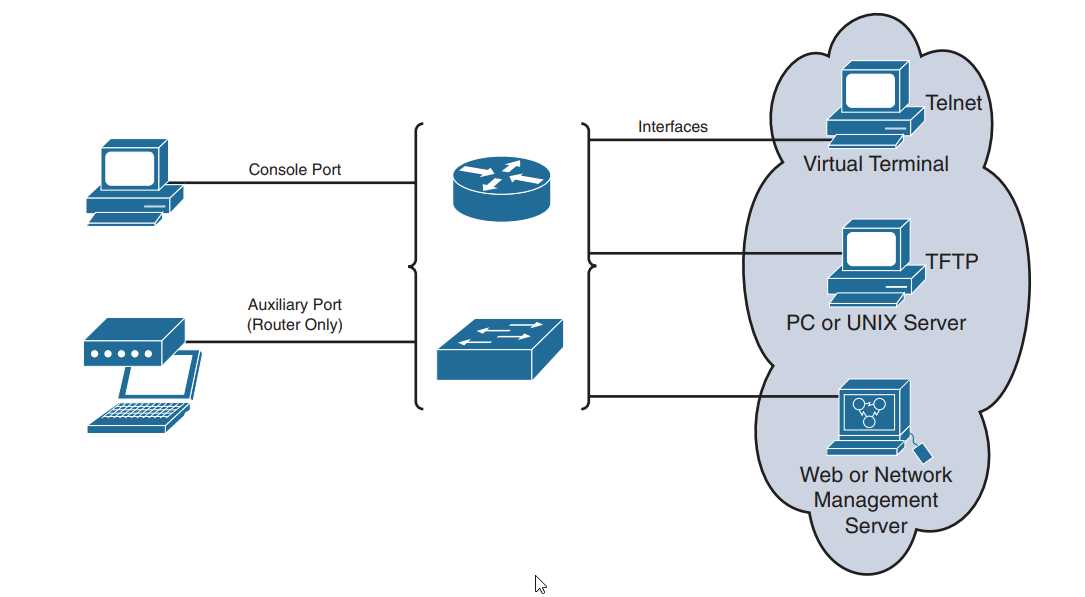
Remoter terminal - external modem

Cisco device access:

Establish a terminal (vty) session using telnet

Configure through current connection

Download config file



CLI Exec sessions:

User EXEC mode - access to limited number of basic monitoring and troubleshooting commands

Privileged EXEC mode - full access to all device commands including config and management

Saving locations:

RAM - internetwork operating system - programs/active config file/tables and buffers

NVRAM - backup config file

Flash - operating systems

RAM command - show running-config

NVRAM command - show startup-config

Half Duplex = unidirectional data flow, device either sends OR receives

Full Duplex = both ends of connection can send AND receive data at the same time (known as bidirectional)

Auto-MDIX (Automatic medium-dependent interface crossover):

* Interface automatically detects required cable connection time

Ways to verify network connectivity:

Can the device ping itself?

Can the device ping its default gateway?

Can the device ping the destination?

LAN switch interface status codes:

**Line status: Protocol Status: Interface status: typical root cause:**

Administratively down disabled shutdown command

Down

Down down notconnect no cable exists

Up down notconnect L2 problem on L3 switch

Down down (err-dis) err-dis port security disabled

Up up connect interface working

Duplex and Speed Mismatches:

Full duplex will experience CRC errors if a mismatch

***Day 28: IPv4 Addressing***

Consist of 32 bits

Network ID - left to right, class A = 8 bits (1 octet), class B = 16 bits (2 octets), class C = 24 bits ( 3 octets)

Host ID = right to left, amount of bits determined after network + borrowed bits worked out

IPv4 Header:

Component (bits)

Version (4)

Header length (4)

Priority and type of service (8)

Identification (16)

Flags (3)

Fragment offset (13)

Time to live (8)

Protocol (8)

Header checksum (16)

Source ip address (32)

Destination ip address (32)

Ip options (0 - 32)

Data (varies)

Subnet masks

1 or 0 to represent a bit

Bit: 1 1 1 1 1 1 1 1

Value: 128 64 32 16 8 4 2 1

Bit number: 8 7 6 5 4 3 2 1

Subnet val: 128 192 224 240 248 252 254 255

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

| **Mask (decimal)** | **Mask (binary)** | **Network bits** | **Host bits** |
| --- | --- | --- | --- |
| 0 | 00000000 | 0 | 8 |
| 128 | 10000000 | 1 | 7 |
| 192 | 11000000 | 2 | 6 |
| 224 | 11100000 | 3 | 5 |
| 240 | 11110000 | 4 | 4 |
| 248 | 11111000 | 5 | 3 |
| 252 | 11111100 | 6 | 2 |
| 254 | 11111110 | 7 | 1 |
| 255 | 11111111 | 8 | 0 |

Private IP addresses:

Class A = 10.0.0.0 - 10.255.255.255

Class B = 172.16.0.0 - 172.31.255.255

Class C = 192.168.0.0 - 192.168.255.255

***Day 27: IPv6 Addressing***

More simple header than IPv4 addresses - better routing efficiency and no broadcast storms!

Also, no check sums!

IPv6 addresses have IPSec enabled on every IPv6 node

IPV6 - 16 octets

IPv6 header:

Attribute (bits)

Version (4)

Traffic Class (8)

Flow Label (20)

Payload length (16)

Next header (8)

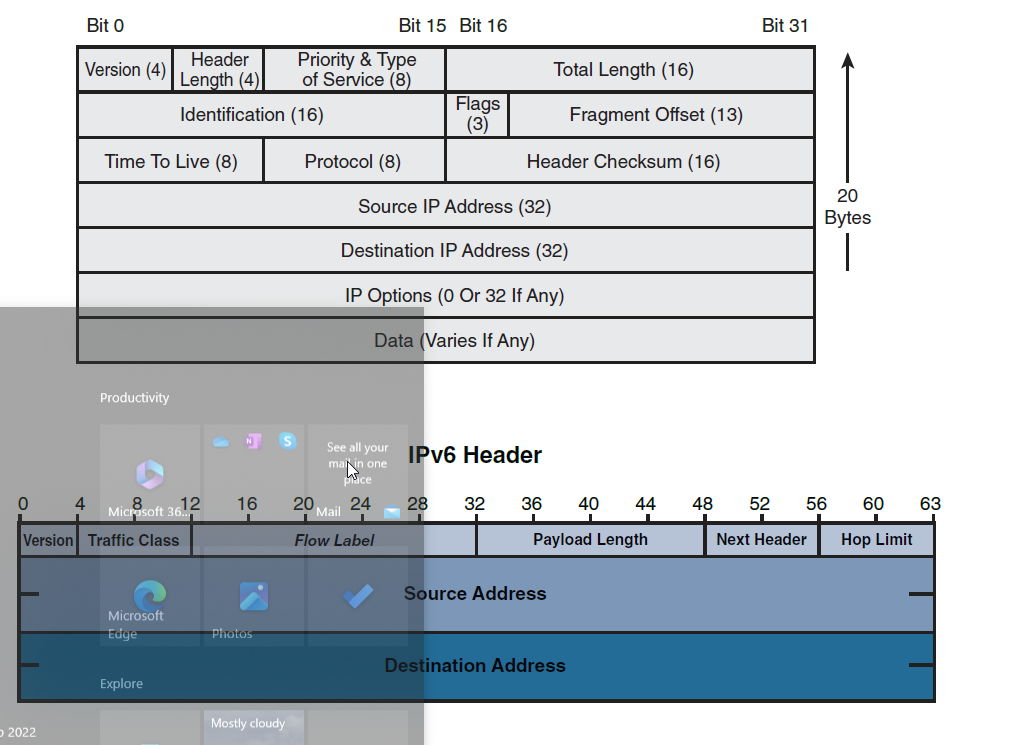
Hop limit (7)

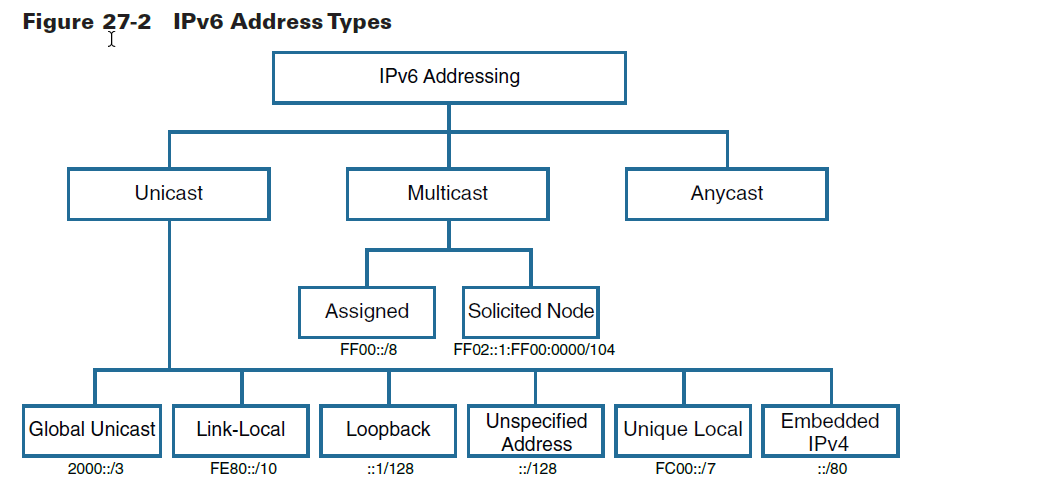
Source address (62/3)

Destination address (62/3)

3 types of IPv4 addresses - unciast, multicast, broadcast

2 types of IPv6 addresses - unicast, multicast





Unicast addresses:

Uniquely identifies an interface on a IPv6 device

Packet sent to unicast address and is received by interface that the address is assigned to

Global Unicast addresses:

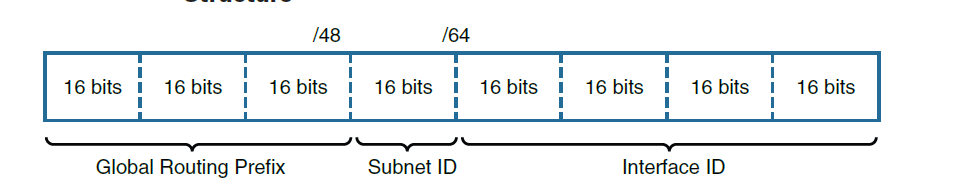
Globally unique

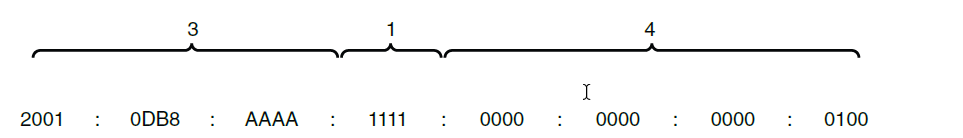
Routed to internet without modification

48 bit global routing prefix

16 bit subnet ID

64 bit interface ID





Global unicast configuration:

Manual - static, eui-64, IPv6 unnumbered

Static - statically configured on interface

EUI-64 - prefix configured normally, eui-64 process uses MAC addresses to generate interface ID (64 bits)

IPv6 unnumbered - interface configured to use the MAC address of another interface on same device

Dynamic - stateless address autoconfig (SLAAC), DHCPv6

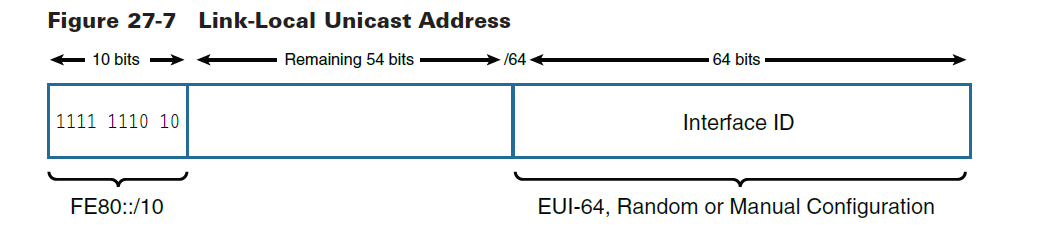
SLAAC - determined prefix and prefix length from neighbour discovery router advertisement messages and creatures interface ID using EUI-64 method

DHCPv6 - device receives some or all of its addressing from DHCPv6 server

Link-Local address:

Configured dynamically by EUI-64, randomly with generated interface ID, statically entering address

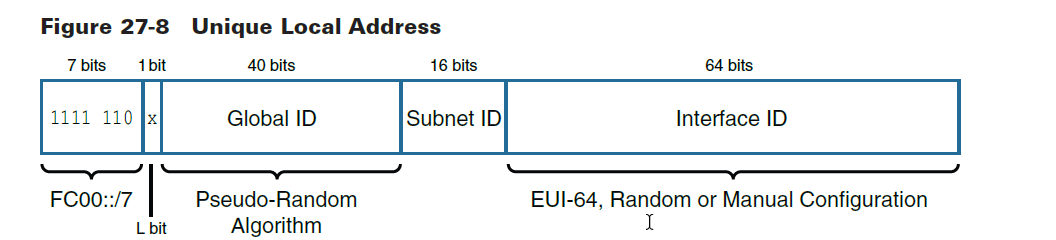
They are confined to single link, must be unique



Loopback address:

Sends IPv6 packet to itself as a tester

Unique local address:



Private addresses

Can be used just like global unicast address

Globally unique prefix, high probability anyway

IPv4 and IPv6 packets not compatible - NAT64 required to translate

Multicast addresses:

Device sends single packet to multiple destinations simultaneously

Two types - assigned multicast, solicited-node multicast

Assigned multicast:

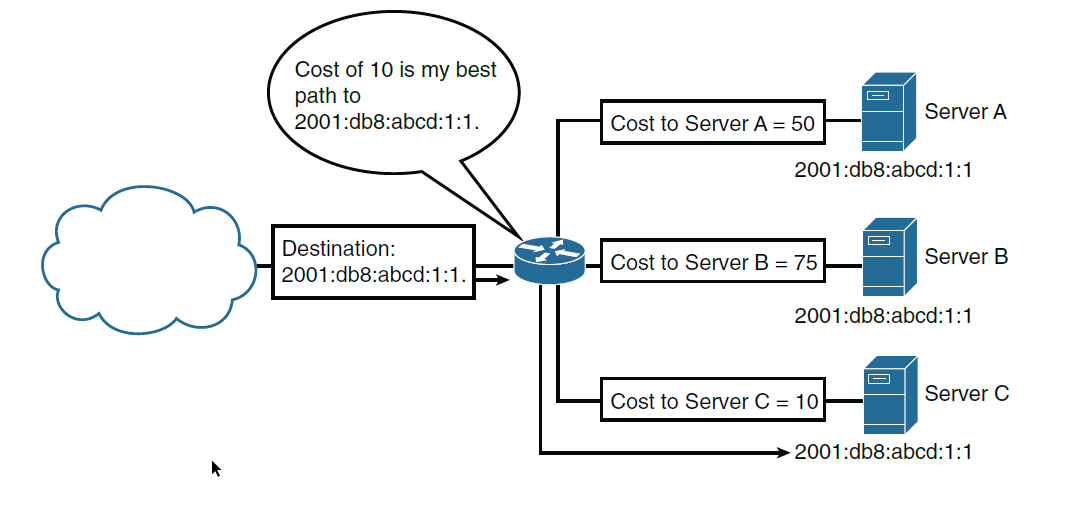
Specific protocols

All nodes multicast group

All routers multicast group

Anycast addresses:

Can be assigned to more than one device

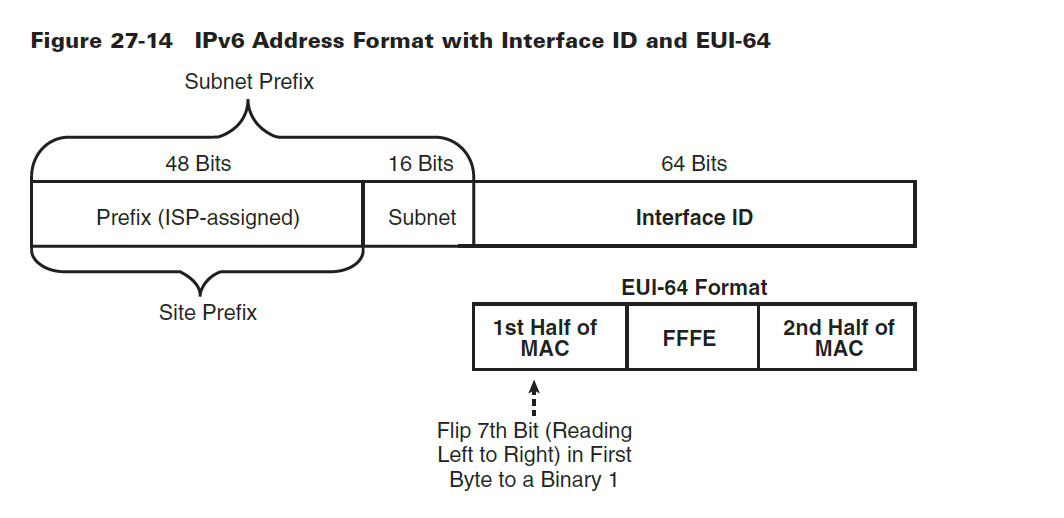


Rules for writing IPv6 addresses:

Omit leading 0s in any hextet

Omit any hextets that are only 0s and represent with ::

To know which prefix an ipv6 address resides in, look at the first 4 hextets



Two methods to migrate to ipv6:

Dual-stacking - node has connection to both ipv4 and ipv6

Tunnelling - transports ipv6 packets over ipv4 network by encapsulating the ipv6 packet inside ipv4

“Dual stack where you can, tunnel where you must!”

***Day 26: VLAN a Trunking Concepts and Configurations***

What are vlans for?

Grouping users by department instead of physical location

Segmenting devices into smaller LANs

Reducing workload of STP

Enforcing better security

Separating IP voice traffic from data traffic

Assisting troubleshooting by reducing size of failure domain

Benefits:

Cost reduction

Security

Higher performance  
Broadcast storm mitigation

Ease of management and troubleshooting

Default VLAN:

All ports on a switch are members of default VLAN when the switch is reset

This is VLAN 1

You cannot rename or delete this

Data VLAN:

Configured to carry only user-generated traffic

Ensures voice and management traffic are separated from data traffic

Native VLAN:

Common identifier on opposing ends of a trunk

Not used for any traffic in switched network unless legacy bridging devices present

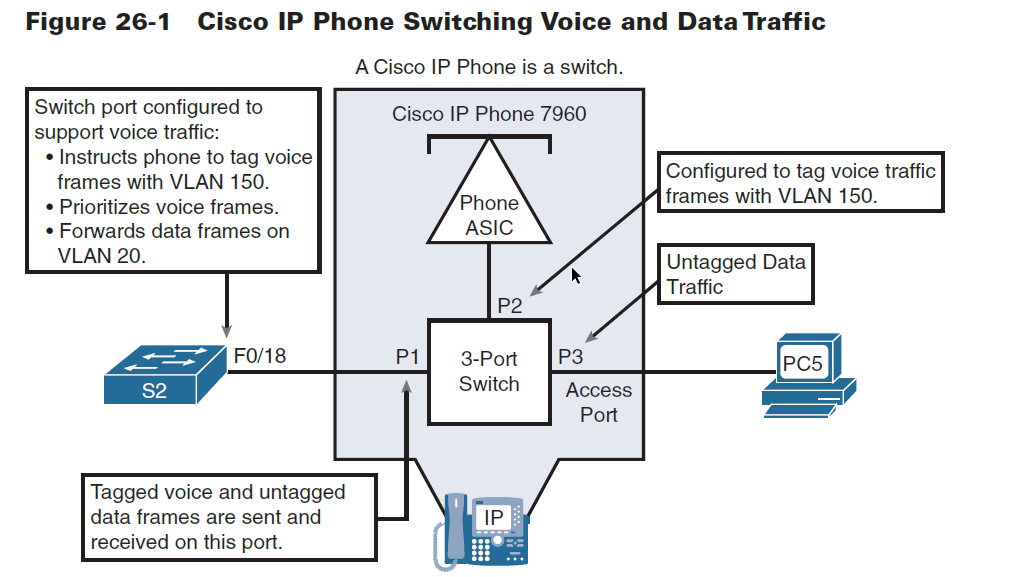
Management VLAN:

Access management capabilities of switch

By default, VLAN 1

Voice VLAN:

Enables switch ports to carry IP voice traffic from an IP phone



Trunking VLANs:

Vlan trunk is an ethernet point-to-point link between an ethernet switch interface and an ethernet interface on another networking device

Carries traffic of multiple VLANs over a single link

Enables you to extend the VLANs across an entire network

When a frame is placed on a trunk link, info about the VLAN it belongs to must be added to frame by using IEEE 802.1Q frame tagging

802.1Q tags are inserted in an Ethernet Frame

The VLAN tag field:

Consists of 16-bits -

3 bits of user priority - expedited transmission of L2 frames such as voice traffic

1 bit of Canonical Format identifier (CFI) - enables token ring frames to be easily carries across Ethernet links

12 bits of VLAN ID (VID) - provides VLAN identification numbers

Dynamic Trunking Protocol:

DTP - cisco proprietary protocol - negotiates status of trunk ports and the trunk encapsulation of trunk ports

Switches must be configured in a mode that supports DTP:

Switchport mode trunk command = switchport periodically sends DTP messages to remote port, advertising unconditional trunk state

Switchport mode trunk dynamic auto = switch port advertises to remote switch port that it is able to trunk but does not request to go into trunking state

Switchport mode dynamic desirable = switch port advertises to remote switchport that it can trunk and asks remote switch to go into trunking state

Switchport nonegotiate = local port is considered to be in unconditional turning state

Trunk negotiation results between a local port and remote port:

|  | **Dynamic auto** | **Dynamic desirable** | **trunk** | **access** |
| --- | --- | --- | --- | --- |
| **Dynamic auto** | access | trunk | trunk | access |
| **Dynamic desirable** | trunk | trunk | trunk | access |
| **trunk** | trunk | trunk | trunk | Not applicable |
| **access** | access | access | Not applicable | access |

VLAN commands:

Show vlan -

Show vlan brief - lists each VLAN and all interfaces assigned to that VLAN (not operational trunks)

Show vlan id <num> - lists both access and trunk ports in VLAN

Show Interfaces switchport -

show interfaces <number> switchport - identifies interface’s access VLAN and voice VLAN, the c configured operation mode (access or trunk) and the state of the ports (up or down)

Show mac address-table - lists MAC table entries including associated VLAN

Show interface status - summarises status listing for all interfaces, VLAN, Duplex, speed, type of port

***Day 25: STP***

STP benefits:

Stop broadcast storms

Prevents Multiple-frame transmission

Solves MAC database instability

General topology:

Access layer

Distribution layer

Core

Distribution layer

Access Layer

Process for STP convergence:

Elect root bridge - switch with lowest bridge ID, all ports are forwarding ports

Elect root port for each nonroot switch - lowest root path cost

Elect designated port for each segment - lowest root path cost on each link

Root ports and designated ports transition to forwarding state, other ports are blocking state

Default IEEE Port Costs:

Eth speed original IEEE cost Revised IEEE cost

10mbps 100 100

100mbps 10 19

1gbps 1 4

10gbps 1 2

Listening and Learning delay = 15 seconds

Loss of BPDU detached = 20 seconds

Rapid PVST = faster version of STP

MSTP = Multi spanning tree protocol allows multiple STP instances (up to 16)

Stp = 802.1D - low resources - slow convergence - all VLANs

RapidSTP = 802.1w, medium resources, fast convergence, all vlans

PVST = cisco prop, high resources, slow convergence, per vlan

rapidPVST+ = cisco, very high resources, fast convergence, per vlan

MSTP = 802.1s, cisco, medium or high resources, fast, per instance

PVST port states:

| **Operation allowed** | **blocking** | **listening** | **learning** | **forwarding** | **disabled** |
| --- | --- | --- | --- | --- | --- |
| Can receive and process BPDUs | yes | yes | yes | yes | no |
| Can forward data frames from same interface | no | no | no | yes | no |
| Can forward data frames from another interface | no | no | no | yes | no |
| Can learn MAC addresses | no | no | yes | yes | no |

A bridge ID = 8 bits

An extended system ID = 12 bits

MAc address = 48 bits

RSTP Interface behaviour:

Edge-type behaviour and portfast = improved convergence for edge-type connections by immediately placing the port in forwarding state when link physically active

Link type point to point = rstp recognises lost paths to roots much more quickly

| **Operational state** | **Stp state (802.1D)** | **RSTP state (802.1w)** | **Forwards data frames in this state?** |
| --- | --- | --- | --- |
| enabled | blocking | discarding | no |
| enabled | listening | discarding | no |
| enabled | learning | learning | no |
| enabled | forwarding | forwarding | yes |
| disabled | disabled | discarding | no |

RSTP removes the need for listening stated and reduces time required for learning by actively discovering the networks new state.

STP passively waits on new BPDUs and reacts to them during listening and learning states

***Day 24: EtherChannel and HSRP***

All interfaces within an EtherChannel muist have the same configuration of speed for the duplex mode, and allowed VLANs on trunks, and access VLAN on access ports

Assign all ports in etherchannel to same VLAN or configure them as trunks.

Ports with different native VLANS cannot form an EtherChannel

First Hop Redundancy Protocols:

FHRP method when active router fails:

Standby router stops seeing hello messages from forwarding router

It then assumes role of forwarding router

Both IP and MAC address of virtual router assumed by this router, end stations do not recognise the disruption

Types of FHRPs:

HSRP (Hot standby router protocol) - cisco prop, standby router monitors operation status of HSRP group

Virtual router redundancy Protocol (VRRP) - IETF standard, dynamically assigns responsibility for one or more virtual routers to VRRP routers

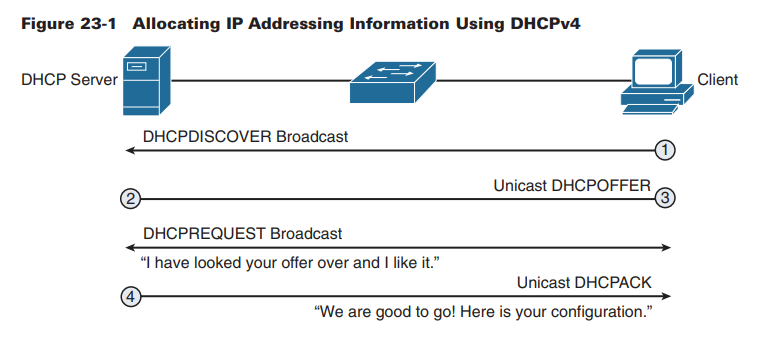
Gateway Load Balancing Protocol (GLBP) - cisco prop

***Day 23: DHCP and DNS***

DHCP4:

Allows a host to obtain an IP address dynamically when connecting to network

Chooses an address from a configured range of addresses called a POOL and assigns the IP for a set period



Notes:

DHCP discover message = broadcast

DHCP offer message = unicast

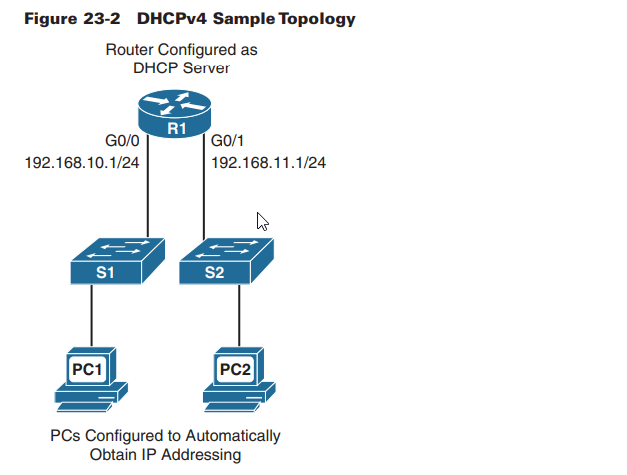
DHCP request message = Broadcast

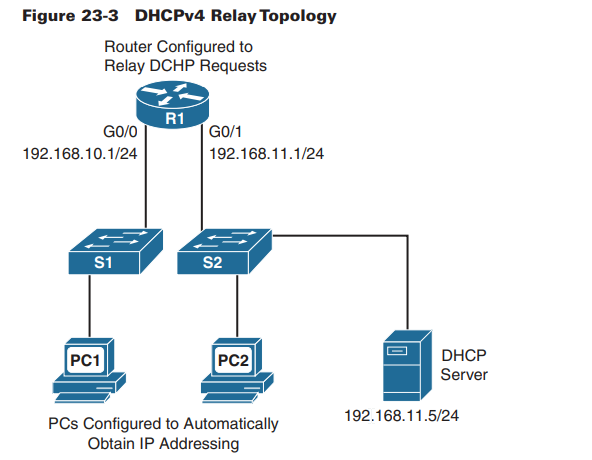
DHCP Pack message = unicast

DHCP configuration options:

Dhcp server

Dhcp relay agent





Stateless vs. stateful DHCPv6:

Stateless = client uses RA message from router to generate global unicast address. Client then sends request to DHCPv6 server to obtain more info

Stateful = RA message tells client to obtain all its addressing info from a DHCPv6 server

***Day 22: Wireless Concepts***

IEEE 802.11 WLAN

2.4ghz non overlapping channels = 1, 6, 11

5ghz

5ghz = less range but faster

Infrastructure mode terminology:

Basic Service Set (BSS) - single AP interconnecting all associated wireless clients

Basic Service Area (BSA) - area bound by reach of APs signal

Basic Service Set ID (BSSID) - unique, machine identifier for AP in MAC format

Service Set ID (SSID) - human-readable, non unique identifier used by AP to advertise service

Distribution system (DS) - APs connect to network infra using wired DS such as Ethernet. Translates frames between 802.3 ethernet and 802.11 wireless protocol

Extended Service Set (ESS) - two or more BSSs joined through common DS

AP Architectures:

Autonomous:

Wired and wireless hardware to bridge to wired VLAN infrastructure wireless clients that belong to SSIDs

Each AP must be configured with management IP so that it can be emotely accessed with telnet, SSH, or web interface

Each AP individually managed and maintained OR maintained with Cisco DNA center

Cloud-Based:

Cisco meraki

Control plane = traffic used to control, configure, manage and monitor AP

Data plane = end-user traffic passing through the AP

Lightweight APs only perform 802.11 wireless operation for wireless clients

LAPs are configured and managed by WLC

CAPWAP Operation:

The division of labor between WLC and LAPs = split MAC Architecture

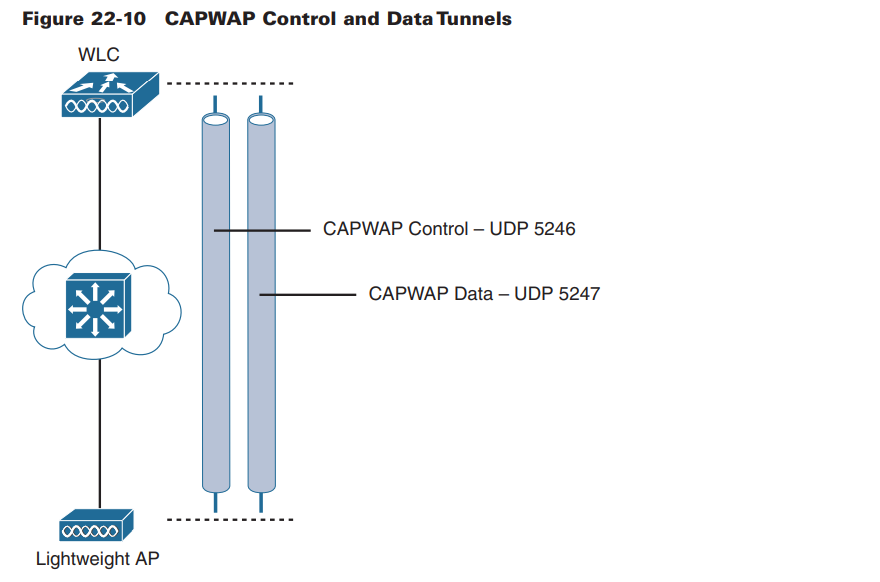
LAP interacts with wireless clients at MAC level

Split-MAC Functions of AP and WLC:

| **AP MAC Functions** | **WLC MAC Functions** |
| --- | --- |
| Beacons and probe responses | authentication |
| Packet acknowledgments and retransmissions | Association and reassociation of roaming clients |
| Frame queuing and packet prioritisation | Frame translation to other protocols |
| Mac layer data encryption and decryption | Termination of 802.11 traffic on wired interface |

CAPWAP:

Uses two tunnels - one for control and one for data



Control message tunnel - used to configure the LAP and manage its operation. Control messages are authenticated and encrypted, so LAP is securely controlled by only appropriate WLC

Used UDP port 5246

Data tunnel - for packers travelling to and from wireless clients associated with AP

Not encrypted by default, but when enabled, packets are protected with Datagram Transport Layer Security (DTLS)

UDP port 5247

Wireless Authentication Methods:

802.11 standard authentication methods = open system and shared key

Open system authentication - where security not needed as something like VPN is in use

Shared key authentication - authenticates and encrypts data between wireless client and AP. Password must be pre-shared to allow connection

Shared key Authentication Methods:

Wired Equivalent Privacy (WEP) = uses Cipher 4 (RC4) with static key, should never be used

Wi Fi Protected Access (WPA) = uses WEP but secures data with Temporal Key Integrity Protocol (TKIP), this changes the key for each packet

WPA2 = industry standard, uses advanced encryption standard (AES) for encryption (strongest protocol for encryption)

WPA3 = next gen, uses Protected Management Frames (PMF)

WPA and WPA2:

Personal use - users authenticate with pre-shared key (PSK)

Enterprise use - requires Remote Authentication Dial-In User Service (RADIUS) authentication server, then authenticate with 802.1X standard using Extensible Authentication protocol (EAP) for authentication

802.1X/EAP:

Open authentication to associate with AP, then dedicated authentication server with following entities:

Supplicant - client device that is requesting access

Authenticator - network device that provides access to network (e.g. the AP forwards the supplicant’s message to WLC

Authentication server (AS) - device that permits or denies network access based on user database and policies (usually RADIUS server)

WPA3 features:

Personal: simultaneous authentication of equals (SAE) makes PSK never exposed

Enterprise: Commercial National Security Algorithm (CNSA)

Open: Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic

IoT onboarding: Device Provisioning Protocol (DPP) hard coded public key to protect devices from attacks

Wireless encryption methods:

TKIP (Temporal Key Integrity Protocol) - encrypts layer 2 payload and does message integrity check (MIC)

AES (Advanced Encryption Standard) - uses CCMP to allow destination hosts to recognise if encrypted and non encrypted bits have been altered

GCMP (Galois/COunter Mode Protocol) - better than CCMP, authenticated encryption

| **feature** | **WPA** | **WPA2** | **WPA3** |
| --- | --- | --- | --- |
| Authentication with pre-shared keys? | yes | yes | yes |
| Authentication with 802.1X? | yes | yes | yes |
| Encryption and MIC with TKIP? | yes | no | no |
| Encryption and MIC with AES and CCMP? | yes | yes | no |
| Encryption and MIC with AES mad GCMP? | no | no | yes |

***Day 21: WLAN Configuration***

-

***Day 20: LAN Security and Device Hardening***

Cisco ESA = device designed to monitor SMTP and protect it from threats

Cisco WSA = combines advanced malware protection, application visibility and control, acceptable use policy controls and reporting. Provides COMPLETE control over how users access the internet

Access Control:

Local Authentication - login and password

SSH

Switchport Hardening

AAA - authentication, authorisation, accounting

AAA protocols:

Terminal Access Controller Access Control System Plus (TACACS+)

Remote Authentication Dial In User Server (RADIUS)

| **feature** | **TACACS+** | **RADIUS** |
| --- | --- | --- |
| Most often used for | Network devices | users |
| Transport protocol | tcp | udp |
| Authentication port number | 49 | 1645, 1812 |
| Protocol encrypts the password? | yes | yes |
| Protocol encrypts entire packet? | yes | no |
| Supports function to authorise each user to a subset of CLI commas? | yes | no |
| Defined by | cisco | RFC2865 |

Uses client/server model in both cases (AAA server)

802.1X is the standard for authentication protocol

Client (supplicant) - 802.1X enabled port on the device

Switch (authenticator) - proxy between client and authentication server

Authentication Server - performs actual authentication of client

Port Security:

Access ports do NOT do any VLAN trunking

| **Option on switchport port-security violation command** | **protect** | **restrict** | **shutdown** |
| --- | --- | --- | --- |
| Discards offending traffic? | yes | yes | yes |
| Sends log SNMP messages? | no | yes | yes |
| Disables interface, discarding all traffic | no | no | yes |

Native and Management VLAN Mods:

IEEE 802.1Q

Native VLAN maintains backward compatibility with untagged traffic

Native VLAN should be an unused VLAN, same with management VLAN

VLAN attacks:

Spoofing - attacker spoofs DTP messages to make switch enter trunking mode. Attacker can then send tagged traffic with target VLAN

Rogue switch - attacker accesses all VLANs on victim switch from rogue switch

Double tagging - vlan hopping that embeds a hidden 802.1Q tag inside the frame that already has an 802.1Q tag, allowing the frame to go to another VLAN other than original

To prevent attacks:

Disable dtp

Disable unused ports and put them in unused VLAN

Manually enable trunk link

Disable dtp negotiations

Set native VLAN to a number other than 1

DHCP attacks:

DHCP starvation

DHCP spoofing

DHCP starvation attacks - denial of service by leasing all available IP addresses to make them unavailable

DHCP spoofing attracts - rogue DHCP server connects to network and provides false IP config parameters to clients

DHCP snooping:

Prevents these attacks with the use of trusted and untrusted ports

DHCP server side is connected to trusted ports

Trusted ports - allow all incoming DHCP messages

Untrusted ports - discard incoming messages that are considered server messages

Untrusted ports, client messages - more complex logic for messages, check for conflicts with new messages versus old messages

Rate limiting - limits number of received DHCP messages per second per port

ARP attacks:

Address resolution protocol replies are called gratuitous arp messages and are sent from hosts. These can be sent by attackers with a spoofed MAC address that is then stores on all other hosts in LAN

Dynamic ARP inspection:

DAI require DHCP snooping and prevents ARP attacks by;

* Not relaying invalid or gratuitous ARP replies out of other ports in same VLAN
* Intercepting ARP requests and replies on untrusted ports
* Verifying each packet
* Dropping and logging replies from invalid sources
* Error disabling if # of configured DAI ARP packets sent

Should be enabled globally, or on selected VLANs (DHCP)

***Day 19: Basic Routing Concepts***

Packet forwarding:

Occurs through path of determination and switching functions

Router searches its routing table for a network address that matches the packet’s destination IP address

This search results in one of three path determinations;

Directly connected network - destination IP address of packet belongs to device on network that is directly connected to one of the router’s interface.

The destination Ip address of the packet is a host address on the same network as this router’s interface

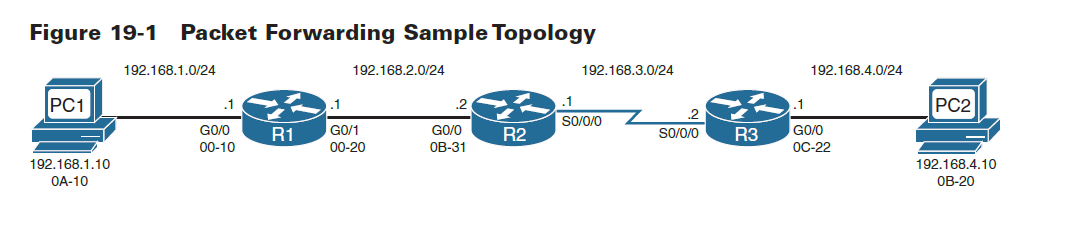
Remote network - destination IP address of packet belongs to remote network, packet is forwarded to another router.

Remote network can only be reached by forwarding packets to another router

No route determined - if destination Ip address of packet does not belong to connected or remote network, and router does not have default route, packet DISCARDED

Router sends Internet COntrol Message Protocol (ICMP) unreachable message

Path determination and switching function example:



1. PC1 has packet to send to PC2. IP source and destination addresses are on different networks. PC1 checks its ARP table for IP of default gateway and MAC address. Packet encapsulated in Ethernet header and forwarded to R1
2. R1 receives Ethernet frame, examines destination MAC which matches MAC address of receiving interface, G0/0. R1 copies frame into its buffer to be processed.R1 decapsulated ethernet frame and reads destination IP. Because it does not match any of R1’s directly connected networks, the router looks at its routing table. R1 selects entry with longest match (longest prefix) and forwards it from G0/1 interface
3. R2 does the same as R1, but as the exit interface is a serial (not ethernet) it encapsulates packet in appropriate frame format for serial interface and sends to R3
4. R3 decapsulated frame and because exit interface of R3 is a directly connected ethernet network, R3 must resolve destination IP address of packet with destination MAC address.R3 searches its table for packets destination IP address in ARP cache. If entry not in ARP cache, R3 sends ARP request out of G0/0 interface to PC2 which will reply so that R3 can update its ARP table and send packet to PC2

Routing Methods:

Directly connected routes - automatically entered in routing table when interface is activated with IP address

Static routes - manually configured by network admin and entered in routing table if exit interface for static route is active

Dynamic routes - learned by routers through sharing routes with other routers using same protocol

Dynamic versus Static Routing:

| **Feature** | **Dynamic Routing** | **Static Routing** |
| --- | --- | --- |
| Configuration complexity | Independent of network size | Increases with network size |
| Required administrator knowledge | Advanced knowledge | No extra knowledge |
| Topology changes | Automatically adapts to topology changes | Requires admin intervention |
| scaling | Suitable for simple and complex topologies | Simple topologies |
| security | Less secure | More secure |
| Resource usage | CPU, memory and link bandwidth | No extra resources |
| predictability | Route that depends on current topology | Always uses same route to destination |

Classification of routing protocols:

| Classification | Distance Vector Routing Protocols | | Link State Routing Protocols | | Path Vector |
| --- | --- | --- | --- | --- | --- |
| Classful | RIP | IGRP | - | - | EGP |
| Classless | RIPv2 | EIGRP | ISPFv2 | IS-IS | BGPv4 |
| IPv6 | RIPng | EIGRP for IPv6 | OSPFv3 | IS-IS for IPv6 | MP BGP-4 (IPv6) |

Routing protocols are classified into different groups according to their characteristics…

IGP or EGP

Distance Vector or Link State

Classful or classless

IGP and EGP:

Autonomous System (AS) is a collection of routers under common admin.

IGP = Interior Gateway Protocol, intra-AS routing (routing inside an AS)

EGP = Exterior Gateway Protocol, inter-AS routing (routing between Autonomous systems)

Distance Vector Routing Protocols:

Distance vector = routes advertised as vectors of distance and direction

Distance = metric such as hop count

Direction = next-hop router or exit interface

They use routers as signposts along a path to a final destination

Routers send updates of their routing info to neighbors

Distance vector protocols work best in these situations;

* Network is simple and flat and does not require hierarchical design
* When admins do not have enough knowledge to config and troubleshoot link-state protocols
* When specific types of networks, such as hub-and-spoke networks, are used
* When worst-case convergence times in a network are not of concern

Link-State Routing Protocols:

Routers create a complete view or topology of network by gathering info from all other routers

Uses link state information to create a topology map and to select best path to each destination network in a topology

Once network is converged, link-state update sent only when topology changes

Link state routing protocols work best in these situations;

* When network design is hierarchical, typical of large networks
* When admins have good knowledge of implemented link-state routing protocol
* When fast convergence of network is crucial

Classful routing protocols:

Do not send subnet mask info in routing updates

Network address allocated based on CLass A, B or C

Network mask determined by first octet of network address

Does not support VLSM

Classless routing protocols:

Include subnet mask with their network address

Support VLSM

Dynamic Routing Metrics:

Routing protocols can learn more than one route to the same destination from the same routing source

METRICS allow them to choose the best path and the routing protocol associated;

RIP - Hop count - best path chosen by route with lowest hop count

IGRP/EIGRP - Bandwidth, delay, reliability, load - best path chosen with smallest composite metric value calculated. By default ONLY bandwidth and DELAY used

IS-IS and OSPF - cost - best path chosen with lowest cost

Administrative Distance:

A number value associated with each dynamic routing protocol. Used when there are numerous dynamic routing protocols for same destination

AD values:

Route source AD value:

Connected 0

Static 1

EIGRP summary 5

External EIGRP 20

Internal EIGRP 90

IGRP 100

OSPF 110

IS-IS 115

RIP 120

External EIGRP 170

Internal BGP 200

IGP Comparison Summary:

| **features** | **RIPv2** | **OSPF** | **EIGRP** |
| --- | --- | --- | --- |
| metric | Hop count | bandwidth | Function of bandwidth, delay |
| Sends periodic updates? | Yes (30sec) | no | no |
| Full or partial routing updates? | full | partial | partial |
| Where updates are sent? | 224.0.0.9 | 224.0.0.5/6 | 224.0.0.10 |
| Route considered unreachable? | 16 hops | Depends on MaxAge of LSA, no more than 3600 seconds | Delay of all 1s |
| Supports unequal cost load balancing? | no | no | yes |

How to prevent looping?

Maximum metric to prevent count to infinity

Hold-down timers

Split horizon (advertisements can be sent back through original interface)

Route poisoning or poison reverse (route marked unreachable in routing update that is sent to other routers - sets metric to max)

Triggered updates

TTL field in IP header (time to live)

Link state routing protocol features:

Send link state updates to neighbouring routers which forward info to their neighbours

Best routes added to their routing tables based on metrics

Building the LSDB (Link State Data Base):

Detailed info is flood about the internetwork to all other routers so that all routers have same info, making best routes easier to work out

***Day 18: Basic Router Configuration***

***-***

***Day 17: The Routing Table***

Router receives an Ip packet on one interface, determines which interface to use to forward packet to destination

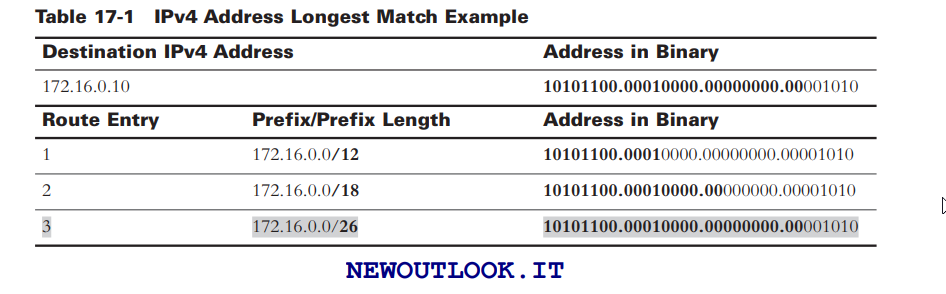
Routers;

* Determine best path for forwarding packets, based on info in routing table
* Forward packets toward their destinations

Longest Match determines best path:

Prefix length determines how close the routes in the routing table are to the network IP address of packet

The close to being identical that the routing table address is to the destination IP, the more likely it is to be the preferred route (longest match)



In the above example: all addresses the same, /26 longest prefix length, wins

Packet Forwarding Decisions:

After a router has determined the best path based on the longest match in routing table, it has three choices:

* Forward packet to device on directly connected network
* Forward packet to next-hop router
* Drop packet because there is no match in routing table

***Day 16: Inter-VLAN Routing***

Concepts:

Traditional inter-VLAN routing

Router on a stick (ROAS)

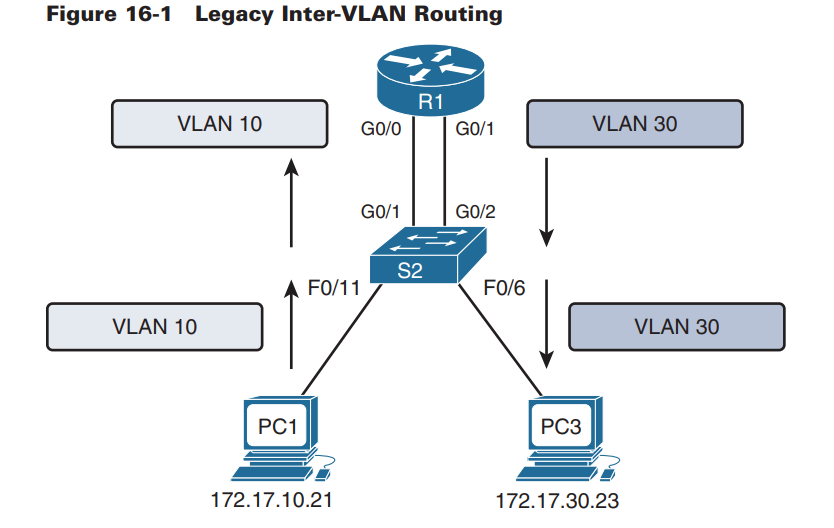
Multilayer Switching

Traditional inter-VLAN routing:

Requires multiple physical interfaces on routers and switches

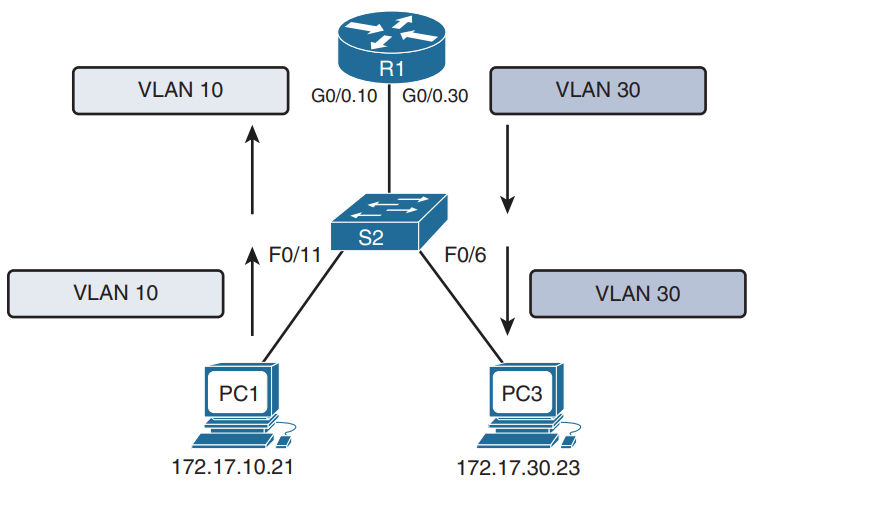
Router interfaces can be connected to separate VLANs

Devices on those VLANs send traffic through router to reach other VLANs



Router on a stick:

One router interface as multiple trunks by using subinterfaces



Multilayer Switching:

Scalable solution in enterprise networks

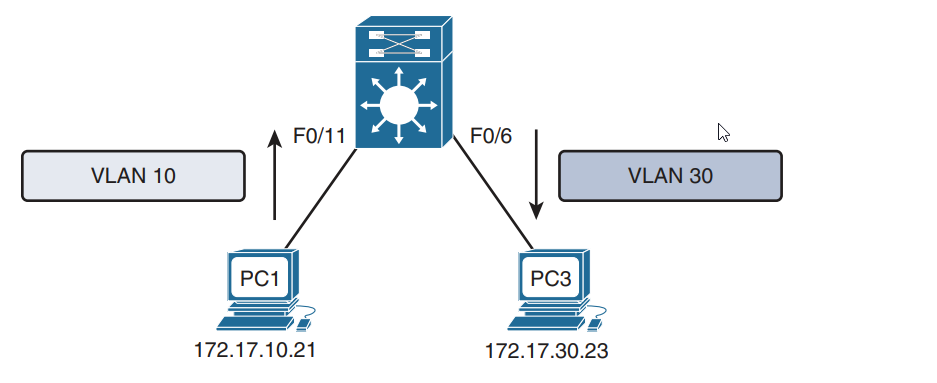
Use multilayer switch to replace both router and switch set up

Multilayer switches can switch traffic within same VLAN and route traffic between VLANs

More scaled because:

* Routers have limited number of available interfaces to connect to networks
* Limited amounts of traffic can be accommodate on physical link at one time

Packets are forwarded down single trunk line to obtain ew VLAN tagging info



ROAS config:

1. Activate interface with no shutdown
2. Configure sub interface for VLAN that needs routing
3. Configure trunking encapsulation with dot1q
4. Configure IP address and subnet mask
5. Repeat steps 2-4 for each vlan

Advantages of a SVI (Switch Virtual Interface):

Faster than ROAS bc everything is hardware switched and routed

No external links needed from switch to router for routing

Not limited to one link. Layer 2 EtherChannels can be used

Latency lower because does not leave switch

***Day 15: Static and Default Route Configuration***

When to use static routing:

Small networks that require simple routing

Hub-and-spoke

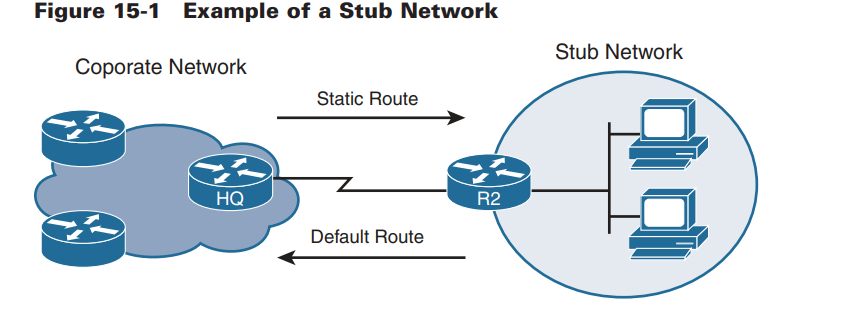
When creating a quick ad hoc route

As a backup when primary route fails

DO NOT use static routes:

In a large network

When network needs to scale in size



***Day 14: OSPF Operation***

The recommended interior gateway protocol (IGP) over Intermediate system - intermediate system (IS-IS)

Cisco chooses OSPF router over RIP routes as OSPF as Administrative Distance (AD) of 100 instead of RIP’s AD of 120

Message format:

1. Data portion encapsulated in a packet
2. OSPF packet header always included, porotocl set to 89
3. Sent to 224.0.0.5 or 224.0.0.6
4. If packet also encapsulated in ethernet frame, destination MAC address is also multicast: 01-00-5e-00-00-05 or 01-00-5e–00-06

OSPF packet types:

Hello - establish and maintain adjacency with other OSPF routers

DBD - Database description, list of sending router’s link-state database

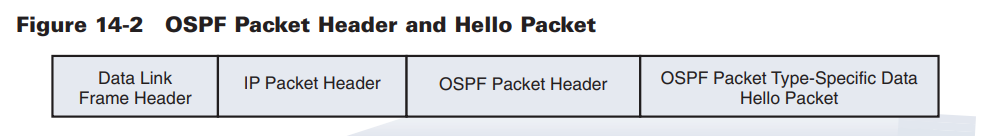
LSR - link state request, receiving routers request more info about DBD entries

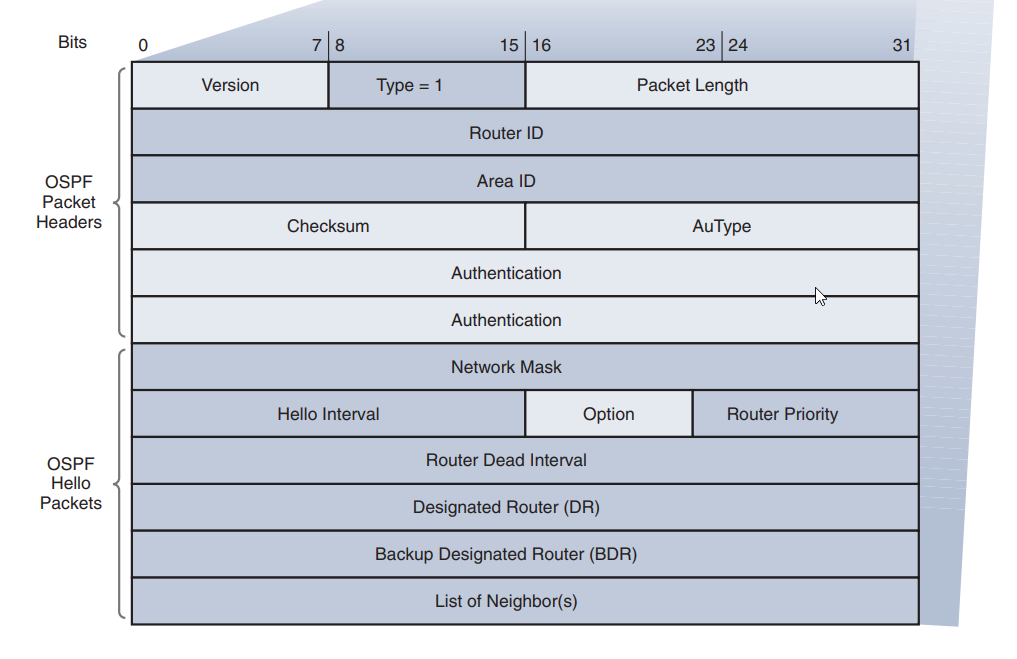
LSU - link state update, reply to LSRs with new info

LSAck - link state acknowledgment, confirms receipt of LSU

Neighbour Establishment:

OSPF neighbours exchange hello packets to establish adjacency





Important fields from above diagram:

Types - packet type - hello (t1), DBD (t2), LSR (t3), LSU (t4), LSack (t5)

Router ID

Area ID

Network mask

Hello interval

Router priority

Designation router (DR)

Backup designated router (BDR)

List of neighbours

Hello packets are use for…

1. Discovering ospf neighbours and establishing neighbour adjacencies
2. Advertising parameters for routers to become neighbours
3. Elect DR and BDR on multiaccess networks

To establish adjacency, two OSPF routers must match the following values:

Hello interval

Dead interval

Network type

Area ID

They must also be part of the same network, subnet mask

A DR and BDR are elected to manage number of adjacencies and flooding of LSAs

Process for Link-State Routing:

1. Router learns its own links and directly connected networks (l3 address configured)
2. Adjacency with neighbours on directly connected networks established with hello pack
3. Each router builds link-state packet (LSP)
4. Each router floods LSP to all neighbours

OSPFv3 used with IPv6