Networks and Network Systems

Introduction

What is a network?

- "a large system consisting of many similar parts connected together to allow movement or communication between or along the parts"
- An arrangement of intersecting horizontal and vertical lines
- A group or system of interconnected people or things

Communication Networks:

Some of the first: postal service & telephone network

- Before telephone networks, phones were connected point to point. Eventually, telephone exchanges were introduced
- PTSN: Public Switched Telephone Network

Computer Network:

A collection of computers, switches, routers, bridges, wi-fi routers/access points, cables, any device that has an NIC

The purpose of a computer network is to communicate information form point A to B efficiently, quickly, and reliably. However, there are many ways in which a Computer Network can be configured.

The internet is one of the more common networks we know of today…

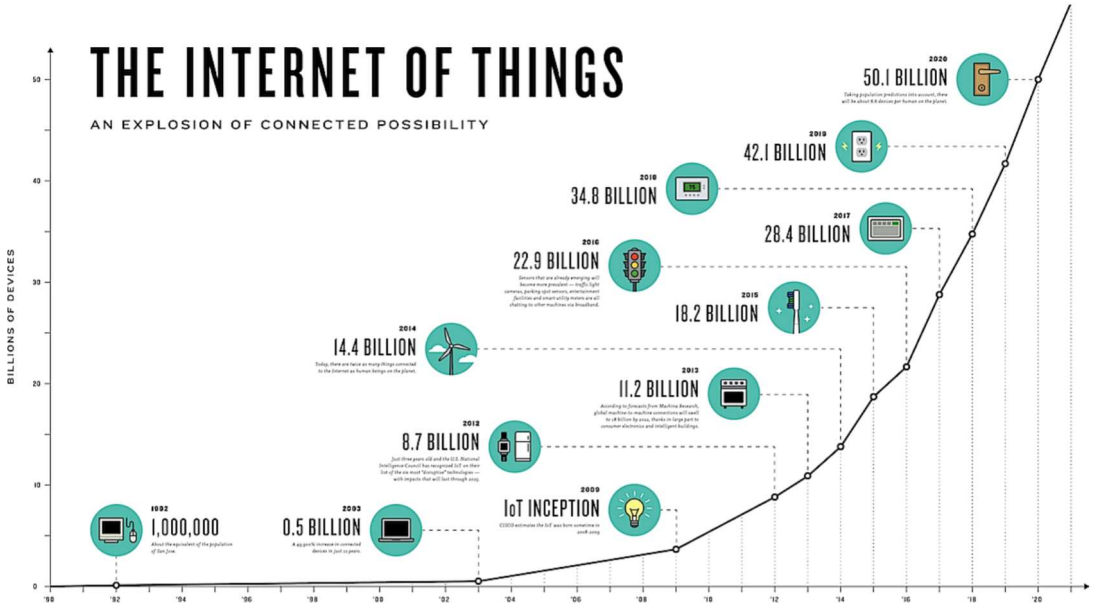
- This is very different from the World Wide Web (WWW)
- Started in the 1960s – ARPAnet

ARPAnet:

Advanced Research Projects Agency Network

- World's first packet switching network
- First network to use TCP/IP
- Created as an experiment by US military to test communications in a nuclear strike
- Later used to connect universities and researchers, and it grew exponentially

Connected Devices

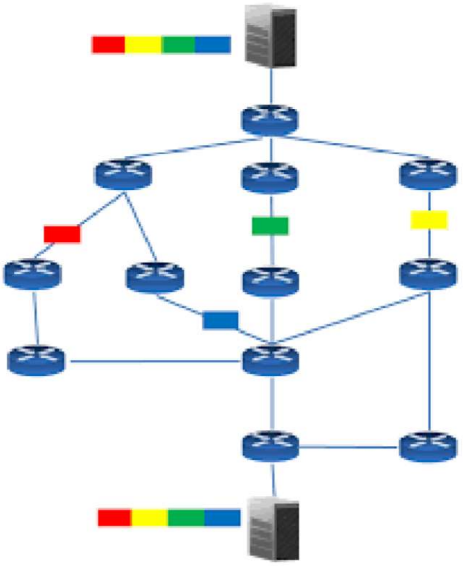


Circuit Switching:

Establishes a point to point connection between two devices

- Channel is dedicated
- Full bandwidth given
- Remains connected for duration of communication
- Designed for voice traffic
- Minimal delays – channel is dedicated
- Highly inefficient

Packet Switching:



- Much more efficient than Circuit Switching
- Data is segmented into small ‘chunks’ of data
- Each ‘chunk’ is called a packet
- Has a destination and a source address
- Allows for much more efficient use of the network
- People can communicate at the same time
- Used to maximise the bandwidth of the network
- Proposed for military use in 1960s, implemented in general ‘home’ networks in 1968
- Allow for much more resilient networks
- Transporting small chunks of data instead of whole files in one go
- Checks on the validity of the packet – checksum, CRC

- TCP is a connection-oriented transportation protocol so will request a resend if a packet/frame is dropped

Network Expansion:

- Networks rapidly grew exponentially
- “I think there is a world market for maybe 5 computers” – Chairman & CEO of IBM, 1874

Communications Media

Physical Layer:

- Foundation on which the network is built
- The properties of different kinds of physical channels determine the performance – throughput, latency, error rate

Guided Transmission Media:

- Physical layer purpose – to transport bits from one place to another – node to node
- Various physical media can be used – each has its own niche in terms of…
    - Bandwidth
    - Delay
    - Cost
    - Ease of installation
    - Maintenance
- Physical/wireless media required…
    - To transfer 'signals' from one place to another
    - To impose a structure – often by the structure the media places upon the designer and installer of a network
- Data:
    - Although a given media is used as the transfer agent, it is the **media protocol** that defines the processes and its characteristics of the data transfer
    - Some media types can be used to support multiple different media protocols
- Structure:
    - Physical media can impose structure
    - That structure is called **topology**
    - Structure and media protocol often define the limitations and expectations of a network in terms of:
        - Number of nodes that can operate within the network
        - Distance over which the network will operate
        - Bandwidth that the network can support

Bandwidth:

- A measure of the amount of data that can be sent over a network connection – it indicates the maximum transmission capacity
- Like a water hose, the bigger the opening, the more water can throw through at any one time
- Bandwidth might incorrectly be referred to as the amount of data transmitted. This is actually 'data transfer'

Broadband:

- A broadband connection is one that allows data to be sent on multiple channels simultaneously. This broadens the available bandwidth
- Measurement – expressed in terms of how much data can be transmitted per second

Units

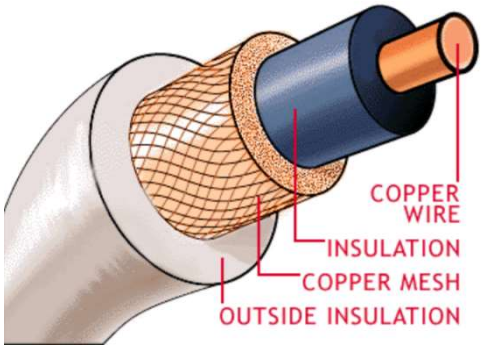
- Units of bandwidth - order of magnitude:
- Bits per second (bps)
- Kilobits per second (kbps)
- Megabits per second (mbps)
- Gigabits per second (gbps)
- Terabits per second (tbps)
  - Each unit is 1,000 times larger than the one that precedes it.

Physical Media:

Copper Cable:

- Cost common form of network media
- Relatively cheap to install
- Easy to modify and manage
- Has the ability to support media protocols
- Can support relatively high speed (high bandwidth) protocols – 1gbps over short distances
- Two distinct forms: Coaxial, twisted pair

Coaxial…



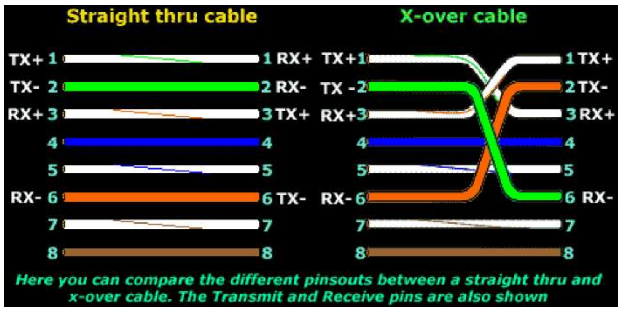
Sometimes multiple layers of "shielding" are provided particularly when very high frequencies are being used, or where extra shielding from interference is required.

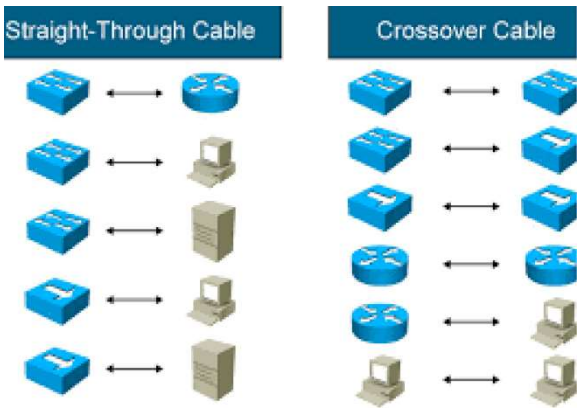
- Uses include…
  - Thin ethernet (cheaper net)
  - Thick ethernet (a much sturdier construction)
  - Satellite interconnections
  - RF connections (radio, TV, microwave)
  - Token ring
- The only differences from one coaxial type to another are…
  - Frequency and range supported (capacitance and resistance of cables and connectors)
  - Physical diameter of construction

    - Materials used in insulation, shielding and conductor – which impose 'properties' of the cable which effect the type and nature of the signals that can be transmitted down them

Twisted Pair…

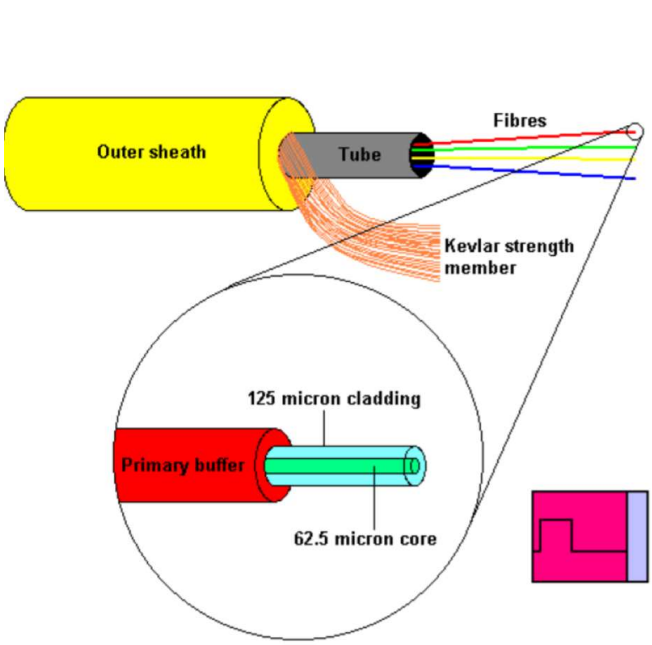
- Individual strands of coppoer wire, sheathed in PVC for insulation
- Paired and twisted with a second conductor
- Multiple pairs possibly included in construction
    - Each pair can be individually earth shielded using braiding or 'tin foil' – Shielded Twisted Pair (STP) rather than Unsheathed Twisted Pair (UTP)
    - A bundle of multiple pairs shielded
    - A bundle without any shielding
- Classified using the 'category system'; Cat I, Cat II, Cat III, Cat IV, Cat V, Cat Ve and Cat VI. The higher the category, the higher the specification
- The category status depends on…
    - The quality of the cores
    - The size of the cores
    - The thickness of the insulation around the individual cores
    - The tightness of the twist
- The specification for categories defines…
    - How high frequency signals 'behave' travelling along the cable
    - The distance it will travel within a tolerance of cross-talk and attenuation - Cross talk is where impulses of electricity down one cable effect through "induction" another, and effectively regenerate the same (although weaker) signal in other physically close cables
- The higher the frequency (the greater the bandwidth) the higher the specification of cable required
- The longer the distance, the higher the specification
- Simple very old telephone lines – Cat I & Cat II
- More modern telephone lines – Cat II & Cat III
- Basic data cables (e.g. serial data cables) – Cat IV
- Faster (100mbps) – Cat V
- High speed (1000mbps) – Cat Ve (enhanced)
- Very High Speed (1Gbps – 10Gbps) Cat VI
- For Cat V and VI special connectors are used to ensure high quality interconnection of nodes to cables (reducing possible signal loss and interference)
- Different LAN standards may use the twisted pairs differently. For example, a 100mbps ethernet uses two out of the four pairs, one for each direction, so two are unused.



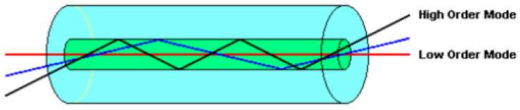


Fibre Optic:

- Uses light pulses to transmit data. It operates over large distances
    - Single-mode fibre: transmits data at 100gbps for 100km without signal being repeated
    - Multi-mode fibre: transmits data at 100mbps for 2km without the signal being repeated
- At one end of a fibre optic is a transmitter which converts electric signals from copper wire into light pulses. Immune to electrical interference and does not suffer from crosstalk
- Each fibre can carry many independent channels, with each using a different wavelength of light.
- It is more difficult to hack because there are no electrical currents running through fibre optics (they can be used in dangerous environments without risk of ignition) and it is harder to wiretap (physically hack)



Multiple signals (light pulses) propagating through an optical Fibre cable. The Fibre can handle multiple channels with each data stream transmitted at different frequencies (the angle at which they are reflected).



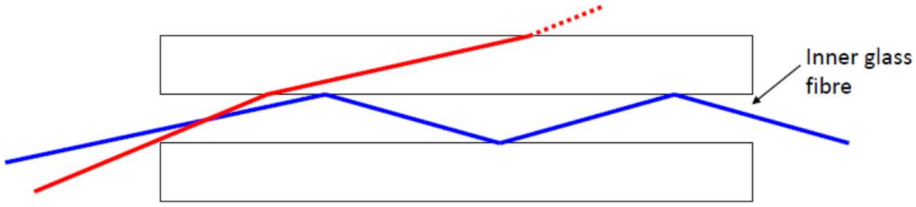
Electrical signals are converted to light pulses and then sent down the optical Fibre cable where they are converted back to electrical signals at the other end.

- A glass fibre is composed of two parts – an inner core, used for transferring the light signal, and an outer sheath, used to ‘trap’ the light signal in the inner core

- Individual cores are usually given a thin surface layer of coloured plastic for identification
- Cores are bundled (4, 8, 12, 16, 24 and more) into a single PVC tube. The tube is usually filled with a water resistance oil jelly for added protection (a cushion)
- Outer PVC tube is usually Blue, Green, Violet or Black depending on the installation

Providing the light signal is within a “critical angle” – the angle of incidence to the boundary of the two glass edges, it will be “reflected”

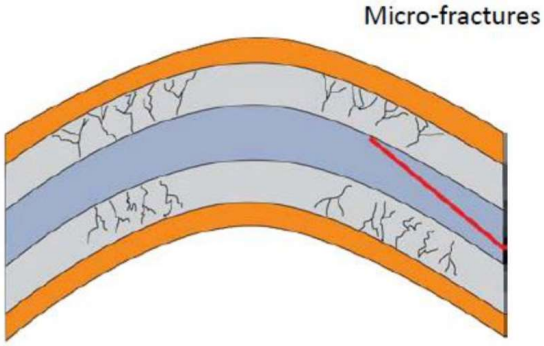
- If it is outside the critical angle – it will escape the glass fibre and be lost



Inner glass fibre is surrounded with a tube of glass that is of slightly varying refractive index

Fibre-optic cables usually have a minimum bend radius of 3.0 cm.

If the cable’s bent more than this, the fibre core can develop micro-fractures, real fractures, or severely leak light.



As it’s the light that’s carrying the network data, a loss of light means a loss of information and network errors.

- Theoretical speeds of 50,000gbps can be achieved using fibre – the faster the speed of data, the smaller the pulse widths and the distance between each pulse
- Practical limits of several gbps are the reality – the light source and the receiver restrict the speed, imperfections in the glass or ‘connections’ can cause losses and reflections, converting light to electrical signals incurs limitations
- 100Mbps over approx. 2Km is practical using Multi-mode fibre
- 100Gbps over 100 Km is practical using Mono-mode fibre
- Multi-mode fibre is cheaper to manufacture than Mono-mode
- Multi-mode fibre is easier to interconnect and join than Mono-mode fibre

- Low-cost laser transmitters are used for mono-mode (smaller aperture is required since it is a smaller fibre) – The issue is purely one of mechanics, connectors for fibre are precision and tend to be quite expensive for mono-mode fibre

Physical Layer:

- Involves the actual physical medium
    - Used in the transfer of messages
    - Most basic network layer
    - Actual signal used varies depending on types of medium (electrical modulation, radio waves, optical signals)
- In theory any medium can be used

List of Services:

The physical layer is responsible for…

- Bit-by-bit delivery
- Providing a standardised interface to the medium
- Modulation
- Line coding
- Flow control
- Multiplexing
- Circuit switching
- Forward error recovery
- Carrier sense

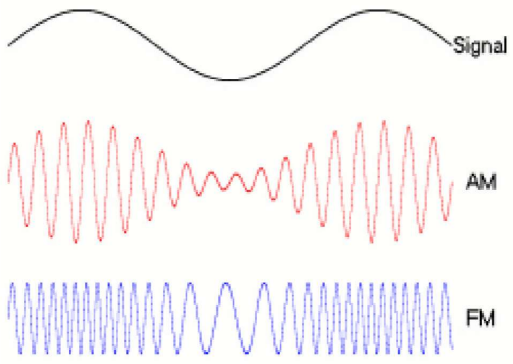
Bit-by-bit Delivery:

- Symbol rate or Baud rate
    - Different from bps
    - Symbol is a pulse or tone that represents the data
- Physical layer places these symbols on the medium at a fixed/known rate
    - A symbol may encode one or several bits of data

$$T_S = \frac{1}{f_S}$$

Modulation:

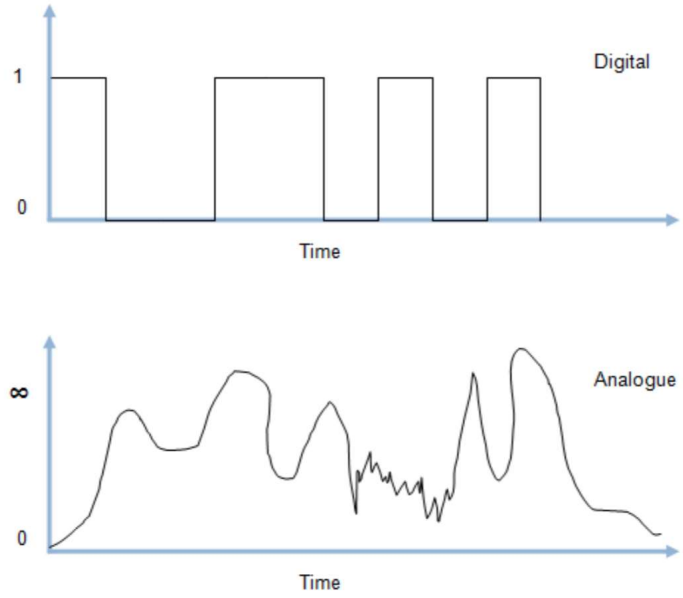
The process of modulating a signal onto a carrier



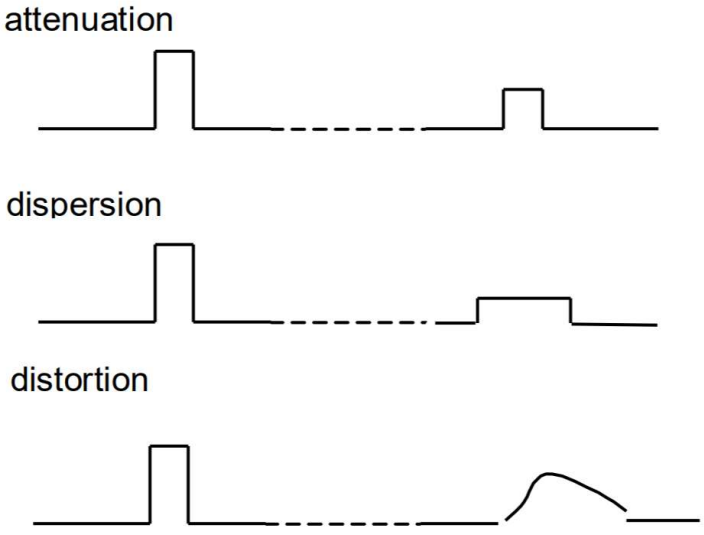
Signals:

- Signals can be analogue or digital
- Analogue signals vary continuously and can take any value within some given range
- Digital signals are chosen from a discrete (limited/finite) range of possibilities e.g. 0,1 or A-Z etc.

Analogue and Digital Signals



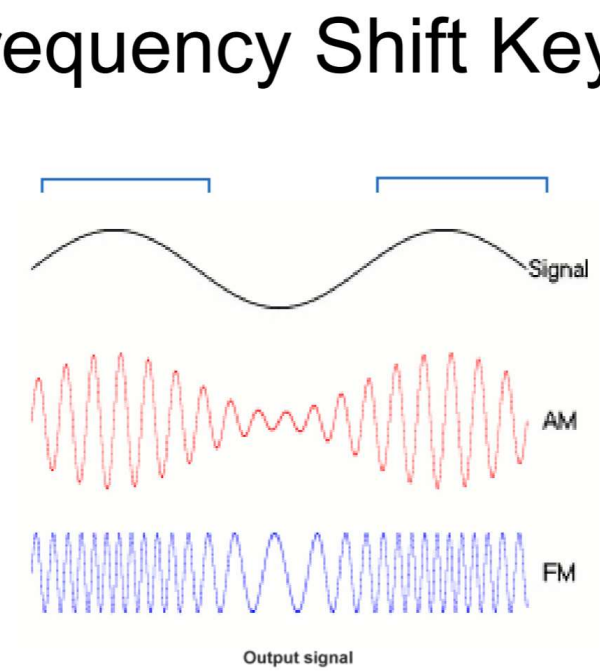
How signals get damaged



Modulation:

Several modulation methods…

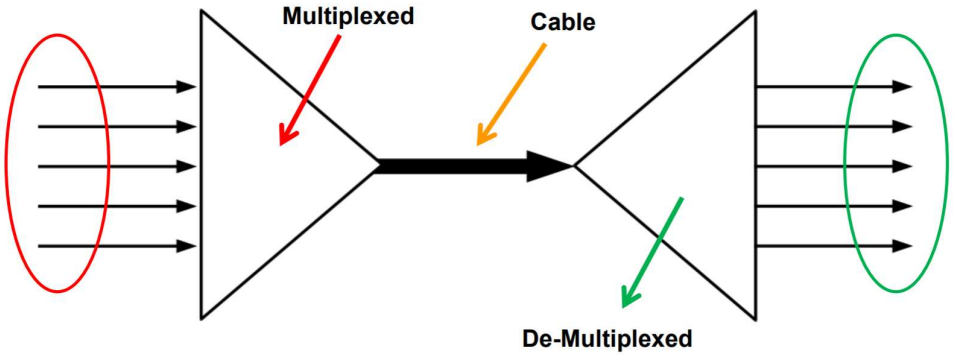
- PSK – Phase Shift Keying – a finite number of phases are used
- FSK – Frequency Shift Keying – a finite number of frequencies used
- ASK – Amplitude Shift Keying – a finite number of amplitudes are used



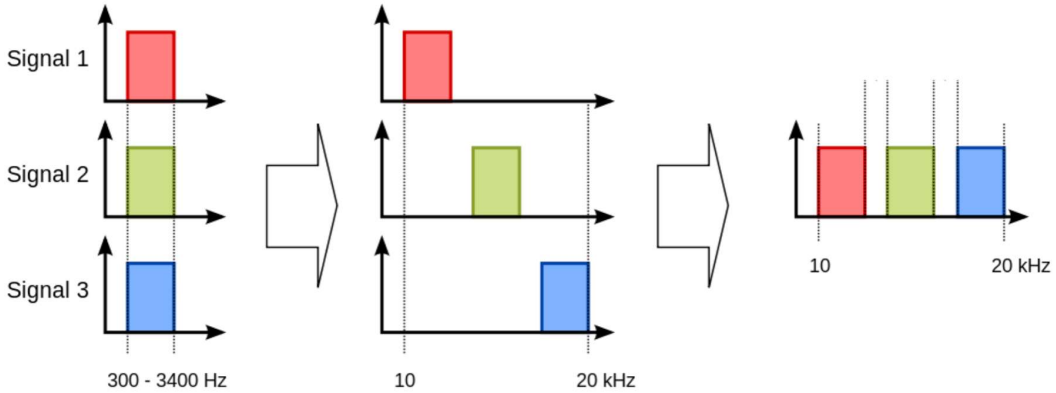
Flow Control:

- Manages the data rate between sender and receiver
    - Prevents a slow receiver being overloaded by a fast sender
- Stop and wait
    - Simplest flow control
    - Receiver says ‘ready’ – ACK
        - For each frame to be sent
        - Must be received before the timeout
- Algorithm:
    1. Sender: transmits a single frame
    2. Receiver: transmits ACK as receives frame
    3. Sender receives ACK – without timeout
    4. Repeat

Multiplexing



Frequency-Division Multiplexing



Time-Division Multiplexing

Network Topologies

(recap packet switching)

Different types of Networks:

- Networks consist of wired and wireless connections
- The communication media can be very different
- Topologies – the shapes of networks

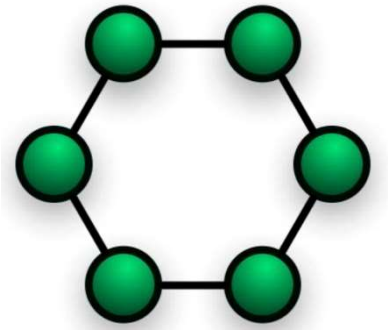
Network Topologies:

4 most common topologies (there are others based around these shapes) …

- Ring network
- Bus network
- Star and extended star (most common)
- Hybrid network

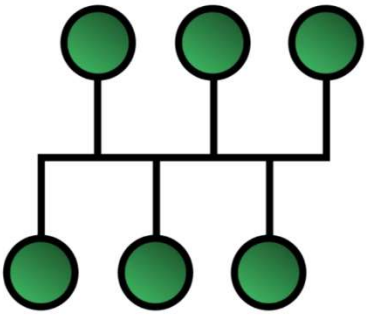
Ring Network:

- Each 'node' connects to exactly two other nodes
- Data travels in a ring. Every packet sent ca be received and handled by every node. The packets are carried by a token hence the term Token Ring
- Advantages: easy to configure, easy to find fault, no central management required, easy to add and remove nodes
- Disadvantages: a failure of a node breaks the network, communication delay is directly proportional to number of nodes, bandwidth is shared, coaxial cabling is slow, difficult to install due to cable thickness



Bus Network:

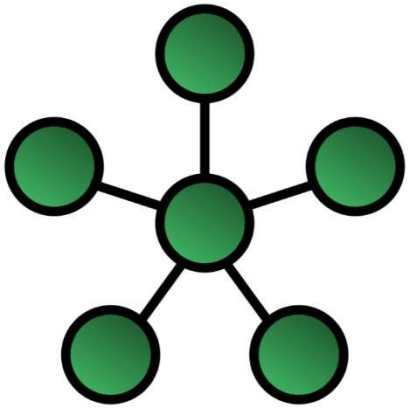
- Connected nodes are 'daisy chained'
- Just like a ring network, all nodes receive all network traffic
- Advantages: easy to add nodes, easy(ish) to find faults
- Disadvantages: all network is received by all nodes, if the network is severed no node can receive data, all nodes have the same transmission property (uses media access control)



Star Network:

- One of the most common computer networks (uses the standard ethernet)
- Each node connects to a central 'hub' – acts as a 'gateway' for traffic
- Advantages:
    - more resilient than previous topologies
    - Central 'hub' broadcasts messages to all nodes in the network

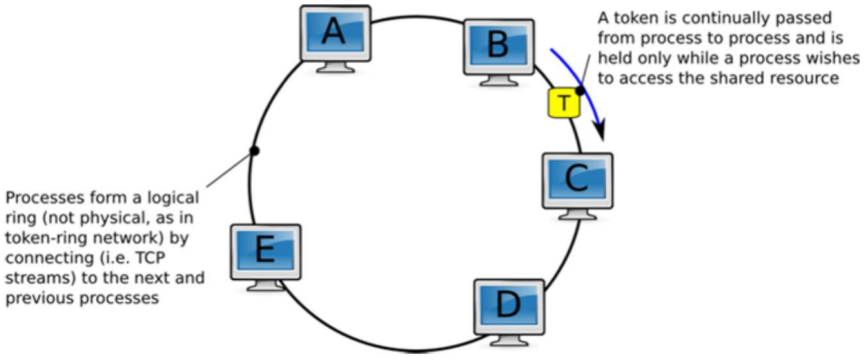
    - A failure of an outside node does not affect the remainder of network
    - Easy to detect faults
    - Expanding and changing is easy
    - Improved performance (less nodes and cables when two nodes communicate)
    - Isolation of devices



- Disadvantages:
    - The hub can be bottlenecked (in modern networks, hubs have largely been replaced with switches to alleviate the bottleneck problem to a point)
    - If the hub fails, the network is unusable
    - Expensive to purchase
    - Large amounts of cable
    - Forms a broadcast domain

Token Ring vs Ethernet:

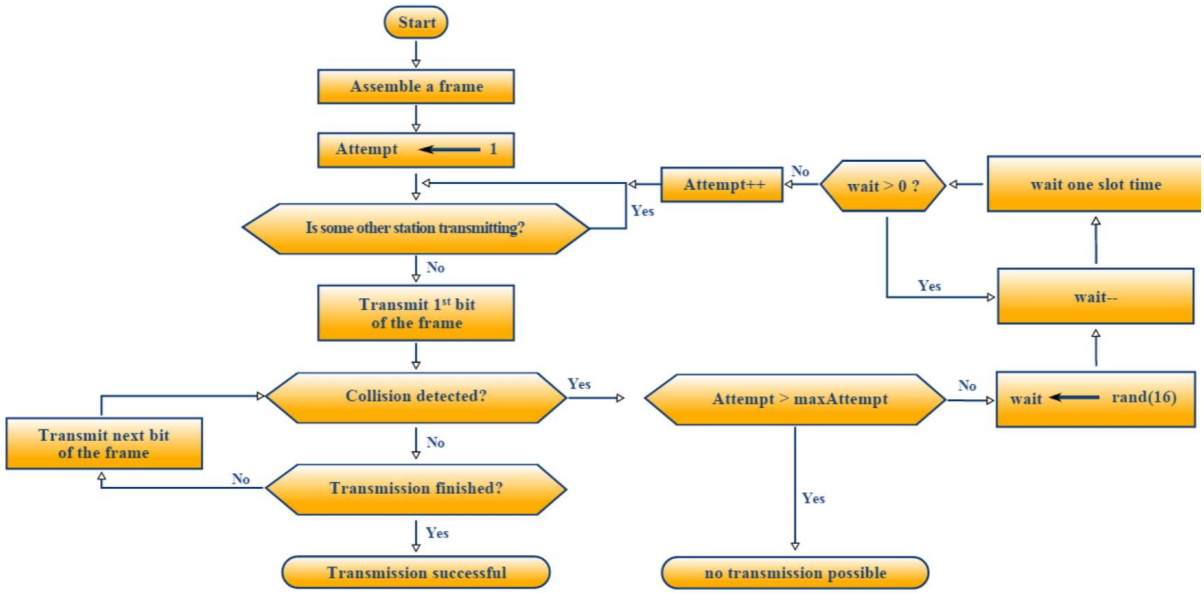
- - if we increase the number of nodes on a network, we get more data, more traffic and more errors
- A collision is when two 'packets' on the network collide, so we lose the packets and have to resend them, congesting the network
- Token ring – solution: a 'token' is passed around the network, allowing nodes the right to transmit



Ethernet solution:

- Ethernet LANs consist of network nodes and interconnecting media. The network nodes fall into two major classes: data terminal equipment (DTE) and data commination equipment (DCE)
- Uses CSMA/CD: Carrier-Sense Multiple Access with Collision Detection
- CSMA/CD is a modification of carrier sense multiple access (CSMA)
    - Improves performance by terminating transmission as soon as a collision is detected
    - Shortening the time required before a retry can be attempted

- Carrier-Sense – determine if another transmission is in progress. If there is another carrier, wait for it to end



Data Terminal Equipment:

DTE – devices that are either the source or the destination of data frames

- DTEs are devices such as PCs, workstations, file servers, or print servers
- Often referred to as end stations

Data Communication Equipment:

DCE – intermediate network devices that receive and forward frames across the network

- DCEs may be either standalone devices such as repeaters, switches and routers, or communications interface units such as interface cards and modems

Networking Standards and Models

Standards:

- The internet works despite differences in devices, topologies, and protocols, because we have 'standards' that define the rules for protocols to communicate effectively
- Standards are required to ensure full compatibility and interoperability between devices

OSI Model:

- Problem addressed by the International Standards Organisation (ISO) and became an international standard
- To create a model that addressed the following:
    - To interconnect equipment, made by different manufacturers, through a standard interface
    - To integrate software and hardware, and to be portable on differing systems
    - Create a model which will be adhered to by all countries of the world
    - To create an open standardised networking model that all vendors would support
- Headed up by the ISO beginning work on what would be known as the Open System Interconnection (OSI) networking model
- ISO had a goal for the OSI model: to standardise data networking protocols to allow communication between computers across the entire planet
- Problem: considering all the different vendors and devices, how does information move between computers and applications?
    - Problem divided into 7 manageable problems/layers
    - Each layer solves one of the problems

OSI 7-Layer Model			
	Data Unit	Layer	
Host Layers	Data	7. Application	Provides user interface
		6. Presentation	Formats data between Application and Session
		5. Session	Establishes and terminates connections
Network Layers	Segments	4. Transport	Manages end-to-end data delivery
	Packets/Datagram	3. Network	Forwarding of data between nodes and networks
	Frame	2. Data Link	Reliable connection between two directly connected nodes
	Bits	1. Physical	Data is converted to bits and placed on the media

7. Application Layer

- Provides the user interface for communication. Functions e.g. email, file transfer, etc.

- Application **Network Services to Application Programs** – provides network services to application programs

6. Presentation Layer

- Formats data for exchange between Application and Session layer

- Masks the differences of data formats between dissimilar systems

- Encodes and decodes data; encrypts and decrypts data; compresses and decompresses data

- Presentation **Data Representation and Interpretation Translation** may need to occur between two different systems using different presentation standards e.g. different character sets or character codes. This layer allows data to be interpreted using a set of translations and can also add data encryption for security purposes

5. Session Layer

- Manages communication between applications after a connection is made. Sets up the session, manages information exchanges, then breaks it down when the session ends

- Session **Inter-host Communication** – Sets up, maintains, and closes down a session. This operation provides an open communication path with another system

4. Transport Layer

- Manages end-to-end message delivery in the network

- Provides both reliable and sequential packet delivery through error recovery and flow control mechanisms – TCP

- Can keep track of segments, providing the ability to resend failed segments and acknowledge successful delivery and send next data

- Provides unreliable transport too – UDP

3. Network Layer

- Manages the transfer of packets that are to be forwarded on different networks and between nodes on the same network

- Networking addressing and determining best path

- Data is routed through a network and can also be routed through interconnected networks. Splitting of data for transmission and re-assembling upon reception. The IP part of the TCP/IP operates at this level

2. Data Link Layer

- Provides a reliable link between two directly connected nodes by detecting and possibly correcting errors that may occur in physical layer

- Ensures that all of the data from the sending computer has been received thereby providing flow, error control, and synchronisation of the physical layer

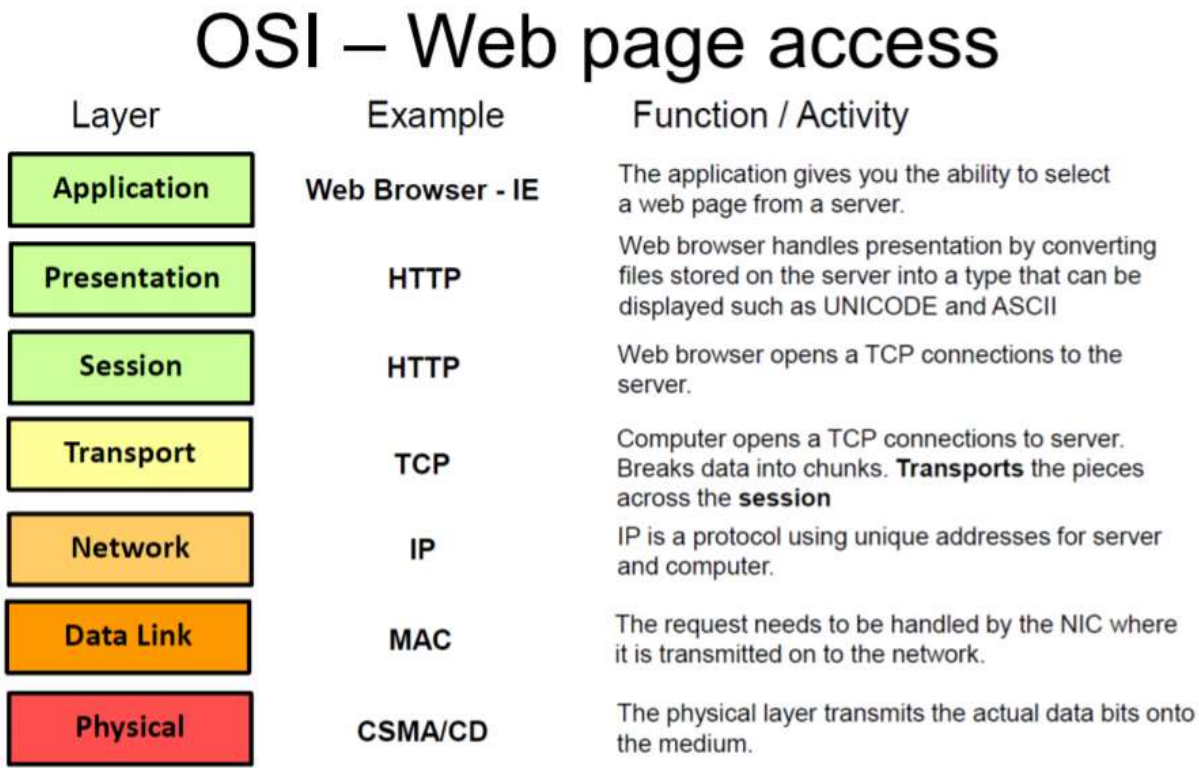
- Error detection – prevents two computers accessing the media simultaneously (collision detection)

- Point-to-point Protocol (PPP) is an example of the data link layer in the TCP/IP stack

1. Physical Layer

- Transmission of binary data via a medium – it defines the cabling, or method of data carriage, connectors, electrical characteristics of the communication channel and the transmitted signal. Defines the protocol to establish and terminate a connection between two 'directly' connected nodes

- The NIC converts the binary data into electrical voltages (high and low). Devices that operate at the physical layer include network interface cards, hubs, bridges, switches and routers (some of these work at other layers too)



OSI Summary

OSI Layer	Devices	Protocols
Application		SMTP, SNTP, FTP, TELNET, HTTP, SMB
Presentation		NCP, AFP, TDI
Session		NetBIOS, Winsock
Transport		TCP, SPX, NeuBEUI
Network	Routers, IP Switches	IP, IPX, Nwlink, ARP
Data Link	Bridges, Switches	
Physical	Hubs, Repeaters, Network Adapters, Token Ring, Wireless	

Benefits of the OSI model:

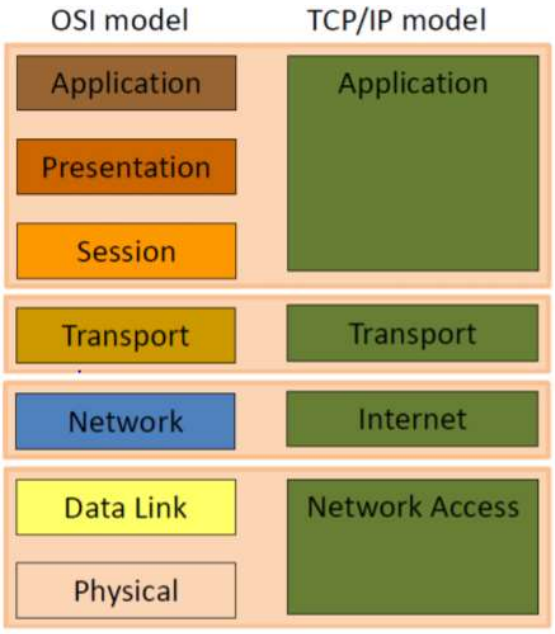
- Reduced complexity – complex problems are decomposed into 7 layers
- Increased evolution – technology can advance and still integrate with old technology
- Guarantees interoperability – ensures data can be transferred between differing computer types, software, operating systems, network and computer hardware
- Allows modular engineering – hardware and software con interface well with each other
- Standardised interfaces – products can be designed to easily plug into one or more physical layers of the model

TCP/IP Model:

- Introduced 10 years before OSI model
- Fewer layers, 4
- Less complex but does same job
- AKA Internet Model

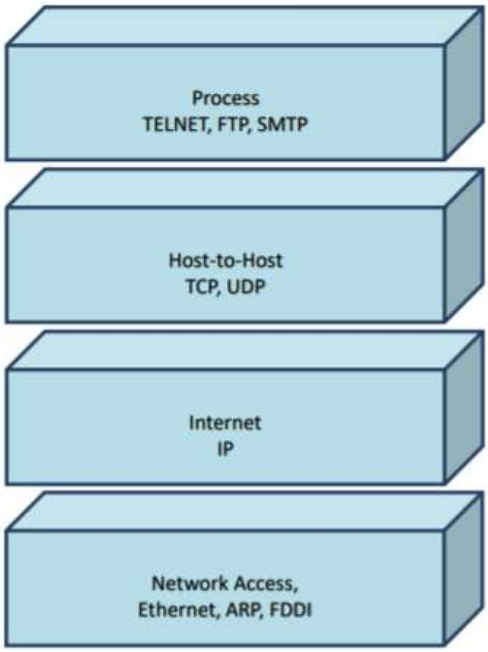
Department of Defence Model (DoD):

- Developed to support development of early networks – specifically the internet
- Important because protocols used on the internet still adhere to it



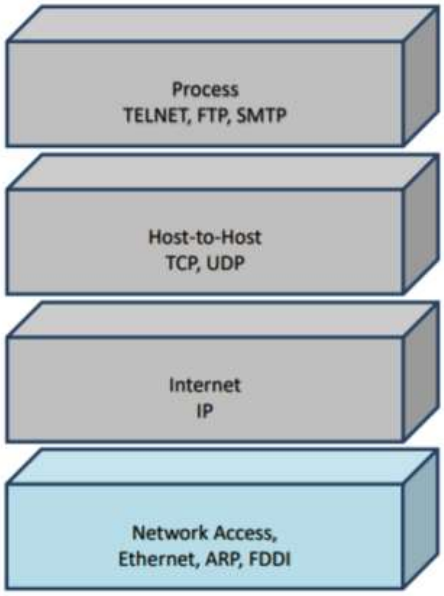
DoD Model

- 4 layer model
- Layers operate in a similar manner to the first 4 layers of the OSI model
- Based on network communications



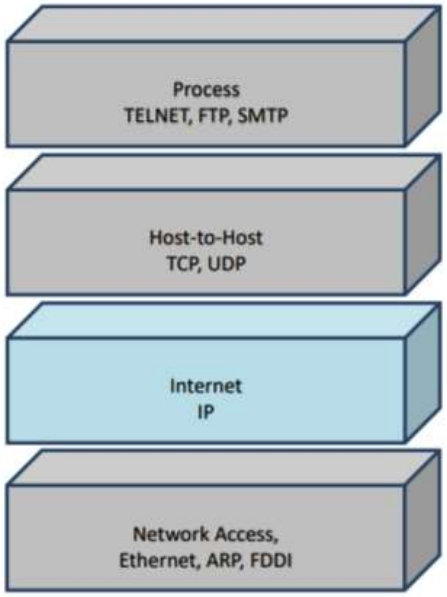
Network Access Layer

- Responsible for delivering data over the particular hardware media in use.
- Different protocols are selected from this layer, depending on the type of physical network



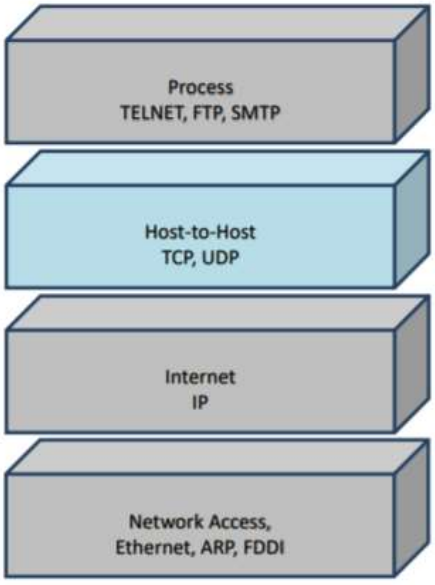
Internet Layer

- Responsible for delivering data across different physical networks that interconnect a source and destination machine
- Routing protocols are most closely associated with this layer, as is the IP Protocol, the Internet's fundamental protocol



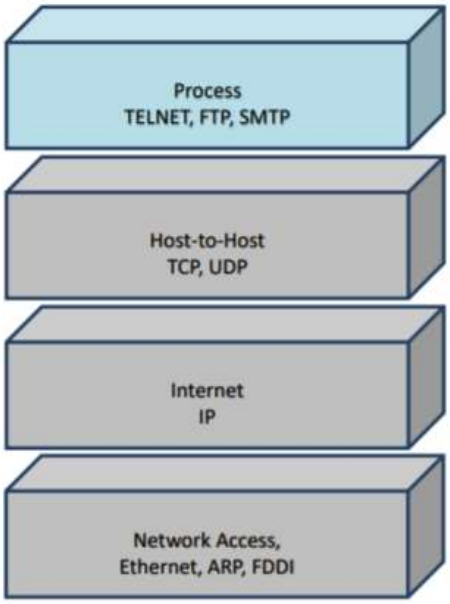
Host-to-Host Layer

- The handles connection rendezvous, flow control, retransmission of lost data
- TCP and UDP protocols are this layer's most important members



Process Layer

- This layer contains protocols that implement user-level functions, such as mail delivery, file transfer and remote login



RFCs:

- Request for Comment
- Standardisation documents
- Detail how a technology will work
- Any interested parties can comment on the content of the RFC and suggest changes

Standards Bodies:

There are a number of bodies that oversee standards relating to computing, e.g.:

- IEEE – Institute of Electrical and Electronics Engineers
- BCS – British Computer Society
- ISO – International Organisation for Standardisation
- IETF – International Engineering Task Force
- ISOC – Internet Society

Network Devices

Data Link Layer:

- Comprises 2 sub layers – LLC: Logical Link Control Layer, MAC: Media Access Control Layer
- LLC:
    - provides flow control, acknowledgement, and error notification
    - controls data exchanged between the source and destination machines
    - Takes packets from network layer – creates frames to send to physical layer
    - Error detection and correction – also responsible for detecting and correcting errors in receiving data
- MAC:
    - Determines who is allowed to access media at any one time – CSMA/CD
    - Determines where one frame ends and another starts – frame synchronisation

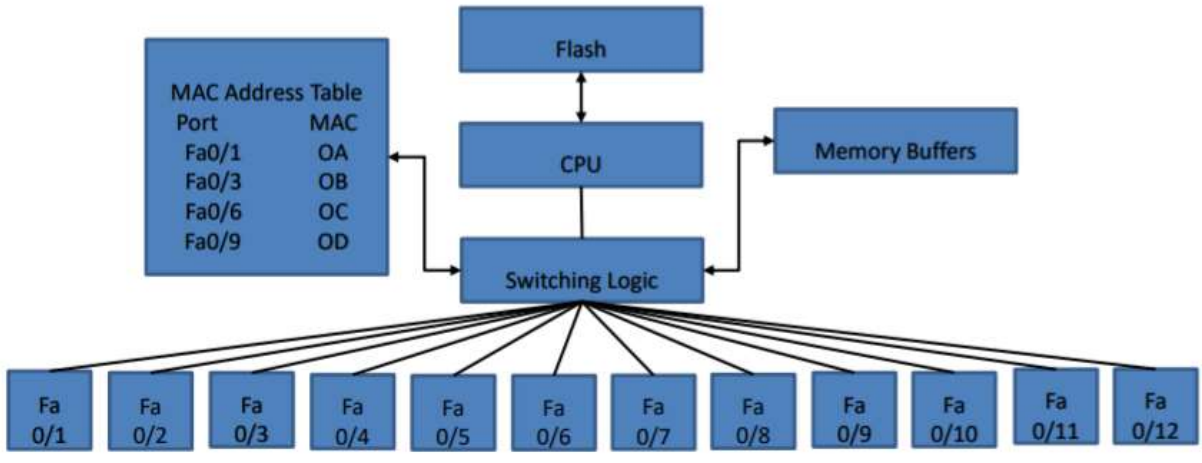
Frame Synchronisation:

4 methods…

- Time based – specified amount of time between frames
- Character counting – counts the characters in the frames header
- Byte stuffing – precedes the frame with a byte character sequence such as data link escape
- Bit stuffing – uses a flag consisting of a special bit pattern a 0, six 1 bits, and a 0

Data Link Layer – Switch:

- Most switches reside at this layer
- Some switches have additional capabilities that make them layer 3 devices



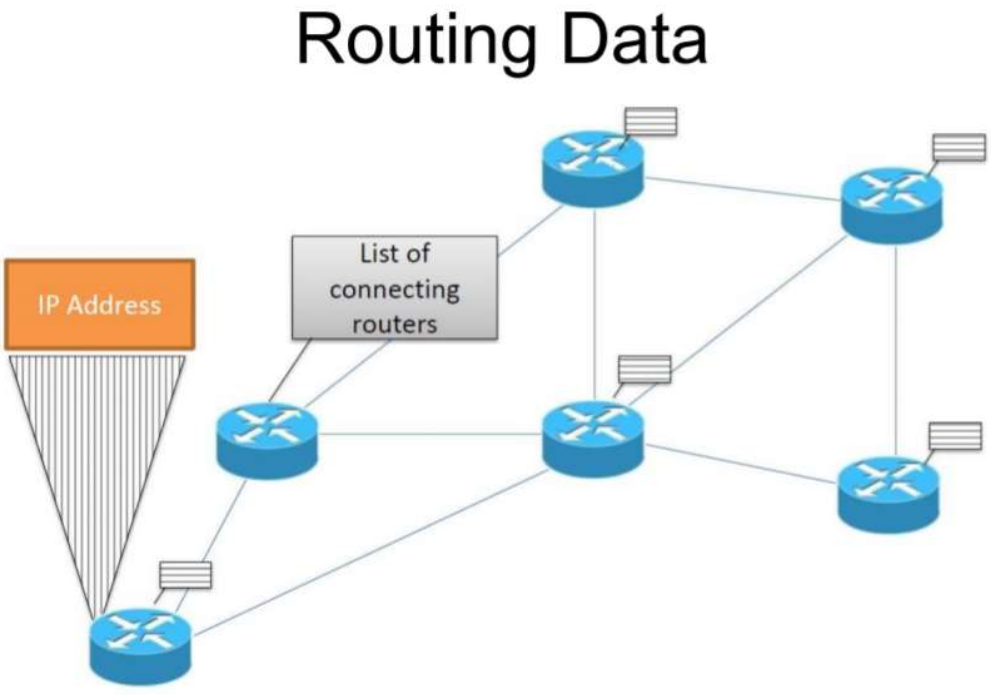
- Device addressing comprises 2 parts: IP address – layer 3 function, MAC address – layer 2 function
- Every device has a MAC address which is embedded during manufacture
- Switches learn about the devices attached to each port
- To do this it uses ARP – address resolution protocol
- ARP is considered by some to be layer 2 and others to be layer 3 – it interacts with both layers

ARP:

- A switch receives a packet which contains an unidentified MAC address
- ARP then broadcasts an ARP request to request information about the known IP address
- All host receive the broadcast frame
- If there is a math the matching device will send the required information – unicast
- MAC information is updated in the MAC address table and that port is associated with that device
- If no match, the ARP is discarded

Network Layer:

- End to end delivery of data – between two computers, this is not 'devices' but an actual entire route
- Addressing
- Routing
- The network layer is responsible for packet forwarding including routing through intermediate routers
- Whereas the data link layer is responsible for media access control, flow control, and error checking



- The network layer defines 3 main features…
    - Routing – routers forward packets to their final destination
    - Logical addressing – each device can have an address that can be used by the routing process
    - Path determination – refers to the work done by routing protocol by which all possible routes are learned, but the best route is chosen for use
- Routing Protocol – aids routers by dynamically learning paths to other routers and other networks…
    - OSPF – Open Shortest Path First
    - RIP – Routing Information Protocol
    - BGP – Border Gateway Protocol
    - IS-IS – Intermediate System to Intermediate System

TCP/IP

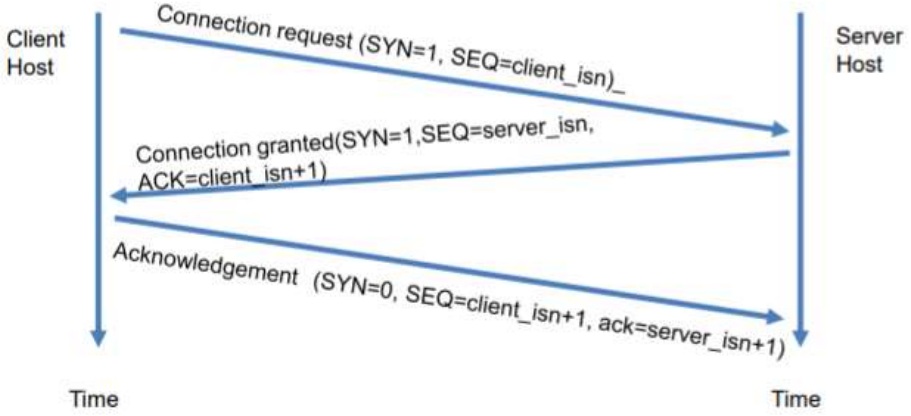
- IP – purpose is to deliver packets with as little per-packet effort as possible – no error checking
- TCP – performs the useful networking functions – error recovery, resending lost packets

TCP and UDP:

- Provide transport for data packets
- TCP is connection orientated
- UDP is connectionless

TCP - 3-Way Handshake

Designed to ensure that data sent using TCP for transport is received and acknowledged by the receiver

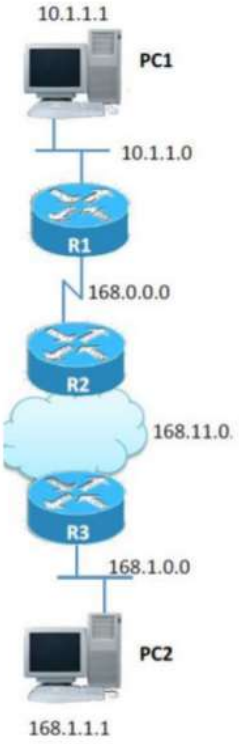


Routers:

- Act as a default gateway – exit to other networks
- Move data between networks
- Restrict network broadcasts (routers do not broadcast)
- A router acts as a dispatcher, choosing the best path for information to travel so its received

Forwarding

- Focuses on the end-to-end logic of data
- Here PC1 is sending to PC2 via interconnected routers
- The logic used by each device varies
- Notice how the network changes for example 10.1.1.0 is a network address



Routing:

- The sending computer does not know much about the network – only very local information e.g. the connected router
- Network devices help to build a 'map' or topology of the network
- Devices know where to send the data and how to get there – what port to forward data out of, what device is attached to which switch port
- Information is managed by routers local knowledge, routing tables, build automatically
- Hop-by-hop: lists the next device in the path to the destination, fundamental in the IP/Network layer

Networks are subject to a number of issues; hardware failures, QoS, Congestion, Bottlenecks, Latency

Hardware failures:

- Causes links to become unavailable
- Causes routes to be re-routed
- Causes temporary increase in network traffic as topologies are updated in the routing table
- Causes disruption and some delay in the end-to-end delivery

Solution…

- Replacement hardware
- Service level agreement that provides replacement hardware

Network Issues:

Effective routing is based on several features…

- Adequate bandwidth: when designing networks we must ensure that the bandwidth will be able to cope with the intended volume of data (e.g. 10mbps will struggle with 10gb)
- Speed of data
- Network card speed
- Number of devices across the network
- Volume of traffic – throughput
- Good design

Speed of data transmission:

Determined by the…

- Bandwidth: backbone and cables to devices
- Speed of operation of the NIC
- Number of routers and switches involved in the route – causes latency

Managing Congestion:

To reduce the effects of congestion we can manage traffic queues…

- FIFO – first in first out, traffic is transmitted out of the interface in the order of arrival, no priorities
- WFQ – Weighted Fair Queueing – fair, dynamic queueing that divides bandwidth across queues of traffic based on weights

QoS:

- Quality of Service
- Traffic is prioritised
- Delay-sensitive traffic prioritised higher

Latency:

- The time it takes to get from source to destination
- Could be the result of…
    - Problems with the transmission medium itself
    - Errors with the router or switches as each device takes time to examine and change the packet header
    - Anti-virus and other security process that often require complete message disassembly and reassembly before sending
    - The propagation time of the time it takes for a packet to physically travel from its source to a destination
    - Software malfunctions at the user level can cause some delays from a user perspective

IP Addressing and Subnetting

IP Addresses:

- Almost every device connected to the network has an IP address
- Unique identifier for that device on the network

Network Classes

Class	Leading Bits	Size of *network* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start Address	End Address
A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
D	1110	N/D	N/D	N/D	N/D	224.0.0.0	239.255.255.255
E	1111	N/D	N/D	N/D	N/D	240.0.0.0	255.255.255.255

- We use classes A B, and C to address our network
- Classes D and E are reserved for experimental purposes
- IP address 127.0.0.1 is reserved as the loopback address – helps with troubleshooting connectivity issues, ping loopback will tell you if your NIC is functioning correctly or not

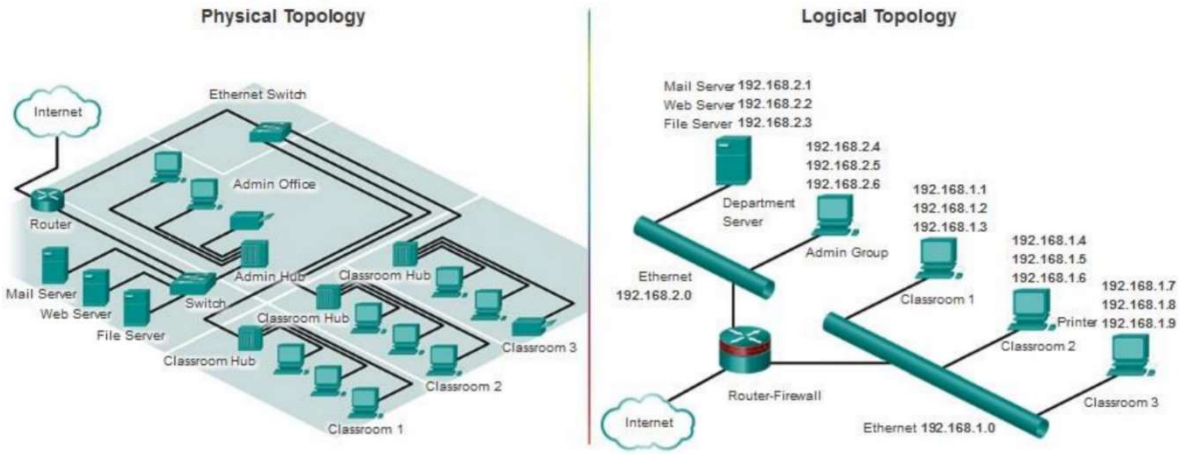
Subnet Masks:

- Each class has its own default subnet mask

Class A 10.10.10.10 **255.0.0.0**
Class B 172.16.25.14 **255.255.0.0**
Class C 192.168.10.1 **255.255.255.0**

Design Topologies:

- Two types: physical and logical
- Physical – the intended location of the devices
- Logical – the ip addresses for each device in that location



Network and Host:

- The router needs to know the network addresses and the switch uses the IP and MAC address
- To find out the network we can use the subnet mask

LEARN HOW TO DO SUBNETTING CALCULATIONS

Network and Host:

- There are numbers in the range that cannot be used for devices
- Total of 256 addresses from 0 to 255
- The network ID is represented with a 0
- The broadcast address is 255
- Leaving 254 available IP addresses to assign to devices 1-254

DCHP:

An IP address can either be manually assigned or automatically configured

Manually assigned…

- Every single node on the network must be configured individually
- Every IP address must be recorded against the machine it is assigned to
- Only useful where nodes need to be known and not change IP address e.g. printers, servers, routers

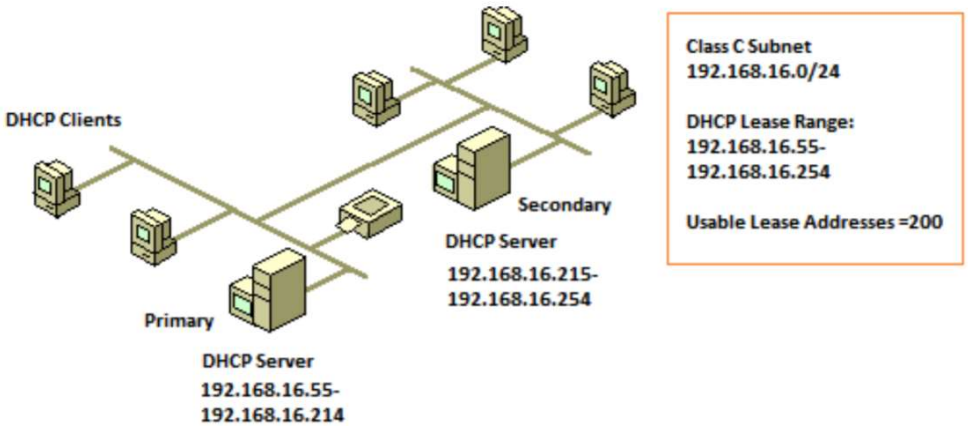
Automatically Configured:

- DHCP – Dynamic Host Configuration Protocol
- Responsible for assigning IP addresses to network nodes
- IP addresses are leased to the nod
- Can change anytime between 24hrs and 30 days
- Node requests a new IP when the lease is up – its often the same address
- Exception…
    - If a device is assigned an IP address that starts 169.252.x.x then it is unable to contact a DHCP server

- This means it will not be given an IP address for the network and will not be able to communicate with other devices
- This IP address is called an APIPA – automatic private IP addressing

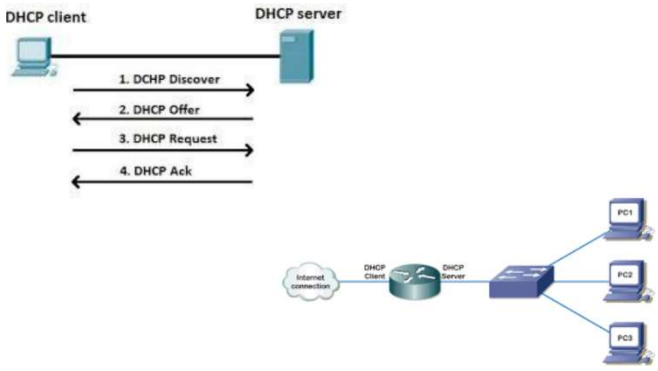
DHCPv4 Operation:

- Works in client/server mode
- Server(s) has a pool of IP addresses
- Shares workload during busy periods and provides redundancy



4 step process…

1. DHCPDISCOVER message is broadcast to find DHCP servers on the network
2. When the DHCP server receives a DHCPDISCOVER message it reserves an IP address and creates an ARP entry of the MAC address of the requesting node. A DHCPOFFER message is sent as a Unicast using the L2 MAC address of the server as source and the L2 MAC address of the requesting node as destination
3. When the node receives the DHCPOFFER it sends back a DHCPREQUEST message. Sent as a broadcast to indicate to all DHCP servers that the offer has been accepted.
4. On receiving the DHCPREQUEST the server verifies the lease information by sending an ICMP and replies with a DHCPACK. The node logs the DHCP configuration information, performs an ARP lookup for the assigned address. If no response to the ARP, the node starts to use the address as its own.

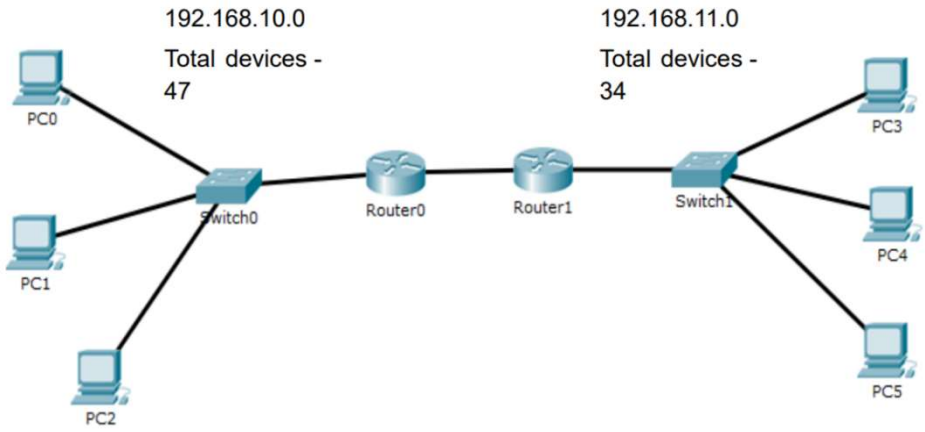


- Using IPv4 addresses on a LAN is fine
- Usually sufficient IP addresses for all devices

- Easy to set up – manually and DHCP
- Easy to maintain and troubleshoot
- Easy to learn
- When we run out of addresses for connecting devices, we subnet our network

Subnetting:

The process of dividing up the default IP address ranges to reduce the number of wasted IP addresses and increase the number of devices on the network



Subnet	Network Address	First IP Address	Last IP Address	Broadcast Address
0	0	1	62	63
1	64	65	126	127
2	128	129	190	191
3	192	192	254	255
4	256			

How to calculate it:

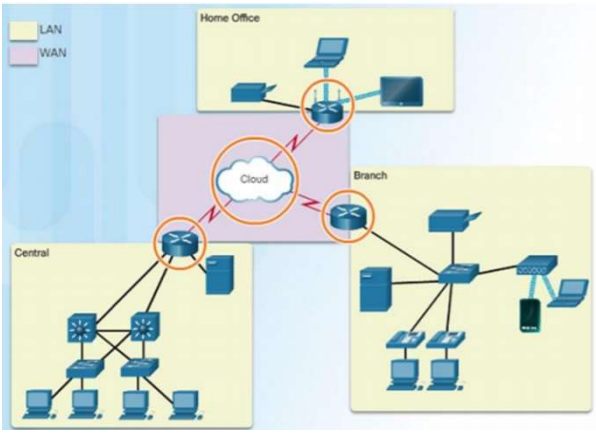
1. Work out how many hosts are needed
2. Write out the magic numbers
3. Draw a line where the number of hosts fits in the magic numbers
4. Write out the table using the headings
5. First network is always 0
6. First available IP address is always 1
7. What is the number on the left-hand side of the line?
8. Add this to the network and continue to add until you reach 256 (no more bits available to turn to 1)
9. Then add one to the first IP address
10. To get the broadcast take the network address on the next line and subtract 1
11. To get the last address subtract 1 from the broadcast address

Network Routing

Characteristics of a Network

Routing:

- Connects networks together regardless of the type of network or traffic being transmitted
- Determines the best and most efficient path to forward data between routers
- Connect LANs and WANs together



The Router

Memory	Description
Random Access Memory (RAM)	Volatile memory that provides temporary storage for various applications and processes including: • Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
Read-Only Memory (ROM)	Non-volatile memory that provides permanent storage for: • Bootup instructions • Basic diagnostic software • Limited IOS in case the router cannot load the full featured IOS
Non-Volatile Random Access Memory (NVRAM)	Non-volatile memory that provides permanent storage for the: • Startup configuration file
Flash	Non-volatile memory that provides permament storage for: • IOS • Other system-related files

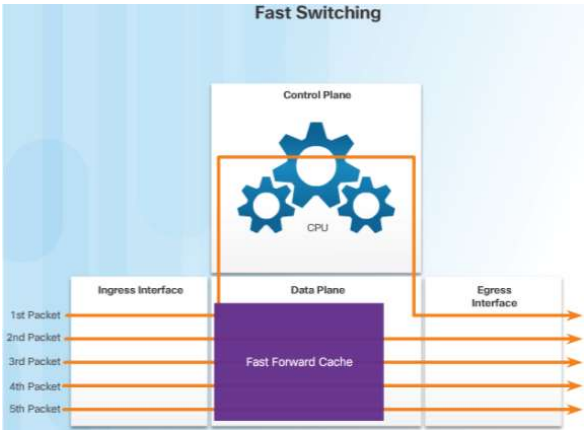
Primary function of a Router:

- Deteremine best path to send packets
- Forward packets toward their destination
- When a router receives a packet, it examines the destination address of the packet and uses the routing table to look for the best path to that network – when a match is found, the router encapsulates the packet into the data link frame of the outgoing exit interface and then forwards the packet out that interface to its destination
- A router can handle different data link layer frame encapsulations – the router might receive a frame from its ethernet interface. It will have to de-encapsulate the packet to search the routing table for a matching network. Once it finds a match, it will encapsulate it inside of the corresponding frame required for the outgoing interface such as PPP (point-to-point) frame

Packet Forwarding Mechanisms:

Routers support 3 packet-forwarding mechanisms…

- Process Switching
    - Slower and older packet forwarding mechanism
    - Packet arrives on an interface, it is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table in order to determine the exit interface
    - Slower because it does this for every packet in a stream
- Fast Switching
    - Common packet forwarding mechanism which uses a fast-switching cache to store the next-hop information
    - Packet arrives on an interface, it is forwarded to the control plane where the CPU searches for a match in the fast-switching cache
    - If no match, it is process-switched and forwarded to the exit interface
    - Packet flow information stored in the fast-switching cache for quick lookup

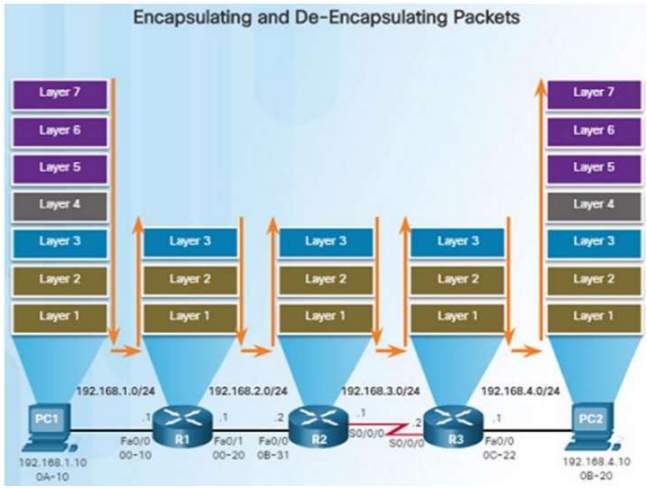


- Cisco Express Forwarding (CEF)
    - Fastest, most recent, and preferred packet-forwarding mechanism
    - CEF builds a Forwarding Information Base (FIB) and an adjacency table
    - Table entries are not packet-triggered like fast switching, but change-triggered when something changes in the network topology
    - When a network has converged, the FIB and adjacency tables contain all the information a router would have to consider when forwarding a packet
    - FIB contains pre-computed reverse lookups, next hop information for routes including the interface and layer 2 information

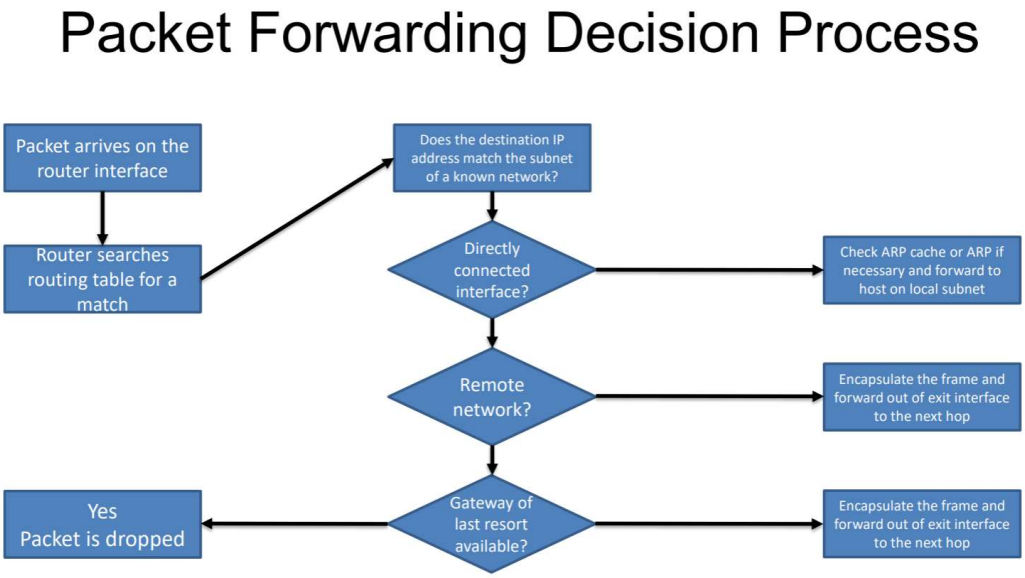
Routing between networks:

When a router receives a packet from one network that is destined for another network, the router performs the following steps…

1. De-encapsulates the layer 2 frame header and trailer to expose the layer 3 packet
2. Examines the destination IP address of the IP packet to find the best path in the routing table
3. If the router finds a path to the destination, it encapsulates the layer 3 packet into a new layer 2 frame and forwards the frame out the exit interface



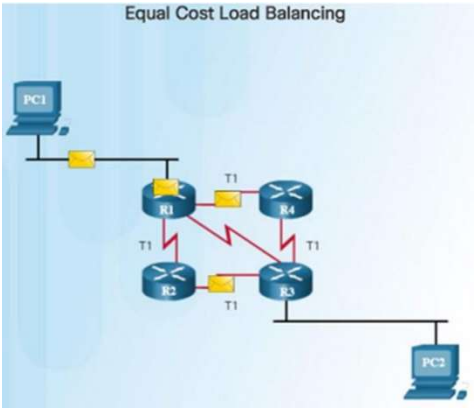
- As a packet travels from the source device to the destination device, the layer 3 IP addresses do not change. However, the layer 2 data link addresses change at every hop as it is de-encapsulated and re-encapsulated



Best path determination and Metrics:

- Best path is calculated to determine the optimum or shortest path to reach a network
- Calculated on the metric used by the routing protocol, usually the lowest value
- Routing Information Protocol (RIPP – hop count
- Open Shortest Path First (OSPF) – cumulative bandwidth from source to destination
- Enhanced Interior Gateway Protocol (EIGRP) – bandwidth, delay, load, reliability

Load Balancing:



- If a router has two or more paths with identical metrics to the same destination network, the router will forward the packets using both paths equally
- The routing table contains a single destination network, but has multiple exit interfaces – one for each equal cost path. Known as equal cost load balancing
- Benefits:
    - Load balancing can increase the effectiveness and performance of the network
    - Equal cost load balancing can be configured to use both dynamic routing protocols and static routes
    - EIGRP supports unequal cost load balancing

Administrative Distances:

- Where multiple protocols are configured and static routes are also available, it is possible to have multiple routes to the same destination network
- Each routing protocol might prefer a different path, how do the routes choose? By using Administrative Distance (AD)
- Represents the trustworthiness of the route – the lower the better

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route (Enhanced Interior Gateway Routing Protocol)	5
External BGP (Border Gateway Protocol)	20
Internal BGP	90
IGRP (Interior Gateway RoutingProtocol)	100
OSPF (Open Shortest Path First)	110
IS-IS (Intermediate System to Intermediate System)	115
RIP (Routing Information Protocol)	120
External EIGRP	170
Internal BGP	200

How do we know about routes?

- The routing table contains all the available routes
- Stored in RAM
- Identifies the next hop for remote networks
    - Directly connected – obtained from the active router interfaces
    - Remote networks – statically configured or learned from dynamic routing protocols

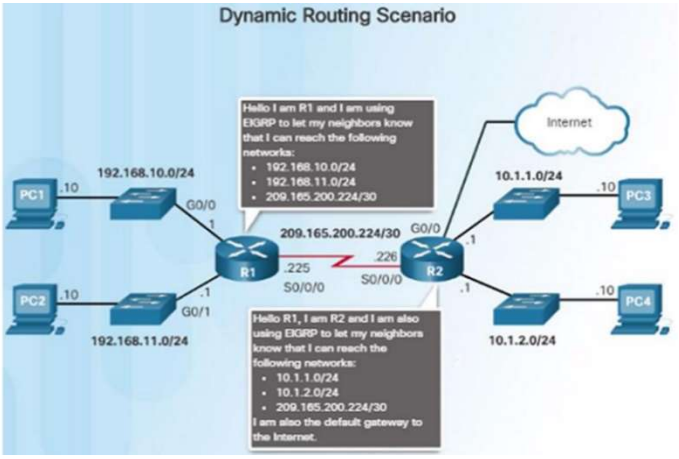
Static Routes:

- Manually configured routes between two points
- Define an explicit path
- If the topology changes static routes can only be changed manually
- Require less bandwidth
- Routes do not have to calculate the route so no CPU cycles are required
- Indicated by an S in the routing table
- S* shows it is a candidate for the static default route

Default Static Route:

- Similar to a gateway
- Specifies an exit point when the routing table does not have a path for the destination network
- In IPv4 it is known as quad zero 0.0.0.0 0.0.0.0
- In IPv6 it is ::/0

Dynamic Routing:



- Dynamic routing protocols share information about the status and reachability of remote networks
- Use the network discovery to share network information with other routers using the same protocol
- All this information is added to the routing table
- Once all the topology information has been exchanged, the network has converged
- If there are changes to the topology such as a link of route failure, dynamic routing protocols will calculate a new route automatically
- Do no need any manual intervention to change routes

Dynamic Routing Protocols:

Three types…

1. Distance vector
2. Link-state
3. Path vector

- RIP Protocol was updated to RIPv2 to accommodate the growth in the network environment – RIPv2 does not scale to current larger network implementations
- Routing protocols developed to meet the need of larger networks include: Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), Enhanced IGRP (EIGRP)
- Border Gateway Protocol (BGP) is used between Internet service providers

Algorithms:

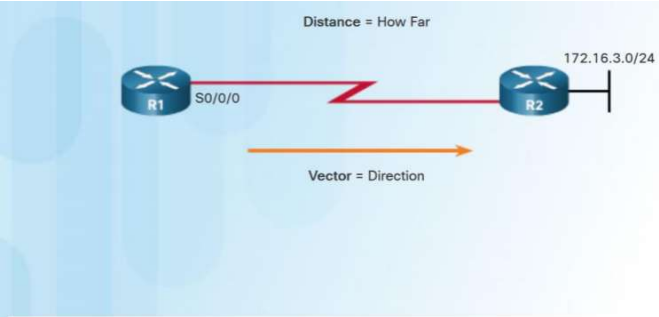
- RIP used the Bellman-Ford algorithm as its routing algorithm
- IGRP and EIGRP use Diffusing Update Algorithm (DUAL) routing algorithm

Distance Vector Routing Protocols:

Distance vector means that routes are advertised by providing two characteristics…

1. Distance – identifies how far it is to the destination network based on a metric such as hop count, cost, bandwidth, delay
2. Vector – specifies the direction of the next-hop router or exit interface to reach the destination

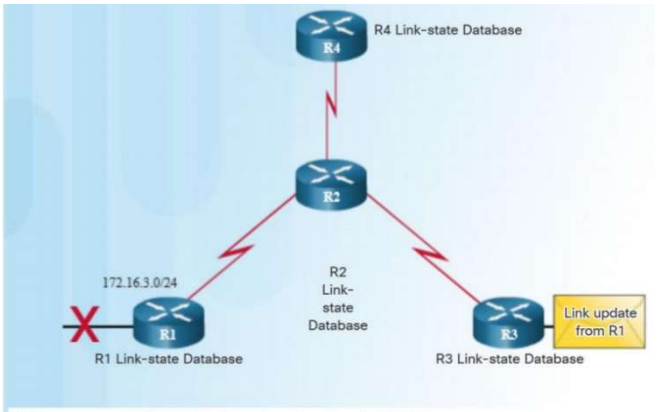
- RIPv1 (legacy), RIPv2, IGRP, EIGRP



For R1, 172.16.3.0/24 is one hop away (distance). It can be reached through R2 (vector).

Link-State Routing Protocols:

- A link-state router uses the link-state information received from other routers to create a topology map and to select the best path to all destination networks in the topology
- Link-state routing protocols do not use periodic updates
- Updates are only sent when there is a change in the topology
- OSPF and IS-Is are link-state routing protocols



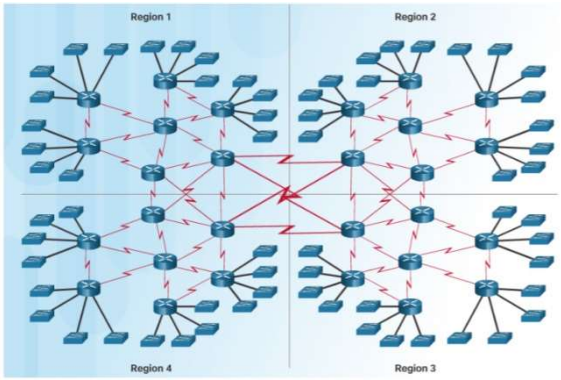
Link-state protocols forward updates when the state of a link changes.

Components of Dynamic Routing Protocols:

- Data structures – tables or databases kept in RAM
- Routing protocol messages – to discover neighbouring routers, exchange routing information, and maintain accurate information about the network
- Algorithms – to facilitate learning routing information and best path determination

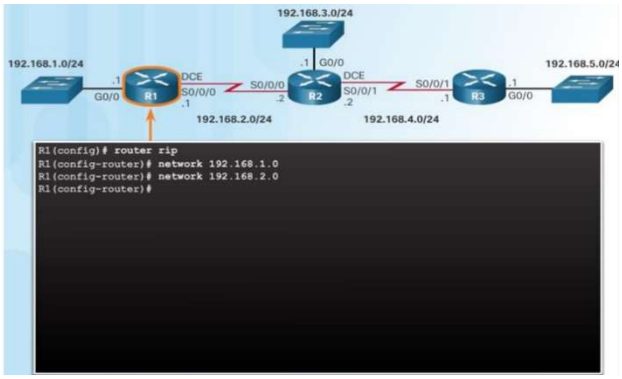
Dynamic Routing Protocol Uses:

- Dynamic routing is the best choice for large networks
- Dynamic routing protocols help the network administrator manage the network by providing redundant paths, and automatically implementing the alternate path when a link goes down

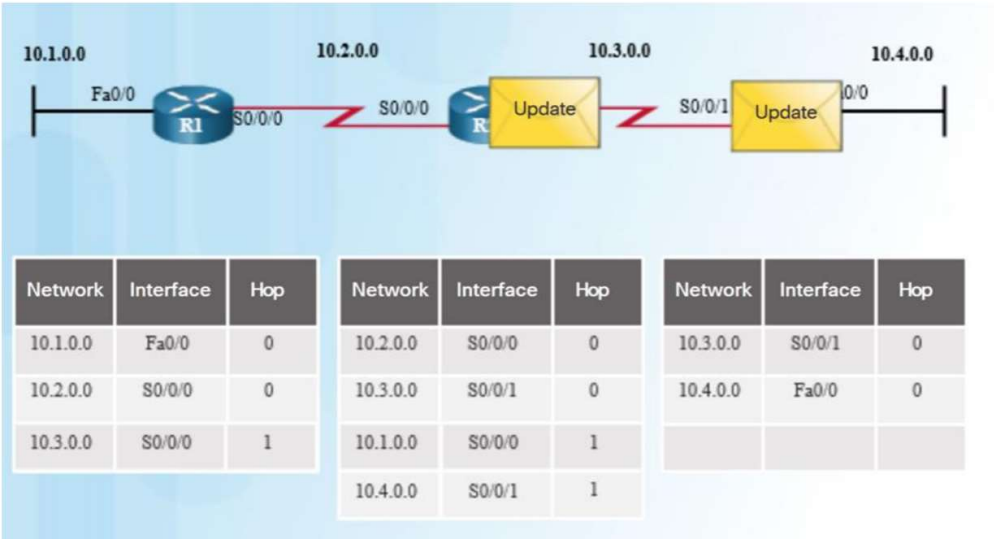


Routing Information Protocol – RIP & RIPv2:

- RIP is a simple routing protocol
- Easy to configure and maintain
- Administrator configures each router interface with the attached networks
- Updates are sent to all other routers every 30 seconds



RIP - Routing Table



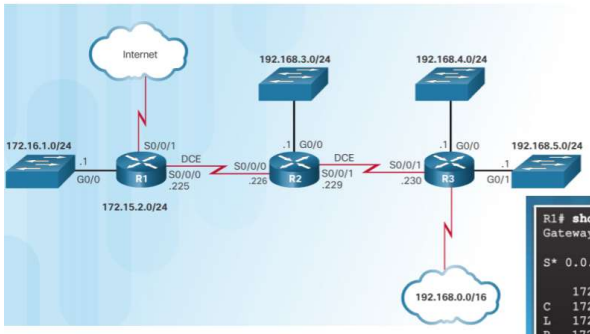
Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0

- The routing table displays the RIP routes configured on that router and the path to take to get to each network
- Interfaces can be configured to stop sending updates out – passive interface

Routing Table



- Directly connected networks are added automatically
- Identified by C and L

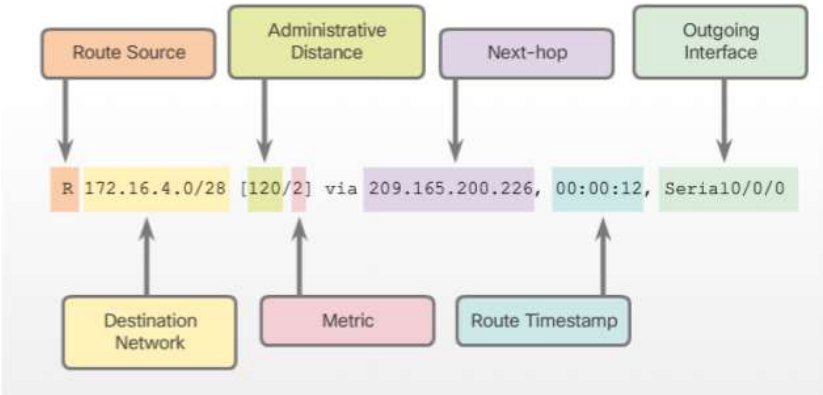
```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                   is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C    172.16.1.0/24 is directly connected, GigabitEthernet0/0
L    172.16.1.1/32 is directly connected, GigabitEthernet0/0
R    172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
R    172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R    172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R    192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
     209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C    209.165.200.224/30 is directly connected, Serial0/0/0
L    209.165.200.225/32 is directly connected, Serial0/0/0
R    209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
C    209.165.200.232/30 is directly connected, Serial0/0/1
L    209.165.200.233/30 is directly connected, Serial0/0/1
R1#
```

- Other routes:
  - S Static Route
  - D EIGRP
  - O OSPF
  - R RIP

Routing Table:

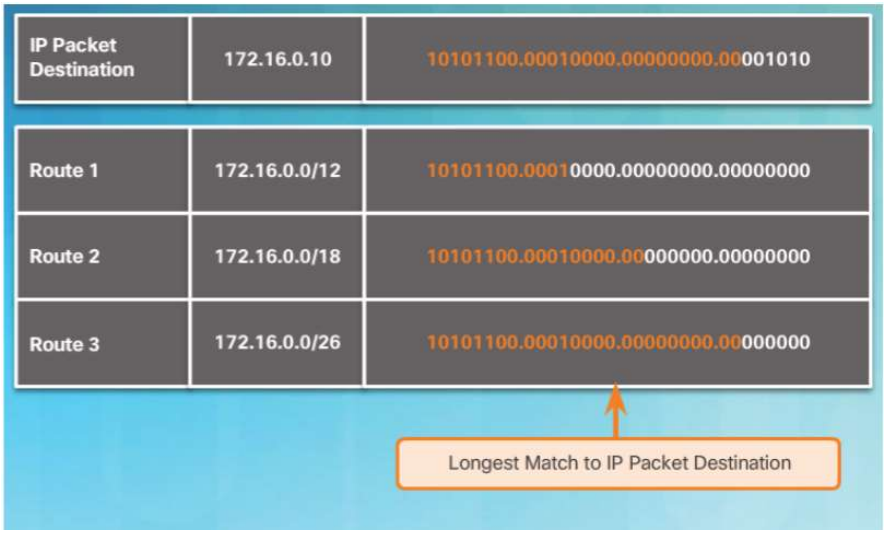
Routes to remote networks contain the following information…

- Route source – how route was learned
- Destination network
- Administrative distance – trustworthiness of route
- Metric – value assigned to reach the remote network (lower is better)
- Next hop – Ipv4 address of the next router that the packet should be forwarded to
- Route timestamp – time since the route was updated
- Outgoing interface – the exit interface to use to forward the packet

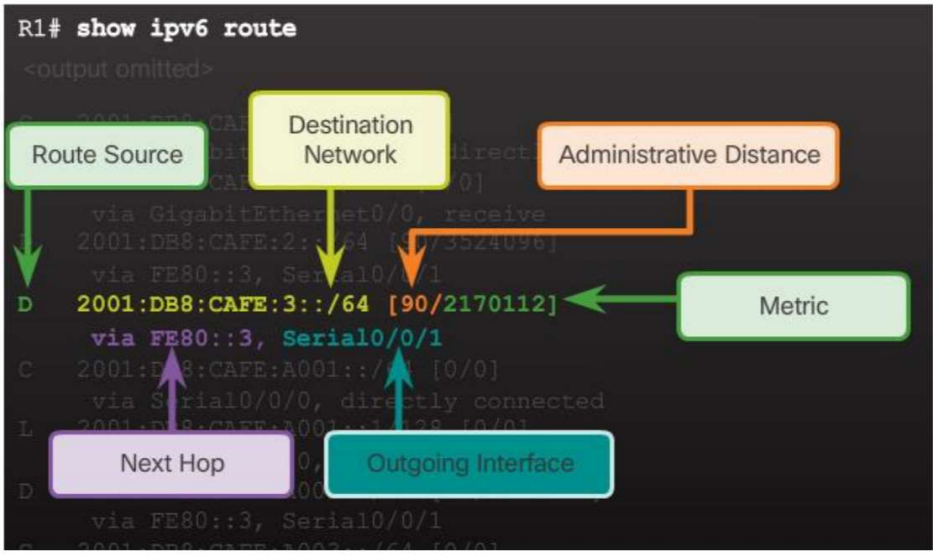


Best path:

- The best match is the route in the routing table that has the most number of far left matching bits with the destination IPv4 address of the packet
- The route with the greatest number of equivalent far left bits, or the longest match, is always the preferred route

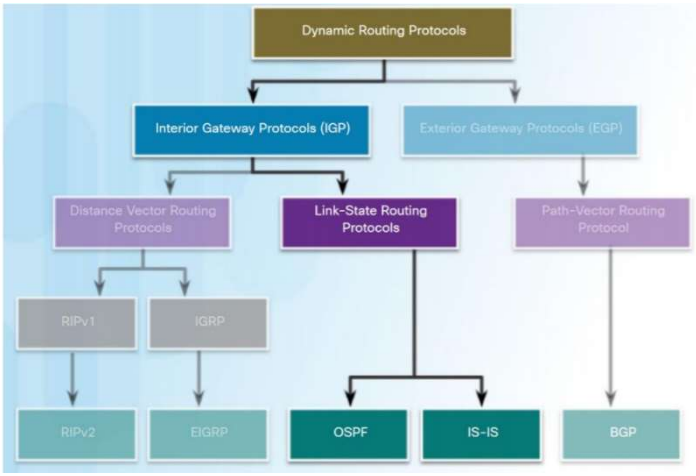


IPv6 Routes



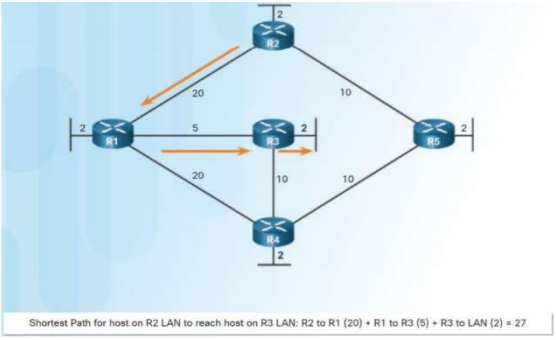
Shortest Path First Protocols:

- Link-state routing protocols, aka shortest path first protocols
- Built around Dijkstra's shortest path first (SPF) algorithm
- IPv4 link-state routing protocols: Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS)



Link-State Routing Protocol Operation – Dijkstra's Algorithm:

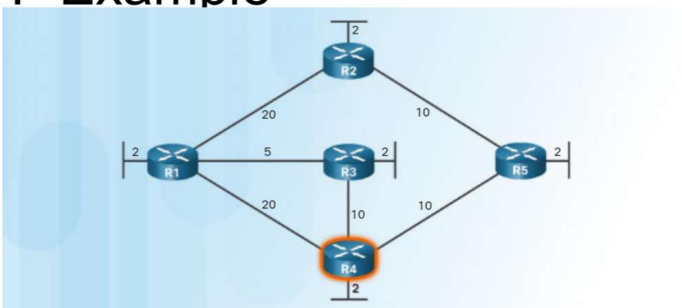
- All link-state routing protocols apply Dijkstra's algorithm to calculate the best path route
- Uses accumulated costs along each path, from source to destination
- Each router determines its own cost to each destination in the topology



Link-State Routing Protocol Operation

SPF Example

- The table displays the shortest path and the accumulated cost to reach the identified destination networks from the perspective of R4.



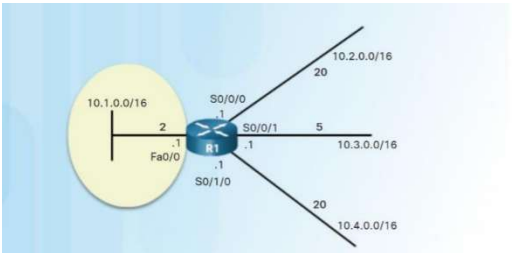
Destination	Shortest Path	Cost
R1 LAN	R4 to R3 to R1	17
R2 LAN	R4 to R5 to R2	22
R3 LAN	R4 to R3	12
R5 LAN	R4 to R5	12

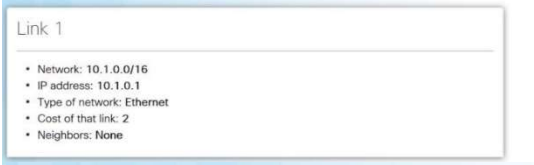
Link-State Routing Process:

- Each router learns about its own directly connected networks
- Each router is responsible for 'saying hello' to its neighbours on directly connected networks
- Each router builds a link-state packet (LSP) containing the state of each directly connected link
- Each router floods the LSP to all neighbours who then store all LSPs received in a database
- Each router uses the database to construct a complete map of the topology and computers the best path to each destination network
- This process is the same for both OSPF for IPv4 and OSPF for IPv6

Link and Link State:

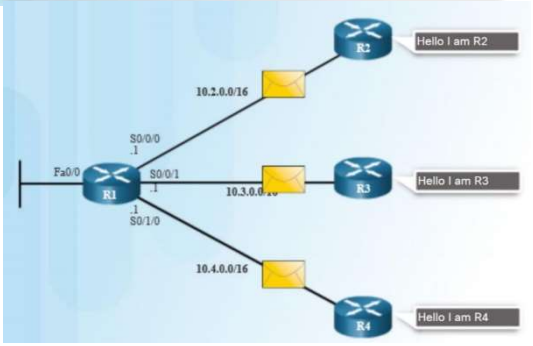
The first step in the link-state routing process is that each router learns its own directly connected networks





Say Hello:

- The second step in the link-state routing process is that each router uses a Hello protocol to discover any neighbours on its links
- When two link-state routers learn that they are neighbours, they form an adjacency
- If a router stops receiving hello packets from a neighbour, that neighbour is considered unreachable

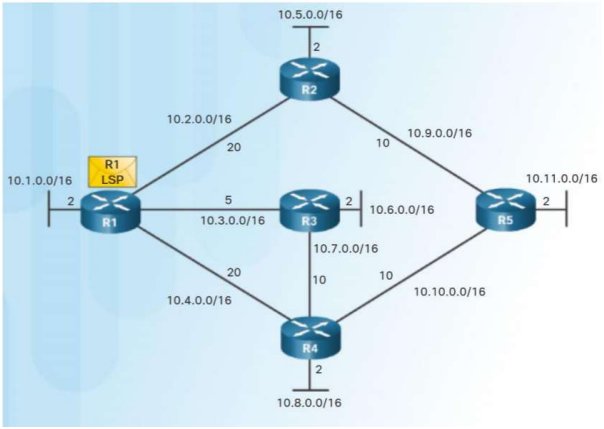


Building the Link-State Packet:

The third step on the link-state routing process is that each router builds a link-state packet (LSP) that contains the link-state information about its links

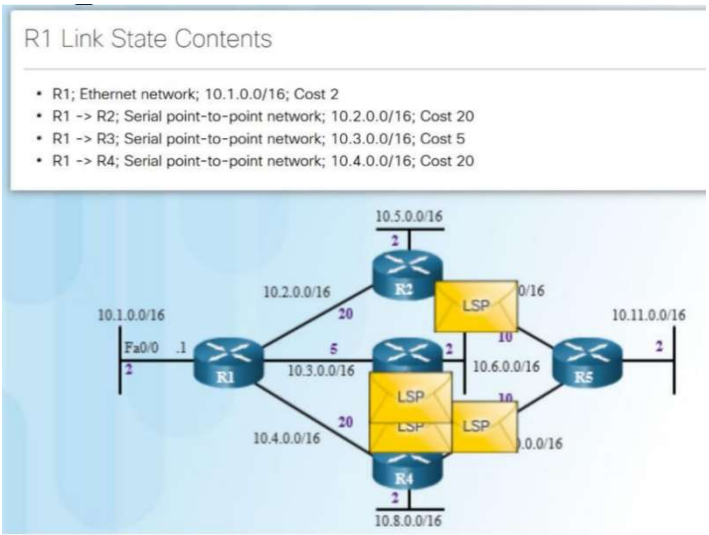
R1 LSP (in diagram) would contain:

- R1; Ethernet network 10.1.0.0/16; Cost 2
- R1 -> R2; Serial point-to-point network; 10.2.0.0/16; Cost 20
- R1 -> R3; Serial point-to-point network; 10.3.0.0/16; Cost 5
- R1 -> R4; Serial point-to-point network; 10.4.0.0/16; Cost 20



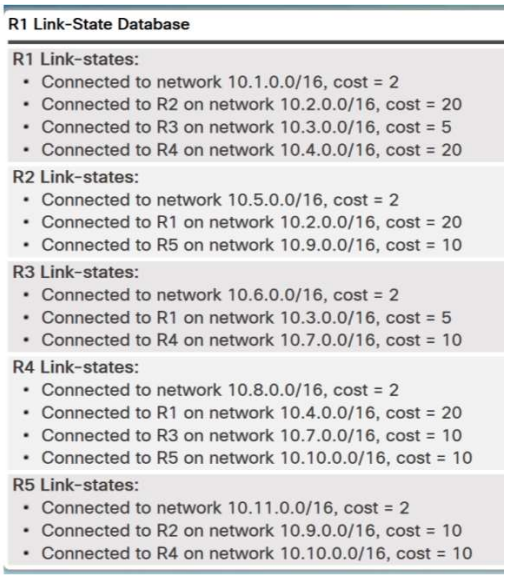
Flooding the LSP:

- The fourth step in the link-state routing process is that each router floods the LSP to all neighbours
- An LSP only needs to be sent during initial start-up of the routing protocol process on that router (e.g. router restart), or whenever there is a change in the topology (e.g. a link going down)
- An LSP also includes sequence numbers and aging information
- Used by each router to determine if it has already received the LSP
- Used to determine if the LSP has newer information



Building the Link-State Database:

The final step in the link-state routing process is that the router uses the database to construct a complete map of the topology and computes the best path to each destination network



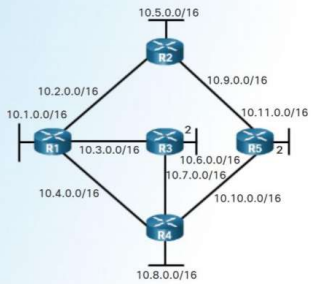
Building the SPF Tree:

- Each router uses the link state database and SPF algorithm to construct the SPF tree

- Each router constructs its own SPF tree independently from all other routers

- R1 identifies its directly connected networks and costs.
- R1 adds any unknown networks and associated costs.
- The SPF algorithm then calculates the shortest paths to reach each individual network resulting in the SPF tree shown in the diagram.

Destination	Shortest Path	Cost
10.5.0.0/16	R1 → R2	22
10.6.0.0/16	R1 → R3	7
10.7.0.0/16	R1 → R3	15
10.8.0.0/16	R1 → R3 → R4	17
10.9.0.0/16	R1 → R2	30
10.10.0.0/16	R1 → R3 → R4	25
10.11.0.0/16	R1 → R3 → R4 → R5	27



Adding OSPF Routes to the Routing Table:

- Using the shortest path first information determined by the SPF algorithm, these best paths are then added to the routing table
- Directly connected routes and static routes are also included in the routing table

Destination	Shortest Path	Cost
10.5.0.0/16	R1->R2	22
10.6.0.0/16	R1->R3	7
10.7.0.0/16	R1->R3	15
10.8.0.0/16	R1->R3->R4	17
10.9.0.0/16	R1->R2	30
10.10.0.0/16	R1->R3->R4	25
10.11.0.0/16	R1->R3->R4->R5	27

R1 Routing Table

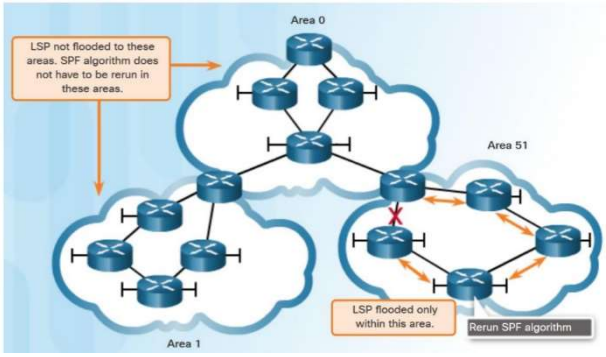
- 10.2.0.0/16 Directly Connected Network
- 10.3.0.0/16 Directly Connected Network
- 10.4.0.0/16 Directly Connected Network

Remote Networks

- 10.5.0.0/16 via R2 serial 0/0/0, cost = 22
- 10.6.0.0/16 via R3 serial 0/0/1, cost = 7
- 10.7.0.0/16 via R3 serial 0/0/1, cost = 15

Advantages of Link-State Routing Protocols:

- Each router builds its own topological map of the network to determine the shortest path
- Immediate flooding of LSPs achieves faster convergence
- LSPs are sent only when there is a change in the topology and contain only the information regarding that change
- Hierarchical design used when implementing multiple areas



Disadvantages of Link-State Protocols:

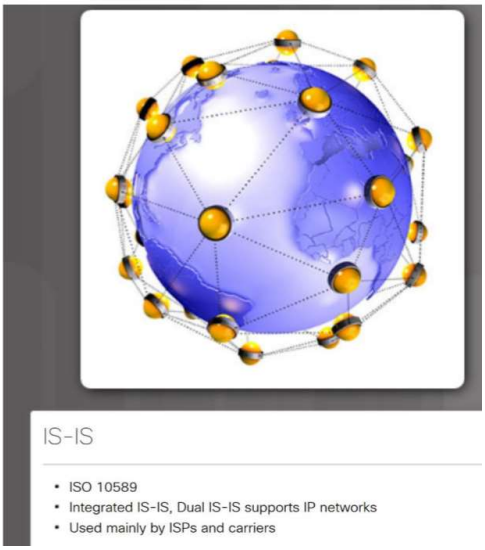
- Memory requirements – they require additional memory
- Processing requirements – can require more CPU processing

- Bandwidth requirements – the flooding of link-state packets can adversely affect bandwidth
- Using multiple areas can reduce the size of the link-state databases
- Multiple areas can limit the amount of link-state information flooding and send LSPs only to those routers that need them

Protocols that Use Link-State

- Two link-state routing protocols, OSPF and IS-IS.Open Shortest Path First (OSPF) - most popular implementation with two versions in use:
  - OSPFv2- OSPF for IPv4 networks (RFC 1247 and RFC 2328)
  - OSPFv3- OSPF for IPv6 networks (RFC 2740)
- Integrated IS-IS, or Dual IS-IS, includes support for IP networks.

–used mainly by ISPs and carriers.



Routing & Routing Protocols

Router:

- The router's job is to forward data between networks
- Uses the network portion of the IP address
- Determines whether the network is at this location or not
- Passes it to another router if it knows where that network is
- If not, it will send to the default route

Default Route:

- 0.0.0.0 aka quad zero
- Very useful address
- If a packet has no destination it can be sent to 0.0.0.0
- Can also be used to route data that is internet bound

Routers and Routes:

- Routes are learned in two ways; static and dynamic
- Static routes are manually added and do not change – good for point-to-point connections and also used for backup in the event of failures

Dynamic Routing:

- Basic dynamic routing algorithms have been in existence since 1969
- Used on Advanced Research Projects Agency Network (ARPANET)
- RIP – Routing Information Protocol 1988
- OSPF – open shortest path first
- BGP – border gateway protocol
- IS-IS – Intermediate System to intermediate system

Routing:

The purpose of dynamic routing protocols includes…

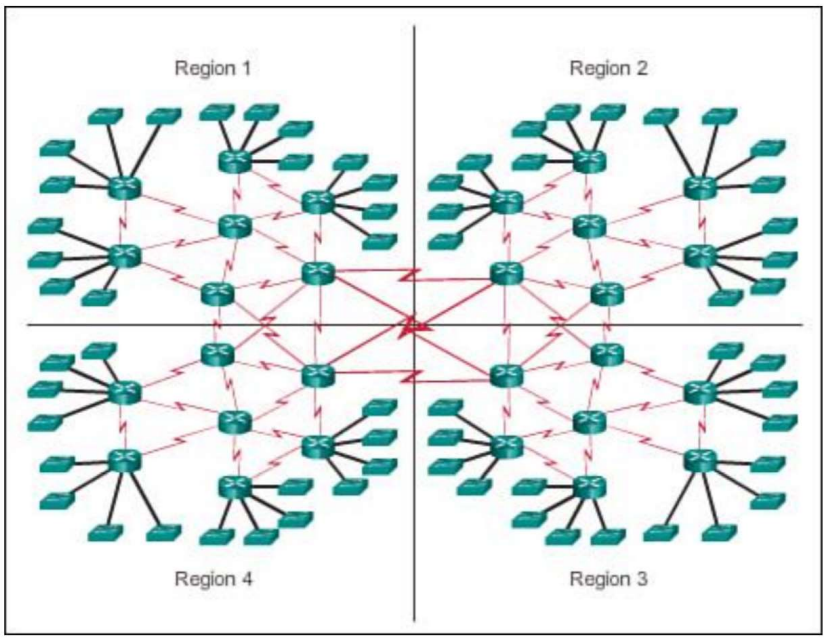
- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

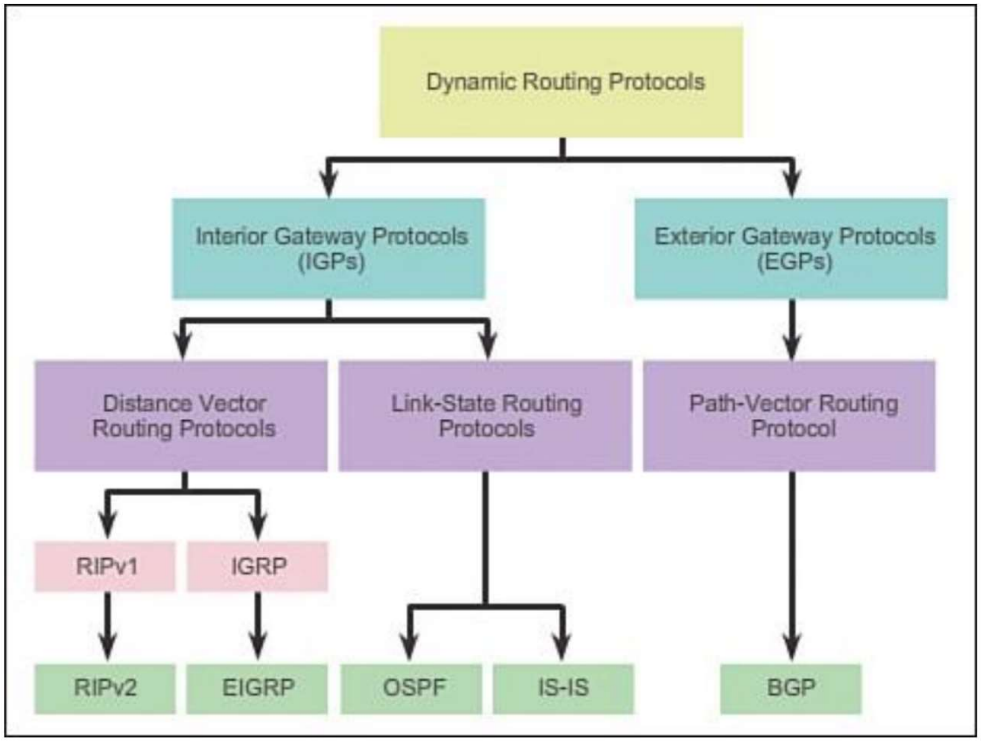
Dynamic Routing Protocols:

- Data structures: routing protocols typically use tables or databases for their operations. This information is kept in RAM
- Routing protocol messages: routing protocols use various types of messages to discover neighbouring routers, exchange routing information, and perform other tasks to learn and maintain accurate information about the network

- Algorithm: an algorithm is a finite list of steps used to accomplish a task. Routing protocols use algorithms for facilitating routing information and for best path determination.

The Need for Dynamic Routing





Link-State Routing Protocols:

- Creates a complete view of the network topology by exchanging information with other routers

- Sends updates to other routers if a link fails
- IS-IS and OSPF are link-state protocols
- Use Dijkstra's Algorithm to calculate the best path

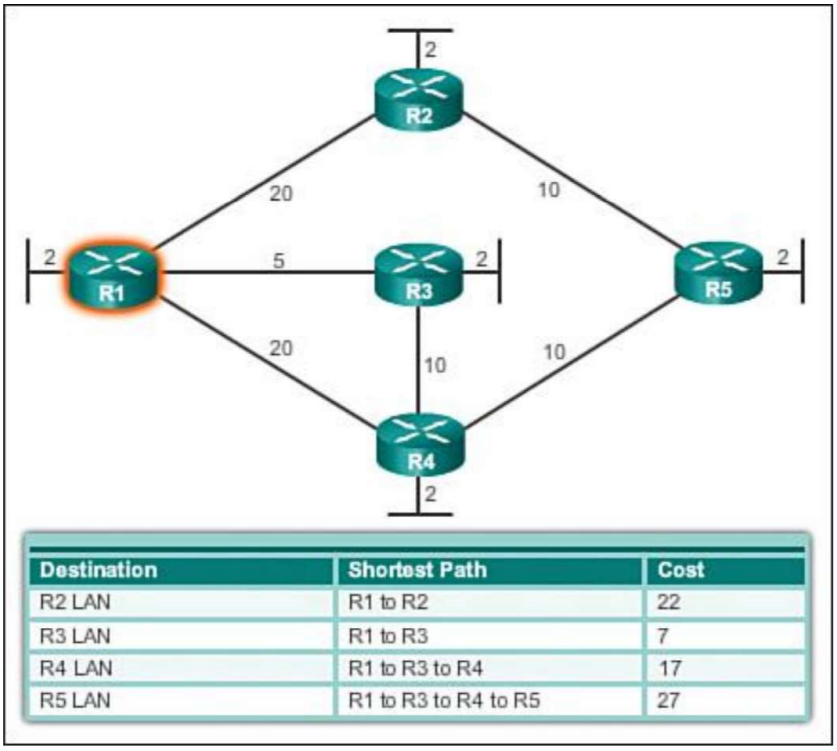
RIP:

- Routing information protocol
- Simple, easy to manage protocol
- Designed for small networks
- Does not scale well
- Broadcasts the entire network topology every 30 seconds
- TTL measured in hops – 16 is unreachable
- RIPv1 does not advertise subnet masks
- RIPv2 sends subnet masks
- Supports VLSM and CIDR

Comparison

Feature	**RIPv1**	**RIPv2**
Routing update address	Broadcast (255.255.255.255)	Multicast (224.0.0.09)
Variable Length Subnet Mask (VLSM)	Does not support	Supports
Classless Inter Domain Routing (CIDR)	Does not support	Supports
Authentication	Does not support	Supports MD5 authentication
Discontinuous network	Does not support	Supports

OSPF



Destination	Shortest Path	Cost
R2 LAN	R1 to R2	22
R3 LAN	R1 to R3	7
R4 LAN	R1 to R3 to R4	17
R5 LAN	R1 to R3 to R4 to R5	27

- Open Shortest Path First
- Uses Dijkstra's Algorithm
- Calculates the shortest path based on metrics
- Can be configured to use a route that has a slower transmission rate by altering the route metrics
- Load balances to ensure each route is used effectively
- Robust, reliable, and scalable

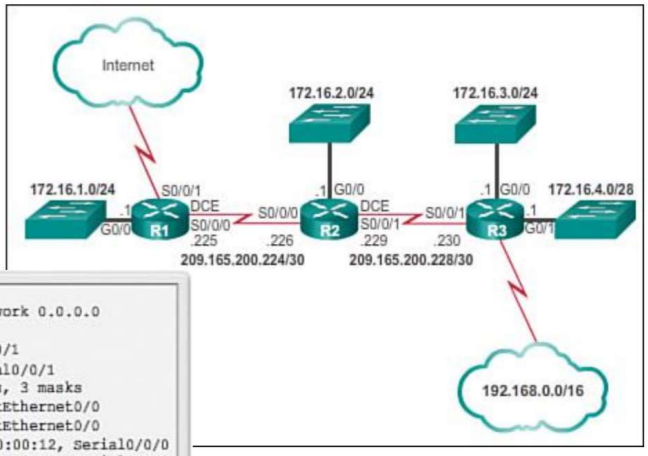
IGRP – interior gateway routing protocol

EIGRP – enhanced interior gateway routing protocol

BGP – border gateway protocol

IS-IS – intermediate system to intermediate system

Routing Table




```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                   is directly connected, Serial0/0/1
   172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C     172.16.1.0/24 is directly connected, GigabitEthernet0/0
L     172.16.1.1/32 is directly connected, GigabitEthernet0/0
R     172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R  192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
   209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C     209.165.200.224/30 is directly connected, Serial0/0/0
L     209.165.200.225/32 is directly connected, Serial0/0/0
R     209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
                    Serial0/0/0
C     209.165.200.232/30 is directly connected, Serial0/0/1
L     209.165.200.233/30 is directly connected, Serial0/0/1
R1#
```

IPv6 Routing Table

A comparison to IPv4

```
R1# show ipv6 route
<output omitted>

C   2001:DB8:CAFE:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:CAFE:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
D   2001:DB8:CAFE:2::/64 [90/3524096]
     via FE80::3, Serial0/0/1
D   2001:DB8:CAFE:3::/64 [90/2170112]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:A001::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:CAFE:A001::1/128 [0/0]
     via Serial0/0/0, receive
D   2001:DB8:CAFE:A002::/64 [90/3523840]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:A003::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:CAFE:A003::1/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

Distance Vector Protocols:

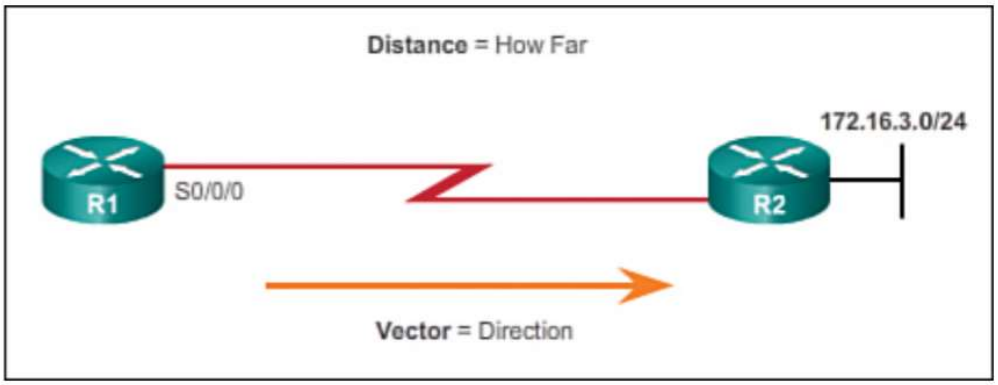
Routes are advertised based on two characteristics…

- Distance – how far is it to the destination network?
- Vector – the direction of the next router or exit interface

Metrics:

Distance vector protocols use metrics to calculate distance…

- Hop count – RIP
- Bandwidth – OSPF
- Cost – OSPF



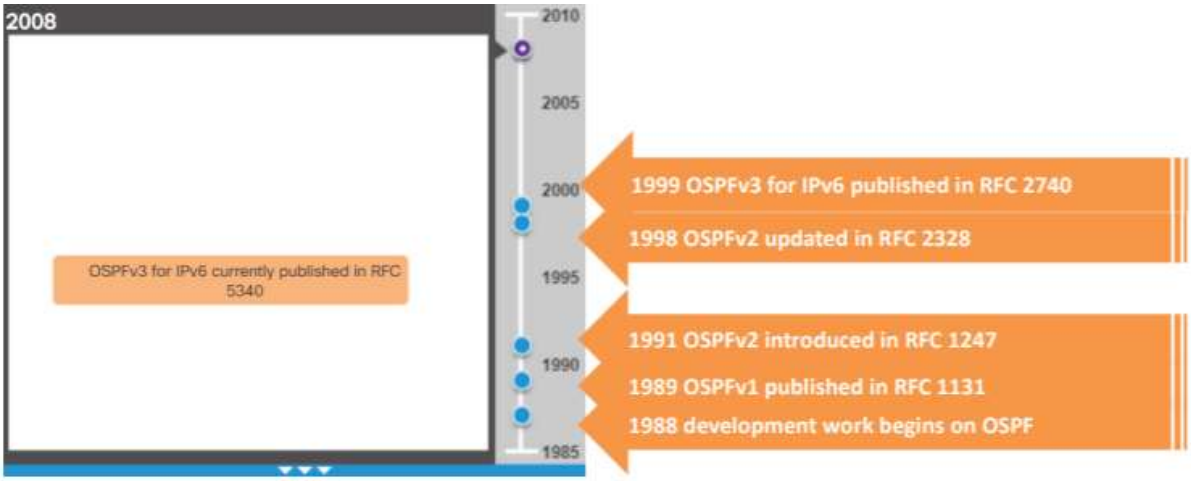
Routing with OSPF

Introducing OSPF:

- Complex routing protocol
- Open source protocol
- Found in common use
- Major feature is the ability to load balance
- Performs well
- Relatively easy to troubleshoot

Evolution of OSPF:

OSPF is a link-state routing protocol, referenced by a number of RFCs



Features of OSPF:

- Uses the Dijkstra shortest path first (SPF) algorithm to choose the best path
- Administrative distance is used in determining what route gets installed in the routing table when the route is learned from multiple sources – the lowest administrative distance is the one added to the routing table

Routing changes trigger routing updates

v2 supports MD5 and SHA authentication
v3 uses IPsec for authentication

Supports a hierarchical design system through the use of areas

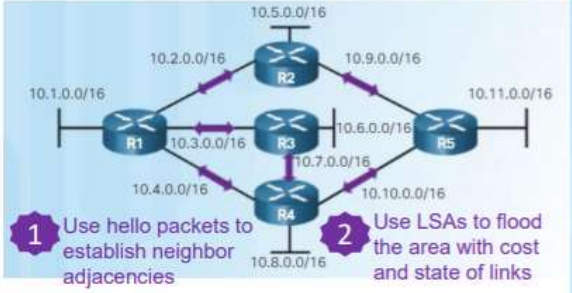
Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

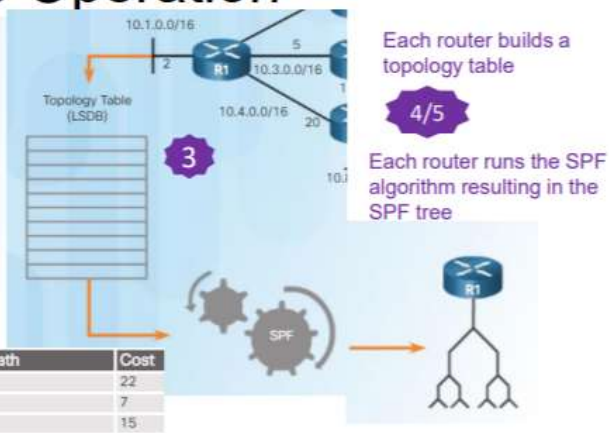
Components of OSPF

Database	Table	Description
Adjacency	Neighbor	• Lists all neighbor routers to which a router has established bidirectional communication • Unique for each router • View using the **show ip ospf neighbor** command
Link-state (LSDB)	Topology	• Lists information about all other routers • Represents the network topology • Contains the same LSDB as all other routers in the same area • View using the **show ip ospf database** command
Forwarding	Routing	• Lists routes generated when the SPF algorithm is run on the link-state database. • Unique to each router and contains information on how and where to send packets destined for remote networks • View using the **show ip route** command

OSPF packet types: hello, database description, link-state request, link-state update, link-state acknowledgment

Link-State Operation



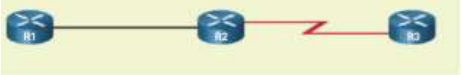


6 Each router builds a routing table that includes the path to get to the distant network and the cost to get there.

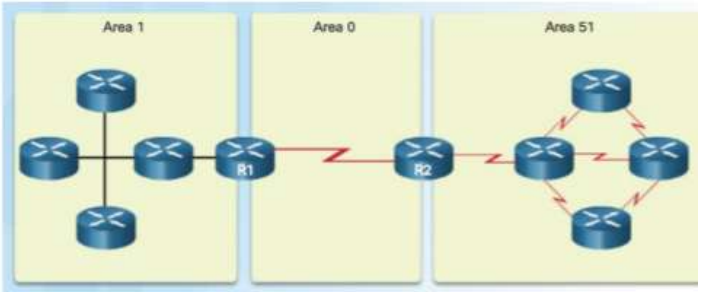
Destination	Shortest Path	Cost
10.5.0.0/16	R1→R2	22
10.6.0.0/16	R1→R3	7
10.7.0.0/16	R1→R3	15
10.8.0.0/16	R1→R3→R4	17
10.9.0.0/16	R1→R2	30
10.10.0.0/16	R1→R3→R4	25
10.11.0.0/16	R1→R3→R4→R5	27
10.5.0.0/16	R1→R2	22

Single-Area and Multiarea OSPF

Single-Area OSPF

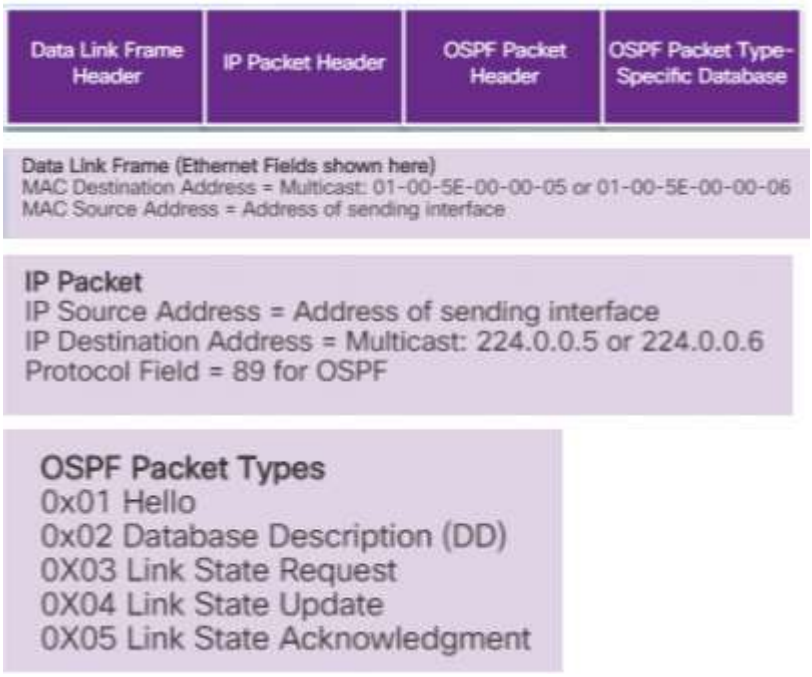


- All routers contained in one area
- Called the backbone area
- Known as Area 0
- Used in smaller networks with few routers



- Designed using a hierarchical scheme
- All areas connect to area 0
- More commonly seen with numerous areas around area 0 (like a daisy or aster)
- Routers that connect area 0 to another area is known as an Area Border Router (ABR)
- Used in large networks
- Multiple areas reduces processing and memory overhead
- A failure in one area does not affect other areas

Encapsulating OSPF Messages:

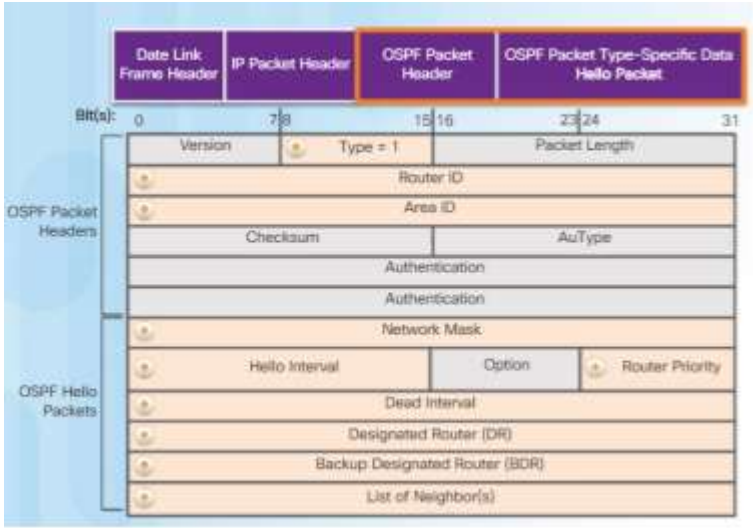


- OSPF adds its own Layer 3 header after the IP Layer 3 header – the IP header contains the OSPF multicast address of either 224.0.0.5 or 224.0.0.6 and the protocol field of 89 which indicates it is an OSPF packet
- OSPF packet header identifies the type of OSPF packet, the router ID, and the area ID
- OSPF packet type contains the specific OSPF packet type information router ID and area ID
- OSPFv3 has similar packet types

OSPF Packet Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	Database Description (DBD)	Checks for database synchronization between routers
3	Link-State Request (LSR)	Requests specific link-state records from router to router
4	Link-State Update (LSU)	Sends specifically requested link-state records
5	Link-State Acknowledgment (LSAck)	Acknowledges the other packet types

Hello Packet:

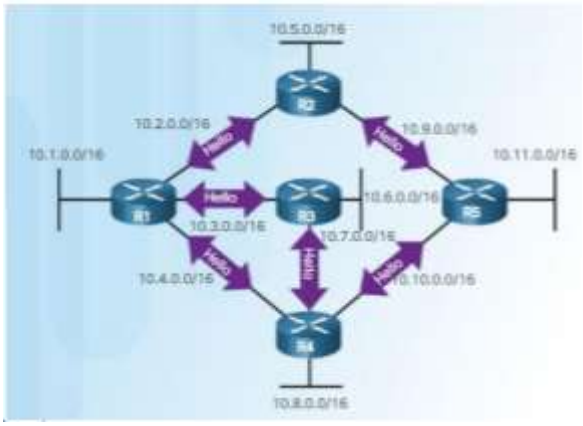
Hello packets are used to discover neighbours, establish neighbour adjacencies, advertise parameters both routers must agree upon in order to become neighbours, and elect the Designated Router (DR) and Backup Designated Router (BDR) on multi-access networks like Ethernet and Frame Relay (not serial point-to-point links)



Hello Packet Intervals:

- Hello and dead intervals must be the same interval setting on neighbouring routers on the same link
- Transmitted to multicast address 244.0.0.5 in IPv4
- Transmitted to multicast addresses FF02::5 in IPv6

- Sent every 10 seconds by default on multi-access networks like Ethernet and point-to-point links
- Sent every 30 seconds by default on non-broadcast multiple access networks (NBMA) like Frame Relay
- Dead intervals by default are 4 times the hello interval – if the dead interval expires before the router receives a hello packet, OSPF removes that neighbour from its link state database (LSDB), the router then floods the LSDB with info about the down neighbour



Link-State Updates:

- A link state update (LSU) contains one or more LSAs which contain route information for destination networks
- Routers initially send Type 2 DBD packets – an abbreviated list of the sending routers LSDB – receiving routers check against their own LSDB
- Type 3 LSR is used by the receiving router to request more information about an entry in the Database Description (DBD)
- Type 4 link-state update is used to reply to an LSR packet

OSPF Packet Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	DBD	Checks for database synchronization between routers
3	LSR	Requests specific link-state records from router to router
4	Link-State Update (LSU)	Sends specifically requested link-state records
5	LSAck	Acknowledges the other packet types

LSA Type	Description
1	Router LSAs
2	Network LSAs
3 or 4	Summary LSAs
5	Autonomous System External LSAs
6	Multicast OSPF LSAs
7	Defined for Not-So-Stubby Areas
8	External Attributes LSA for Border Gateway Protocol (BGP)
9, 10, 11	Opaque LSAs

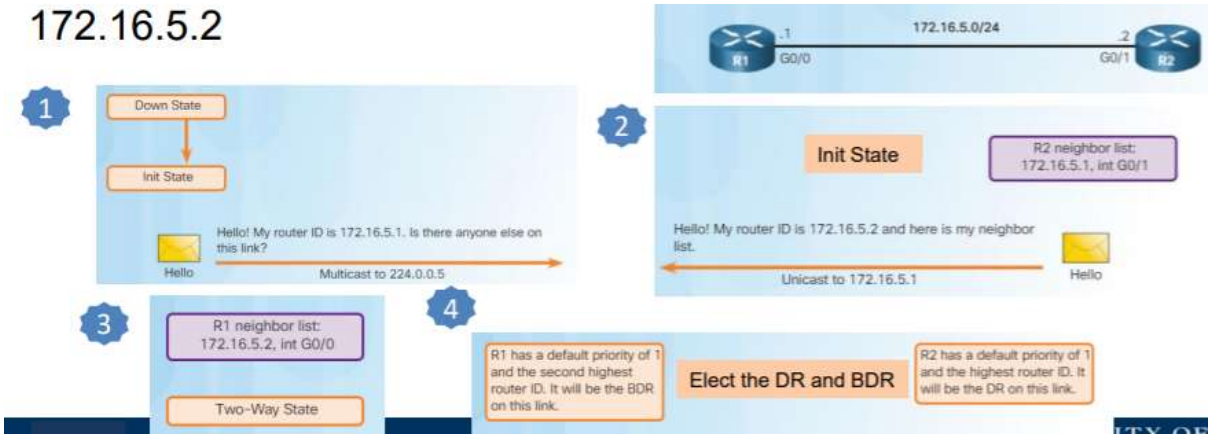
OSPF Operational States:

OSPF progresses through several states while attempting to reach convergence…

- Down – no hello packet received; router sends hello packet
- Init – hello packets are received that contain the sending router's ID
- Two-Way – used to elect a DR and a BDR on an Ethernet link
- ExStart – Negotiate master/slave relationship and DBD packet sequence number

Establish Neighbour Adjacencies:

Without a pre-configured router ID (RID) or lookup addresses, R1 has a RID of 172.16.5.1 and R2 has an RID of 172.16.5.2

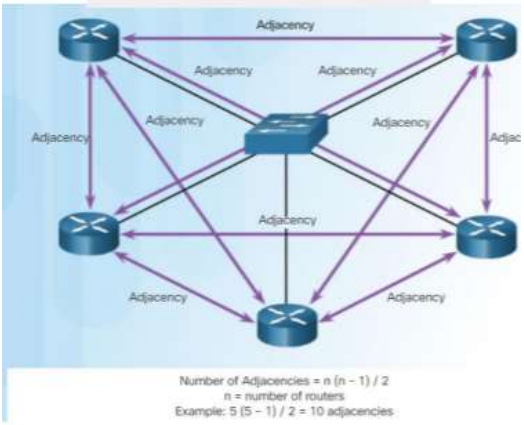


OSPF DR and BDR:

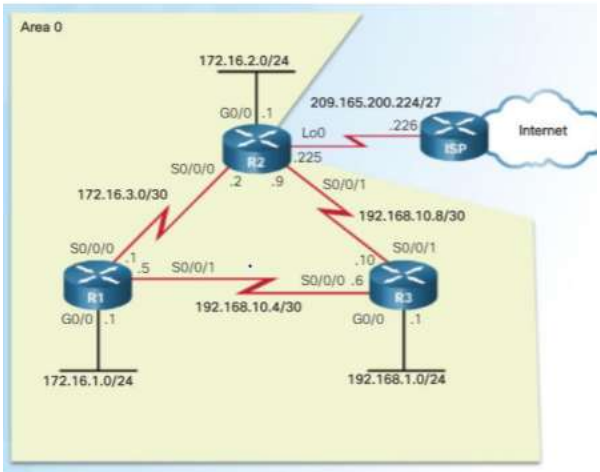
DR/BDR election…

- Reduce the number of LSAs sent – the DR is the only router used to send LSAs for the shared network
- Reduce the number of adjacencies over a multi-access network like Ethernet

Routers	Adjacencies
n	n (n - 1) / 2
5	10
10	45
20	190
100	4,950



Single-Area OSPFv2



OSPF Network Topology:

- Topology to describe OSPF configuration
- Defines the area or range of coverage
- Shows links to external networks – WAN links

Router OSPF Configuration Mode:

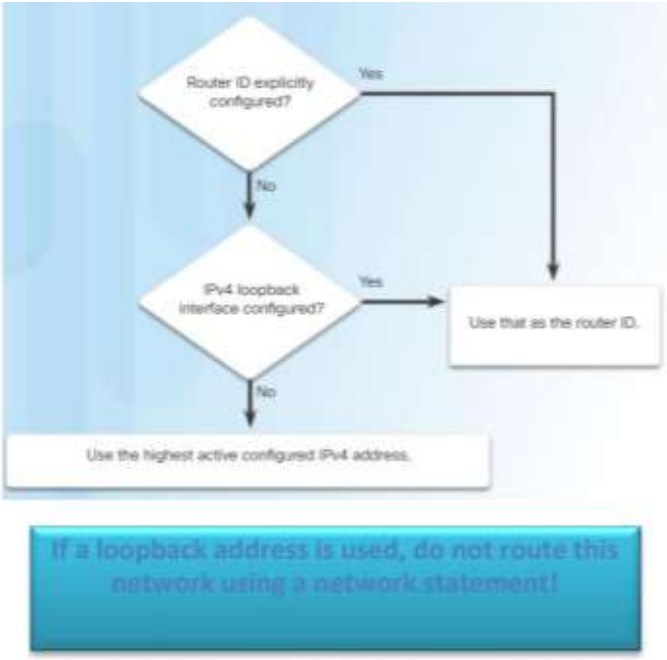
OSPFv2 configuration uses the router OSPF configuration mode – from global configuration mode, type router ospf process-id to enter commands

```
R1(config)# router ospf 10
R1(config-router)# ?
Router configuration commands:
auto-cost                   Calculate OSPF interface cost according to
                            bandwidth
network                     Enable routing on an IP network
no                          Negate a command or set its defaults
passive-interface           Suppress routing updates on an interface
priority                    OSPF topology priority
router-id                   router-id for this OSPF process
```

Router IDs:

- Router IDs are used to uniquely identify an OSPF router
- Router IDs are 32bits long in both OSPFv2 (IPv4) and OSPFv3 (IPv6)
- Used in the election of the DR if a priority number is not configured

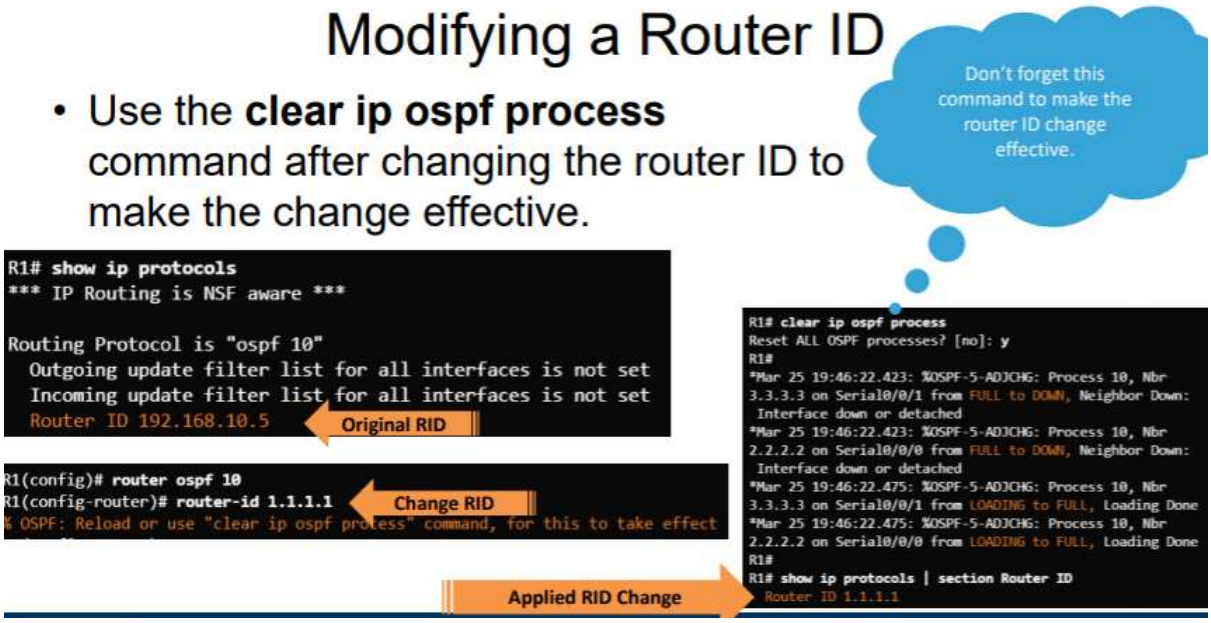
1. Configured using the router-id rid OSPF router configuration mode command
2. If a router ID is not configured, the highest configured loopback interface is used
3. If there are no configured loopback interfaces, then the highest active IPv4 address is used (not recommended because if the interface with the highest IPv4 address goes down, the router ID selection process starts over)



Configuring an OSPF Router ID:

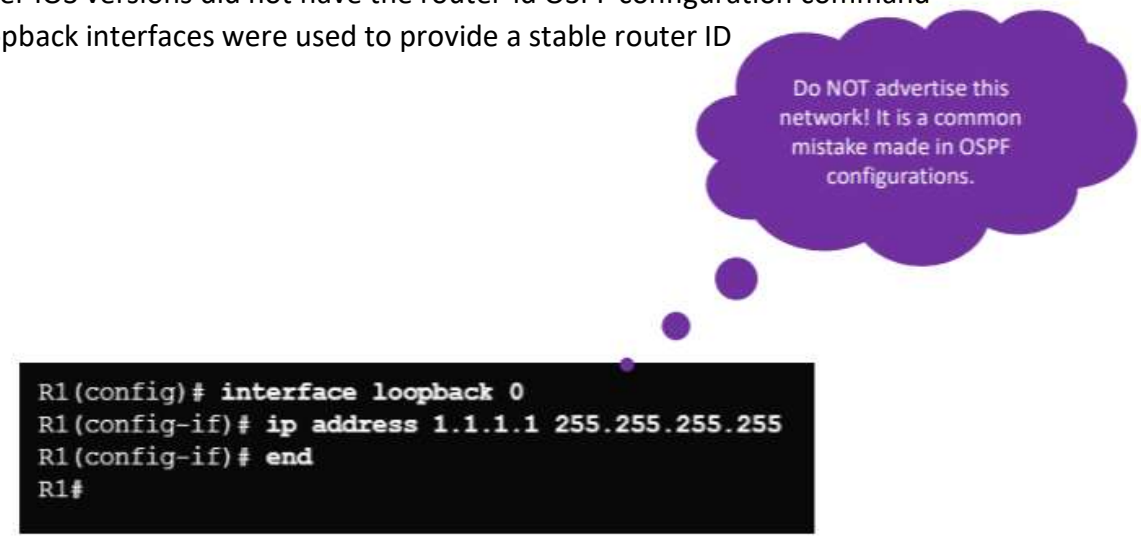
- Use the router-id x.x.x.x command to configure a router ID
- Use the show ip protocols command

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# end
R1#
*Mar 25 19:50:36.595: %SYS-5-CONFIG_I: Configured from console by console
R1#
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
   Outgoing update filter list for all interfaces is not set
   Incoming update filter list for all interfaces is not set
   Router ID 1.1.1.1
   Number of areas in this router is 0. 0 normal 0 stub 0 nssa
   Maximum path: 4
   Routing for Networks:
   Routing Information Sources:
   Gateway         Distance      Last Update
   Distance: (default is 110)
```



Using a Loopback interface as the Router ID:

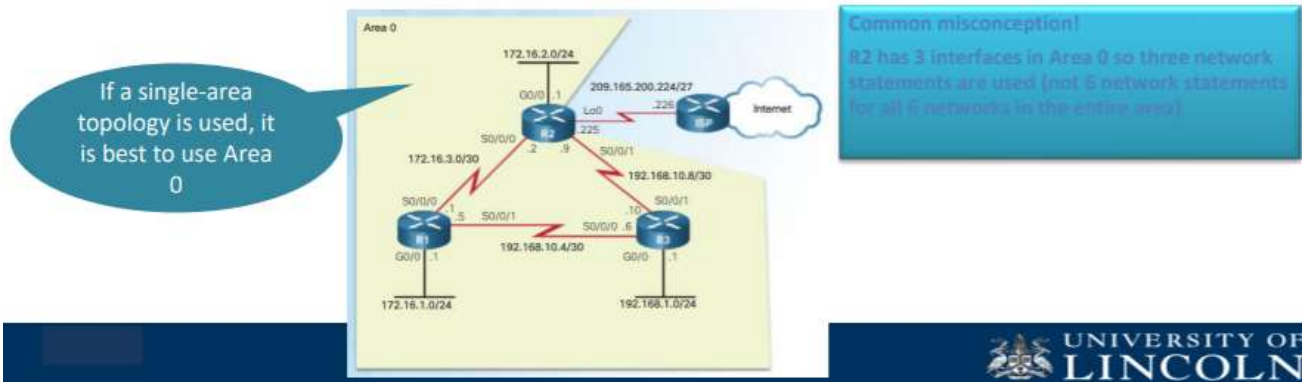
- Older IOS versions did not have the router-id OSPF configuration command
- Loopback interfaces were used to provide a stable router ID



Enabling OSPF on interfaces:

Use the network command to specify which interface(s) participate in the OSPFv2 area

- (config)# router ospf *x*
- (config-router)# *network x.x.x.x wildcard_mask* area *area-id*



Wildcard Mask:

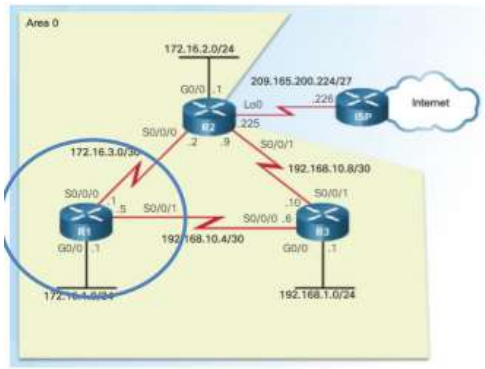
- To determine the wildcard mask, subtract the normal mask from 255.255.255.255
- A wildcard mask bit of 0 - match the bit
- A wildcard mask bit of 1 - ignore the bit
- A wildcard mask is a series of 0s with the rest 1s

/24 mask **/26 mask**

The network command:

Two ways to use the network command…

- Advertise the particular network, calculating the wildcard mask
- Advertise the IP address on the router interface with a 0.0.0.0



Method 1 Traditional Method Network Number and Wildcard Mask

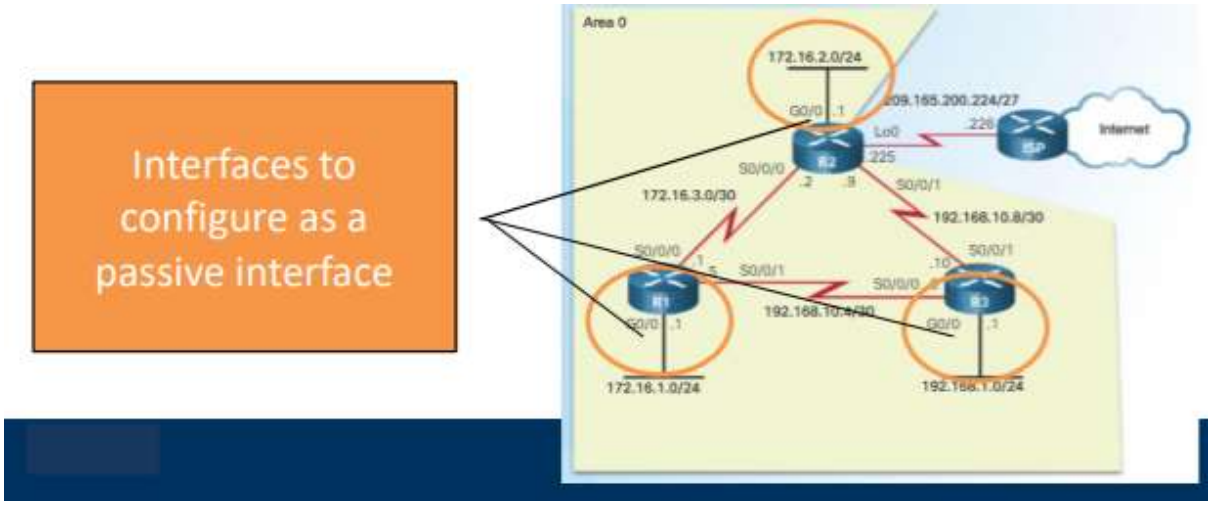
```
R1(config)# router ospf 10
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
```

Method 2 Interface IP Address and 0.0.0.0

```
R1(config)# router ospf 10
R1(config-router)# network 172.16.1.1 0.0.0.0 area 0
R1(config-router)# network 172.16.3.1 0.0.0.0 area 0
R1(config-router)# network 192.168.10.5 0.0.0.0 area 0
```

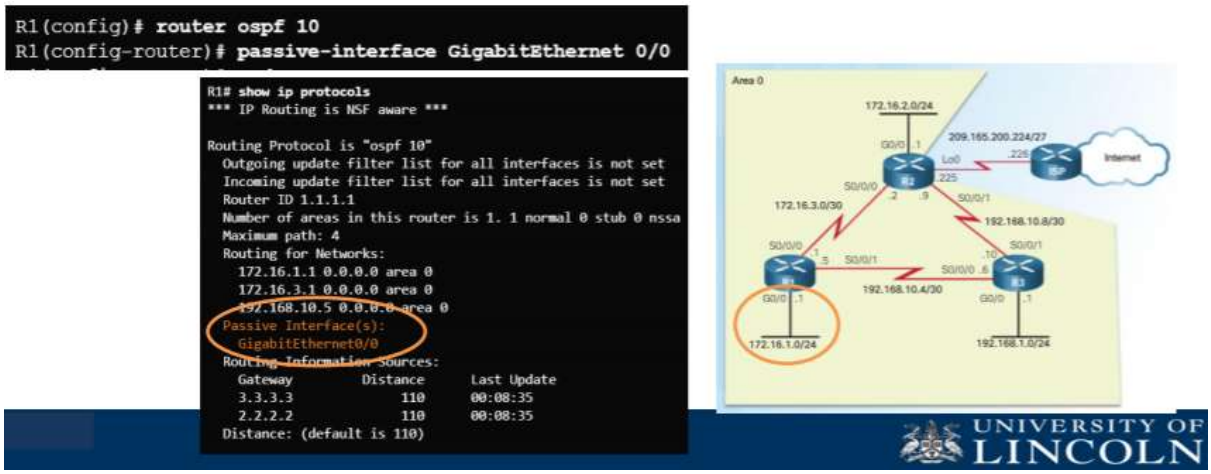
Passive Interface:

- An interface configured as a passive interface does not send OSPF messages
- Best practice for interfaces that have users attached (security)
- Doesn't waste bandwidth sending messages out OSPF-enabled interfaces that don't have another router attached



Configuring Passive Interfaces:

- Use the passive-interface command to configure
- Use the show ip protocols to verify



OSPF Metric = Cost:

- OSPF uses the metric of cost to determine the best path used to reach a destination network (cost = reference bandwidth / interface bandwidth)
- Lowest cost is better path
- The interface bandwidth influences the cost assigned – a lower bandwidth interface has a higher cost

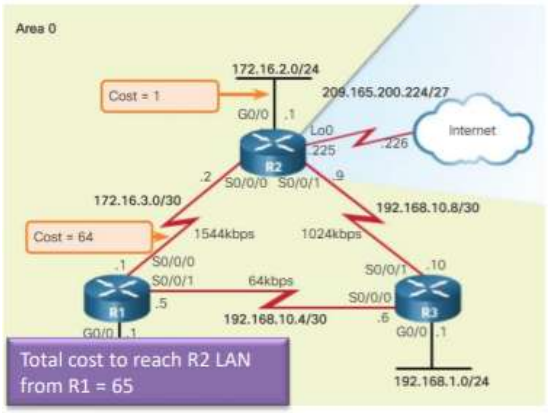
Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
10 Gbps Ethernet	100,000,000	÷	10,000,000,000	1
1 Gbps Ethernet	100,000,000	÷	1,000,000,000	1
100 Mbps Ethernet	100,000,000	÷	100,000,000	1
10 Mbps Ethernet	100,000,000	÷	10,000,000	10
1.544 Mbps Serial	100,000,000	÷	1,544,000	64
128 kbps Serial	100,000,000	÷	128,000	781
64 kbps Serial	100,000,000	÷	64,000	1562

This is an issue because it is the same cost due to the default reference bandwidth. Needs to be adjusted!

UNIVERSITY OF LINCOLN

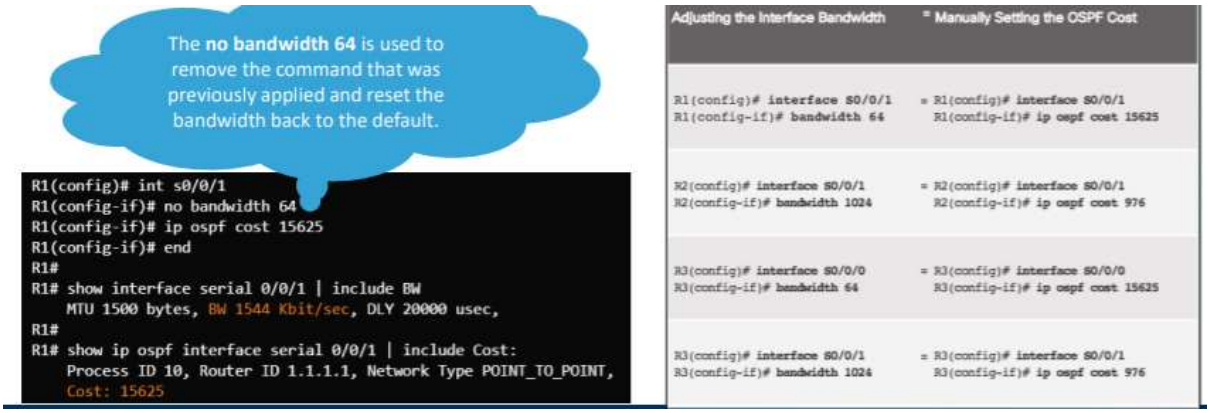
OSPF Accumulates Costs:

- The ‘cost’ for a destination network is an accumulation of all cost values from source to destination
- The cost metric can be seen in the routing table as the second number in brackets



Manually setting the OSPF cost:

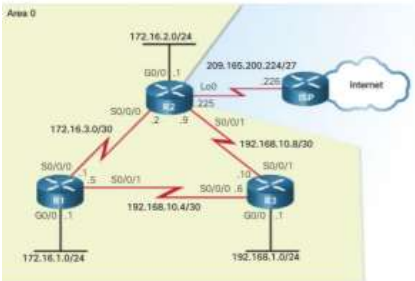
Instead of manually setting the interface bandwidth, the OSPF cost can be manually configured using the ip ospf cost value interface configuration mode command



Verify OSPF Neighbors

- Use the **show ip ospf neighbor** to verify the router has formed an adjacency with a directly-connected router.

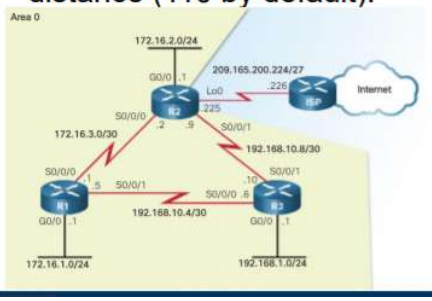
```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:37    192.168.10.6    Serial0/0/1
2.2.2.2           0   FULL/  -        00:00:30    172.16.3.2      Serial0/0/0
```



Output	Description
Neighbor ID	The router ID of the neighbor router
Pri	The OSPFv2 priority of the interface used in the DR/BDR election process
State	The OSPFv2 state – Full means that the link-state database has had the algorithm executed and the neighbor router and R1 have identical LSDBs. Ethernet multi-access interfaces may show as 2WAY. The dash indicates that no DR/BDR is required.
Dead time	Amount of time remaining before expecting to receive a hello packet from the neighbor before declaring the neighbor down. This value is reset when a hello packet is received.
Address	The address of the neighbor’s directly-connected interface
Interface	The interface on R1 used to form an adjacency with the neighbor router

Verify OSPF Protocol Settings

- The **show ip protocols** command is used to verify the OSPFv2 process ID, router ID, networks being advertised by the router, neighbors that are sending OSPF updates, and the administrative distance (110 by default).




```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not
  set
  Incoming update filter list for all interfaces is not
  set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0
  nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.255 area 0
    172.16.3.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    2.2.2.2              110      00:17:18
    3.3.3.3              110      00:14:49
  Distance: (default is 110)
```

Verify OSPF Process Information

- The **show ip ospf** command is another way to see the OSPFv2 process ID and router ID.

```
R1# show ip ospf
Routing Process "ospf 10" with ID 1.1.1.1
Start time: 01:37:15.156, Time elapsed: 01:32:57.776
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode:
cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0
nssa
```

```
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 1000 mbps
      Area BACKBONE(0)
      Number of interfaces in this area is 3
      Area has no authentication
      SPF algorithm last executed 01:30:45.364 ago
      SPF algorithm executed 3 times
      Area ranges are
      Number of LSA 3. Checksum Sum 0x02033A
      Number of opaque link LSA 0. Checksum Sum 0x000000
      Number of DCbitless LSA 0
      Number of indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0
```

UNIVERSITY OF

Verify OSPF Interface Settings

- Use the **show ip ospf interface** command to see details for every OSPFv2-enabled interface especially to see if the network statements were correctly composed.
- Use the **show ip ospf interface brief** command to see key information about OSPFv2-enabled interfaces on a particular router.

```
R1# show ip ospf interface brief
Interface  PID   Area  IP Address/Mask    Cost  State Nbrs F/C
Se0/0/1    10    0     192.168.10.5/30    15625 P2P   1/1
Se0/0/0    10    0     172.16.3.1/30      647   P2P   1/1
Gi0/0      10    0     172.16.1.1/24      1     DR    0/0
```

Single-Area OSPFv3

OSPFv3:

- OSPFv3 is used to exchange IPv5 prefixes and build an IPv6 routing table
- OSPFv3 builds 3 tables – neighbour table, topology table, routing table

Similarities Between OSPFv2 and OSPFv3

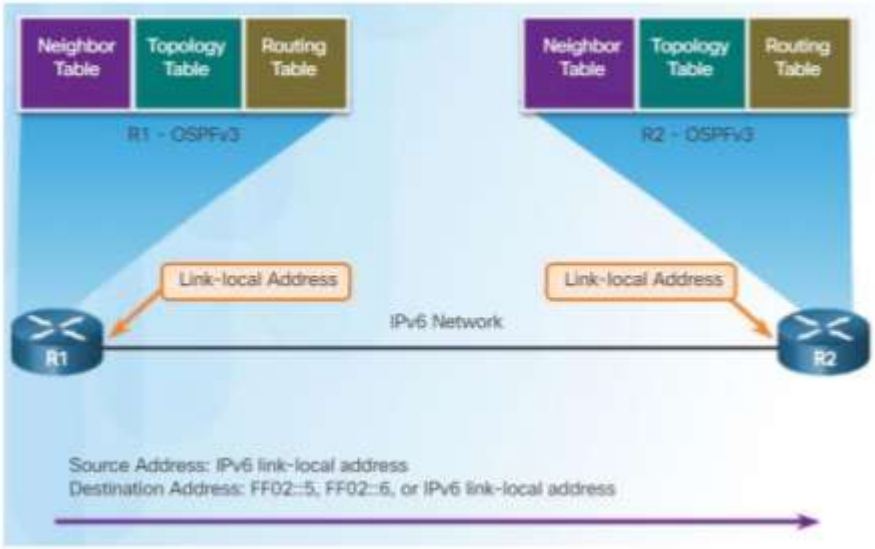
Feature	Comments
Link-State	Both are this type of routing protocol
Routing algorithm	Shortest Path First (SPF)
Metric	Cost
Areas	Both use and support a two-level hierarchy with areas connecting to Area 0
Packet types	Both use the same Hello, DBD, LSR, LSU, and LSAck packets
Neighbor discovery	Transitions through the same states using Hello packets
DR/BDR	Function and election process is the same
Router ID	Both use a 32-bit router ID; determined by the same process

Differences Between OSPFv2 and OSPFv3

Feature	OSPFv2	OSPFv3
Advertisements	IPv4 networks	IPv6 prefixes
Source address	IPv4 source address	IPv6 link-local address
Destination address	Choice of: • Neighbor IPv4 unicast address • 224.0.0.5 all-OSPF-routers multicast address • 224.0.0.6 DR/BDR multicast address	Choice of: • Neighbor IPv6 link-local address • FF02::5 all-OSPF-routers multicast address • FF02::6 DR/BDR multicast address
Advertise networks	Configured using the **network** router configuration command	Configured using the **ipv6 ospf** *process-id* **area** *area-id* interface configuration command
IP unicast routing	IPv4 unicast routing is enabled by default	IPv6 unicast forwarding is not enabled by default. Use the **ipv6 unicast-routing** global configuration command to enable.
Authentication	Plain text and MD5	IPv6 authentication (IPsec)

Link-Local Addresses

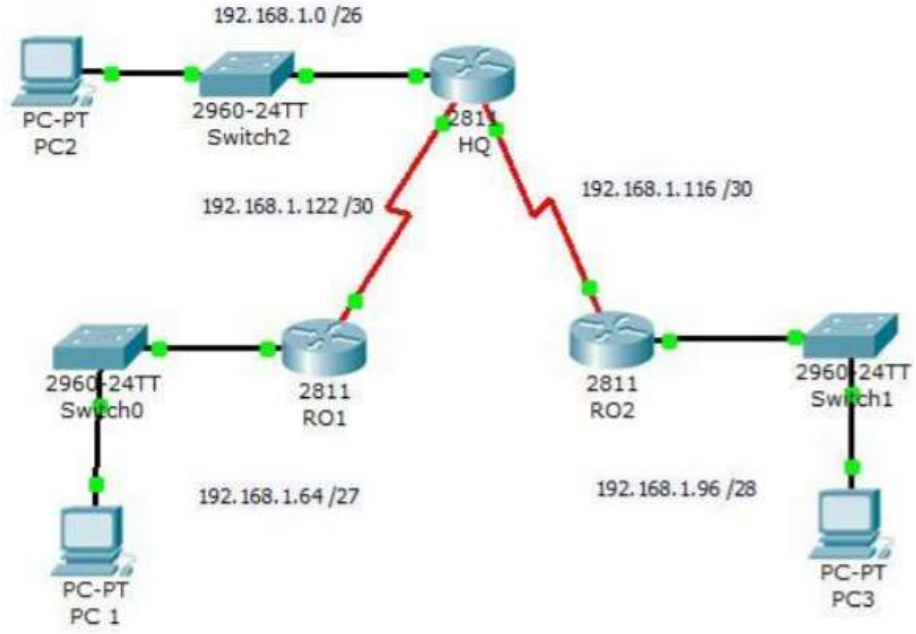
- An IPv6-link-local address enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet) – packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated
- IPv6 link-local addresses are used to exchange OSPFv3 messages


Neighbor Table
Topology Table
Routing Table
R1 - OSPFv3
Neighbor Table
Topology Table
Routing Table
R2 - OSPFv3
Link-local Address
Link-local Address
IPv6 Network
R1
R2
Source Address: IPv6 link-local address
Destination Address: FF02::5, FF02::6, or IPv6 link-local address

VLSM

VLSM:

- Variable Length Subnet Masks
- More flexible approach than Subnetting
- Allows for multiple subnetworks to be addresses out of the same address space



VLSM Subnetworks

Subnet Mask	Slash Notation	Hosts per Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Departments:

- In each department there are a number of nodes…
  - Sales 110
  - Purchasing 51
  - Accounts 25
  - Management 5
- Allocate the highest range of IPs to the highest requirement

- Assign 192.168.1.0 /25 (255.255.255.128) to the Sales department
- This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses - enough for the number of nodes
- The subnet mask used for this subnet has 10000000 as the last octet

11111111.11111111.11111111.10000000

- Allocate the next highest range
- Assign 192.168.1.128 /26 (255.255.255.192) to the Purchasing department
- This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses
- The subnet mask used is 255.255.255.192 or 11000000 as the last octet.

11111111.11111111.11111111.11000000

- Allocate the next highest range - Accounts
- The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs
- The network number of Accounts department will be 192.168.1.224
- The last octet of subnet mask is 11100000

11111111.11111111.11111111.11100000

- Allocate the next highest range to Management
- The Management department contains only 5 nodes
- The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has 6 valid host IP addresses so this can be assigned to Management
- The last octet of the subnet mask will contain 11111000

11111111.11111111.11111111.11111000

Allocating the Subnets

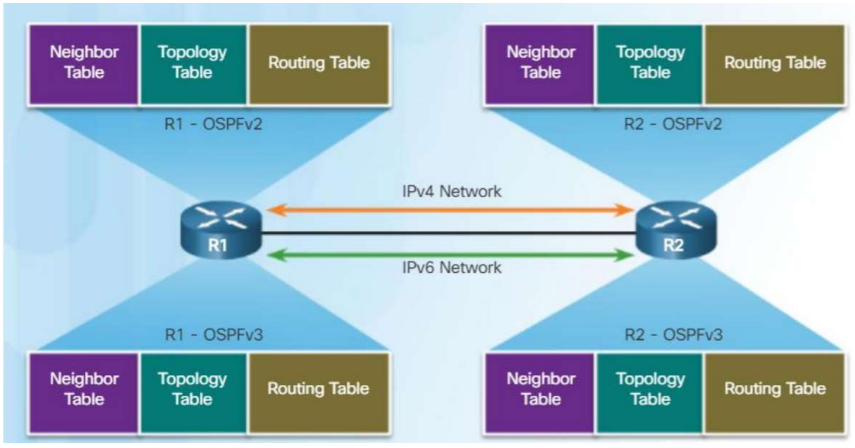
Subnet	Network	First IP Address	Last IP Address	Broadcast Address	Department
0	0	1	126	127	Sales
1	128	129	190	191	Purchasing
2	192	193	230	231	Accounts
3	232	233	238	239	Management

Much more flexible approach to handling networks of different sizes

Single-Area OSPFv3

OSPFv3:

- OSPFv3 is used to exchange IPv6 prefixes and build an IPv6 routing table
- OSPFv3 builds three OSPF tables: neighbour, topology, and routing



Similarities Between OSPFv2 and OSPFv3

Feature	Comments
Link-State	Both are this type of routing protocol
Routing algorithm	Shortest Path First (SPF)
Metric	Cost
Areas	Both use and support a two-level hierarchy with areas connecting to Area 0
Packet types	Both use the same Hello, DBD, LSR, LSU, and LSAck packets
Neighbor discovery	Transitions through the same states using Hello packets
DR/BDR	Function and election process is the same
Router ID	Both use a 32-bit router ID; determined by the same process

Differences Between OSPFv2 and OSPFv3

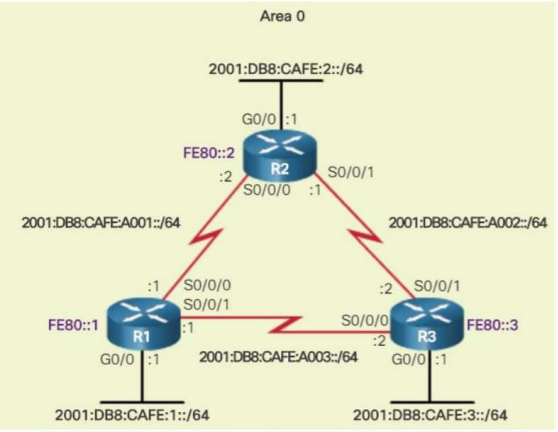
Feature	OSPFv2	OSPFv3
Advertisements	IPv4 networks	IPv6 prefixes
Source address	IPv4 source address	IPv6 link-local address
Destination address	Choice of: • Neighbor IPv4 unicast address • 224.0.0.5 all-OSPF-routers multicast address • 224.0.0.6 DR/BDR multicast address	Choice of: • Neighbor IPv6 link-local address • FF02::5 all-OSPF-routers multicast address • FF02::6 DR/BDR multicast address
Advertise networks	Configured using the **network** router configuration command	Configured using the **ipv6 ospf** *process-id* **area** *area-id* interface configuration command
IP unicast routing	IPv4 unicast routing is enabled by default	IPv6 unicast forwarding is not enabled by default. Use the **ipv6 unicast-routing** global configuration command to enable.
Authentication	Plain text and MD5	IPv6 authentication (IPsec)

Link-Local Addresses:

- An IPv6-link-local address enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet)
    - Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated
- IPv6 link-local addresses are used to exchange OSPFv3 messages

OSPFv3 Network Topology

Turn on IPv6 routing and assign IPv6 addresses to interfaces before enabling OSPFv3.




```
R1(config)# ipv6 unicast-routing
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# description R1 LAN
R1(config-if)# ipv6 address 2001:DB8:CAFE:1::1/64
R1(config-if)# no shut
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ipv6 address 2001:DB8:CAFE:A001::1/64
R1(config-if)# clock rate 128000
R1(config-if)# no shut
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# description Link to R3
R1(config-if)# ipv6 address 2001:DB8:CAFE:A003::1/64
R1(config-if)# no shut
```

Steps to configure OSPFv3:

1. Enable IPv6 unicast routing in global configuration mode – ipv6 unicast-routing
2. (optional) configure link-local addresses
3. Configure a 32-bit router ID in OSPFv3 router configuration mode – router-id rid
4. Configure optional routing specifics such as adjusting the reference bandwidth
5. (optional) configure OSPFv3 interface specific setting such as setting the interface bandwidth on serial links
6. Enable OSPFv3 routing in interface configuration mode – ipv6 ospf area

Assigning Link-Local Addresses:

Manually configuring link-local addresses make it easier to manage and verify OSPFv3 configurations

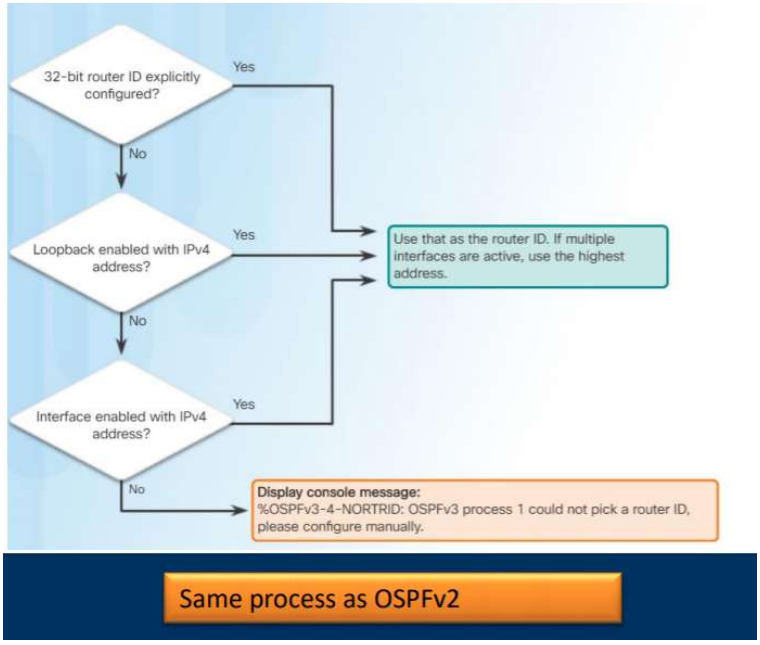
- Use the ipv6 address link-local interface command to apply
- Use the show ipv6 interface brief command to verify

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface Serial0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface Serial0/0/1
R1(config-if)# ipv6 address fe80::1 link-local
```

```
R1# show ipv6 interface brief
Em0/0                  [administratively down/down]
    unassigned
GigabitEthernet0/0     [up/up]
    FE80::1
    2001:DB8:CAFE:1::1
GigabitEthernet0/1     [administratively down/down]
    unassigned
Serial0/0/0            [up/up]
    FE80::1
    2001:DB8:CAFE:A001::1
Serial0/0/1            [up/up]
    FE80::1
    2001:DB8:CAFE:A003::1
```

Configuring the OSPFv3 Router ID

- Use the ipv6 router ospf process-id global configuration command to enter router configuration mode.
- Use the router-id rid command in router configuration mode to assign a router ID and use the show ipv6 protocols command to




```
R1(config)# ipv6 router ospf 10
R1(config-rtr)#
*Mar 29 11:21:53.739: %OSPFv3-4-NORTRID: Process OSPFv3-1-
IPv6 could not pick a router-id, please configure manually
R1(config-rtr)#
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)#
R1(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-1-IPv6:  Reference bandwidth is changed. Please
ensure reference bandwidth is consistent across all routers.
R1(config-rtr)#
R1(config-rtr)# end
R1#
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 0 normal, 0 stub, 0 nssa
  Redistribution:
    None
```

Modifying an OSPFv3 Router ID:

Use the clear ipv6 ospf process privileged EXEC mode command after changing the router ID to complete the router ID change and force a router to renegotiate neighbor adjacencies using the new router ID.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 10.1.1.1
  Number of areas: 0 normal, 0 stub, 0 nssa
  Redistribution:
   None
```

Original router ID

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# end
R1#
```

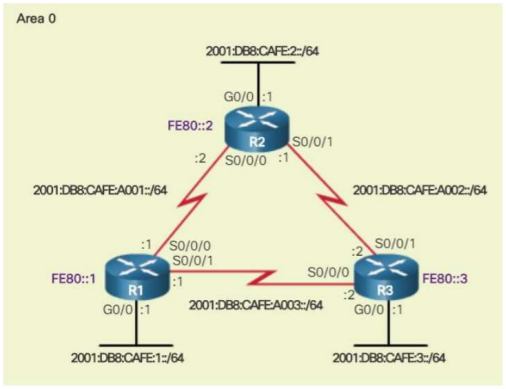
Change the router ID.

```
R1# clear ipv6 ospf process
Reset selected OSPFv3 processes? [no]: y
R1#
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 0 normal, 0 stub, 0 nssa
  Redistribution:
    None
```

Complete the router ID change.

Enabling OSPFv3 on Interfaces:

- Use the ipv6 ospf area interface configuration mode command to enable OSPFv3 on a specific interface. Ensure the interface is within an OSPF area.
- Use the show ipv6 ospf interfaces brief command to verify.




```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# end
R1#
R1# show ipv6 ospf interfaces brief
Interface  PID   Area      Intf ID  Cost   State  Nbrs F/C
Se0/0/1    10    0         7        15625  P2P    0/0
Se0/0/0    10    0         6        647    P2P    0/0
Gi0/0      10    0         3        1      WAIT   0/0
R1#
```

Verifying OSPFv3 Neighbours:

Use the show ipv6 ospf neighbour command to verify neighbour connectivity with directly-connected routers

```
R1# show ipv6 ospf neighbor

OSPFv3 Router with ID (1.1.1.1) (Process ID 10)

Neighbor ID     Pri   State           Dead Time   Interface ID  Interface
3.3.3.3           0   FULL/  -        00:00:39    6             Serial0/0/1
2.2.2.2           0   FULL/  -        00:00:36    6             Serial0/0/0
```

Output	Description
Neighbor ID	The router ID of the neighbor router
Pri	The OSPFv3 priority of the interface used in the DR/BDR election process
State	The OSPFv3 state – Full means that the link-state database has had the algorithm executed and the neighbor router and R1 have identical LSDBs. Ethernet multi-access interfaces may show as 2WAY. The dash indicates that no DR/BDR is required.
Dead time	Amount of time remaining before expecting to receive an OSPFv3 Hello packet from the neighbor before declaring the neighbor down. This value is reset when a hello packet is received.
Address	The address of the neighbor's directly-connected interface
Interface	The interface on R1 used to form an adjacency with the neighbor router

Verifying the OSPFv3 Protocol Settings:

- Use the show ipv6 protocols command to verify vital OSPFv3 configuration information

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
 Router ID 1.1.1.1
 Number of areas: 1 normal, 0 stub, 0 nssa
 Interfaces (Area 0):
   Serial0/0/1
   Serial0/0/0
   GigabitEthernet0/0
```

Verify OSPFv3 Interfaces:

- Use the show ipv6 ospf interface command to display a detailed list for every OSPFv3-enabled interface.
- The show ipv6 ospf interface brief command is an easier output to verify which interfaces are being used with OSPFv3

```
R1# show ipv6 ospf interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Se0/0/1      10    0               7          15625 P2P   1/1
Se0/0/0      10    0               6          647   P2P   1/1
Gi0/0        10    0               3          1     DR    0/0
```

Verifying the IPv6 Routing Table:

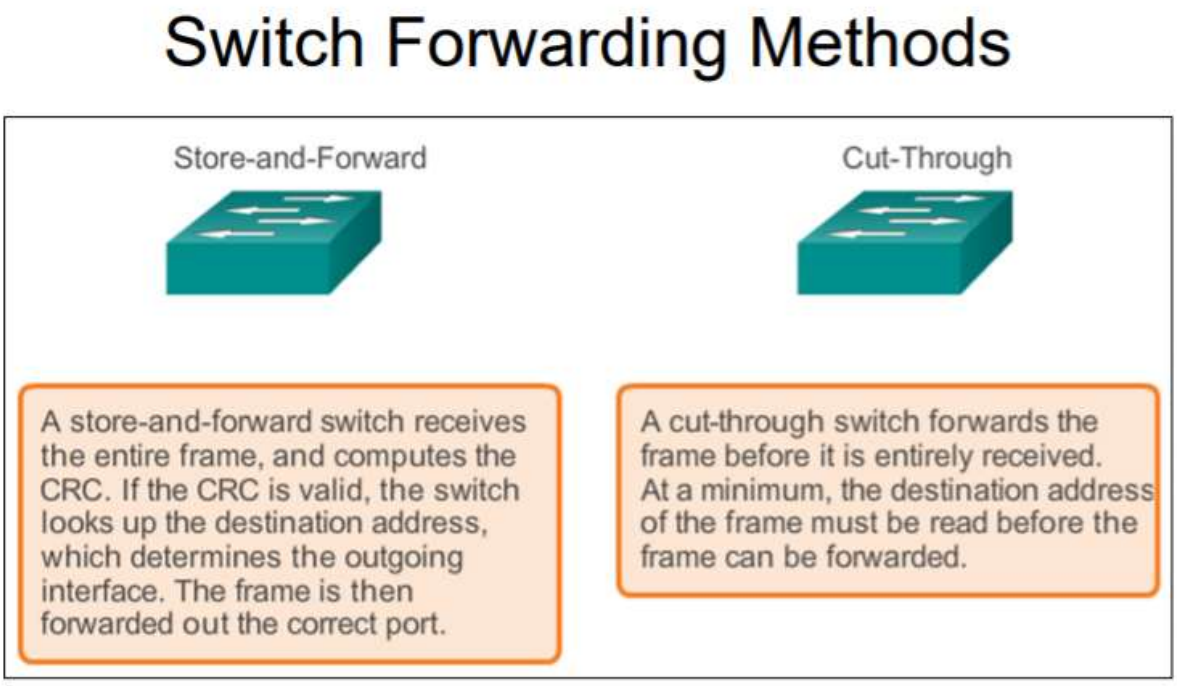
- Use the show ipv6 route command to see an IPv6 routing table.
- Use the show ipv6 route ospf command to see just the OSPFv3 routes

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 10 entries
Codes:C - Connected, L - Local, S - Static, U - Per-user Static route
      B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
      I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
      EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
      NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
     OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
 O   2001:DB8:CAFE:2::/64 [110/657]
     via FE80::2, Serial0/0/0
 O   2001:DB8:CAFE:3::/64 [110/1304]
     via FE80::2, Serial0/0/0
 O   2001:DB8:CAFE:A002::/64 [110/1294]
     via FE80::2, Serial0/0/0
```

The Switched Network

The Switched Network:

- Switches connect devices together – switch to another switch, peripheral devices to the network, are only used for wired networks
- Makes decisions based on the physical address in the packet header
- Maintains a table with the physical address mapped to the port the destination device is attached to
- Called the CAM – Content Addressable Memory table
- CAM is a special type of memory used in high-speed searching applications
- The information in the MAC address table is used to send frames
- When a switch receives an incoming frame with a MAC address that is not found in the CAM table, it floods it to all ports, except the one that received the frame



Store-and-Forward vs Cut-Through:

Store-and-Forward:

- Performs error checking on the packet (FCS check)
- Slower forwarding process
- Automatic buffering

Cut through:

- Can start forwarding the packet within 10microseconds
- No FCS check

- No buffering

The Problem with Switches:

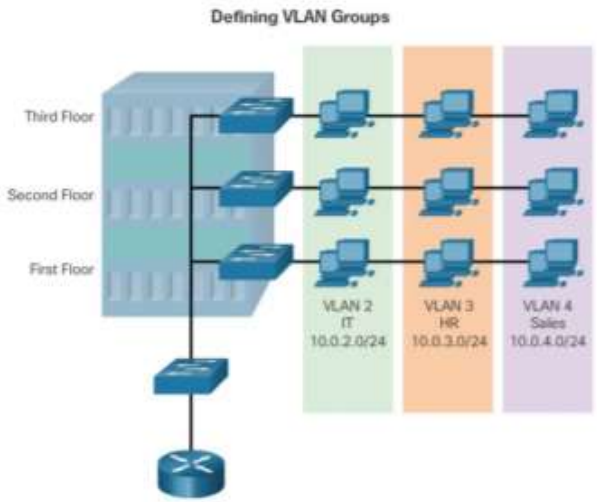
- Switches broadcast
- For example, when a new device is connected an ARP is sent out to request information to add to the CAM table
- Broadcasting means that the request is passed out of every port except the one the packet arrived on. So, for a 24-port switch 23 ports would broadcast
- With lots of switches, it's a lot of broadcasting
- Collison Domains – where devices compete for the right to communicate. Can lead to packet collisions
- Broadcast domains – broadcast frames are forwarded to all ports, so the more switches, the bigger the broadcast domain
- Routers do not broadcast so the easiest way to alleviate this issue is to segment the network into separate collision domains

Switch vs. Router:

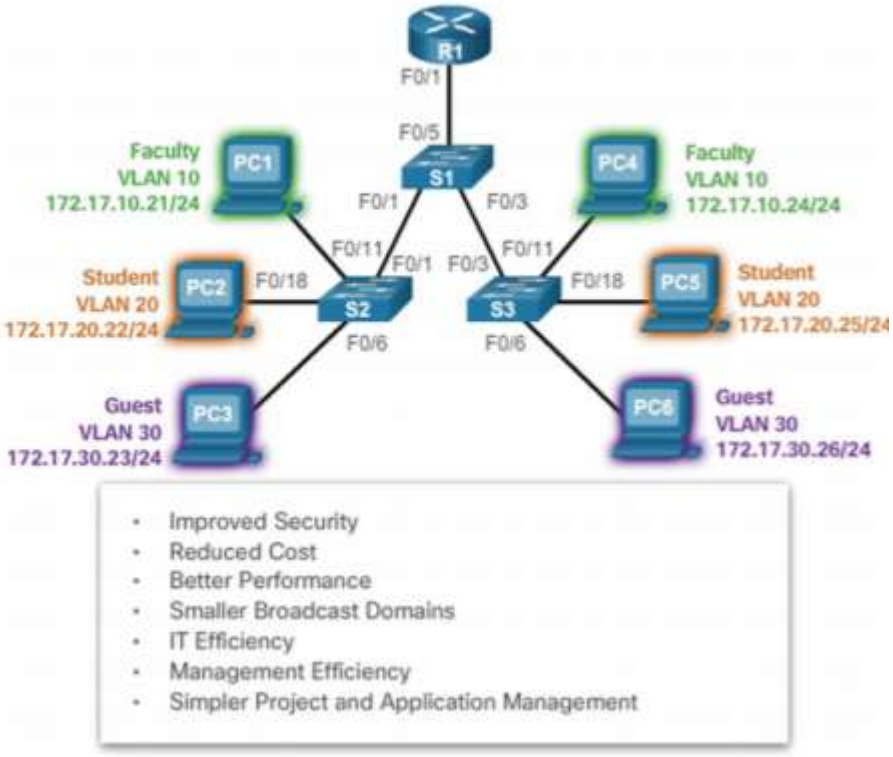
- By default all ports on a router are turned off
- By default all ports on a switch are turned on
- The expectation is that switch ports will be used
- The unused ports should be turned off so rouge devices cannot be attached to the network

VLANs:

- Virtual Local Area Networks
- Define groups by the floors in a building or by groups or use types
- Logical partition of a Layer 2 Network
- Enable the implementation of security and access policies according to the specifics of the groups
- Each VLAN is a broadcast domain
- VLANs are mutually isolated and packets can only pass between them via a router
- Invisible to end user



Benefits of VLANs

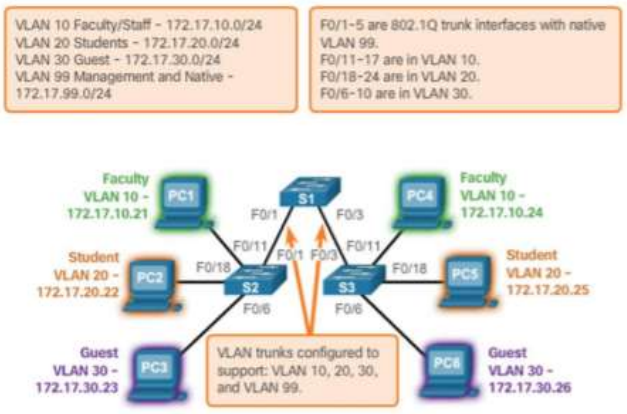


Types of VLANs:

- Data VLAN – user generated traffic
- Default VLAN – all switch ports become part of this VLAN until switch is configured
- Native VLAN – used for untagged traffic
- Management VLAN – used to access management capabilities
- VLANs can be configured to include voice traffic
- Voice traffic is prioritized over all other traffic to ensure quality

VLAN Trunk

- The links between switches S1 and S2, and S1 and S3 are configured to transmit traffic coming from VLANs 10, 20, 30, and 99 across the network
- This network could not function without VLAN trunks.
- Point-to-point link that carries more than one VLAN

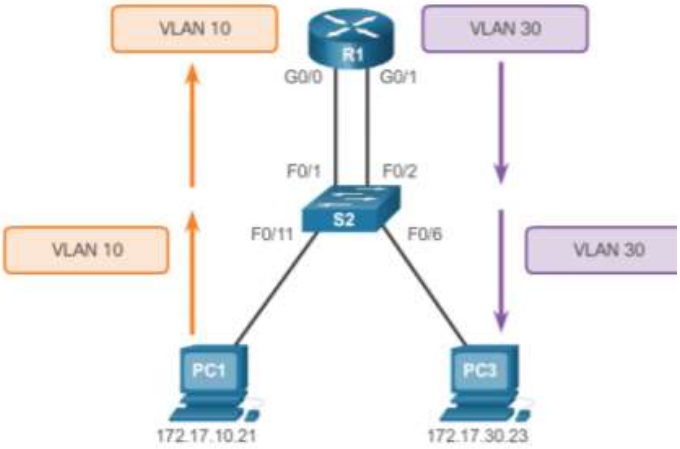


Tagging Frames:

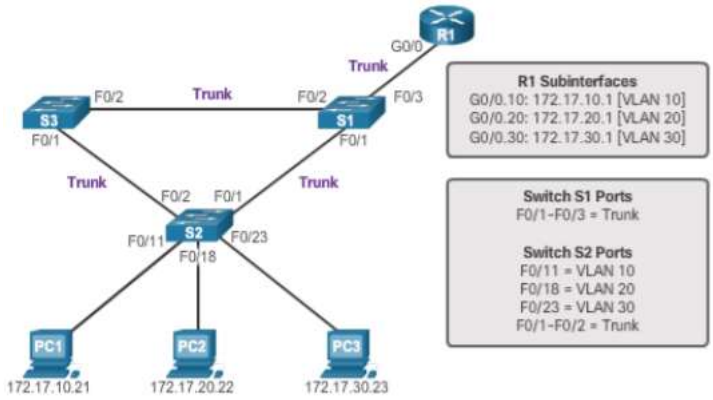
- Frame tagging is the process of adding VLAN identification header to the frame
- It is used to properly transmit multiple VLAN frames through a trunk link
- Switches tag frames to identify the VLAN to which they belong
- Different tagging protocols exist (e.g. IEEE 802.1Q) which define the structure of the tagging header added to the frame
- Switches add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through non-trunk ports
- When properly tagged, the frames can transverse any number of switches via trunk links and still be forwarded within the correct VLAN at the destination

Inter-VLAN routing:

- Layer 2 switches cannot forward traffic between VLANs without assistance from a router, known as inter-VLAN routing
- In this instance the router has two configured ports which provide forwarding between the VLANs



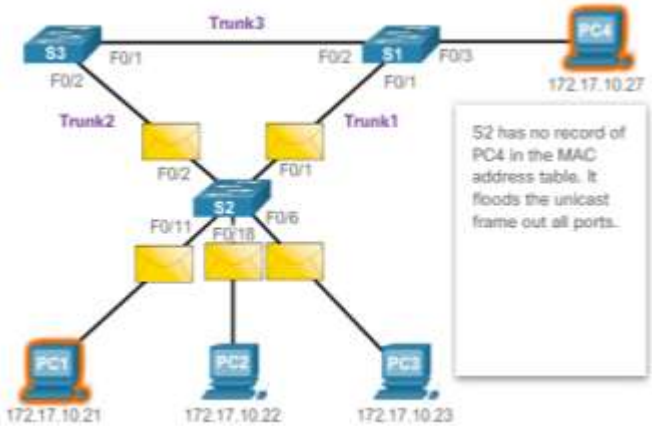
Router-on-a-stick:



The alternative is a router-on-a-stick where only one port is configured and operates as a trunk link, connected to a trunked switch port

Spanning Tree Protocol (STP):

- STP ensures that there is only one logical path between all destinations on the network
- Blocks redundant paths that could cause a loop
- For example, an unknown unicast frame is when the switch does not have the destination MAC address in its MAC

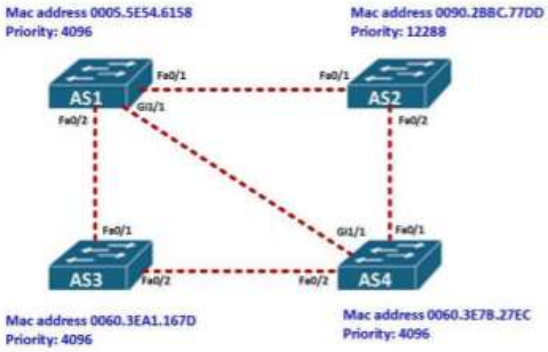


address in its MAC address table and must forward the frame out all ports, except the ingress port

- Unknown unicast frames sent onto a looped network can result in duplicate frames arriving at the destination device

STP Operation:

- Ports on the switch are designated a role…
    - Root ports – ports closest to the root bridge
    - Designated ports – non-root ports permitted to forward traffic
    - Alternate and backup ports – blocking state to prevent loops
    - Disabled ports – a switch port that is shut down
    - The root bridge serves as a reference point for all STP calculations
    - The switch with the lowest BID will become the root bridge
- The root bridge serves as a reference point for all STP calculations
- The switch with the lowest BID will become the root bridge
- The root bridge can be configured manually according to network requirements



STP works out the port costs based on the speed the port operates at

Link Speed	Cost
10 Gb/s	2
1Gb/s	4
100 Mb/s	19
10 Mb/s	100

The formula for calculating STP path cost is

$$\frac{\text{1 Gigabit / second}}{\text{bandwidth}}$$

More Spanning Tree Protocols

The family of Spanning Tree Protocols includes:

Protocol	Standard	Resources Needed	Convergence	Tree Calculation
STP	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	All VLANs
RSTP	802.1w	Medium	Fast	All VLANs
Rapid PVST+	Cisco	Very High	Fast	All VLANs
MSTP	802.1, Cisco	Medium	Fast	Per Instance

All are designed to reduce the possibility of loops and broadcast storms from occurring

Wireless Networks

Standards:

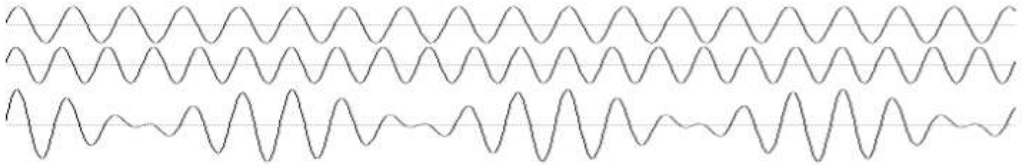
- 802.11ac -> 802.11ad – provides us with access to stream and access the internet
- 802.11ah – used by smart meters to monitor electricity and gas usage, used on industrial sensors and in hospitals

Wireless Technologies:

- PAN/WAN (Personal Area Network) – Bluetooth, IEEE 802.15.4
- LAN (Local Area Network) – IEEE 802.11
- MAN (Metropolitan Area Network – IEEE 802.11, IEEE 802.16, IEEE 802.20
- WAN (Wide Area Network) – GSM, CDMA, Satellite

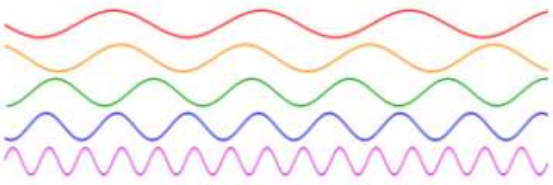
Electromagnetic Waves

- Wireless technologies use electromagnetic waves



- CCommunications medium for wireless is the Earth's Atmosphere

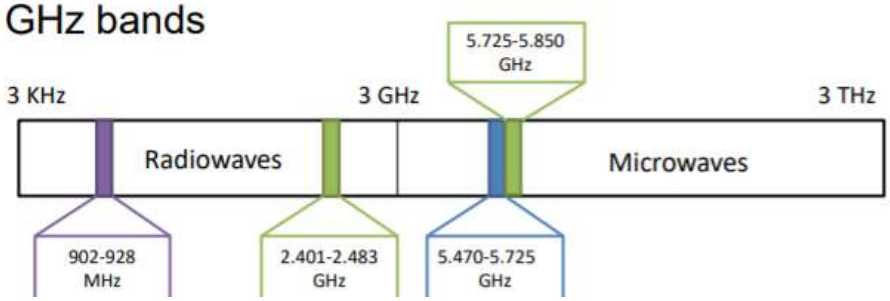
- Frequency (*f* - Hz)
  - –**Frequency** is the number of occurrences of a repeating event per unit time.
- Higher frequency:
  - –Greater speed
  - –Shorter range
  - –High reflection rate
  - –Higher absorption in the Earth's atmosphere
  - –Higher costs



Frequency in LAN?

- ISM – Industrial Scientific Medical
  - –Free to transmit
  - –Reserved for industrial, scientific and medical
  - –http://en.wikipedia.org/wiki/ISM_band
- 2,4 and 5 GHz bands

- Disadvantage:
  - –They are very occupied
  - –The frequencies are high



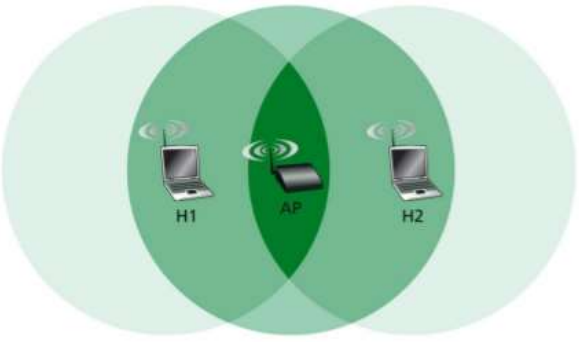
The Problem of Accessing the Medium

Wireless will always be half-duplex because of the communication environment
If 2 stations transmit at the same time, a collision will occur
Detectable by unsteady frequencies and incorrect modulation
The conclusion?
An access control method is needed for the wireless environment

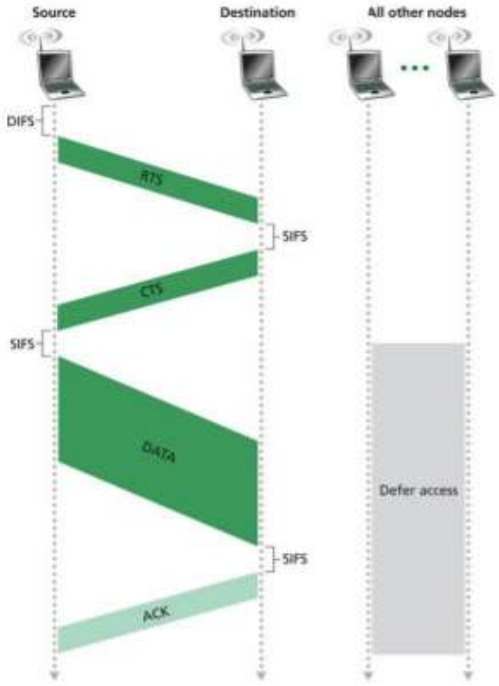
Access Control:

CSMA/CD is not used with ACK messages…

- For each frame sent an ACK message is required
- If no ACK message is received, retransmission is done



Access control



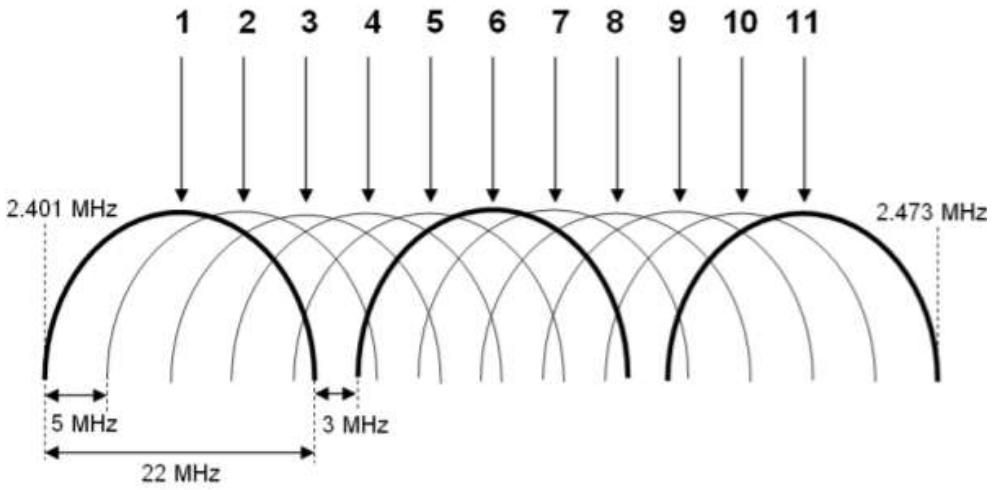
CSMA/CA

Carrier-Sense Multiple Access with Collision Avoidance

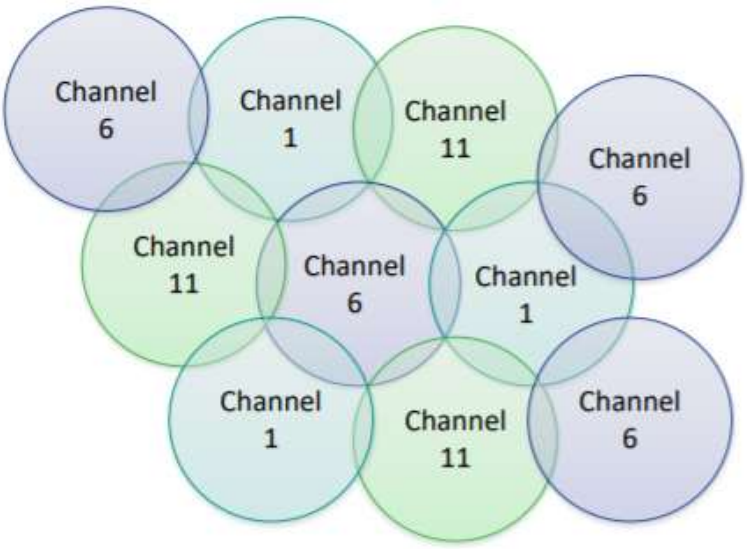
Communications Channel:

- The wireless transmission medium is shared
- It is not possible to transmit in the exact same frequency without collisions
- 22Mhz is needed to transmit 54mbps in 802.11g
- We can split the ISM band into channels and map each WLAN/SSID on a single channel, having multiple networks in the same band

Multiple channels



Multiple channels



It is possible to cover any surface using just 3 channels

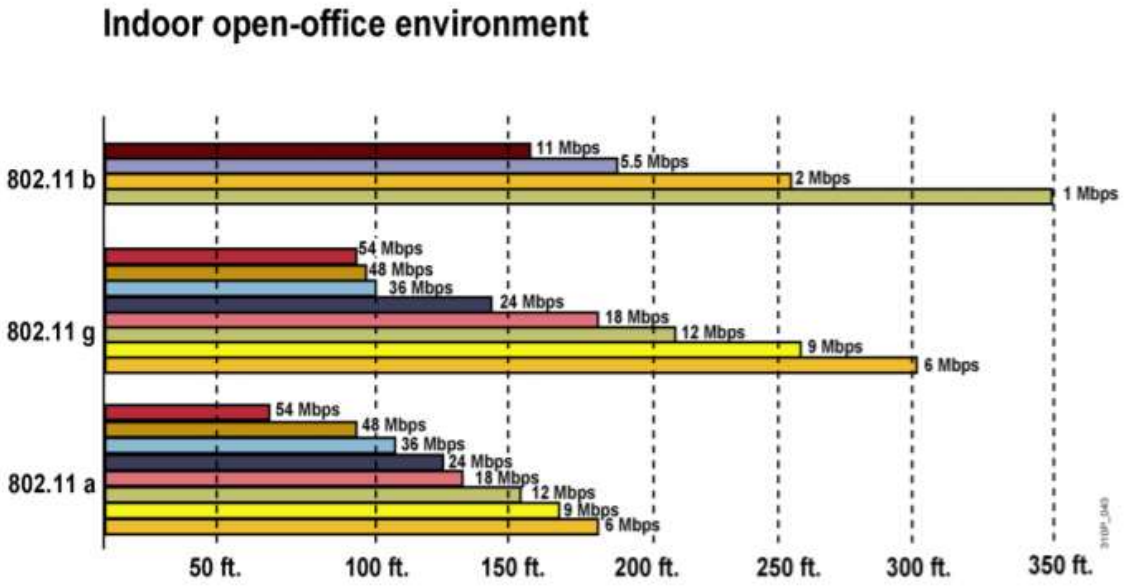
802.11:

- legacy – released in 1997
- specified in infrared and wireless
- Spread spectrum – FHSS/DSSS
- Speed: 1-2mbps
- Frequency: 2.4Ghz and 900mhz

802.11 a & b:

- both standards appeared about the same time – 1999
- 802.11a – speed up to 54mbps, frequency band 5ghz, distance to transmit signal 25m
- 802.11b – bandwidth 11mbps, frequency band 2.4ghz, became very popular (Wi-Fi)

802.11a/b/g – Area coverage



802.11n:

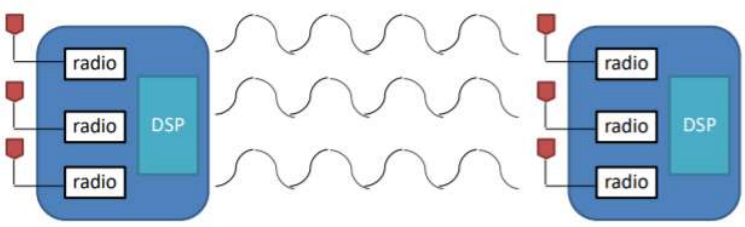
- Standardised in 2009
- Far greater speeds (theoretical maximum of 600mbps)
- Better coverage and density of the signal
- Backwards compatible with 802.11 a/b/g
- Uses multiple antenaes and MIMO technology
- Increased channel width to 40mhz
- Improved immunity to noise using complex modulation techniques
- Support packet aggregation (one header for multiple data packets)

MIMO:

“Multiple-Input Multiple-Output (MIMO) is a wireless technology that uses multiple transmitters and receivers to transfer more data at the same time. All wireless products with 802.11n support MIMO. The technology helps allow 802.11n to reach higher speeds than products without 802.11n”

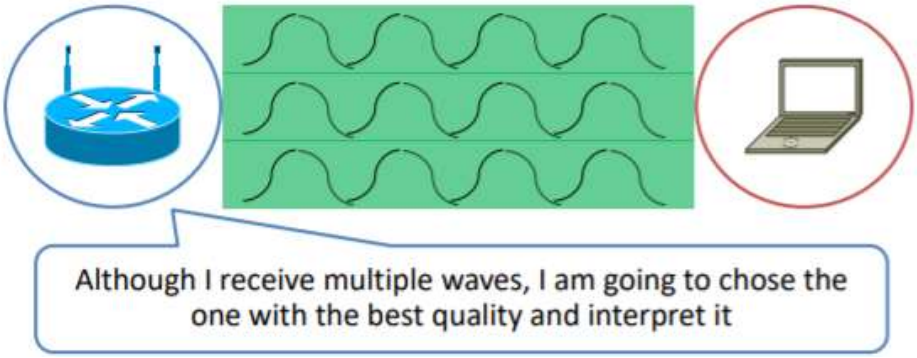
802.11n - MIMO

- MIMO uses digital signal processors (DSP) to multiplex and demultiplex the signal



802.11n – Maximum Ratio Combining

- The multipath effect = the process in which many waves carrying the same information are reflected differently from surfaces and with varying clarity
- In 802.11g, the DSP chose the wave with the best signal to noise ratio



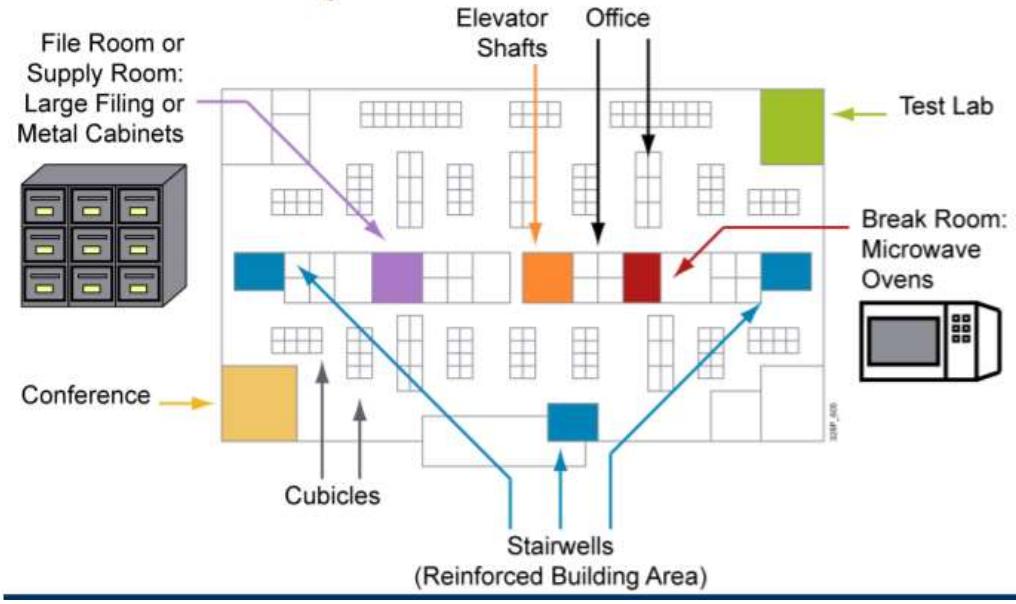
802.11n – Maximum Ratio Combining:

- Problem: some weaker waves are ignored even if there is the possibility that they contain relevant information
- In 802.11n, MRC is implemented in the NIC's DSP so that it takes all the waves and composes just one high-quality wave, thus increasing throughput
- Concluding: MRC is a client-side technology, if you have a 802.11n board in a 802.11g network you will have higher throughput

General comparison of standards

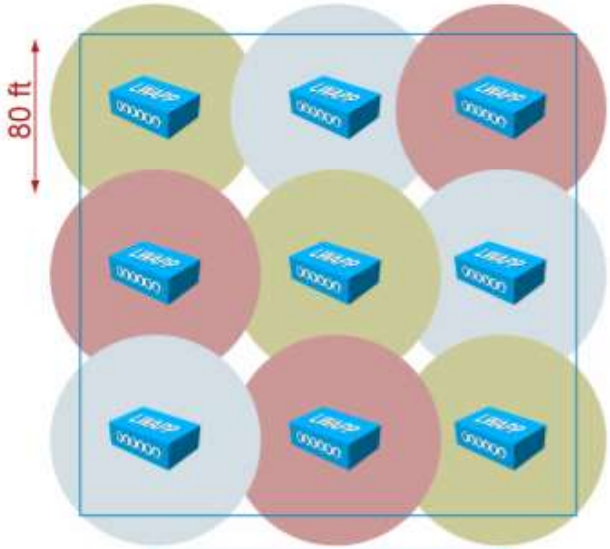
Standard	802.11a	802.11b	802.11g	802.11n
Published	1999	1999	2003	2009
Frequency	5GHz	2.4GHz	2.4GHz	2.4GHz / 5GHz
Bandwidth	54Mbps	11Mbps	54Mbps	160-600 Mbps
Modulation	OFDM	DSSS	OFDM, DSSS	OFDM
Coverage Interior Exterior	35m 120m	38m 140m	38m 140m	70m 250m
Advantages	Strong signal in a small office	Low price	Good speed and good coverage	Very big speed Very big coverage
Disatvantages	Incompatible with g and b	Interference	Interference	More expensive

Identify Problematic Areas



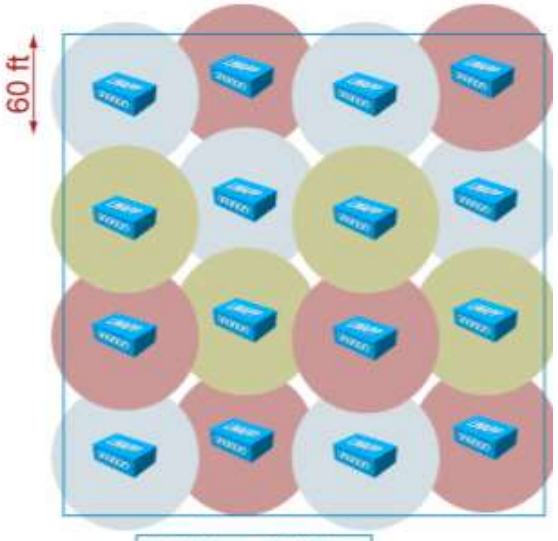
WLAN Coverage and Capacity

Basic coverage, low cost



Graphic is using only 3 channels
for interference avoidance

Entreprise coverage and capacity

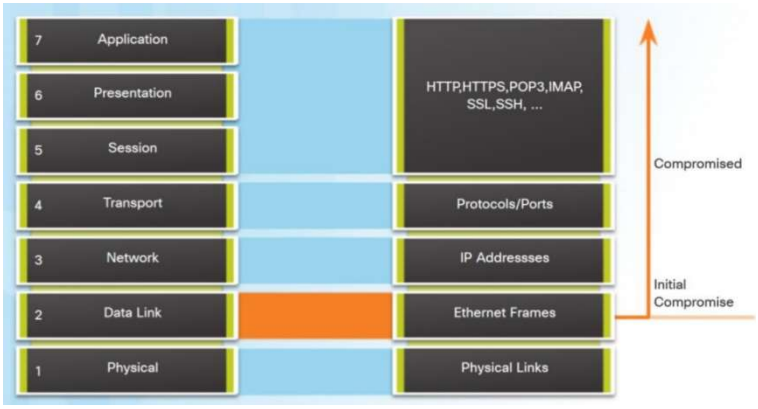


802.11a: 22 Mbps
802.11g: 20 Mbps
802.11b/g: 6 Mbps
802.11b: 5.5 Mbps

LAN Security

Common LAN Attacks:

- Common security solutions using routers, firewalls, Intrusion Prevention System (IPS), and VPN devices protect layer 3 up through layer 7
- Layer 2 must also be protected
- Common layer 2 attacks include:
    - CDP Reconnaissance Attack
    - Telnet Attacks
    - MAC Address Table Flooding Attack
    - VLAN Attacks
    - DHCP Attacks



CDP Reconnaissance Attack:

- The Cisco Discovery Protocol (CDP) is a proprietary layer 2link discovery protocol, enabled by default
- CDP can automatically discover other CDP-enabled devices
- CDP information can be used by an attacker
- Use the 'no cdp run' global configuration command to disable CDP globally
- Use the 'no cdp enable' interface configuration command to disable CDP on a port

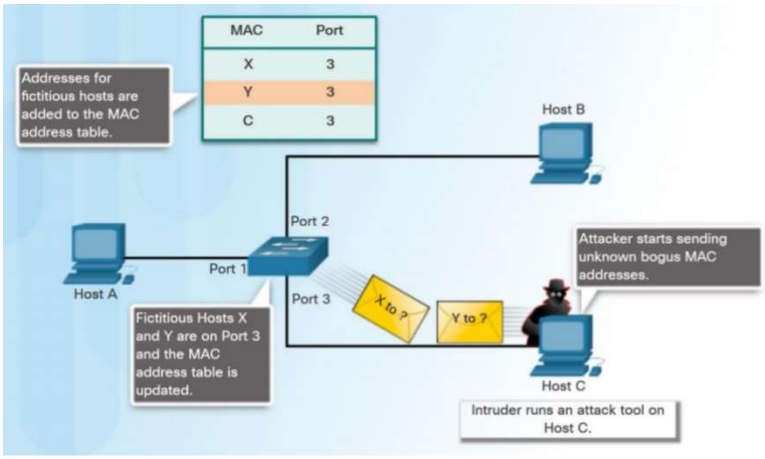
Telnet Attacks:

- There are two types of Telnet attacks…
    - Brute Force Password Attack – trial and error method used to obtain the administrative password
    - Telnet DoS Attack – Attacker continuously requests Telnet connections in an attempt to render the Telnet service unavailable
- To mitigate these attacks…
    - Use SSH
    - Use strong passwords that are changed frequently
    - Limit access to the vty lines using an access control list (ACL)

MAC Address Table Flooding Attacks:

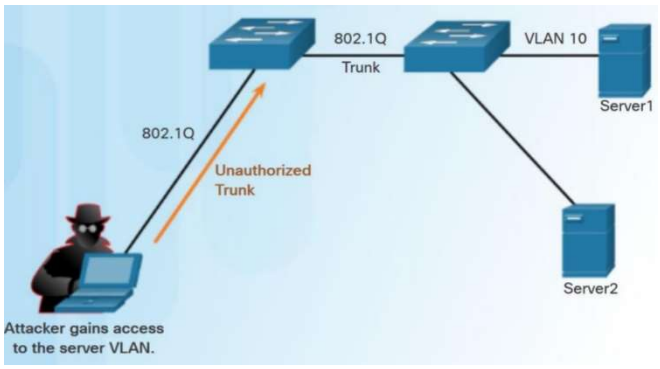
- Common LAN switch attack is the MAC address table flooding attack

    - An attacker sends fake source MAC addresses until the switch MAC address table is full and the switch is overwhelmed
    - Switch is then in fail-opened mode and broadcasts all frames, allowing the attacker to capture those frames
- Configure port security to mitigate these attacks



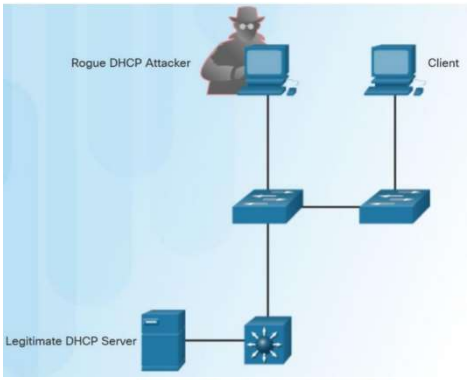
VLAN Attacks:

- Switch spoofing attack – an example of a VLAN attack
    - Attacker can gain VLAN access by configuring a host to spoof a switch and use the 802.1Q trunking protocol and DTP to trunk with the connecting switch
- Methods to mitigate VLAN attacks…
    - Explicitly configure access links
    - Disable auto trunking
    - Manually enable trunk links
    - Disable unused ports, make them access ports, and assign to a black hole VLAN
    - Change the default native VLAN
    - Implement port security



DHCP Attacks:

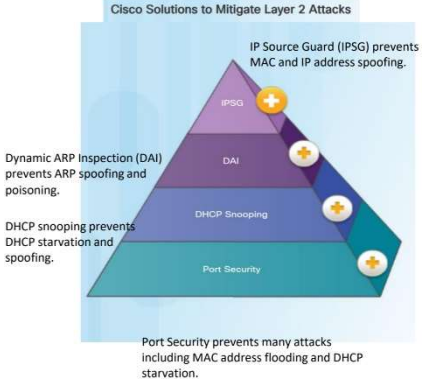
- DHCP spoofing attack – an attacker configures a fake DHCP server on the network to issue IP addresses to clients
- DHCP starvation attack – an attacker floods the DHCP server with bogus DHCP requests and leases all of the available IP addresses. This results in a denial-of-service (DoS) attack as new clients cannot obtain an IP address



Secure the LAN:

Strategies to help secure layer 2 of a network…

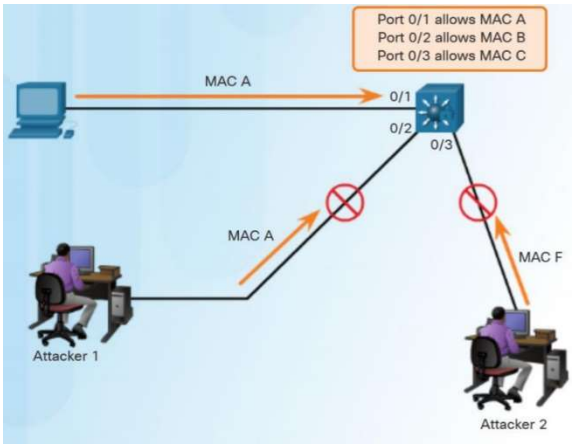
- Always use secure variants of protocols such as SSH, SCP, and SSL
- Use strong passwords and change them often
- Enable CDP on select ports only
- Secure Telnet access
- Use a dedicated management VLAN



- Use ACLs to filter unwanted access

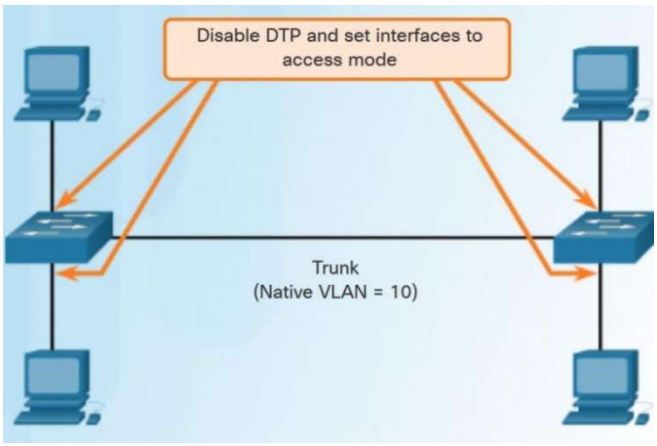
Mitigate MAC Address Table Flooding Attacks:

- Enable port security to prevent MAC table flooding attacks
- Port security allows an administrator to do the following…
    - Statically specify MAC addresses for a port
    - Permit the switch to dynamically learn a limited number of MAC addresses
    - When the maximum number of any MAC addresses is reached, any additional attempts to connect by unknown MAC addresses will generate a security violation



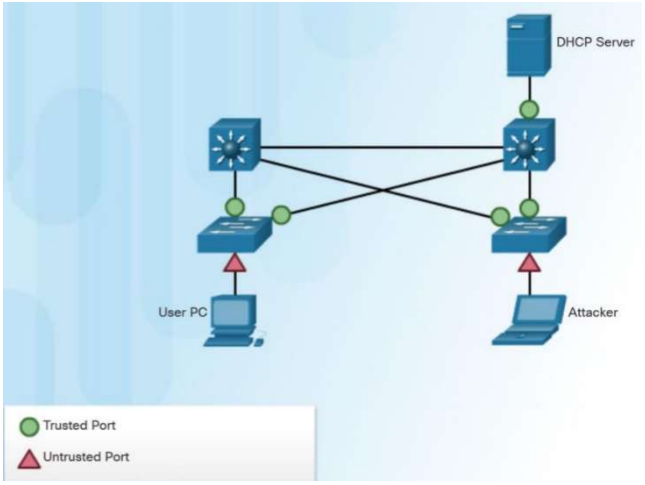
Mitigate VLAN Attacks:

- Disable DTP (auto trunking) negotiations on non-trunk ports and use ‘switchport mode access’
- Manually enable trunk links using ‘switchport mode trunk’
- Disable DTP (auto trunking) negotiations on trunking and non-trunking ports using ‘switchport nonegotiate’
- Change the native VLAN from VLAN 1
- Disable unused ports and assign them to an unused VLAN



Mitigate DHCP Attacks:

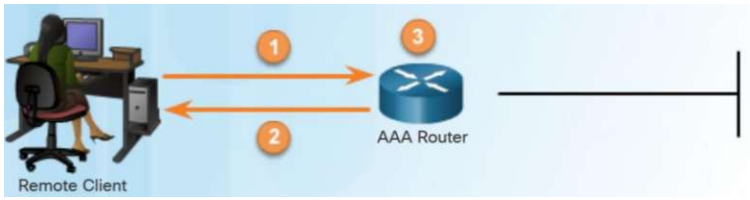
- To prevent DHCP attacks use DHCP snooping
- With DHCP snooping enabled on an interface, the switch will deny packets containing:
    - Unauthorised DHCP server messages coming from an untrusted port
    - Unauthorized DHCP client messages not adhering to the DHCP Snooping Binding Database or rate limits
- DHCP snooping recognises two types of ports…
    - Trusted DHCP ports – only ports connected to upstream DHCP servers should be trusted
    - Untrusted ports – these ports connect to the host that should not be providing DHCP server messages



Secure Administrative Access using AAA:

Local AAA Authentication

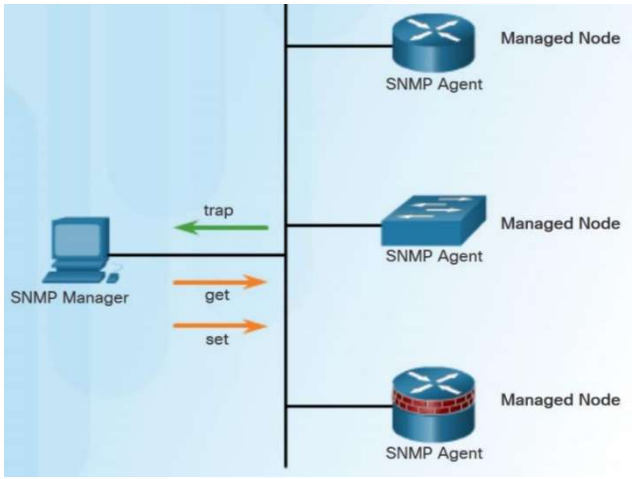
1. Client establishes a connection with the router
2. AAA router prompts the user for username and password
3. Router authenticates the username and password using the local database, and allows user access



SNMP

Introduction to SNMP:

- Simple Network Management Protocol (SNMP) enables network administrators to monitor and manage network nodes
- The SNMP system consists of three elements:
    1. SNMP manager – collects information from an SNMP agent using the 'get' action. Changes configurations on an agent using the 'set action
    2. SNMP agents (managed node)
    3. Management Information Base (MIB) – stores data and operational statistics about the managed device



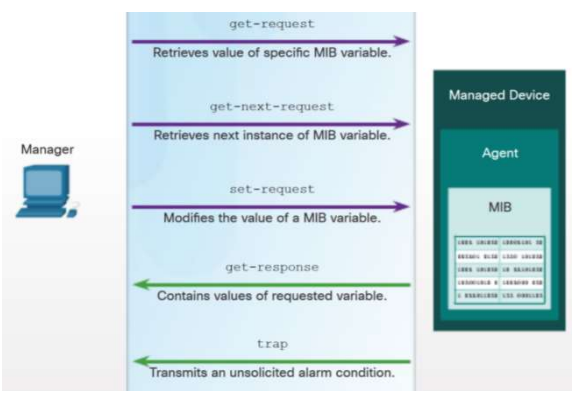
SNMP Operation:

- SNMP agents that reside on managed devices collect and store information about the device
- This information is stored by the agent locally in the MIB
- SNMP manager then uses the SNMP agent to access information within the MIB
- SNMP agent responds to the SNMP manager requests as follows…
    - Get a MIB variable – the SNMP agent preforms this n response to a GetRequest-PDU from the network manager
    - Set a MIB variable – the SNMP agent preforms this in response to a SetRequest-PDU from the network manager

Operation	Description
`get-request`	Retrieves a value from a specific variable.
`get-next-request`	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
`get-bulk-request`	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
`get-response`	Replies to a `get-request`, `get-next-request`, and `set-request` sent by an NMS.
`set-request`	Stores a value in a specific variable.

SNMP Agent Traps:

- A Network Management System (NMS) periodically polls the SNMP agents using the get request
- Using this process, the SNMP can collect information to monitor traffic loads and to verify device configurations of managed devices
- SNMP agents to generate and send traps to inform the NMS immediately of certain events – traps are unsolicited messages alerting the SNMP manager to a condition or event such as improper user authentication or link status



SNMP Versions:

Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication (an improvement over SNMPv2c).
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: • DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. • 3DES 168-bit encryption. • AES 128-bit, 192-bit, or 256-bit encryption.

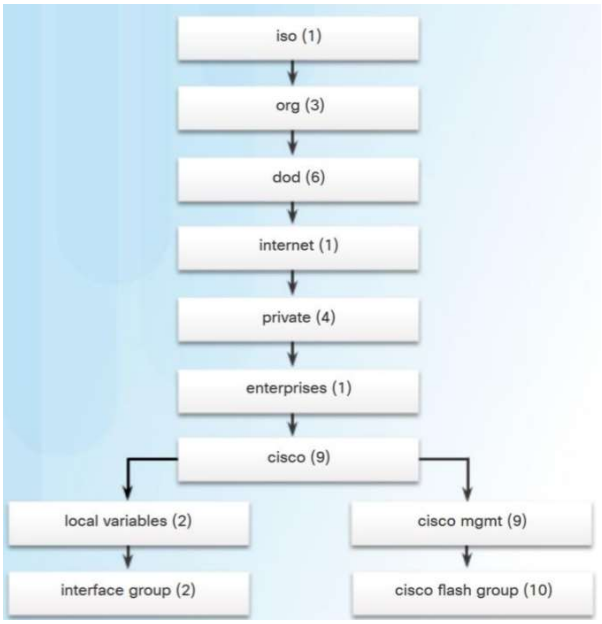
- All versions use SNMP managers, agents, and MIBs, we focus on versions 2c and 3
- A network administrator must configure the SNMP agent to use the SNMP version supported

Community Strings:

- SNMPv1 and SNMPv2c use community strings that control access to the MIB
- Two types of community strings…
    - Read-only (ro) – provides access to the MIB variables, but no changes can be made
    - Read-write (rw) – provides read and write access to all objects in the MIB

Management Information Base Object ID:

- The MIB defines each variable as an object ID (OID)
    - OIDs uniquely identify managed objects
    - OIDs are organised based on RFC standards into a hierarchy or tree
- Most devices implement RFC defined common public variables – vendors such as cisco can define private branches on the tree to accommodate their own variables
- CPU is one of the key resources, it should be measured continuously
- An SNMP graphing tool can periodically pol SNMP agents, and graph the values
- The data is retrieved via the snmpget utility



SNMPWALK examples

```
~]$ snmpwalk localhost IF-MIB::ifDescr
IF-MIB::ifDescr.1 = STRING: lo
IF-MIB::ifDescr.2 = STRING: eth0
IF-MIB::ifDescr.3 = STRING: eth1
~]$ snmpwalk localhost IF-MIB::ifOutOctets
IF-MIB::ifOutOctets.1 = Counter32: 10060699
IF-MIB::ifOutOctets.2 = Counter32: 650
IF-MIB::ifOutOctets.3 = Counter32: 0
~]$ snmpwalk localhost IF-MIB::ifInOctets
IF-MIB::ifInOctets.1 = Counter32: 10060699
IF-MIB::ifInOctets.2 = Counter32: 78650
IF-MIB::ifInOctets.3 = Counter32: 0
```

SNMPv3:

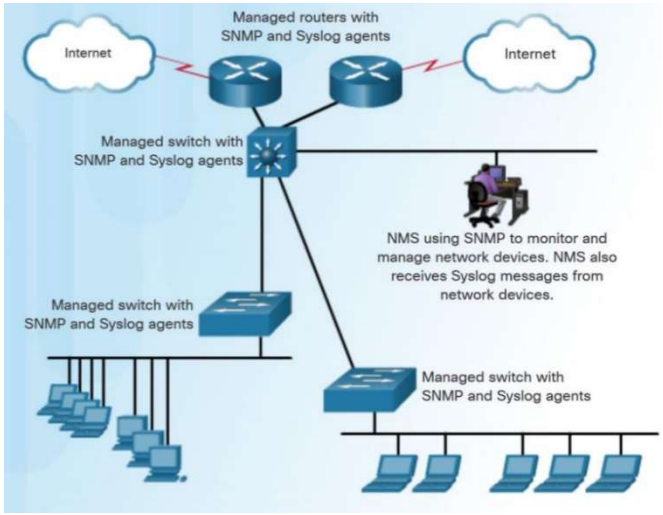
- SNMPv3 authenticates and encrypts packets over the network to provide secure access to devices
- SNMPv3 provides three security features
    - Message integrity and authentication – transmissions from the SNMP manager to agents (managed nodes) can be authenticated
    - Encryption – SNMPv3 messages can be encrypted to ensure privacy

- Access control – restricts SNMP managers to certain actions on specific portions of data

Steps for configuring SNMP:

1. Configure the community string and access level using snmp-server community string ro | rw command
2. (optional) document the location of the device using the snmp-server location text command
3. (optional) document the system contact using the snmp-server contact text command
4. (optional) use an ACL to restrict the SNMP access to NMS hosts (SNMP managers). Reference the ACL using snmp-server community string access-list-number-or-name

SNMP Best Practices:



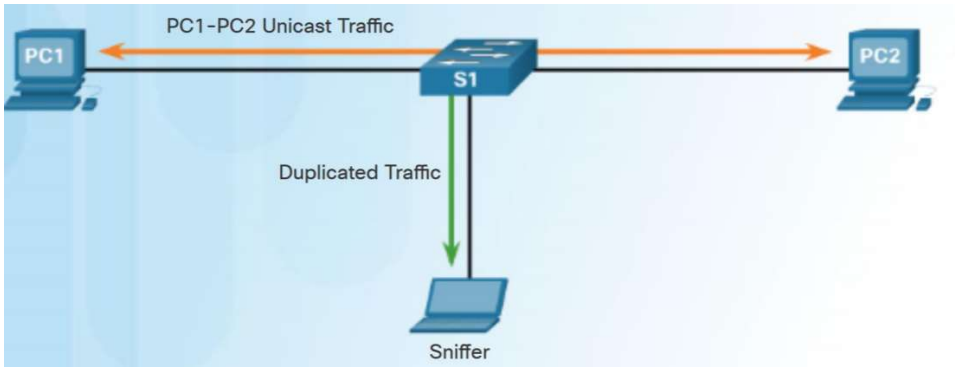
- SNMP can create security vulnerabilities
- For SNMPv1 and SNMPv2c, community strings should be strong and changed frequently
- ACLs should be used to prevent SNMP messages from going beyond the required devices and to limit access to monitored devices
- SNMPv3 is recommended because it provides security authentication and encryption
    - The snmp-server group groupname {v1 | v2c | v3 {auth | noauth | priv}} command creates a new SNMP group on the device.
    - The snmp-server user username groupname command is used to add a new user to the group.

SNMPv3 Configuration:

- The example configures a standard ACL named PERMIT-ADMIN. It is configured to permit only the 192.168.1.0/24 network. All hosts attached to this network will be allowed to access the SNMP agent running on R1.
- An SNMP view is named SNMP-RO and is configured to include the entire ISO tree from the MIB

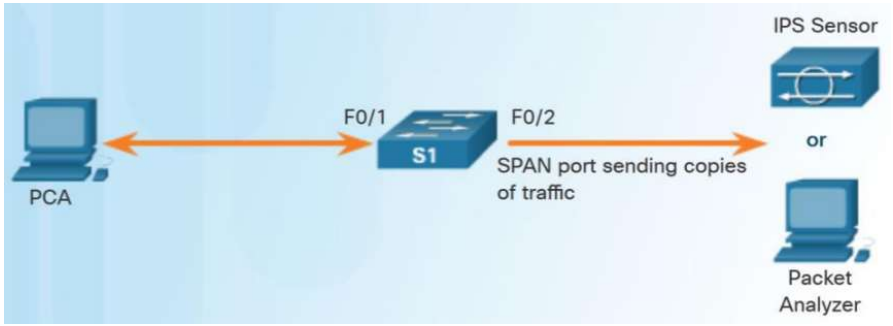
Port Mirroring:

Port mirroring allows a switch to copy and send Ethernet frames from specific ports to the destination port connected to a packet analyser



Analysing suspicious traffic:

- SPAN is a type of port mirroring that allows administrators or devices to collect and analyse traffic
- SPAN is commonly implemented to deliver traffic to specialised devices including:
    - Packet analysers – using software such as Wireshark to capture and analyse traffic for troubleshooting purposes
    - Intrusion Prevention Systems (IPSs) – focused on the security aspect of traffic and are implemented to detect network attacks as they happen
- SPAN can be implemented as either Local SPAN or Remote SPAN (RSPAN)



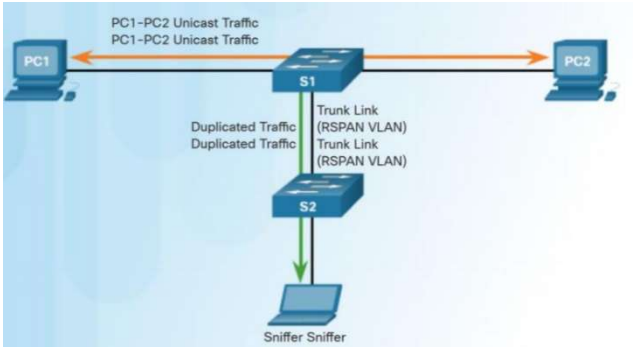
Local SPAN:

- Local SPAN is when traffic is mirrored to another port on that switch
- A SPAN session is the association between source ports (or VLANs) and a destination port
- There are three important things to consider when configuring a SPAN:
    - The destination port cannot be a source port, and the source port cannot be a destination port
    - The number of destination ports is platform-dependent
    - The destination port is no longer a normal switch port. Only monitored traffic passes through that port.

Term	Definition
Ingress traffic	This is traffic that enters the switch.
Egress traffic	This is traffic that leaves the switch.
Source (SPAN) port	This is a port that is monitored with use of the SPAN feature.
Destination (SPAN) port	This is a port that monitors source ports, usually where a packet analyzer, IDS or IPS is connected. This port is also called the monitor port.
SPAN session	This is an association of a destination port with one or more source ports.
Source VLAN	This is the VLAN monitored for traffic analysis.

Remote SPAN:

- Remote SPAN (RSPAN) allows source and destination ports to be different in switches
- RSPAN uses two sessions:
    - One session is used as the source and one session is used to copy or receive the traffic from a VLAN
    - The traffic for each RSPAN session is carried over trunk links in a user-specified RSPAN VLAN



Term	Definition
RSPAN source session	This is the source port/VLAN to copy traffic from.
RSPAN destination session	This is the destination VLAN/port to send the traffic to.
RSPAN VLAN	• A unique VLAN is required to transport the traffic from one switch to another. • The VLAN is configured with the `remote-span` vlan configuration command. • This VLAN must be defined on all switches in the path and must also be allowed on trunk ports between the source and destination.

Configuring Local SPAN:

- A session number is used to identify a local SPAN session.
- Use monitor session command to associate a source port and a destination port with a SPAN session.
- A separate monitor session command is used for each session.
- A VLAN can be specified instead of a physical port.

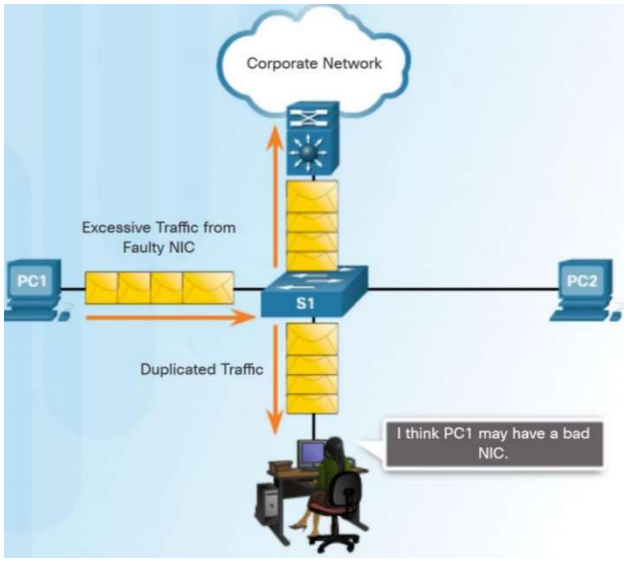
Verifying Local SPAN:

Use the show monitor command to verify the SPAN session. It displays the type of the session, the source ports for each traffic direction, and the destination port.

Troubleshooting with SPAN:

SPAN allows administrators to troubleshoot network issues…

- To investigate a slow network application, a network administrator can use SPAN to duplicate and redirect traffic to a packet analyser such as Wireshark
- Older systems with faulty NICs can also cause issues. If SPAN is enabled a network technician can detect and isolate the end device causing the problem.



ACLs:

- Access Control Lists
- Permit or deny network traffic
- Can be done by IP address or protocol
- Filter internal and external traffic
- Provides a basic level of security
- Can be used to prevent users from misusing the system
- Associated with the interface, so placement during configuration is key

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```