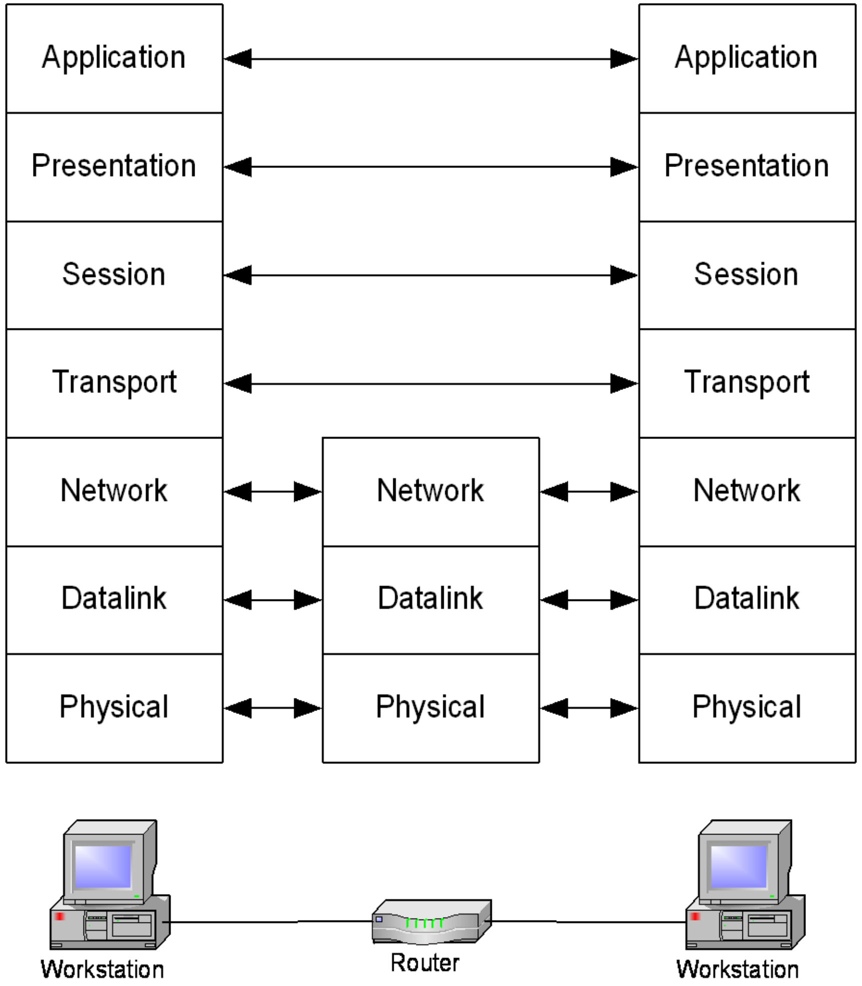
Basic Network Training

Larry Mathews
Brocade Systems Engineer
lmathews@brocade.com

Training Objectives

- Assumption is that attendees have no prior knowledge in regard to network operation or functions
- Emphasis on basic network operations with focus on ITS environment
- Attendees will learn the fundamentals
- Primary focus is on technology not vendor specifics

OSI reference model



OSI reference model (cont'd)

- Hierarchical
  - Divides complex network operation into manageable layers.
  - 3 upper layers define how the applications within the end stations will communicate with each other and with users:
    - Application: provides user interface (file, print etc.)
    - Presentation: presents data (compression, conversion etc.)
    - Session: keeps applications data deparate (dialog control)
  - 4 lower layers define how data is transmitted end-to-end:
    - Transport: end to end connection (TCP & UDP), <u>PDU segment</u>
    - Network: logical addressing (routing), <u>PDU packet</u>
    - Data link: MAC framing, <u>PDU frame</u>
    - Physical: moves bits between devices, <u>PDU bit</u>
- Allows different vendors to interoperate
  - Defines the standard interface for the ”plug and play” multivendor integration.

Fundamentals of Ethernet

- Ethernet standard review
- MAC Addresses
- Ethernet frame
- Ethernet components

Ethernet Definition

A system for connecting a number of computer systems (hosts) to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems.

- Ethernet is a *link layer* protocol in the OSI stack, describing how networked devices can format data for transmission to other network devices on the same network segment. It touches both Layer 1 (the physical layer) and Layer 2 (the data link layer) on the OSI network protocol model.

- Ethernet defines the unit of transmission as a frame. The frame includes not just the "payload" of data being transmitted but also addressing information identifying the physical "Media Access Control" (MAC) addresses of both sender and receiver.

Common Networking Terms

- Unicast - message sent across a network by a single host to a single client or device
- Broadcast - a message sent intended for all devices
- Broadcast Domain - a portion of a computer network, with boundaries defined by routers
- Multicast - a message sent across a network by a single host to group of devices
- Protocol - a standard used to define a method of exchanging data over a computer network

Original Ethernet Common Characteristics

- Shared media technology
- 10 Mbps
- Frame Size
  - Min. 64 bytes; 512 bits; 51.2us
  - Max. 1518 bytes; 12,144; 1.2ms
- InterFrame Gap (IFG) or Interpacket Gap = 9.6us
- Round Trip Delay = Collision Detect Window = 51.2us
- Passive media

Ethernet at L2

- Hardware or MAC addressing
  - 48 bit MAC address is burned into each Ethernet device
  - error detection (not correction) form CRC
- Uses frames to encapsulate packets for transmission

Standard IEEE 802.3 Ethernet Frame

8 bytes Preamble	6 bytes DA	6 bytes SA	6 bytes Length	Up to 1500 bytes Data	4 bytes FCS

Ethernet Terminology

- Collisions - the result of two or more stations transmitting simultaneously
- Jabber Protection - self-interrupt capability that monitors xmit lines for excessively long transmissions
- Jam - a signal that produces a packet fragment used to reinforce a collision
- Partitioning - a faulty device is disconnected when 32 collisions or jabber is detected
- Broadcast - transmitting a packet that will be received by <u>every</u> device on the network

Ethernet - CSMA/CD

- Station Listens
  - If busy waits
  - If clear, xmits
- Continues to listen
- If collision is detected
  - Stops transmitting
  - Sends Jam Signal
  - Waits random period of time before trying to retransmit

Ethernet Naming Convention

- 10Base-T
  - Leading number indicates speed
  - Base indicates that a baseband frequency is used
  - T indicates media being used – in this case twisted pair cabling

100Base-FX

100Mbps

Baseband

Fiber

Ethernet Devices

- Network Interface Card (NIC)
  - A network interface card (NIC) is a circuit board or card that is installed in a computer so that it can be connected to a network.
- Repeater/Hub
  - An Ethernet repeater is a physical layer device with two or more Ethernet ports and is used to extend an Ethernet. Broadcast domain remains intact.
- Bridge
  - An Ethernet network bridge is a device which connects two different local area networks together creating separate segments.
- Switch
  - Connects devices together on a LAN, by using packet switching to receive, process and forward data to the destination device. Unlike less advanced network hubs, a network switch forwards data only to one or multiple devices that need to receive it, rather than broadcasting the same data out of each of its ports.

Ethernet Today

- Today Ethernet can run from 10 Mbps to 100 Gbps in switched, full duplex mode with traffic prioritization and can utilize multiple parallel links running over just about any type of physical media.

Ethernet Switch Overview

- Basic switch operation
- Switch characteristics

Layer 2 switching

- Switch is multiport bridge creating separate broadcast domains
- Address learning
  - On frame ingress the source address is entered into MAC database table (forward / filter table)
- Forward / filter decisions
  - On frame egress checks destination address and forwards only to right port

Half duplex Ethernet

- Uses only one wire pair with digital signal running in both directions on the wire.
- Uses CSMA/CD.
- Inefficient
  - Recommended utilization rate 30%
  - E.g. half duplex 10Base-T transmits only 3-4Mbps at most

Full duplex Ethernet

- Transmit and receive simultaneously
- Better performance
  - Offers 100% efficiency
  - If the system is symmetrical (transmits and receives equal amount) performance doubles, e.g. 10Base-T -> 20Mbps
- Switches offer full duplex capabilities

Overview of commonly used interfaces and optics

- Typical interface types
- Explanation of commonly used optics
- Cable distances

Twisted pair cabling

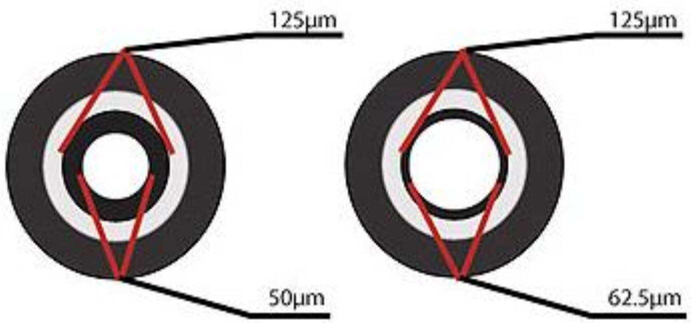
Type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources for example, electromagnetic radiation from unshielded twisted pair(UTP) cables, and crosstalk between neighboring pairs

Name	Typical construction	Bandwidth	Applications
Level 1		0.4 MHz	Telephone and modem lines
Level 2		4 MHz	Older terminal systems, e.g. IBM 3270
Cat 3	UTP[9]	16 MHz[9]	10BASE-T and 100BASE-T4 Ethernet[9]
Cat 4	UTP[9]	20 MHz[9]	16 Mbit/s[9] Token Ring
Cat 5	UTP[9]	100 MHz[9]	100BASE-TX & 1000BASE-T Ethernet[9]
Cat 5e	UTP[9]	100 MHz[9]	100BASE-TX & 1000BASE-T Ethernet[9]
Cat 6	UTP[9]	250 MHz[9]	10GBASE-T Ethernet
Cat 6_A	U/FTP, F/UTP	500 MHz	10GBASE-T Ethernet
Cat 7	F/FTP, S/FTP	600 MHz	10GBASE-T Ethernet. POTS/CATV/1000BASE-T over single cable.
Cat 7_A	F/FTP, S/FTP	1000 MHz	10GBASE-T Ethernet. POTS/CATV/1000BASE-T over single cable.

Multi-Mode Fiber vs. Single-Mode Fiber

Multi-mode Fiber (MMF)

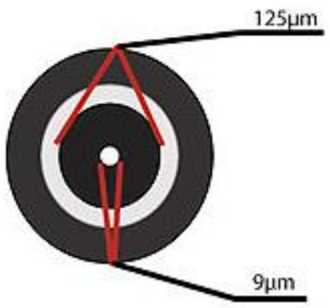
- Multimode fiber optic cable has a large diameter core that allows multiple modes of light to propagate.
- Due to the high dispersion and attenuation rate with this type of fiber, the quality of the signal is reduced over long distances.
- This application is typically used for short distance, data and audio/video applications in LANs



Multimode fiber is usually 50/125 and 62.5/125 in construction. This means that the core to cladding diameter ratio is 50 microns to 125 microns and 62.5 microns to 125 microns

Single-Mode Fiber (SMF)

- Single Mode fiber optic cable has a small diameter core that allows only one mode of light to propagate.
- the number of light reflections created as the light passes through the core decreases, lowering attenuation and creating the ability for the signal to travel faster, further.
- This application is typically used in long distance, higher bandwidth runs



Single Mode fiber is usually 9/125 in construction. This means that the core to cladding diameter ratio is 9 microns to 125 microns

Typical Interface Types

- RJ-45 – unshielded twisted pair interface
- DAC (Direct Attach Cable) – Twinax copper
- ST (Straight Tip) – Fiber optic interface
- LC (Lucent Connector/Little Connectors) – Fiber optic interface
- SC (Subscriber Connector/Square Connector) – Fiber optic interface
- MPO/MTP (Multiple-Fiber Push-On/Pull-off) - Fiber optic interface
- SFP (Small Form-factor Pluggable) – 1G compact, hot pluggable transceiver
- SFP+ (Small Form-Factor Pluggable enhanced) – 10G compact, hot pluggable transceiver
- QSFP (Quad Small Form-factor Pluggable) – 40G hot pluggable transceiver

Optic Characteristics and Distances

	IEEE Standards	Domestic Safety Standards	International Safety Standards	Wavelength (nm)	Fiber Type	Maximum Cable Distance	Digital Optical Monitoring
Fast Ethernet							
EIMG-100FX-OM	802.3u	FDA 21CFR 1040.10 Class 1, CSA 60950-1-03/UL 60950-1	EN 60825-1, EN 60950-1	1,310	MMF	2 km	Yes
EIMG-100FX-IR-OM	802.3			1,310	SMF	15 km	Yes
EIMG-100FX-LR-OM	802.3			1,310	SMF	40 km	Yes
1 GbE Fiber							
EIMG-SX-OM/ EIMG-SX-OM-T	802.3z	FDA 21CFR 1040.10 Class 1, CSA 60950-1-03/UL 60950-1	EN 60825-1, EN 60950-1	850	MMF	220 m to 550 m	Yes
EIMG-LX-OM/ EIMG-LX-OM-T	802.3z			1,310	MMF/SMF	550 m to 10 km	Yes
EIMG-LHA-OM/ EIMG-LHA-OM-T	802.3z			1,550	SMF	70 km	Yes
EIMG-LHB	802.3z			1,550		150 km w/0.18 dB/km cable, 91 km w/ standard 0.3 dB/ km cable	No
EIMG-BXD	802.3ah			TX: 1,490 RX: 1,310		10 km	No
EIMG-BXU	802.3ah			TX: 1,310 RX: 1,490		10 km	No
EIMG-CWDM80-XXXX	802.3z			1,470 to 1,610		80 km	No
1000BASE-T Copper							
EIMG-TX, XBR-000190	802.3z	CSA 60950-1-03/UL	EN 60950-1	N/A	Cat5	100 m	N/A
1G-SFP-TWX-0x01	802.3z	Direct-attached SFP copper cables				1 m, 5 m	No
10 GbE Fiber							
10G-XFP-SR	802.3ae	FDA 21CFR 1040.10 Class 1, CSA 60950-1-03/UL 60950-1	EN 60825-1, EN 60950-1	850	MMF	26 m to 300 m	Yes
10G-XFP-LR	802.3ae			1,310	SMF	10 km	
10G-XFP-ER	802.3ae			1,550		40 km	
10G-XFP-ZR	802.3ae			1,550		80 km	
10G-XFP-1310-LRM	802.3aq			1,310		220 m	
10G-SFPP-USR	N/A			850	MMF	100 m	
10G-SFPP-SR	802.3ae			850	MMF	26 m to 300 m	
10G-SFPP-LR	802.3ae			1,310	SMF	10 km	
10G-SFPP-ER	802.3ae			1,550	SMF	40 km	
10G-SFPP-ZR	802.3ae			1,550	SMF	80 km	
10G-SFPP-ZRD-T	802.3-2005 Clause 52 standard			102 C-band tunable wavelengths from 1,528 to 1,568 (50 GHz apart)	SMF	80 km	
10G-SFPP-LRM	802.3ae			1,310	MMF	220 m	

Commonly Used Optics

10G-SFPP-ER	10GBASE-ER SFP+ optic (LC), for up to 40km over SMF
10G-SFPP-LR	10GBASE-LR, SFP+ optic (LC), for up to 10km over SMF
10G-SFPP-LRM	10GBASE-LRM SFP+ optic (LC), for up to 220m over MMF
10G-SFPP-SR	10GBASE-SR, SFP+ optic (LC), target range 300m over MMF
10G-SFPP-TWX-0101	DIRECT ATTACHED SFPP ACTIVE COPPER,1M,1-PACK
10G-SFPP-TWX-0301	DIRECT ATTACHED SFPP ACTIVE COPPER,3M,1-PACK
10G-SFPP-TWX-0501	DIRECT ATTACHED SFPP ACTIVE COPPER,5M,1-PACK
10G-SFPP-USR	10GE USR SFP+ optic (LC), target range 100m over MMF, 1-pack
10G-SFPP-ZR	10GBASE-ZR SFP+ optic (LC), for up to 80km over SMF

40G-QSFP-C-00501	40GE QSFP Direct Attached Copper Cable, 0.5m, 1-pack, passive
40G-QSFP-C-0101	40GE QSFP Direct Attached Copper Cable, 1m, 1-pack
40G-QSFP-LR4	40GBase-LR4 QSFP+ optic (LC), for up to 10km over SMF, 1-pack
40G-QSFP-QSFP-C-0101	40GE Direct Attached QSFP+ to QSFP+ Active Copper cable, 1m, 1-pack
40G-QSFP-QSFP-C-0301	40GE Direct Attached QSFP+ to QSFP+ Active Copper cable, 3m, 1-pack
40G-QSFP-QSFP-C-0501	40GE Direct Attached QSFP+ to QSFP+ Active Copper cable, 5m, 1-pack
40G-QSFP-SR-BIDI	40GE SR QSFP+ optic (LC), Bidirectional, 100m over OM3 MMF
40G-QSFP-SR4	40GBASE-SR4 QSFP+ optic (MTP 1x8 or 1x12), 100m over MMF, 1-pack
E1MG-100FX-IR-OM	100Base-FX IR SFP optic for SMF with LC connector, Optical Monitoring Capable. For distances up to 15Km.
E1MG-100FX-LR-OM	100Base-FX LR SFP optic for SMF with LC connector, Optical Monitoring Capable. For distances up to 40Km.
E1MG-100FX-OM	100Base-FX SFP optic MMF, LC connector, Optical Monitoring Capable
E1MG-LX-OM	1000Base-LX SFP optic, SMF, LC connector, Optical Monitoring Capable
E1MG-SX-OM	1000Base-SX SFP optic, MMF, LC connector, Optical Monitoring Capable
E1MG-TX	1000BASE-TX SFP Copper, RJ-45 Connector

Layer 2 Networking

- Virtual Local Area Networks (VLANs)
- Spanning tree
- Link Aggregation

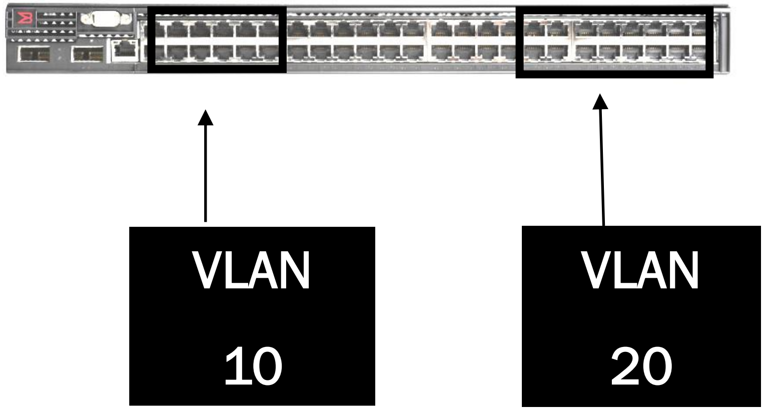
Virtual Local Area Networks (VLANs)

- A virtual LAN (VLAN) is a logical grouping of ports to limit layer 2 broadcast domains
- A VLAN might comprise a subset of the ports on a single switch or subsets of ports on multiple switches
- Systems on one VLAN don't see the traffic associated with systems on other VLANs on the same device(s)
- VLANs allow the partitioning of networks to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure

VLANs

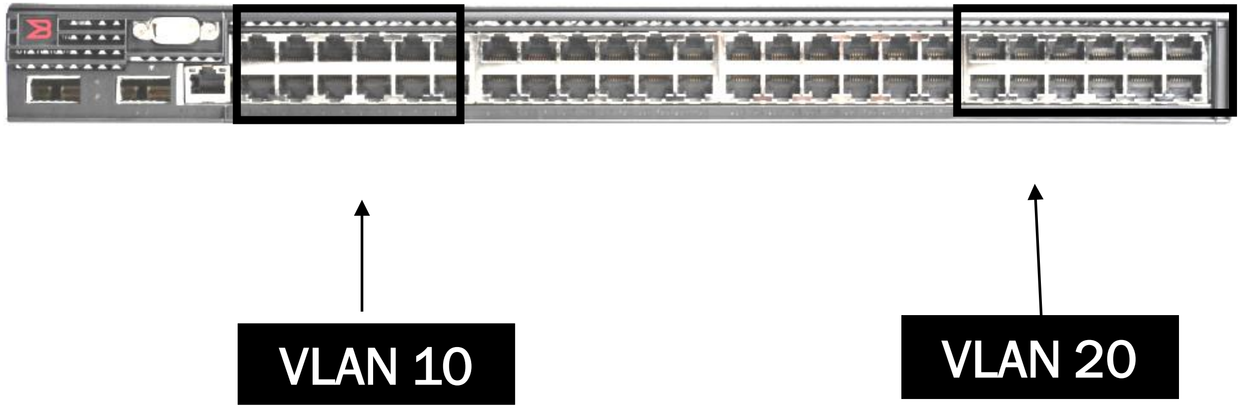
- A VLAN is:
  - A subgroup within a local area network
  - A separate broadcast domain
  - A logical partitioning of a physical LAN into one or more Virtual LANs (VLANs)

- Each VLAN has an ID
  - VLAN IDs (VID) can range from 1 – 4095
    - IDs above 4089 are reserved
  - The default VLAN is 1
    - By default all interfaces belong to VLAN 1
  - VLAN 1 should only be used as a container for unused ports



Port-based VLAN

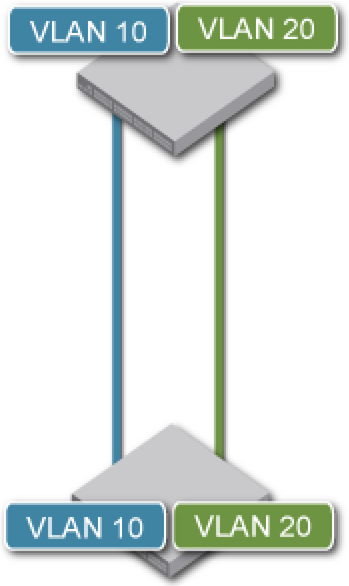
- A port-based VLAN is a broadcast domain, composed of a subset of ports on a Brocade device
- Traffic is bridged within a port-based VLAN and unknown unicasts, broadcasts and multicasts are flooded to all the ports within the VLAN, except the incoming port
- This is the most common type of VLAN



VLAN Without 802.1Q Tagging

- Ports require dedicated uplinks for each VLAN between switches

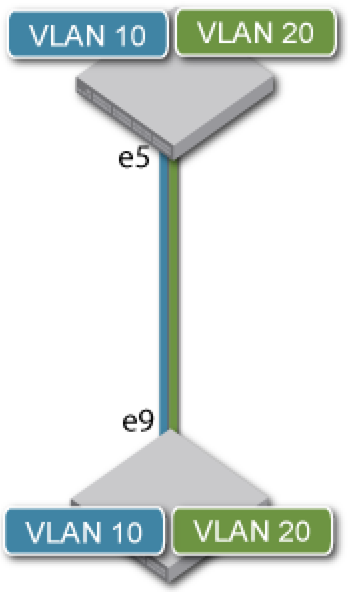
- There is no question where broadcast traffic went from port-to-port



VLAN - 802.1Q Tagging

- VLAN tagging allows multiple VLANs to span switches over a single physical link

- VLAN tagging is needed when a link is connected between any two switches carrying traffic from multiple VLANs

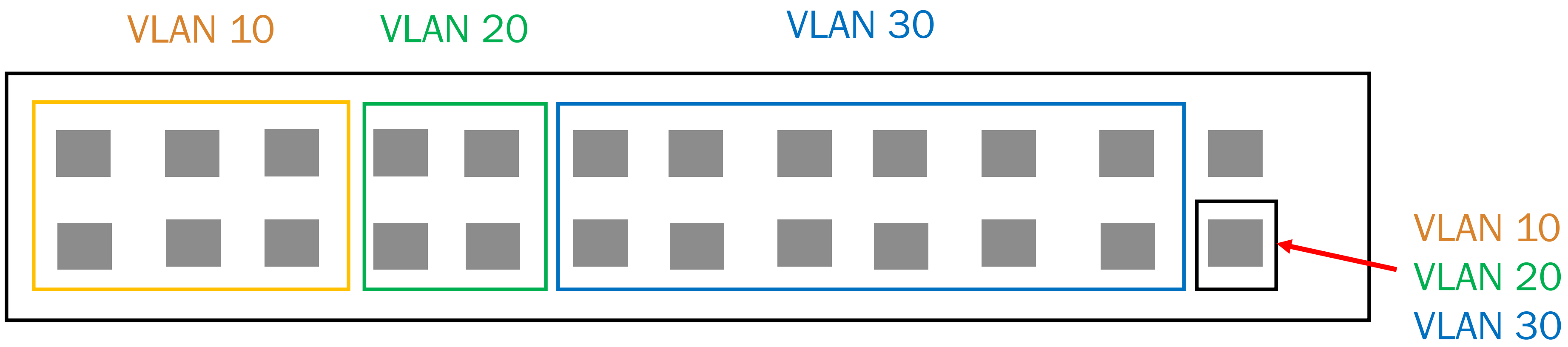


VLAN Types

Port-based VLANs
A group of ports which constitutes a layer 2 broadcast domain. This allows the partitioning of user traffic into logical network segments

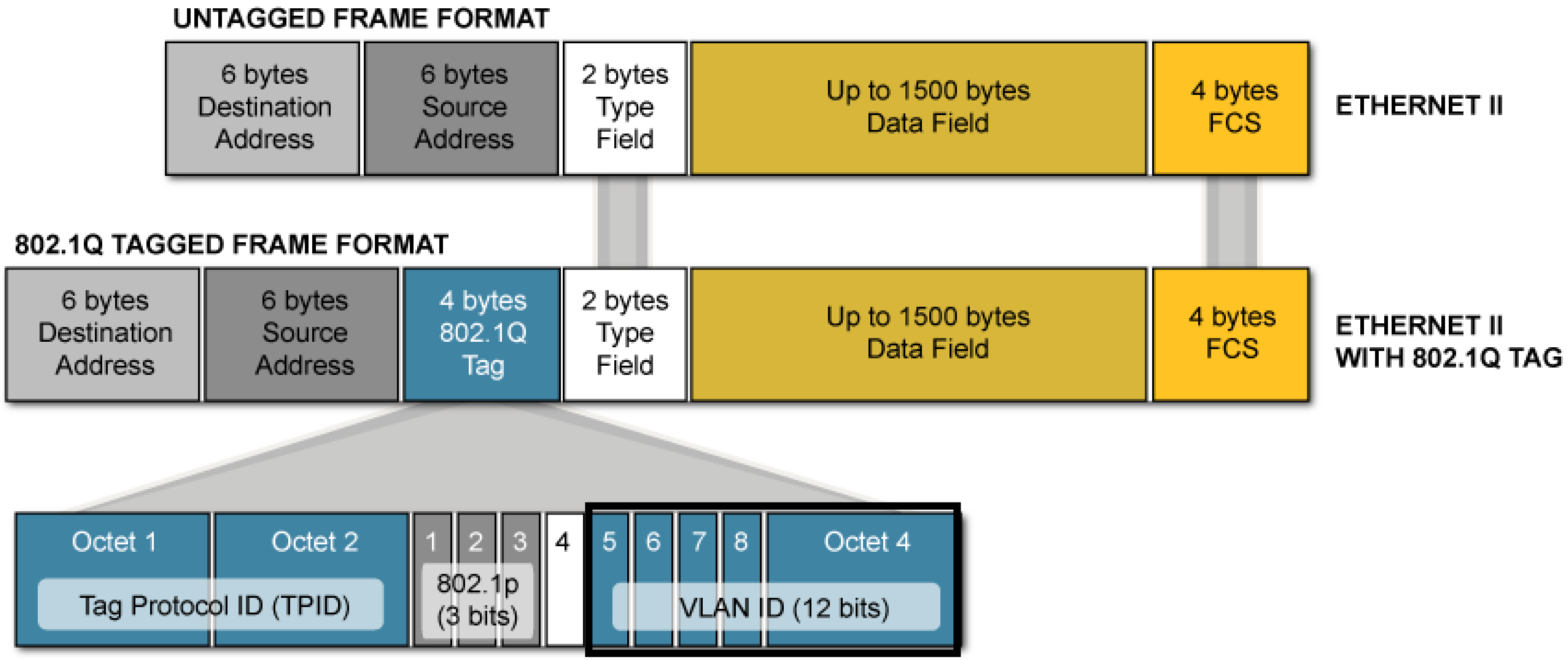
Untagged – No explicit tagging (Q-tag) is added to ethernet frame
- ➢An untagged port can only be a member of one vlan

Tagged Port – Explicit tagged (Q-tag) is added to ethernet frame (used for vlan “trunking” over a single link)
- ➢A tagged port can be a member of multiple vlans

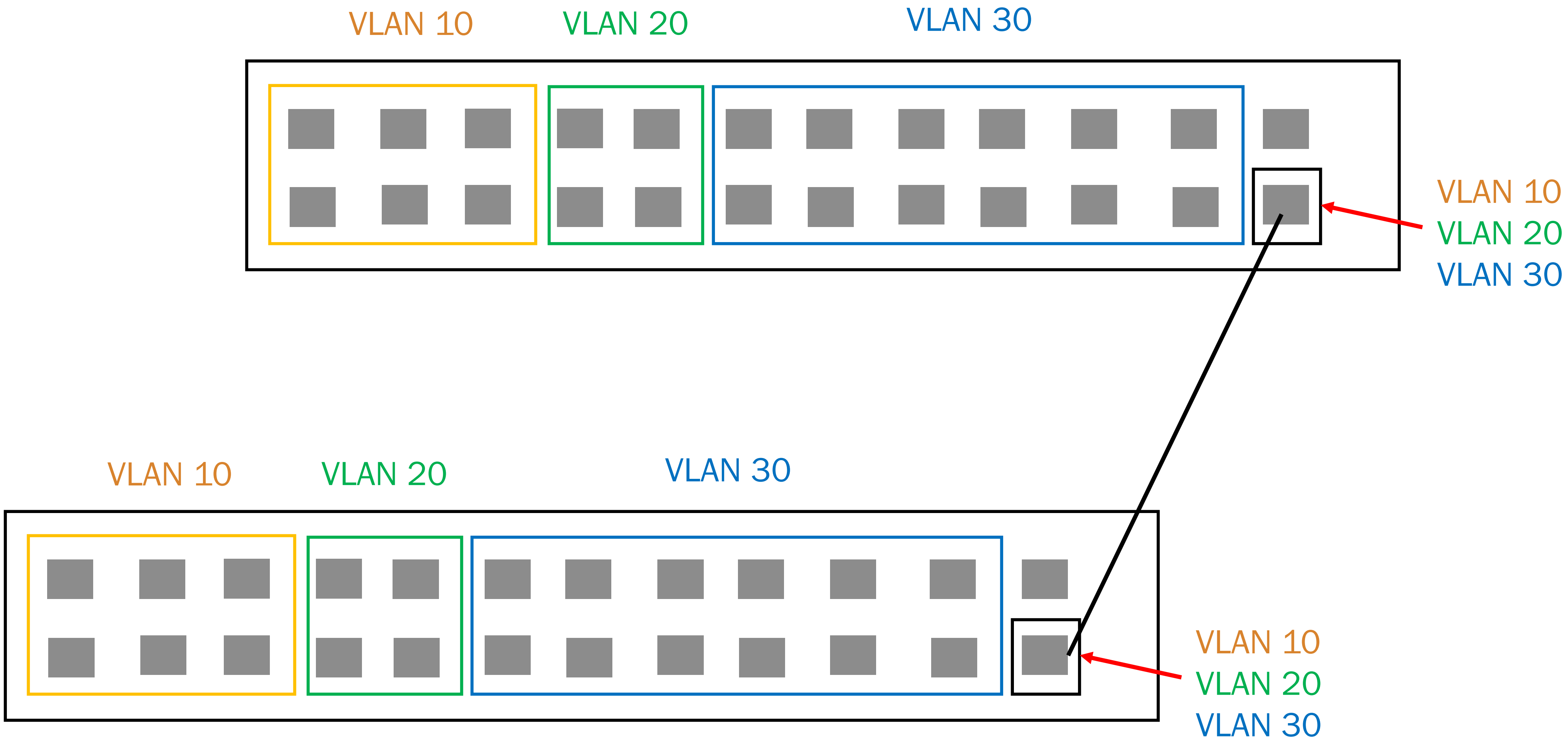


VLAN - 802.1Q Tagging (cont.)

- An 802.1Q tag adds 4 bytes to the frame



VLAN Tagging (Trunk)



Spanning Tree

STP

- STP is defined in IEEE 802.1D
- The spanning tree algorithm ensures a loop free topology by enabling a single path through any physical arrangement of bridges
- STP does the following:
  - Detects redundant links
  - Blocks redundant links
  - Allows for failover to redundant links
- STP is enabled by default on Brocade Layer 2 code
- STP is disabled by default on Brocade Layer 3 code

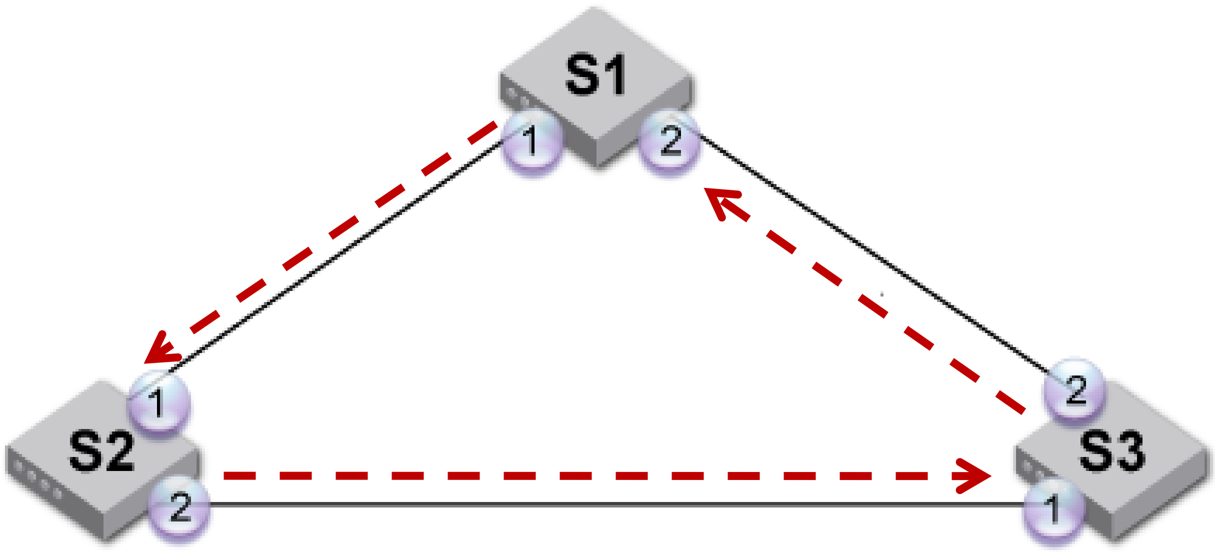
Brocade Spanning Tree Support

- Brocade supports the following STP standards:
  - 802.1D - Spanning Tree Protocol
  - 802.1w - Rapid Spanning Tree (RSTP)
  - 802.1s - Multiple Spanning Tree (MSTP)

- Brocade supports the following STP enhancements:
  - Per-VLAN Spanning Tree
  - Single Instance Spanning Tree (SSTP)
  - Topology Group

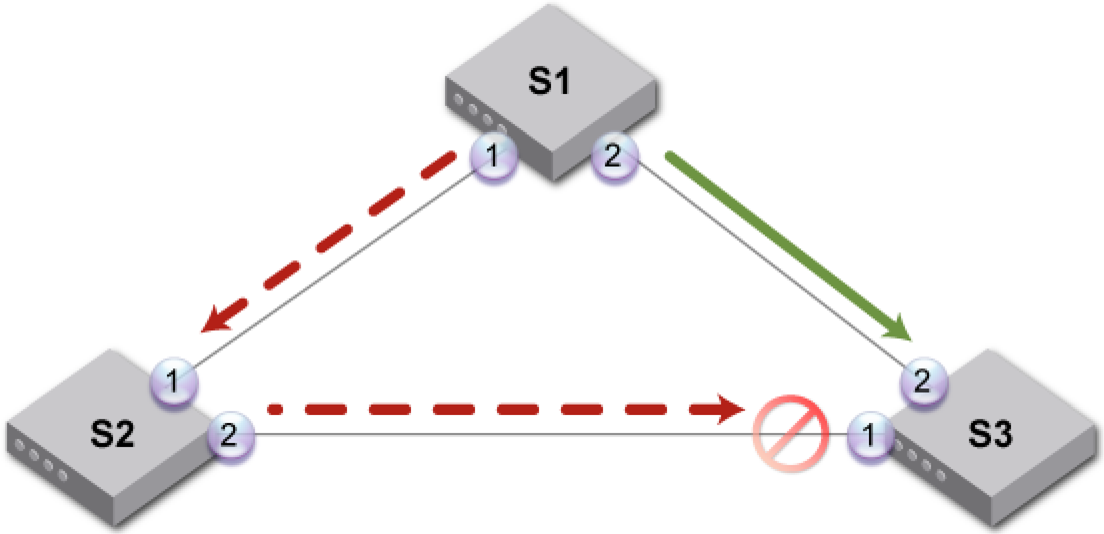
STP (cont.)

- Without STP enabled, redundant links can cause endless loops, especially with broadcast traffic
  - Ethernet has no time out value on frames



STP (cont.)

- With STP enabled, redundant links are blocked, and traffic is forwarded to its destination



Spanning Tree Port States

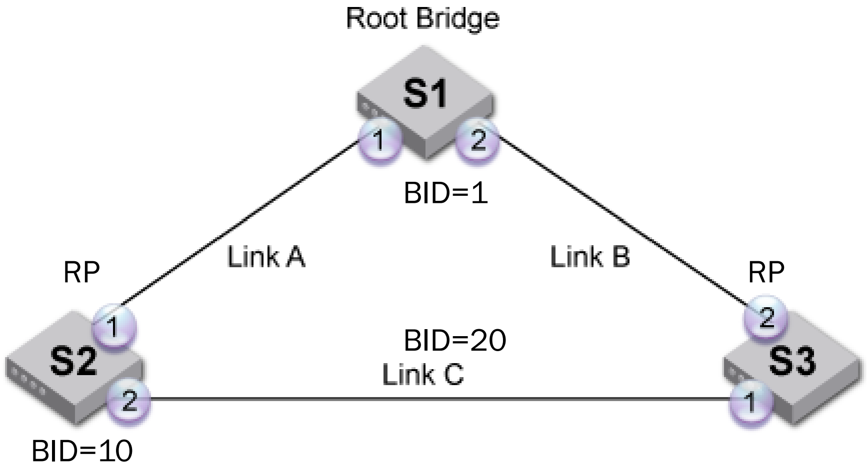
- Disabled
  - Entered when the network administrator explicitly removes a port from operation
- Forwarding
  - The normal (active) operating state where addresses are learned and frames are forwarded
- Blocking
  - The standby state used to prevent loops. Addresses are not learned nor are frames forwarded

Spanning Tree Port States

- Listening State
  - Entered when a port first leaves the Blocking state
- Learning State
  - Entered from Listening state. In the Learning state, addresses are learned, but frames are not forwarded
- The Listening and Learning states are intermediate states that a network goes through in the transition from Blocking to Forwarding. Their purpose is to prevent loops during network reconfiguration

STP Terminology

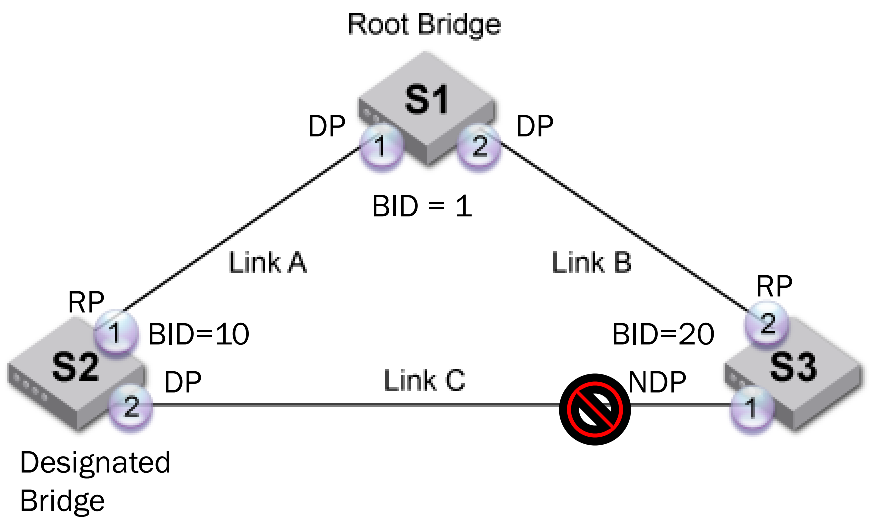
- **Root bridge** - The switch used as a reference point by all other switches in the network for eliminating loops, and determining when an alternate path is required due to a topology change
  - It has the (numerically) lowest bridge ID (BID)
  - By default, each bridge has a configurable priority number, called the bridge priority, and a unique MAC address
  - The BID is a combination of the bridge priority and the MAC address
  - The lowest numerical BID has the highest priority for root bridge selection



  - All other switches in the network calculate path cost to the root bridge to determine which ports will be used, and which will be blocked to eliminate loops
- **Root port** - The port on a non-root bridge that will be used to reach the root bridge
  - If there is more than one port headed toward the root bridge, the one with the lowest path cost is selected

STP Terminology (cont.)

- **Designated bridge** - The bridges on a network segment collectively determine which bridge has the least-cost path from the network segment to the root
- **Designated port** - The port connecting this bridge to the network segment is called the Designated Port (DP) for the segment
  - All ports on the root bridge are designated ports
- **Non-designated port** - The ports that lose the election for designated port are the non-designated ports
  - These are blocked by STP



Bridge Protocol Data Units (BPDUs)

- BPDUs are messages exchanged between switches in a LAN or VLAN to form and maintain a loop free topology

- BPDUs are exchanged between bridges to detect loops in a network topology

- The loops are then removed by placing redundant switch ports in a blocked state

- BPDUs contain information about switches, ports, addresses, priorities, and costs

- There are two types of BPDUs:
  - Configuration BPDUs are generated only by the root bridge and sent to non-root bridges
  - Topology Change Notification BPDUs (TCN BPDUs) are generated by the designated bridge of a LAN segment, and sent towards the root bridge when the designated port goes down

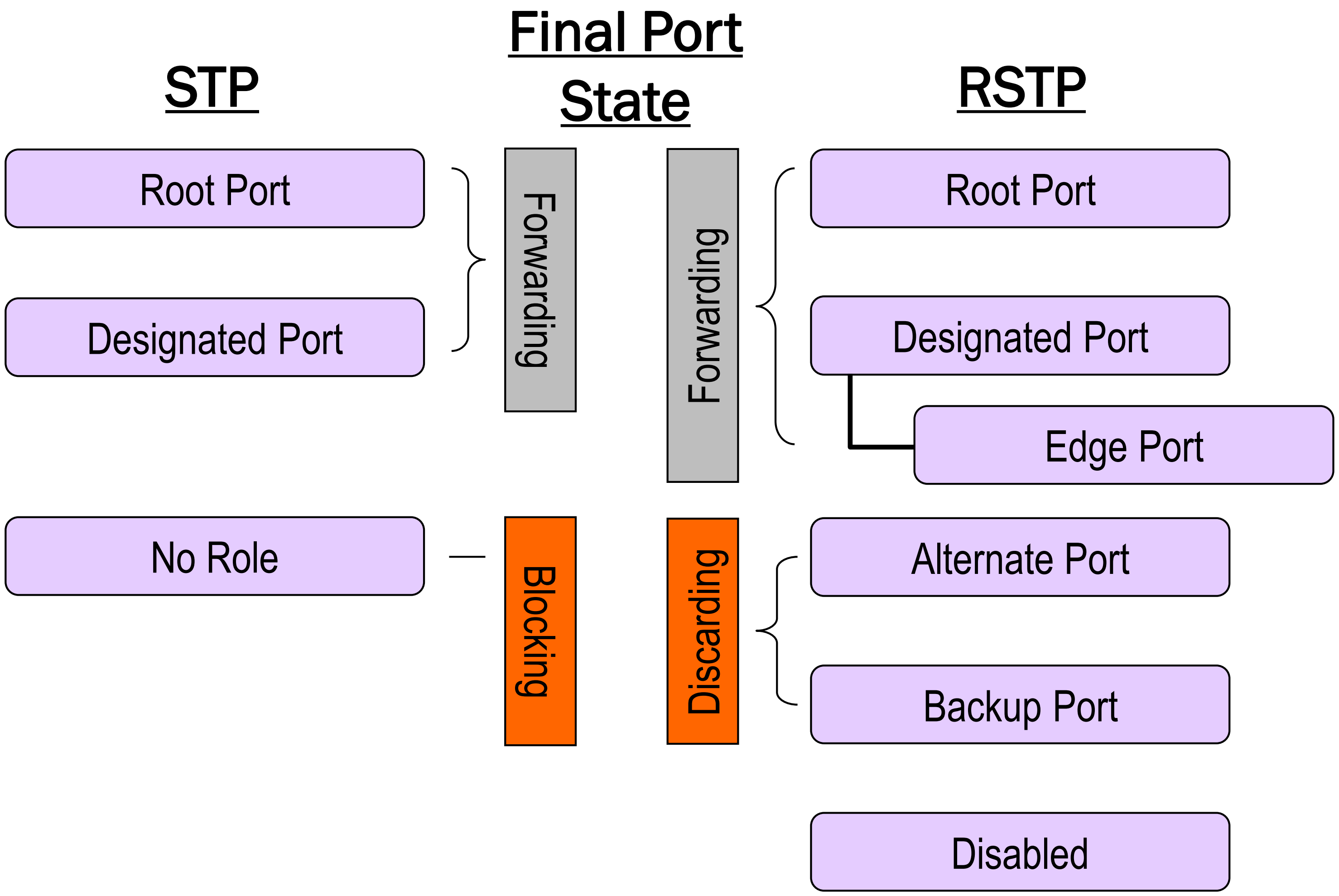
IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)

- 802.1w is an enhancement to the 802.1D Spanning Tree Protocol

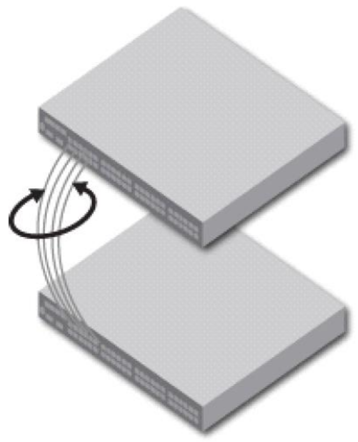
- Convergence in 802.1w is not based on any timer values
  - It is based on the explicit handshakes between directly connected inter-switch links to determine their role

- Convergence time is less than 3 seconds in most cases

STP (802.1d) vs. RSTP (802.1w) – Port Roles



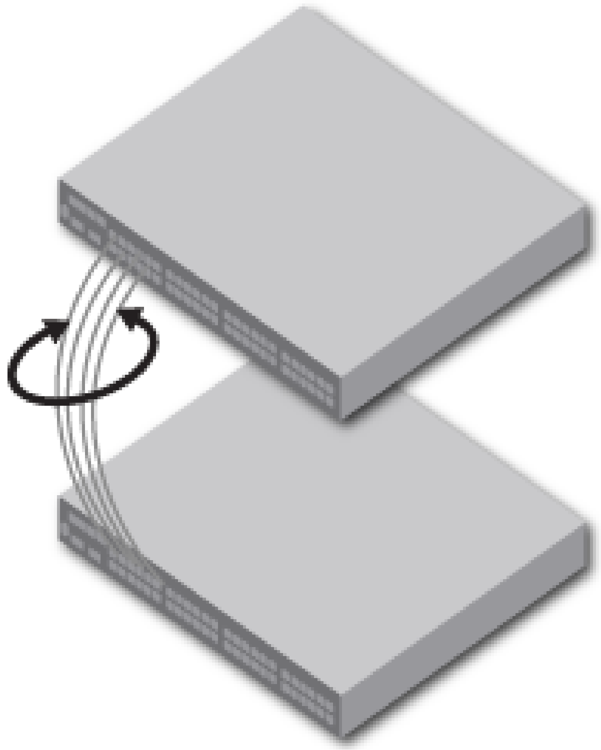
Link Aggregation



- Link Aggregation allows an administrator to combine multiple Ethernet links into a larger logical aggregated link known as a Link Aggregation Group (LAG). Also referred to as a trunk.
- The switch treats the aggregated link as a single logical link.
- In addition to traffic load sharing, trunk groups provide redundant alternate paths for traffic if any of the segments fail
- There are two types of LAG:
  - Static LAG - Manually configured aggregate links containing multiple ports
  - Dynamic LAG: (802.3ad Link Aggregation) - Dynamically created and managed trunk groups using Link Aggregation Control Protocol (LACP)

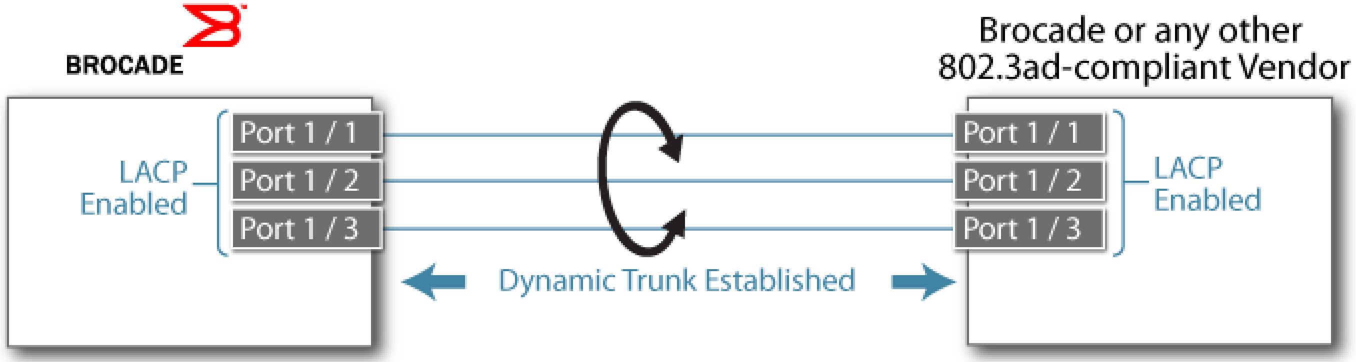
LAG Benefits

- Increased bandwidth
- Increased availability
- Load-sharing
  - More on this later in the presentation
- Sub-second failover to the remaining links in the LAG



802.3ad Dynamic Link Aggregation

- **Link Aggregation Control Protocol (LACP)** is the protocol used to control the bundling of several physical ports together to form a single logical link
- LACP allows a network device to negotiate an automatic bundling of links by sending Link Aggregation Control Protocol Data Units (LACPDUs) to a directly connected device
  - Both devices must be configured to use LACP



Static LAGs

- A dynamic port channel uses special LACP control frames, or protocol data units (PDUs), to negotiate and communicate port information and port channel membership status with the remote network device
- A static port channel does **not** use LACP and essentially forces the ports to join a port channel
- Static configuration is used when connecting the Ethernet switch to another switch or device that does not support LACP
- When using a static configuration, a cabling or configuration mistake by either end of the LAG switch could go undetected and thus can cause undesirable network behavior

LAG Load Sharing (cont.)

- Maximum total bandwidth across a LAG depends on the hash and the specific host-to-host flow. A hash based on a single metric such as a MAC address will limit the BW to the speed of an individual link within the LAG.
- Examples of hash load sharing:

Traffic Type	Hash Algorithm Elements
Layer 2 bridged non-IP	Source and destination MAC addresses
Layer 2 bridged TCP/UDP	Source and destination IP addresses and Source and Destination TCP/UDP ports
Layer 2 bridged IP (non-TCP/UDP)	Source and destination IP addresses
Layer 3 routed traffic	Source and destination IP addresses and protocol field

Demonstration of switch configuration and operation

- VLAN
- Spanning Tree
- Link Aggregation

IGMP Snooping

IGMP Snooping

- When a device processes a multicast packet, by default, it broadcasts the packets to all ports except the incoming port of a VLAN. Packets are flooded by hardware without going to the CPU. This behavior causes some clients to receive unwanted traffic.

- IGMP snooping provides multicast containment by forwarding traffic to only the ports that have IGMP receivers for a specific multicast group (destination address). A device maintains the IGMP group membership information by processing the IGMP reports and leave messages, so traffic can be forwarded to ports receiving IGMP reports.

IGMP Snooping

- You can configure active or passive modes on the device globally or per vlan. If you specify the mode for a vlan, it over rides the global setting. The default mode is passive

- ACTIVE – When active is enabled, the device actively sends out IGMP queries to identify multicast groups on the network and builds entries in the IGMP table based on group membership reports received. Each broadcast domain needs one device running active or a multicast router.
- PASSIVE – When passive is enabled, it forwards the reports to the router ports which receive queries. IGMP snooping in passive mode does not send queries. However it forwards queries to the entire VLAN.
- To Globally set the IGMP mode to active:

```
Brocade(config)# ip multicast active
```

Syntax: [no] ip multicast [active | passive]

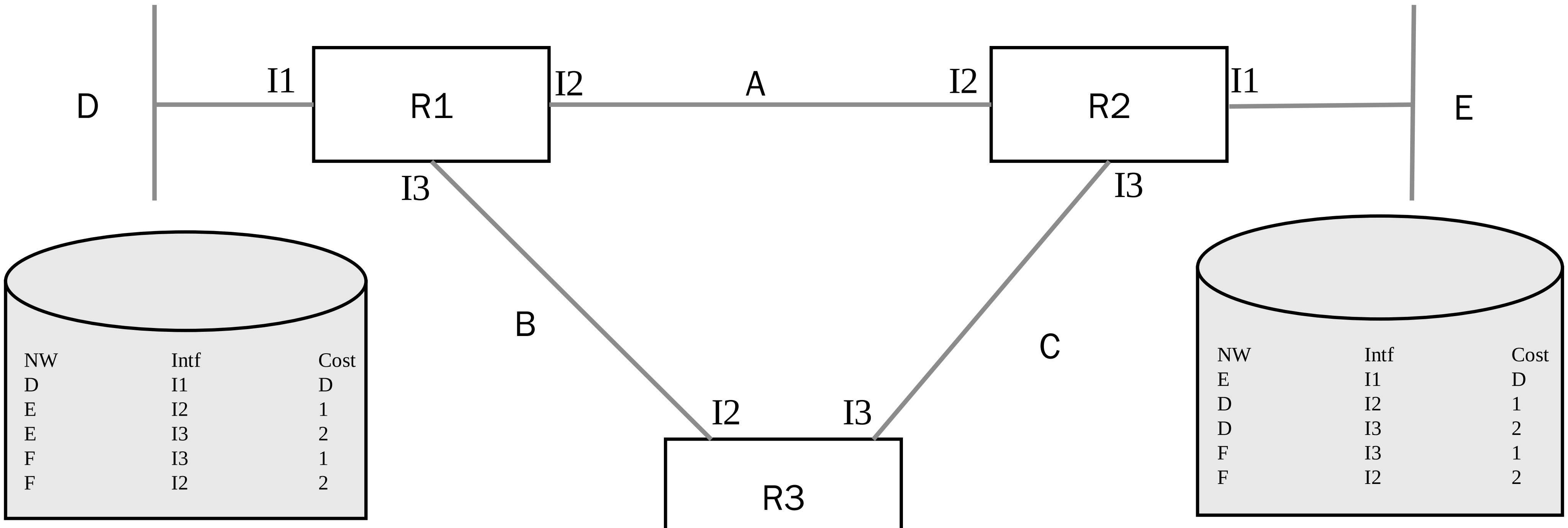
If you do not enter either *active* or *passive*, the passive mode is assumed.

IP Addressing

Routing

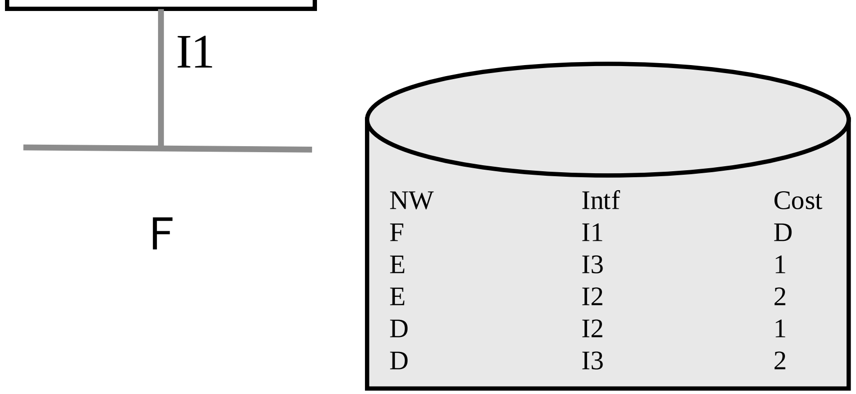
- Routing explanation
- IP addressing overview
- Routing protocol basics
- Multicast overview

Routing Explanation



NW	Intf	Cost
D	I1	D
E	I2	1
E	I3	2
F	I3	1
F	I2	2

NW	Intf	Cost
E	I1	D
D	I2	1
D	I3	2
F	I3	1
F	I2	2



NW	Intf	Cost
F	I1	D
E	I3	1
E	I2	2
D	I2	1
D	I3	2

Layer 3 Networks
Administator assign addressing

Routing Protocol Basics

- Direct attached networks – networks assigned to local interfaces on router
- Static Routes – Routes that are manually configured on router

Dynamic Protocols

- RIP (Routing Information Protocol) – All routes are exchanged between routers.
  - Based on hop count.
  - Typically used in small networks
- OSPF (Open Shortest Path First) –
  - Only exchanges route updates.
  - Based on link cost
  - Scales to larger networks

Routing vs. Routed Protocols

- A routed protocol is a protocol by which data can be sent among routers.
  - Examples: IP, IPX, AppleTalk
- A routing protocol is only used between routers to help routers build and mainta
  - Examples: RIP, OSPF, IS-IS, BGP
- Routing Table:

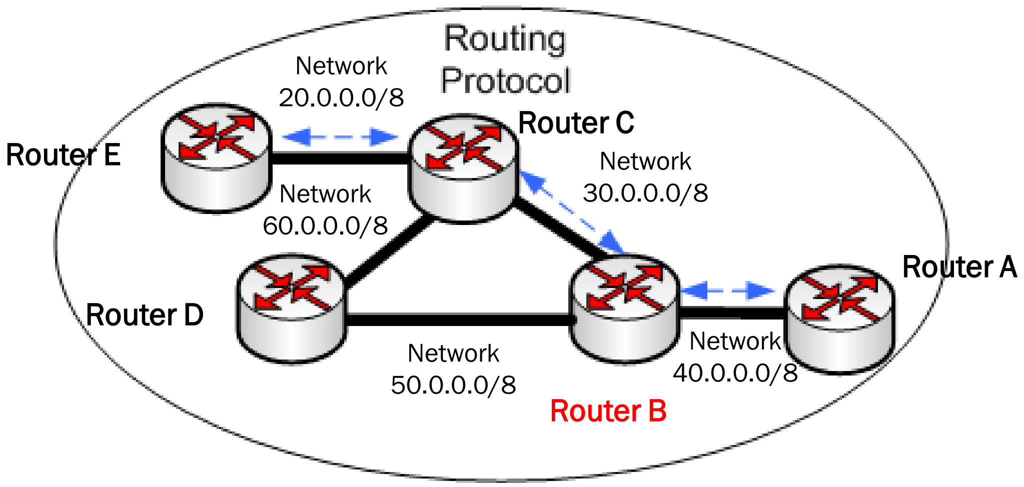
```
FastIron#show ip route
Total number of IP routes: 2
Start index: 1 B:BGP D:Connected R:RIP S:Static O:OSPF *:Candidate default
  Destination         NetMask     Gateway                Port        Cost Type
1 209.157.20.0   255.255.255.0    0.0.0.0                lb1         1    S
2 209.157.22.0   255.255.255.0    0.0.0.0                4/11        1    D
3 172.17.41.4    255.255.255.252  137.80.127.3           4/12        2    O
```

Routing Tables

- A router uses its routing table to determine the next hop for the packet's destination and forwards the packet appropriately[1]
  - The next router repeats this process using its own routing table until the packet reaches its destination
  - At each stage, the IP address in the packet header is used to determine the next hop
  - If either a destination network or a default route are not in the routing table, the packet is dropped

Routing Tables (cont.)

```
RouterB# show ip route
Total number of IP routes: 5, avail: 79994 (out of max 80000)
B:BGP D:Connected  R:RIP  S:Static  O:OSPF *:Candidate default
     Destination     NetMask         Gateway         Port       Cost    Type
1    20.0.0.0        255.0.0.0       30.1.1.1        12         2       R
2    30.0.0.0        255.0.0.0       0.0.0.0         12         1       D
3    40.0.0.0        255.0.0.0       0.0.0.0         10         1       D
4    50.0.0.0        255.0.0.0       0.0.0.0         11         1       D
5    60.0.0.0        255.0.0.0       30.1.1.1        12         2       R
```



Routing Tables (cont.)

- **Destination and NetMask:** The destination network and network mask of the route
- **Gateway:** The next-hop router
- **Port:** The local router port used to send packets to the destination route
- **Cost:** The route's cost or metric
- **Type:** The source of the learned route

```
RouterB# show ip route
Total number of IP routes: 5, avail: 79994 (out of max 80000)
B:BGP D:Connected  R:RIP  S:Static  O:OSPF *:Candidate default
     Destination     NetMask         Gateway         Port       Cost    Type
1    20.0.0.0        255.0.0.0       30.1.1.1        12         2       R
2    30.0.0.0        255.0.0.0       0.0.0.0         12         1       D
3    40.0.0.0        255.0.0.0       0.0.0.0         10         1       D
4    50.0.0.0        255.0.0.0       0.0.0.0         11         1       D
5    60.0.0.0        255.0.0.0       30.1.1.1        12         2       R
```

Classful IP Addressing

Class	Subnet Mask decimal	No. of Hosts per Network	No. of Networks	Start -End Address
A	255.0.0.0	16 Million	127	1.0.0.0 - 126.255.255.255
B	255.255.0.0	65000	16000	128.0.0.0 - 191.255.255.255
C	255.255.255.0	254	2 Million	192.0.0.0 - 223.255.255.255
D	Reserved for multicast groups			224.0.0.0 - 239.255.255.255
E	Reserved for future use, or Research and Development Purposes			240.0.0.0 - 254.255.255.254

IP Subnetting

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1000000	01000000	0010000	00010000	00001000	00000100	00000010	00000001
128	64	32	16	8	4	2	1

192.168.1.0/24

Use logical AND function

11000000.10101000.00000001.00000000 192.168.1.0
11111111.11111111.11111111.00000000 255.255.255.0
11000000.10101000.00000001.00000000 192.168.1.0

IP Subnetting Example

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1000000	01000000	0010000	00010000	00001000	00000100	00000010	00000001
128	64	32	16	8	4	2	1

192.168.1.0/27

11000000.10101000.00000001.00000000 192.168.1.0
11111111.11111111.11111111.XXX00000 255.255.255.224

000	192.168.1.0
001	192.168.1.32
010	192.168.1.64
011	192.168.1.96
100	192.168.1.128
101	192.168.1.160
110	192.168.1.192
111	192.168.1.224

8 Subnets
With each subnet handling 32 hosts

Multicast Routing

Protocol Independent Multicast (PIM)

- PIM is a routing protocol used for forwarding multicast traffic between IP subnets or network segments
- As the name implies, PIM works independently of any particular routing protocol
  - PIM does not create and maintain a multicast routing table
    - It uses the unicast routing table, which, since it can be populated by more than one protocol, is also protocol independent
- There are two operating modes for PIM
  - **Dense mode** - suitable for densely populated multicast groups, primarily in the LAN environment
  - **Sparse mode** - suitable for sparsely populated multicast groups with the focus on WAN

PIM Dense Mode (PIM-DM)

- This mode works on the premise that there are members throughout the entire network
- PIM-DM builds its multicast tree by flooding traffic from the source to all dense mode routers in the network
  - This will propagate unnecessary traffic for a short time
- Each router checks to see if it has active group members waiting for the data
  - If so, the router remains quiet and lets the traffic flow
  - If no hosts have registered for that group, the router sends a prune message toward the source, and that branch of the tree is “pruned” off to stop unnecessary traffic flow
- Trees built with this flood and prune method are called Source Trees

PIM Sparse Mode (PIM-SM)

- Sparse Mode works on the premise that multicast receivers are not positioned in all areas of the network
- One router is designated as the Rendezvous Point (RP), and is usually centrally located in the network
  - Receivers send join messages to the RP, to let it know which multicast groups they are interested in
  - Sources send register messages to the RP, to let it know which groups they are sending
  - Multicast traffic from all sources is sent to the RP for redistribution out to the receivers
  - Since all source traffic flows through the RP, this configuration is called a shared tree