INF0 341

Switching, VLANs, and Spanning Tree

By

Bob Larson

Email: blabob@uw.edu
Linkedin: https://www.linkedin.com/in/boblarson
Web site: http://faculty.washington.edu/blabob/bob/

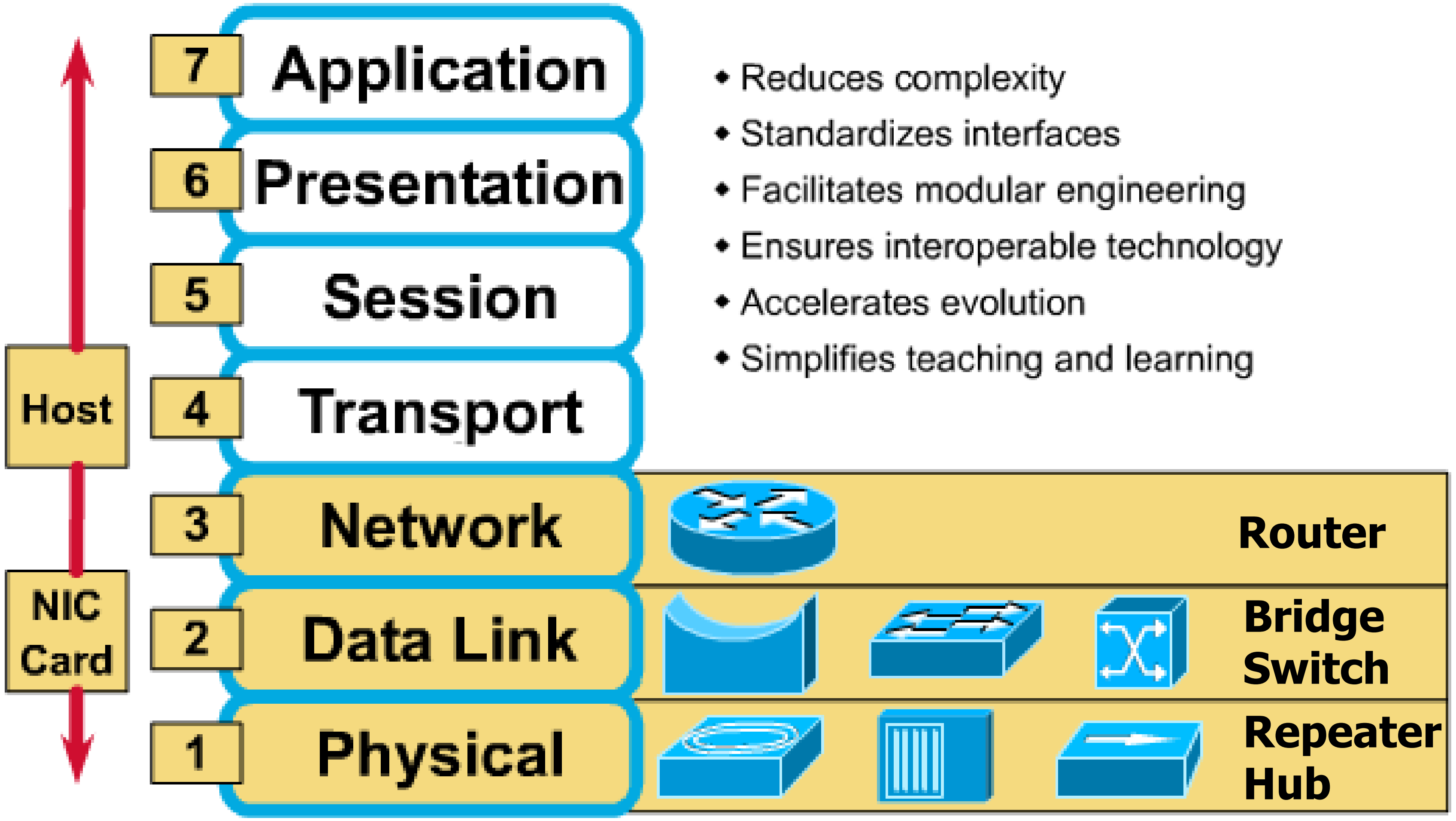
Plan for this Week

- TCP/IP and OSI Reference Models
- Ethernet Broadcast Domains
- Layer 2 (LAN) Switches
- What Layer 2 LAN Switches Do
- Three Switching (Forwarding) Modes
- Blocking vs non-Blocking LAN Switches
- Virtual LAN (VLAN)
- What is a Switching Loop or Bridge Loop?
- Spanning Tree Protocol (STP)

TCP/IP and OSI Reference Models

DATA	OSI MODEL		TCP MODEL
Data	7	Application Network Process to Application	Application
Data	6	Presentation Data Representation and Encryption	
Data	5	Session Inter host Communication	
Segment	4	Transport End to End connection and reliability	Transport
Packet	3	Network Best path determination and IP (Logical) Addressing	Internet
Frame	2	Data Link MAC and LLC (Physical Addressing)	Network Access
Bits	1	Physical Media, Signal and Binary Transmission	

Reference Model Devices



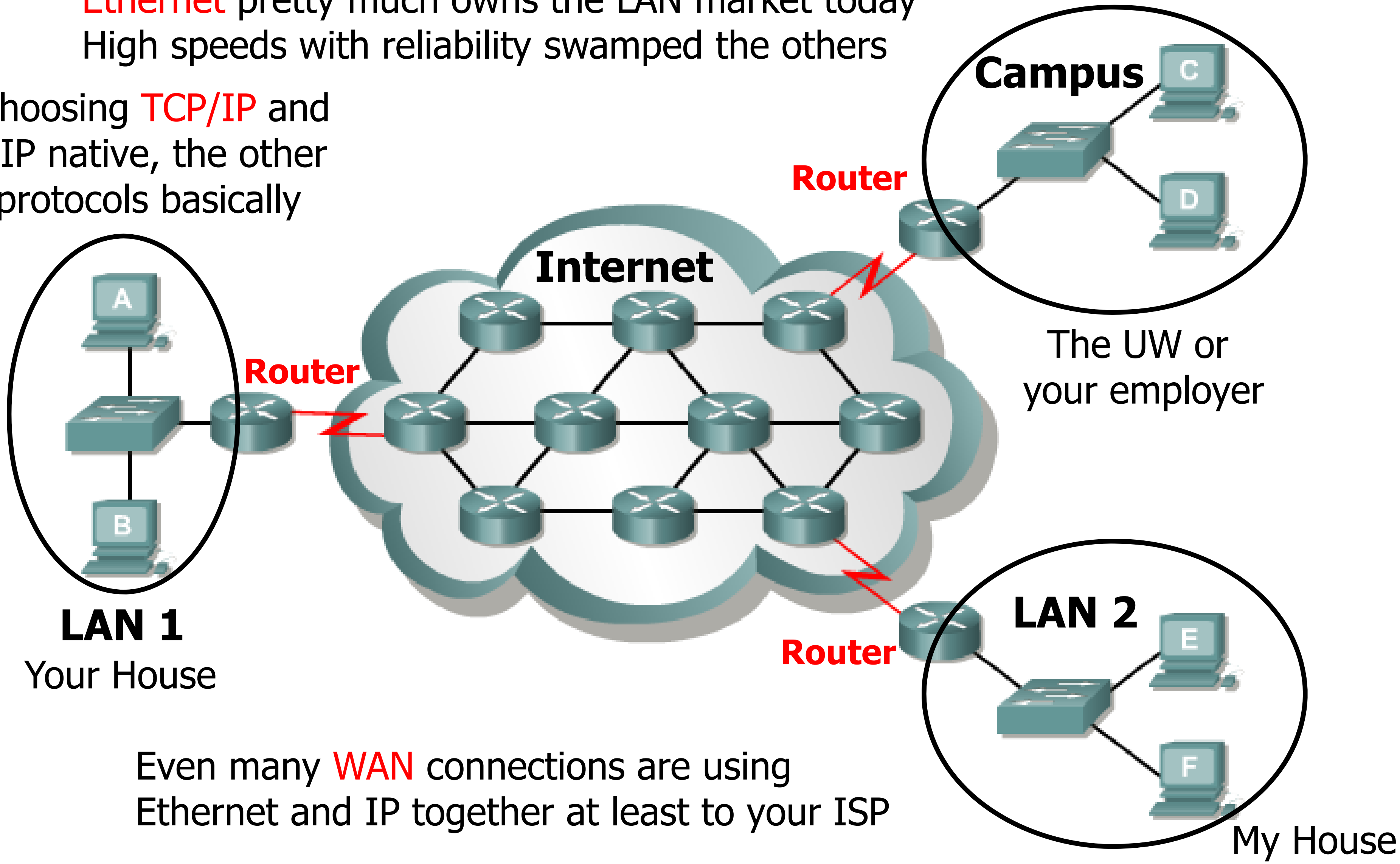
- Reduces complexity
- Standardizes interfaces
- Facilitates modular engineering
- Ensures interoperable technology
- Accelerates evolution
- Simplifies teaching and learning

Supports any Physical connection protocol including Ethernet
Supports any Network address and protocol including TCP/IP (IP addresses)

LANs and WANs

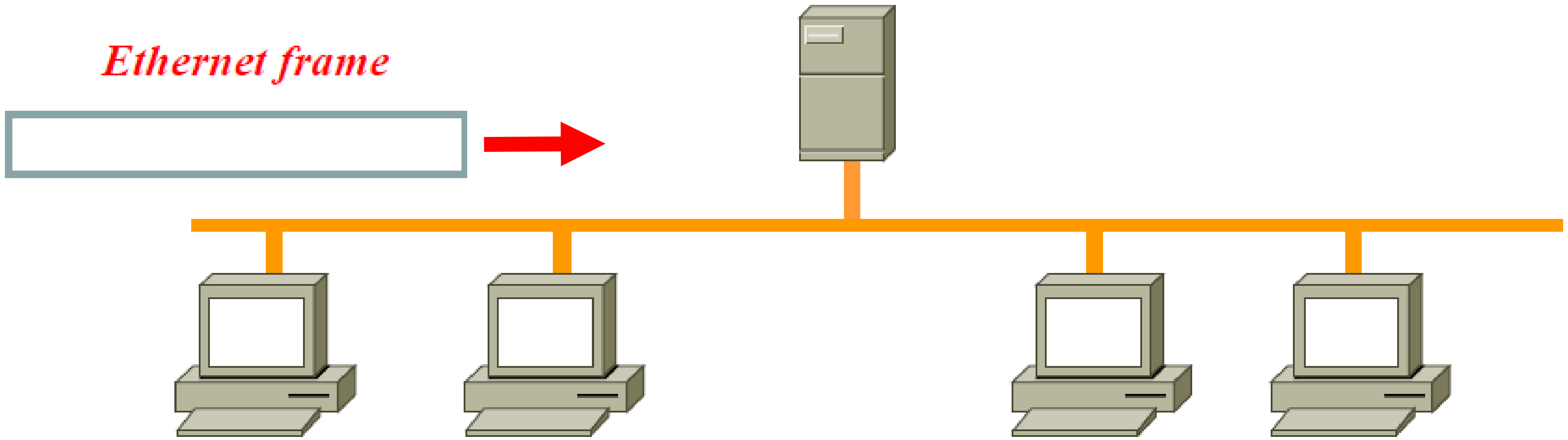
Ethernet pretty much owns the LAN market today
High speeds with reliability swamped the others

With the Internet choosing TCP/IP and Windows 95 going IP native, the other Network (Layer 3) protocols basically withered away



Even many WAN connections are using
Ethernet and IP together at least to your ISP

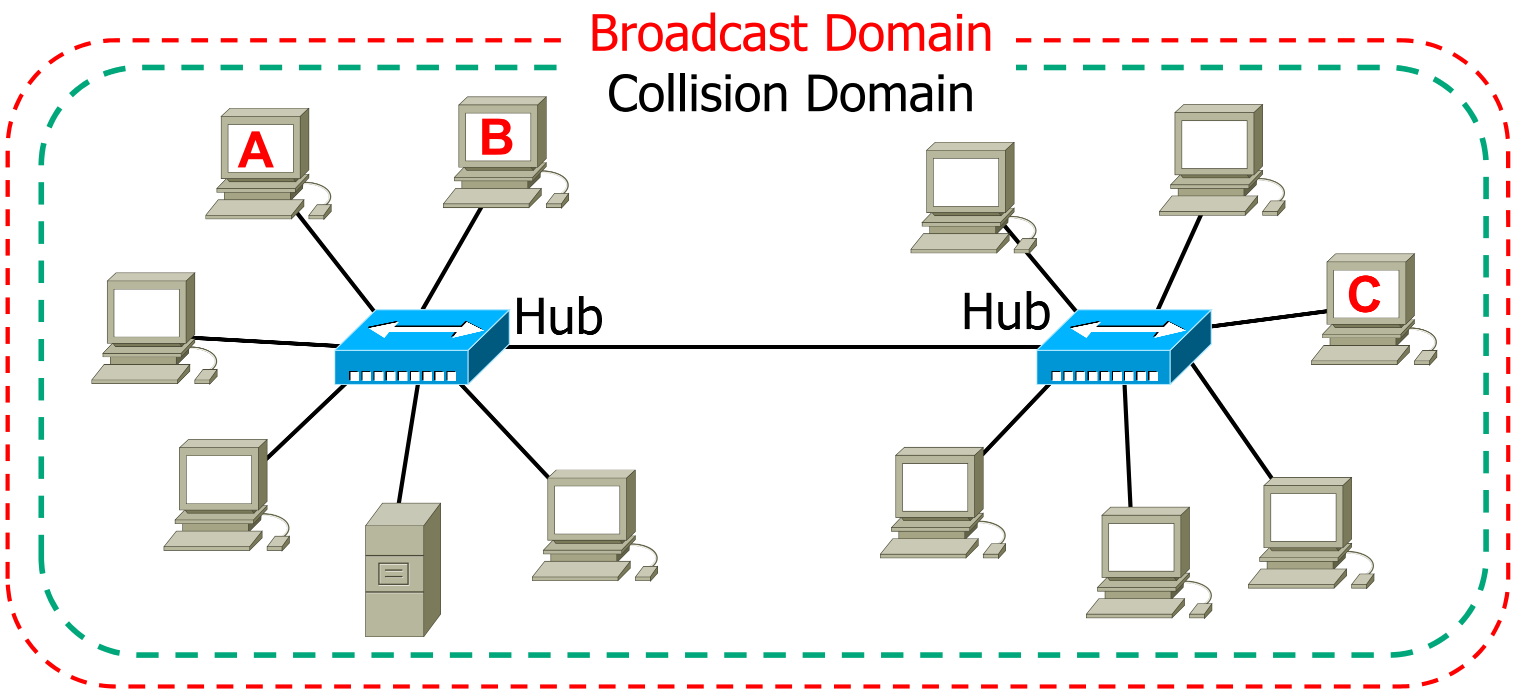
Ethernet Broadcast Domain



- In a shared media LAN segment (originally coaxial cable)
  - Every device sees every transmitted frame
  - Every device sees every collision
    - Segment needs to be cleared and retransmit process starts
  - One frame at a time in one direction (Half-Duplex)

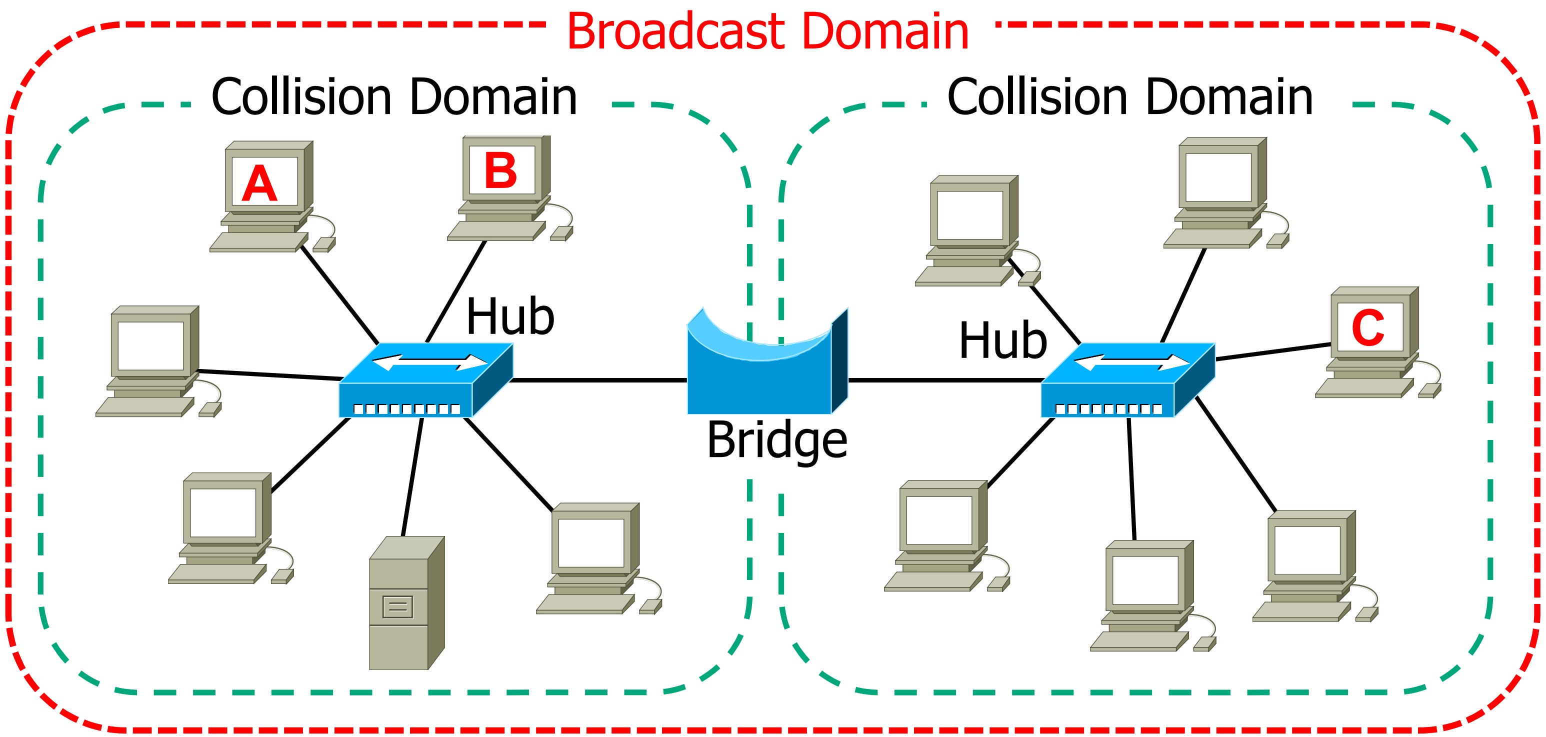
Broadcast & Collision Domain – Hubs

Hubs emulate coaxial cable (Half-Duplex)



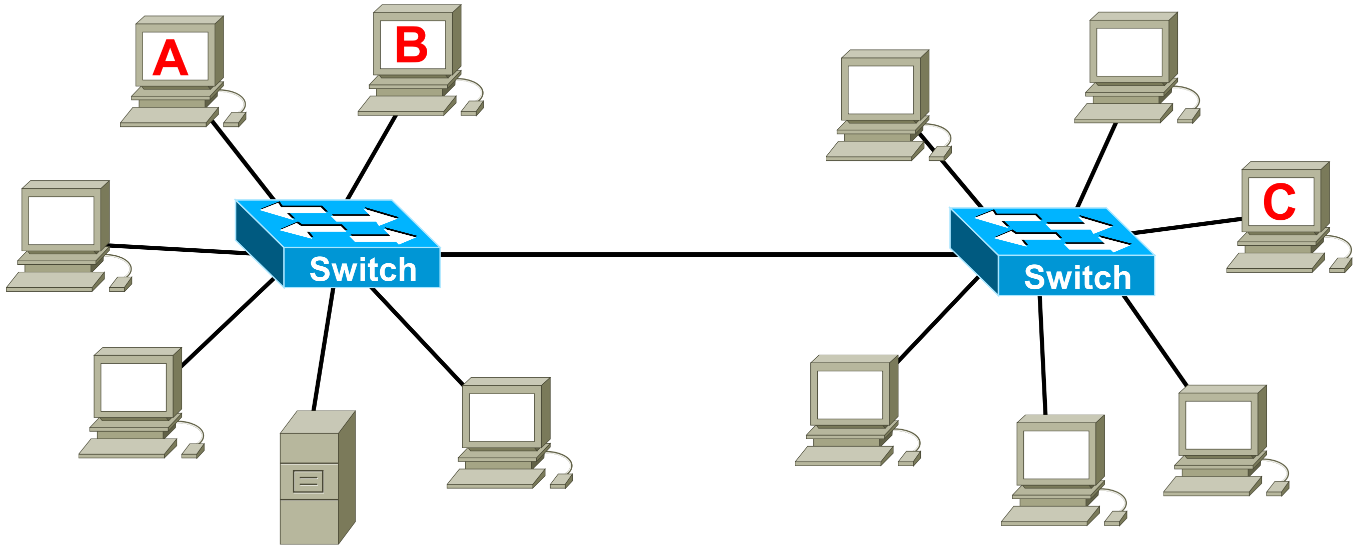
- Broadcast Domain
  - Any broadcast frame (MAC FF:FF:FF:FF:FF:FF) is seen by all devices
  - All frames in an all Hub network are treated the same as a broadcast
- Collision Domain
  - Any two devices transmitting frames at the same time will collide

Broadcast & Collision Domain – Bridge



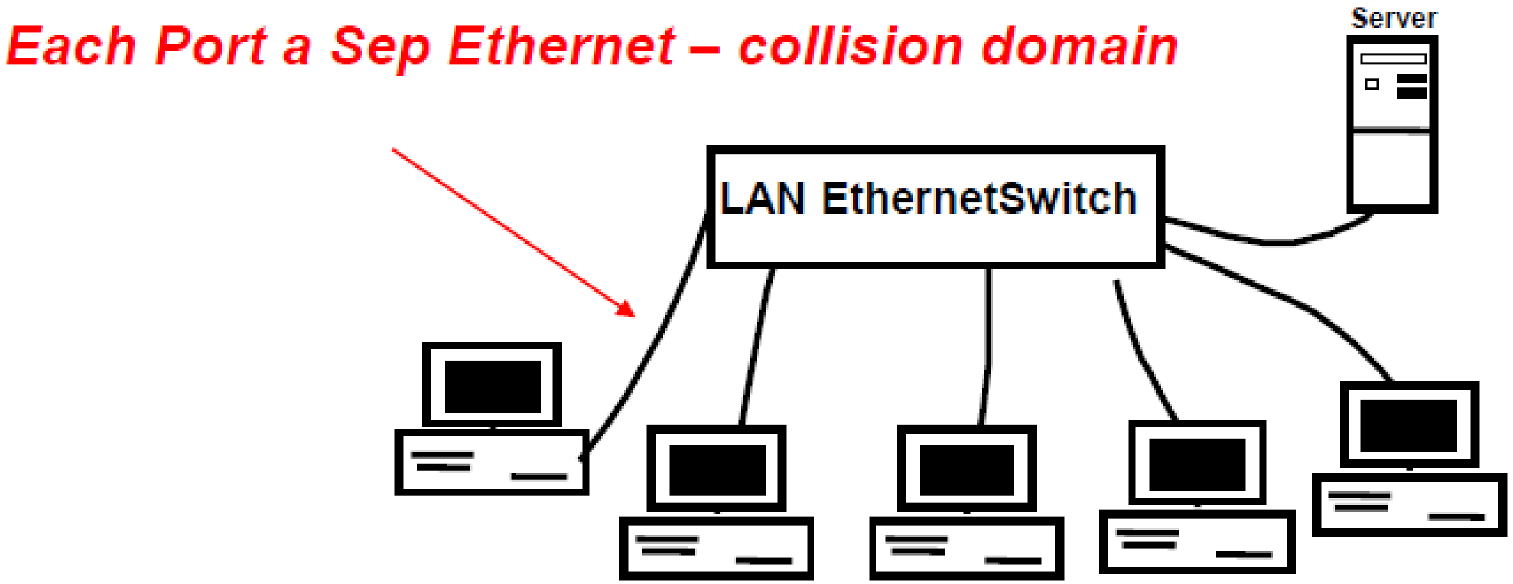
- Bridge splits Collision Domain in two
  - All unicast frames only cross Bridge if destination not in source domain
    - Filter (discard) if source and destination are on the same port
    - Forward if source and destination are on different ports
  - Any broadcast frame (MAC FF:FF:FF:FF:FF:FF) is still seen by all devices

Layer 2 (LAN) Switching



- Layer 2 switches are basically multi-port bridges (and more)
  - Each segment (between two devices) is
    - A separate collision domain
    - Is not a shared media (doesn't emulate coax) – uses separate wire pairs
      - Capable of full-duplex – simultaneous bidirectional traffic (2x throughput max)
      - Collision free segment
    - Capable of independent bandwidth (speed) based on slowest device

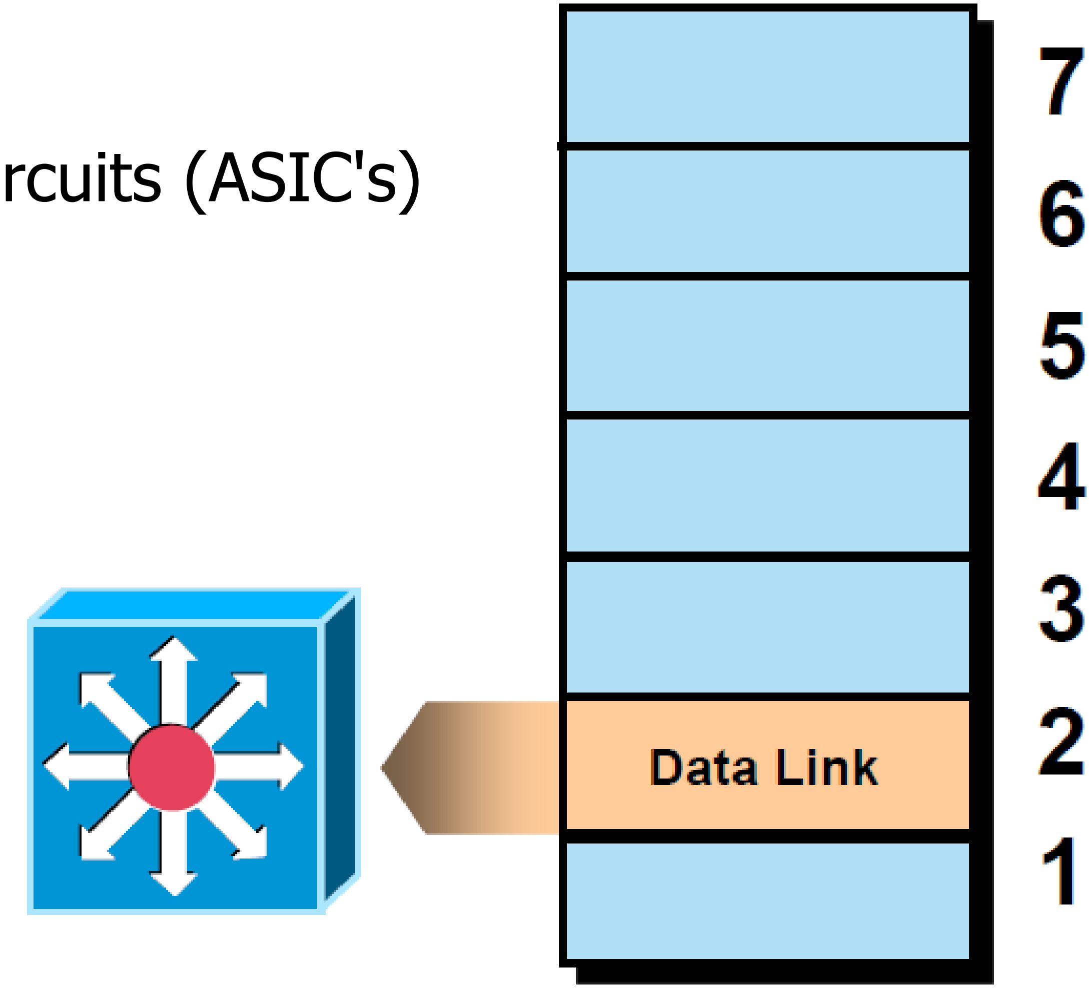
LAN Switching Quick Quiz



- Is each LAN Switch port a separate broadcast domain?
- How might a LAN Switch complicate LAN troubleshooting?

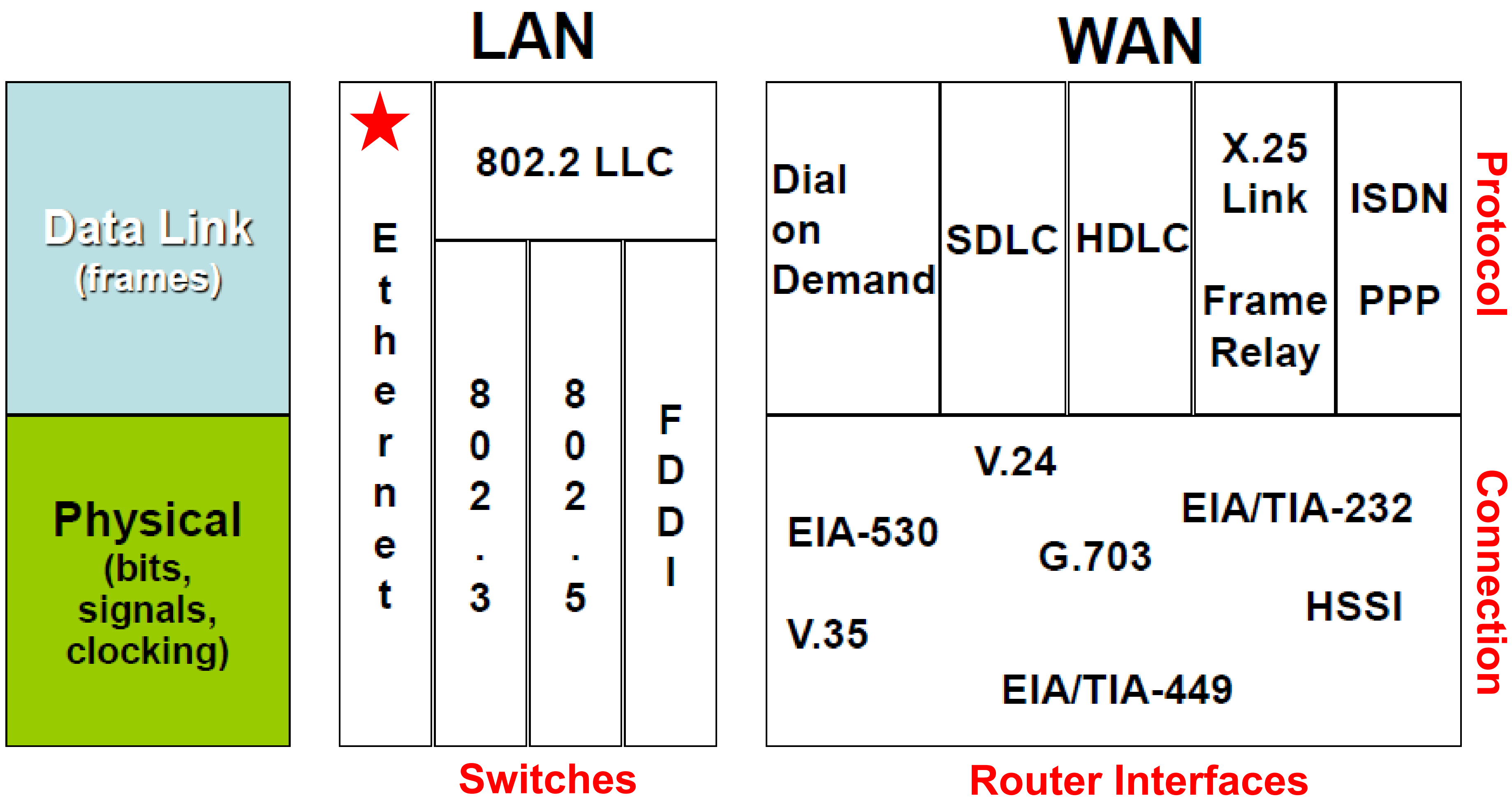
Layer 2 Switching

- Hardware-based bridging
  - Application Specific Integrated Circuits (ASIC's)
- Wire-speed* performance
- High-speed scalability
- Low latency
- MAC address (Layer 2)
- Low cost



* No latency (delay) within switch – two same "speed" ports can send data between them at maximum port speed with no packet loss

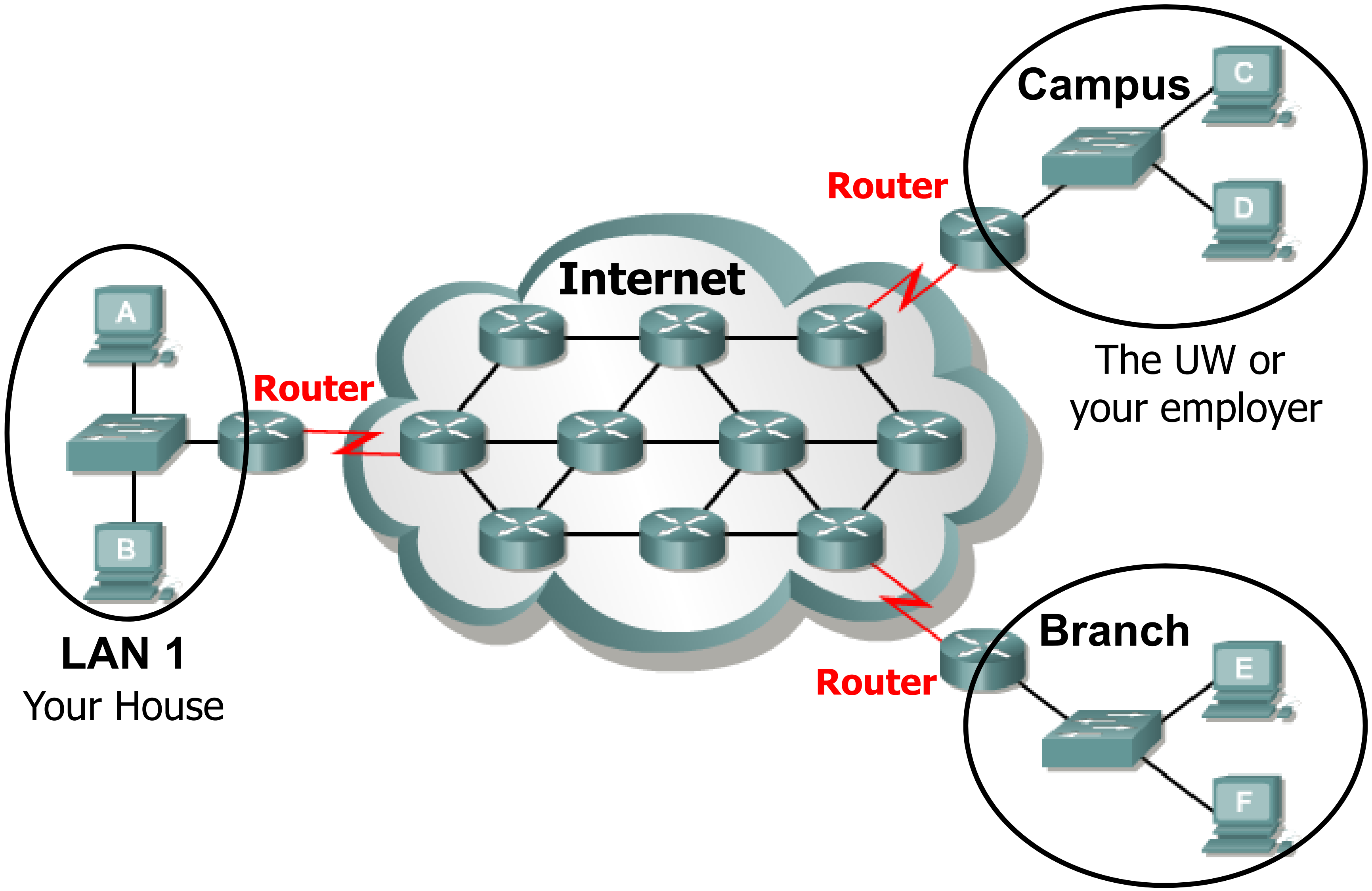
Physical and Data-Link Standards



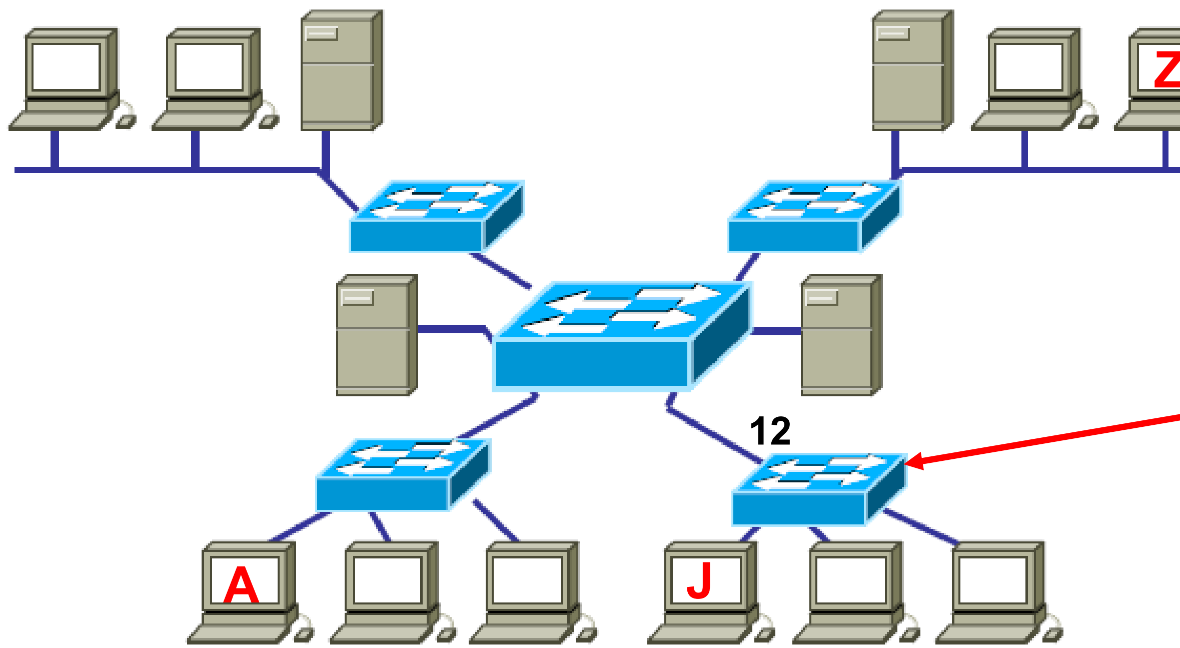
- Separate physical and data link layers for LAN and WAN

WAN Links – the Router-to-Router Links*

* In this diagram



What Layer 2 LAN Switches Do



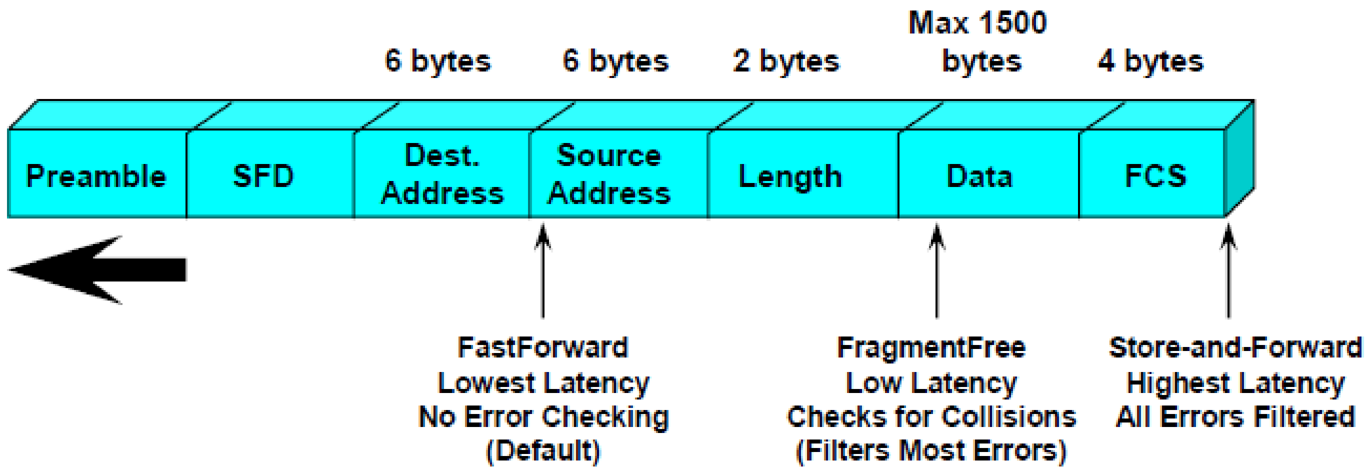
CAM Table*

MAC Address	Int
EC-F4-BB-8D-2E-7E	2
56-27-1E-FA-F9-6F	6
54-27-1E-FA-F9-6F	12
54-27-1E-F4-95-6A	7
56-27-1E-FF-19-23	12
56-27-1E-67-FA-C1	12
EC-F4-BB-91-24-8C	12
...	...

* Content Addressable Memory table

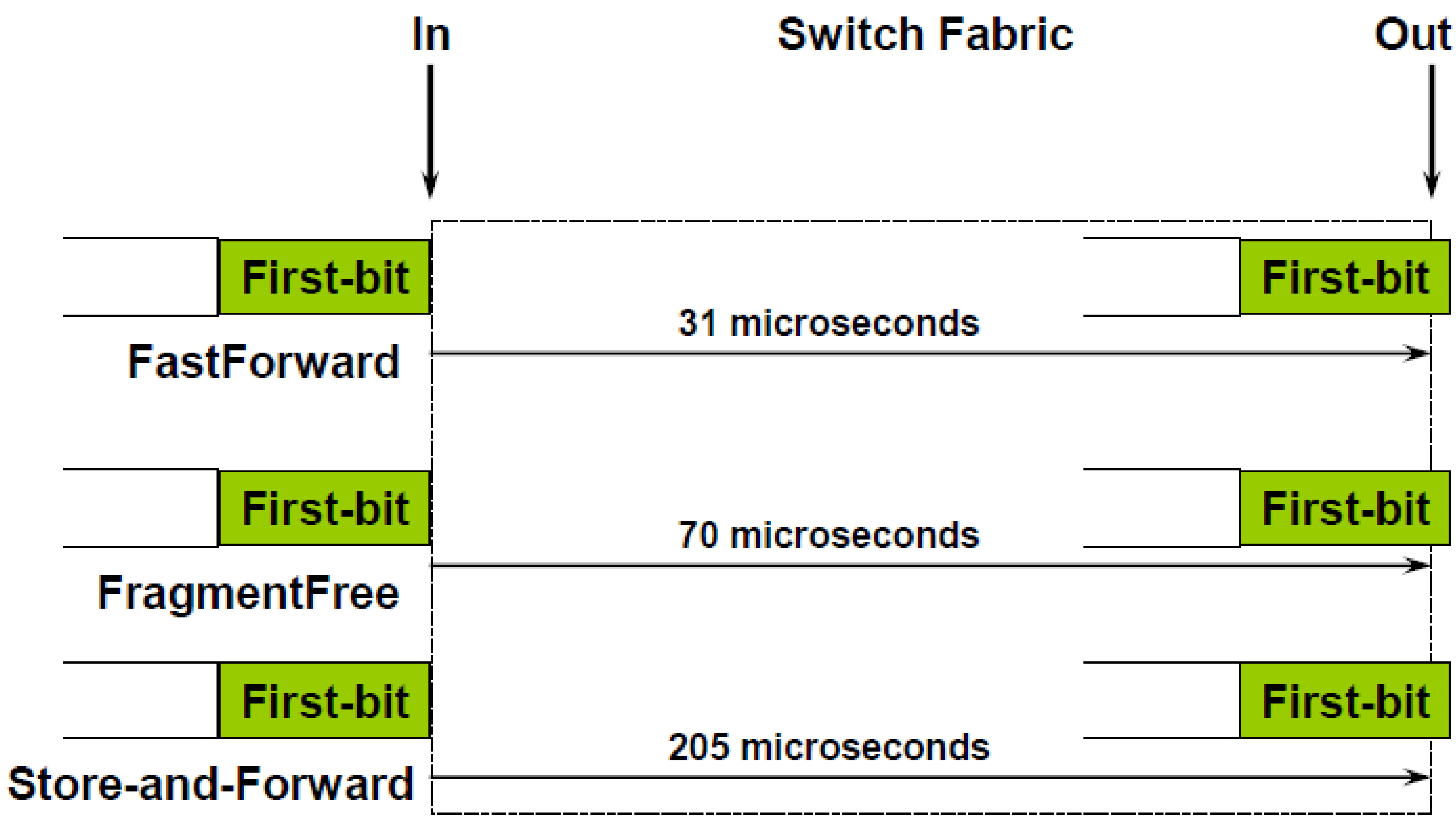
- Three basic functions a Switch has to perform:
  - Build a table (CAM) listing all layer 2 address and source port
  - Make forwarding decisions based on destination MAC address
    - Filter (discard) if source and destination are on the same port
    - Forward if source and destination are on different ports
  - Break up loops (Spanning Tree)

Three Switching (Forwarding) Modes



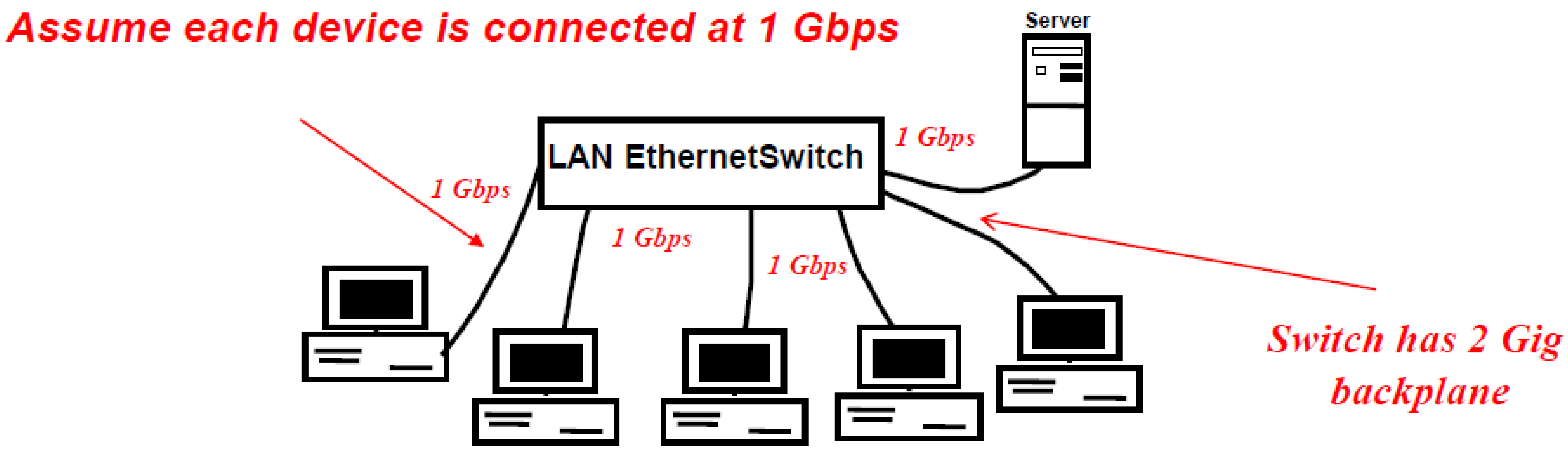
- FastForward (cut-through)
  - Checks just enough to see where to send it
- FragmentFree (modified cut-through or hybrid)
  - Checks that the header is good – would catch most collisions
- Store-and-Forward (default)
  - Checks the entire frame

Forwarding Method Latency Comparison



Latency comparison with 256-byte packet on cisco 1900

Blocking vs non-Blocking* LAN Switches

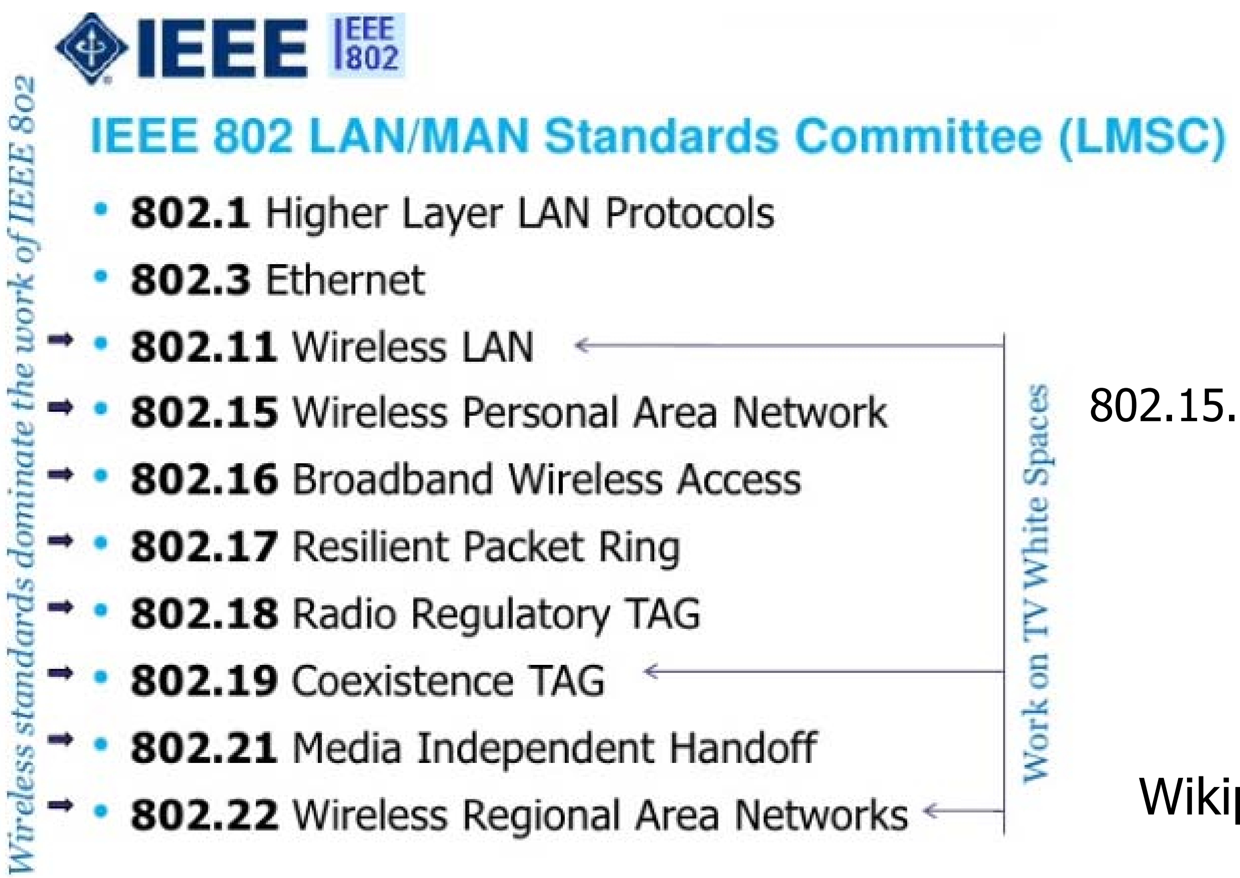


- Non-blocking – internal bandwidth (BW) can handle all the port bandwidths, at the same time, at full capacity
  - Sum of all ports maximum BW is less than Backplane BW
  - Backplane is internal architecture capacity

* Almost all switches today are non-blocking

IEEE Standards

- 802 – IEEE Committee for Layer 1 and 2 Standards
  - Local Area Networks (LAN) and Metropolitan Area Networks (MAN)
- 802.# – # is the Working Group (specific technology 802.3)
- 802.#x – x is the Standard (feature and/or version 802.3y)



802.15.1 Bluetooth Standard

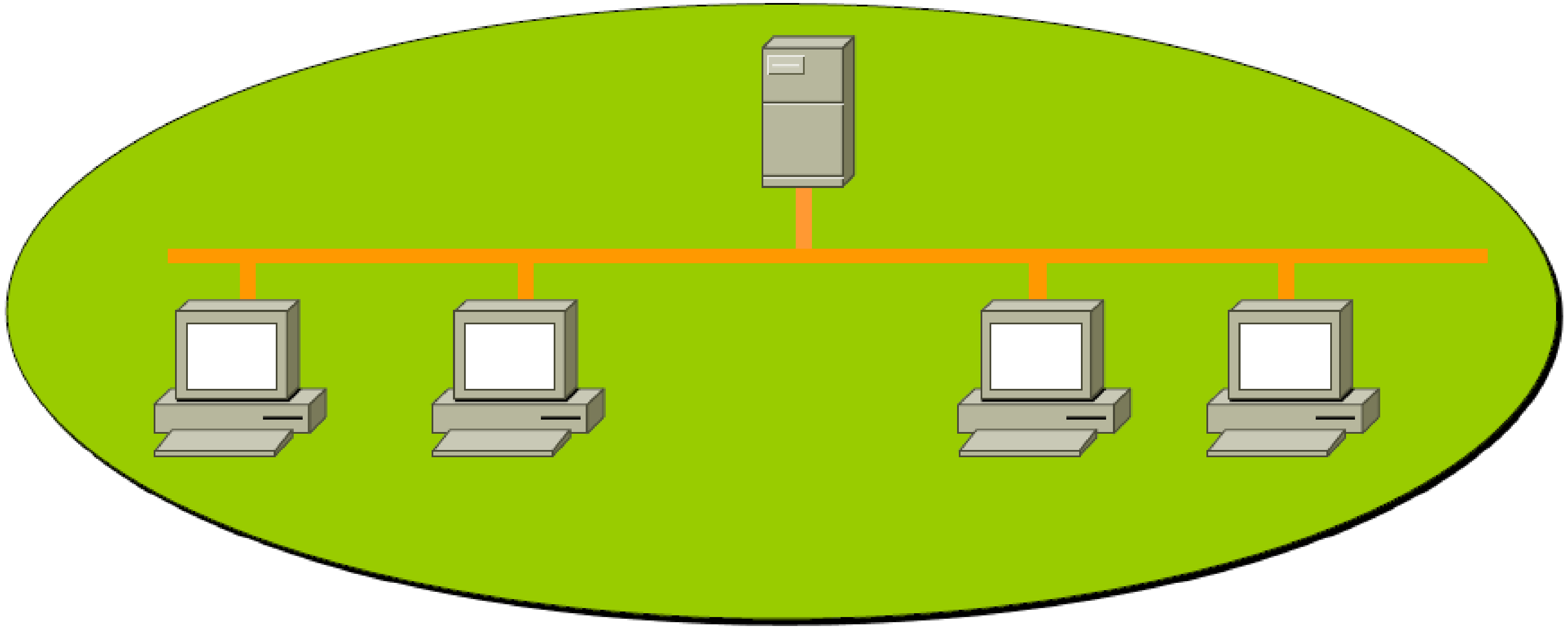
Wikipedia: IEEE 802

Timeouts and Keepalive Packet Intervals

- ARP Flush Timeout
  - Default is 14,400 seconds (4 hours)
  - Configurable from 60 to 86,400 seconds (24 hours)
- CAM Table timeout – 300 seconds (5 minutes) configurable
- Ethernet Keepalives – 10 seconds configurable
- Serial Keepalives (WAN) – 10 seconds configurable
- BPDU Keepalive interval – 2 seconds (Spanning Tree STP)
  - Bridge Protocol Data Unit (BPDU)
    - Data message transmitted across a LAN to detect loops in network topologies.

Use special Layer 2 Hello packets to maintain status

Virtual LAN (VLAN)

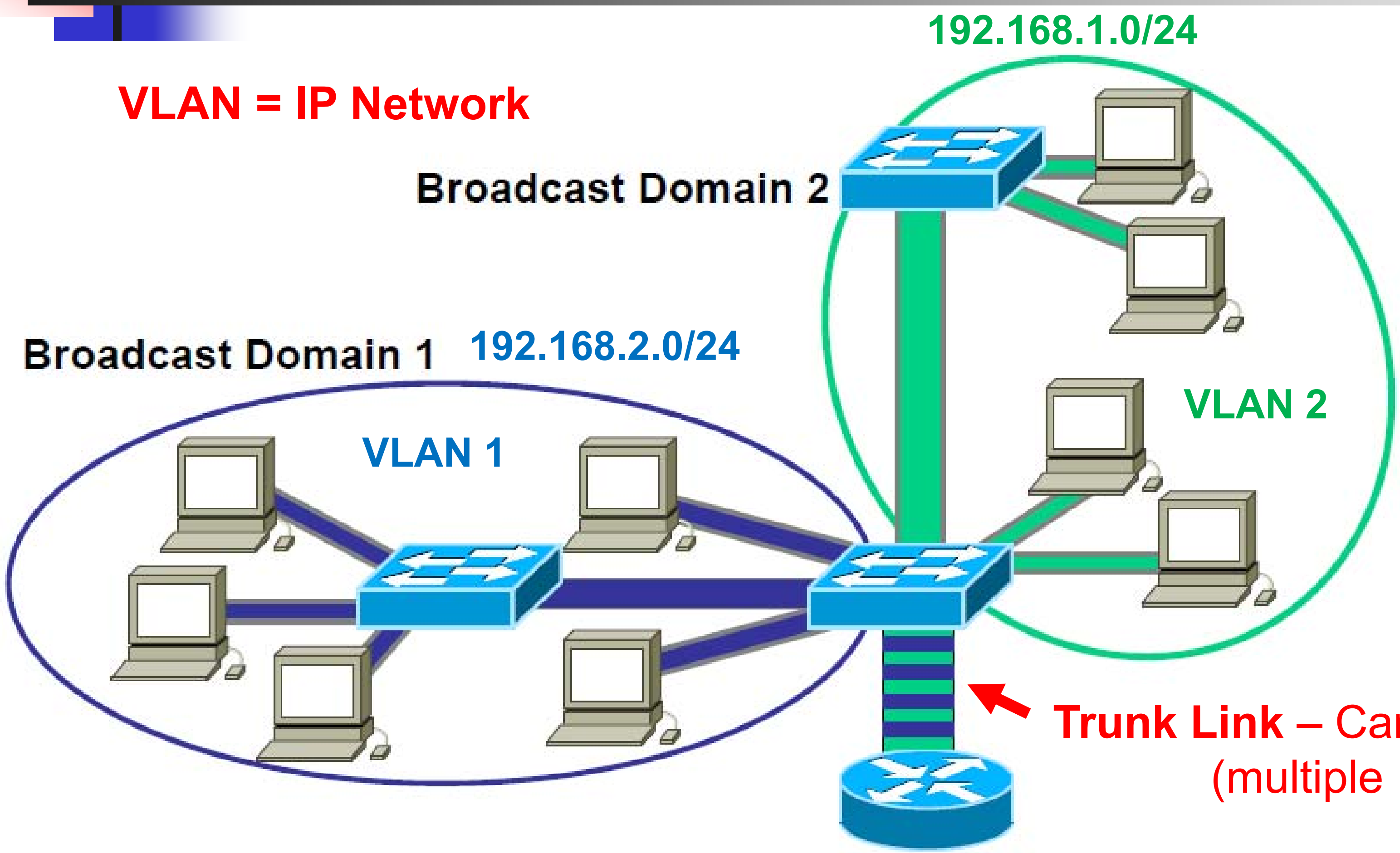


- A virtual Broadcast Domain within a switched LAN
  - Effectively segments switches into separate LANs
    - Invisible to each other (security improved, fewer broadcasts)
    - Each has its own IP address pool (Network)

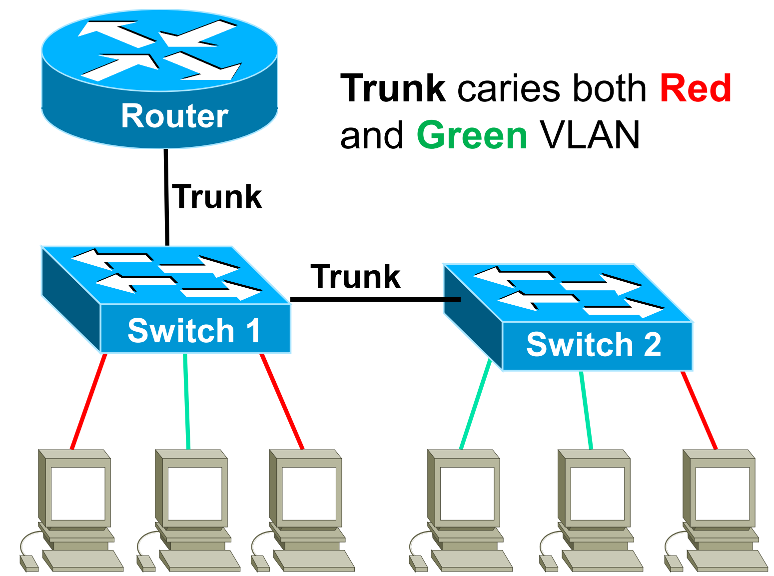
VLANs Establish Broadcast Domains

VLAN = IP Network

VLANS basically partition the network.
Why? To carry multiple IP networks.

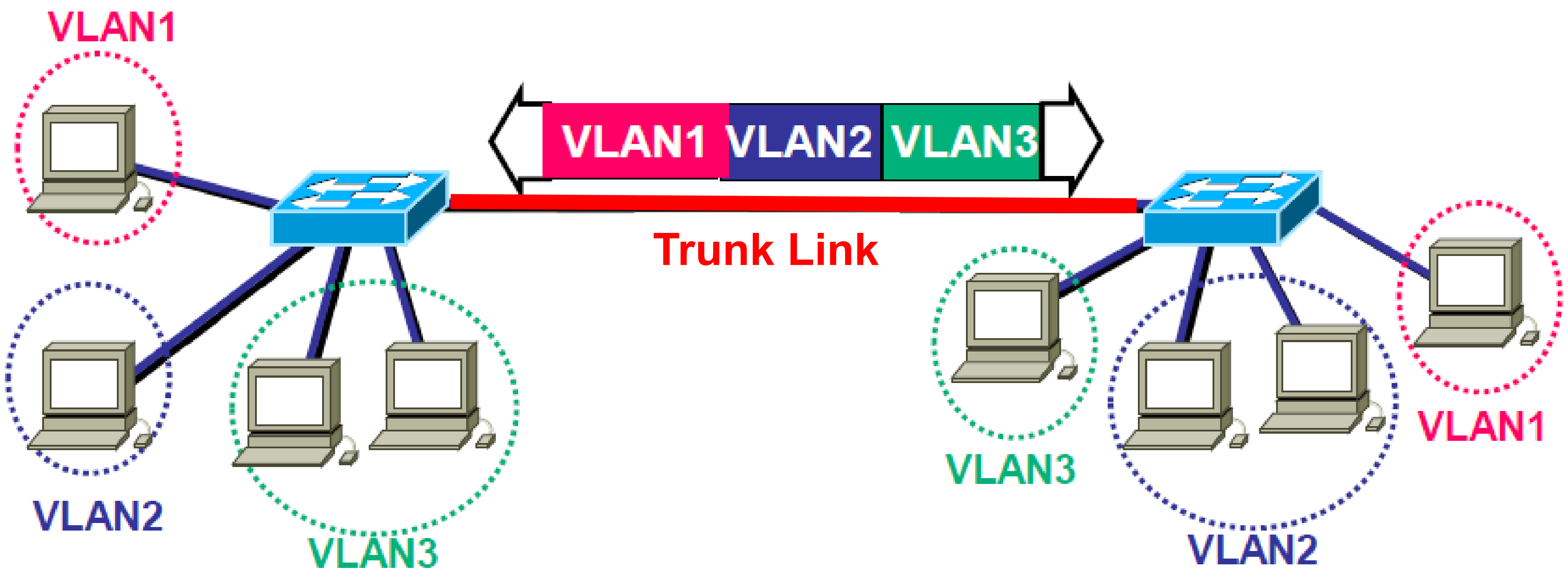


Trunk Link – Carries multiple VLANs (multiple IP networks)



- VLANs contain broadcasts within originating domain (IP network)
- Router is the only device that can forward traffic between VLANs
- Routers do not forward broadcasts (keeps broadcast from spreading)

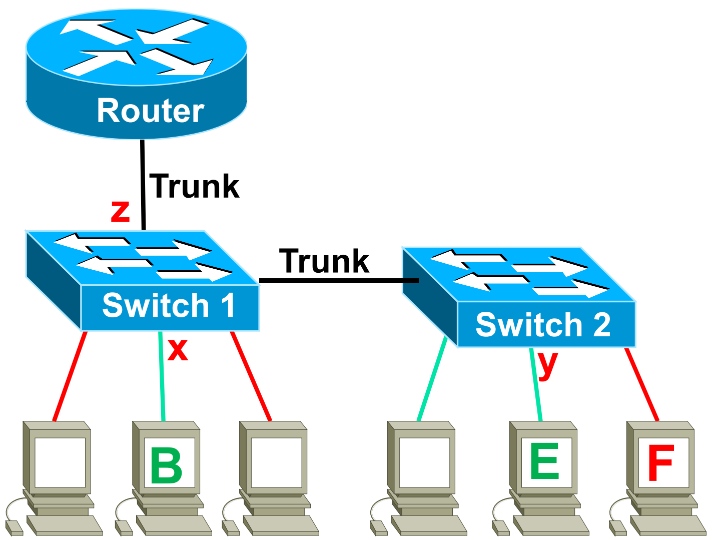
VLAN Frame Identification (VLAN Tag)



- Developed for multi-VLAN, inter-switch communications
- Places a unique identifier (Tag) in header of each frame
- Functions at Layer 2

Analogy: Color coded name badges at a conference or at work

IEEE 802.1Q Trunks (Tagging)



Original Ethernet Frame

Preamble	SFD	Destination	Source	Type	Data & Pad	FCS	
7	1	8	8	2	46-1500	4	Bytes

Ethernet vs. 802.1Q Frame

Preamble	SFD	Destination	Source	802.1Q Hdr	Type	Data & Pad	FCS	
7	1	8	8	4	2	46-1500	4	Bytes

CAM Table

MAC Address	Int
EC-F4-BB-8D-2E-7E	2
56-27-1E-FA-F9-6F	6
54-27-1E-FA-F9-6F	9
54-27-1E-F4-95-6A	7
56-27-1E-FF-19-23	12
56-27-1E-67-FA-C1	12
EC-F4-BB-91-24-8C	12
...	...

- Open standard using frame tags to label traffic
  - Inserts a 4-Byte header while within the VLAN switches
    - Like an Event Badge – determines where you can go
    - Switch only sees MAC addresses in that VLAN when forwarding
      - Just like the switch is partitioned, so is the CAM table
    - Header added at x for frame from A / removed at z or y

IEEE 802.1Q VLAN Identification Tag

Original Ethernet Frame

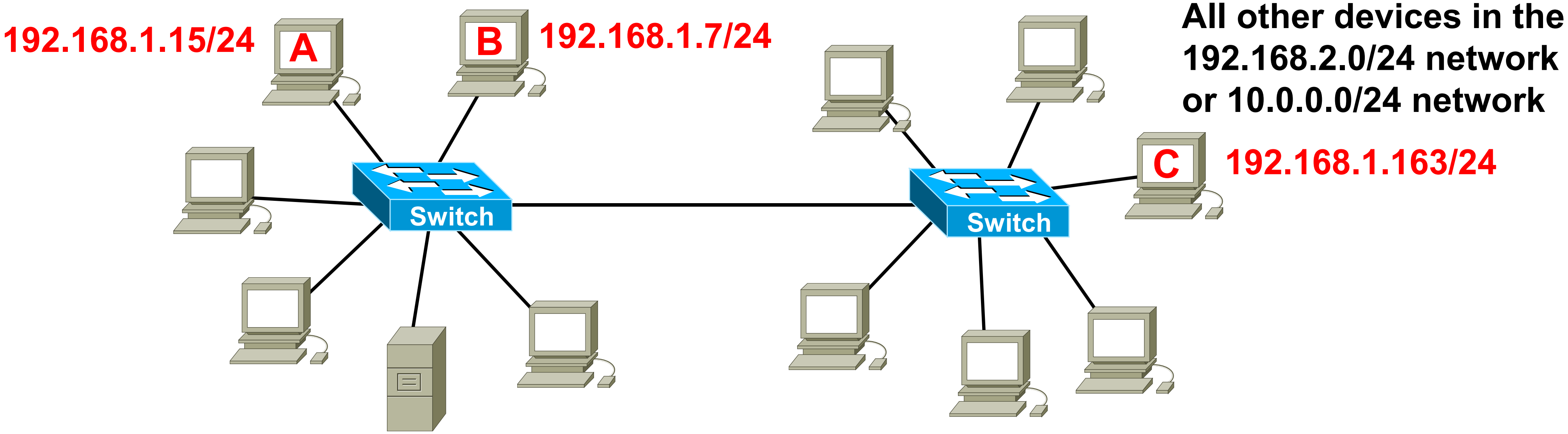
Preamble	SFD	Destination	Source	Type	Data & Pad	FCS	
7	1	8	8	2	46-1500	4	Bytes

Ethernet vs. 802.1Q Frame

Preamble	SFD	Destination	Source	802.1Q Hdr	Type	Data & Pad	FCS	
7	1	8	8	4	2	46-1500	4	Bytes

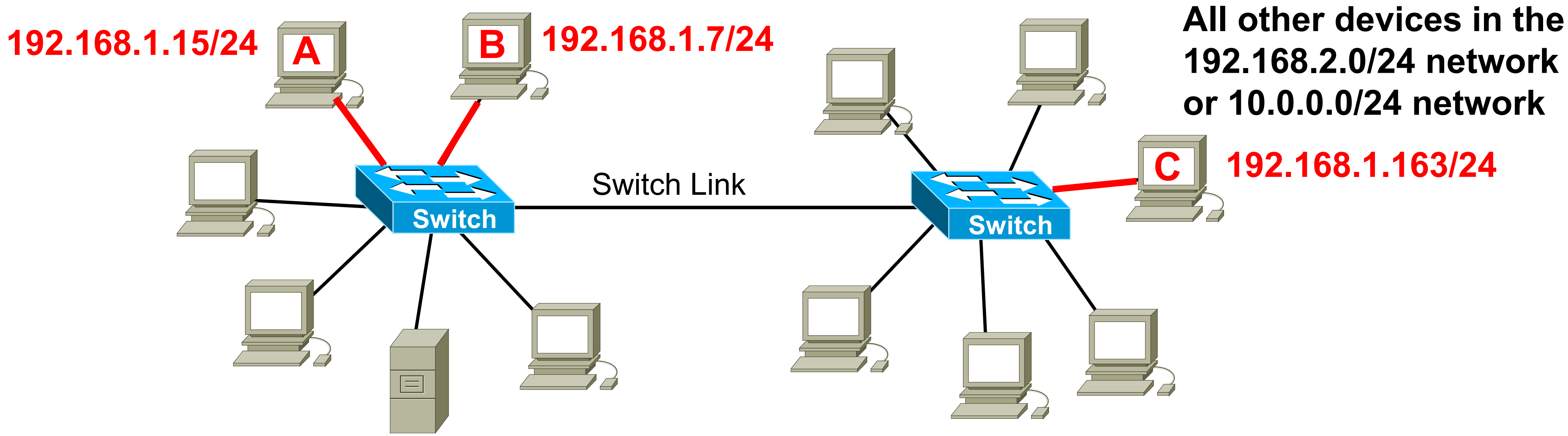
- The industry standard
  - 2-byte Tag Protocol Identifier (TPID)
    - A fixed value of 0x8100
    - Indicates the frame carries 802.1Q/802.1p tag information
  - 2-byte Tag Control Information (TCI)
    - VLAN Identifier plus Priority and Drop Eligible codes

How it really works – Scenario #1



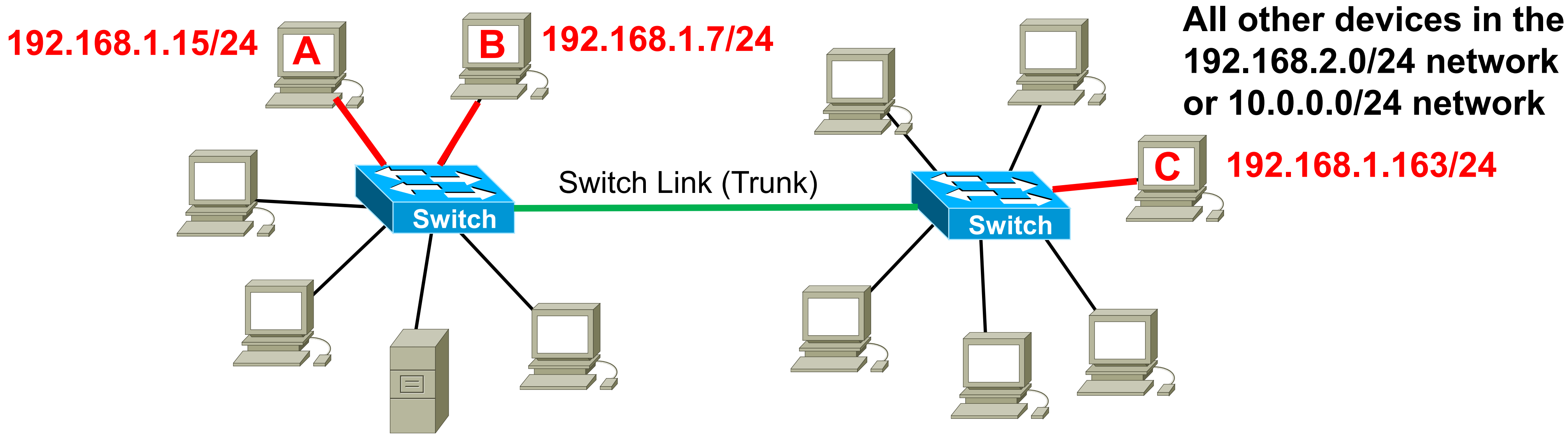
- No VLANs – Blue devices could be Hubs or Switches
  - A, B and C could communicate or ping each other
    - They could not communicate with or ping any of the other devices
  - All other devices could communicate or ping each other
    - They could not communicate with or ping A, B or C
  - All devices would see all broadcasts – could be sniffed (WireShark)
    - Neither network could sniff the other's unicasts (device to device traffic)

How it really works – Scenario #2



- VLANs – Blue devices must be Switches
  - A, B and C are on ports configured for VLAN 2 (or any number but 1)
  - All other ports are in VLAN 1 by default
  - Devices in each VLAN no longer see any traffic from other VLAN
  - VLAN 1 devices can communicate with or ping each other (but not A, B or C)
  - A and B can communicate or ping each other – but C is an orphan (stranded)
    - Switch Link ports are in VLAN 1 (default) – can't carry any other VLANs
    - Putting Switch Link ports are in VLAN 2 would connect A, B & C but would split VLAN 1

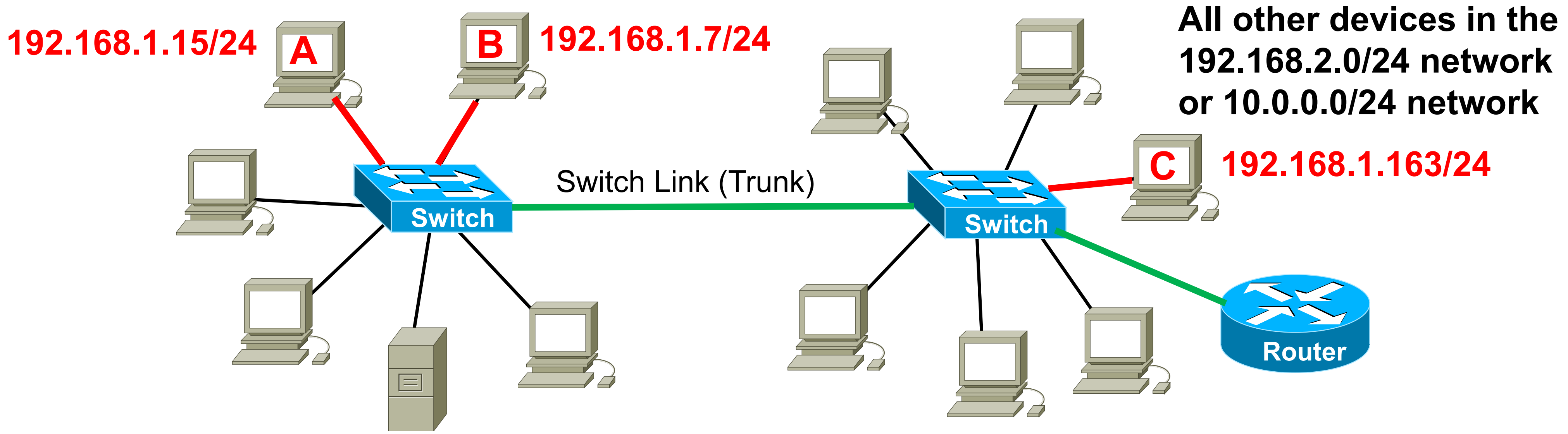
How it really works – Scenario #3



- VLANs with trunk – Blue devices must be Switches
  - Switch Link ports are configured as trunks* for all VLANs (default)
  - A, B and C can now communicate (but not with VLAN 1 devices including the server)
  - VLAN 1 devices can communicate with each other (but not A, B or C)
  - Devices in each VLAN still no longer see any traffic from other VLAN
  - Nothing in this scenario will allow the VLANs to communicate with each other

* Must be full-duplex Ethernet 100 Mb minimum

How it really works – Scenario #4



- VLANs with trunks and router – Blue devices must be Switches
  - Router connected via Trunk to either switch
    - Configured with virtual interface in VLAN 1 (192.168.2.1/24 – default gateway for all VLAN 1 devices)
    - Configured with virtual interface in VLAN 2 (192.168.1.1/24 – default gateway for all VLAN 2 devices)
  - All devices can now communicate with each other
    - VLAN 1 devices directly, or through the router to get to VLAN 2 devices
    - VLAN 2 devices directly, or through the router to get to VLAN 1 devices
  - Life is good!

VLAN Uses Example

- IP Desk Phones
- Video Cameras
- Door Access Card Readers
- Credit Card Readers
- Point of Sale Devices
- Video Displays

Note: Computers B, D, and E could view the security camera directly. All others would need to go through the router (router could block).

To Verify Your VLANs – show vlan

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
2    Sales                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15
3    Accounting                       active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20

1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

* brief is optional – cleans up display at the bottom

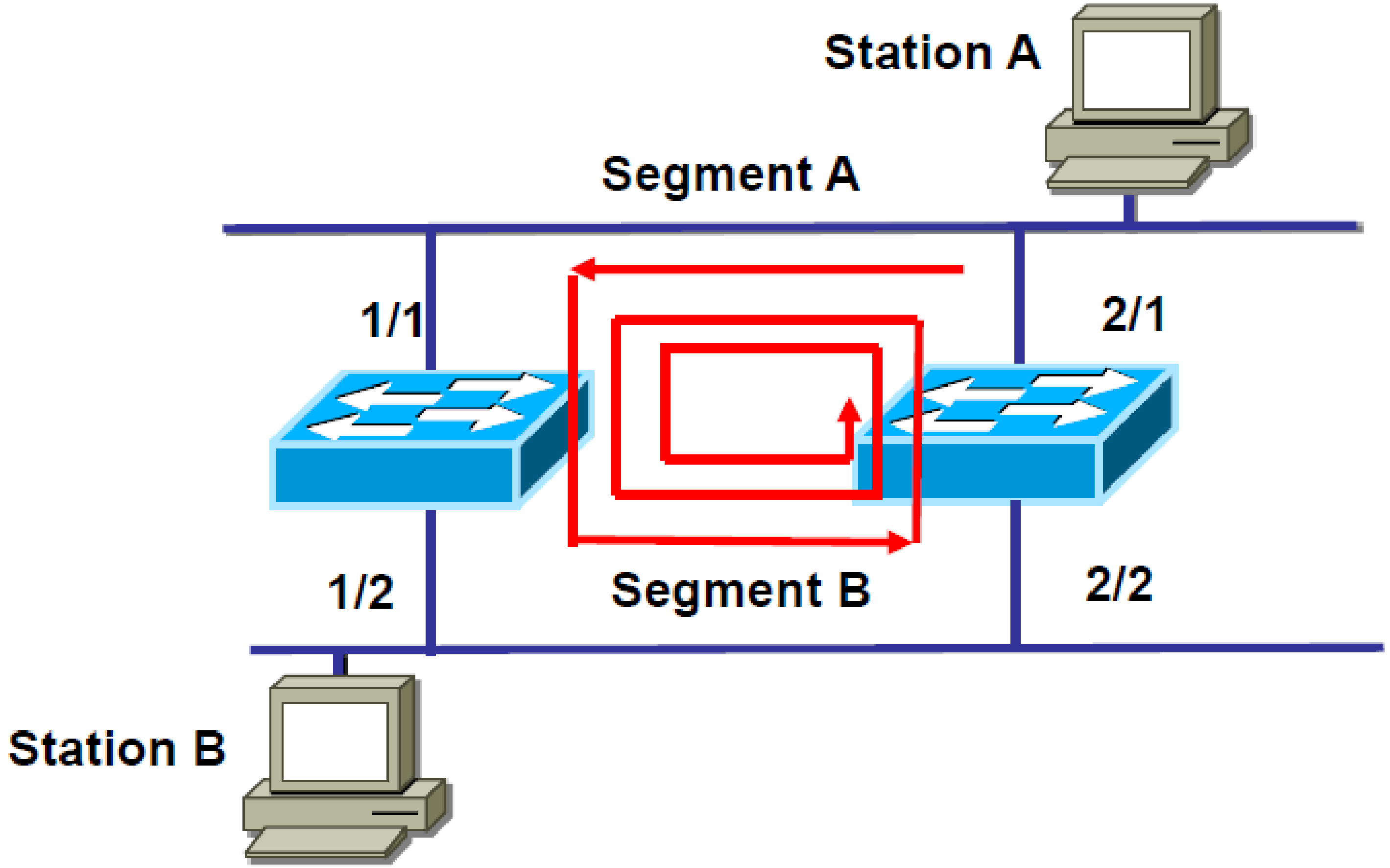
Confirm Trunks – show interfaces trunk

```
Switch#show interfaces trunk
Port        Mode            Encapsulation  Status        Native vlan
Fa0/1         on              802.1q         trunking      1

Port          Vlans allowed on trunk
Fa0/1         1,2

Port          Vlans allowed and active in management domain
Fa0/1         2

Port          Vlans in spanning tree forwarding state and not
pruned
Fa0/1         2
```

Confirm Interfaces - show interface status

```
Switch#show interface status
Port     Name               Status       Vlan       Duplex  Speed Type
Fa0/1                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/2                       notconnect   1            auto   auto 10/100BaseTX
Fa0/3                       notconnect   1            auto   auto 10/100BaseTX
Fa0/4                       notconnect   1            auto   auto 10/100BaseTX
Fa0/5                       notconnect   1            auto   auto 10/100BaseTX
Fa0/6    IT Department VLAN connected    1          a-full  a-100 10/100BaseTX
Fa0/7    IT Department VLAN notconnect   1            auto   auto 10/100BaseTX
Fa0/8    IT Department VLAN notconnect   1            auto   auto 10/100BaseTX
Fa0/9    IT Department VLAN notconnect   1            auto   auto 10/100BaseTX
Fa0/10   IT Department VLAN notconnect   1            auto   auto 10/100BaseTX
Fa0/11   Sales Department V connected    2          a-full  a-100 10/100BaseTX
Fa0/12   Sales Department V notconnect   2            auto   auto 10/100BaseTX
Fa0/13   Sales Department V notconnect   2            auto   auto 10/100BaseTX
Fa0/14   Sales Department V notconnect   2            auto   auto 10/100BaseTX
Fa0/15   Sales Department V notconnect   2            auto   auto 10/100BaseTX
Fa0/16   Accounting Departm notconnect   3            auto   auto 10/100BaseTX
Fa0/17   Accounting Departm notconnect   3            auto   auto 10/100BaseTX
Fa0/18   Accounting Departm notconnect   3            auto   auto 10/100BaseTX
Fa0/19   Accounting Departm notconnect   3            auto   auto 10/100BaseTX
Fa0/20   Accounting Departm notconnect   3            auto   auto 10/100BaseTX
****Output Omitted****
```

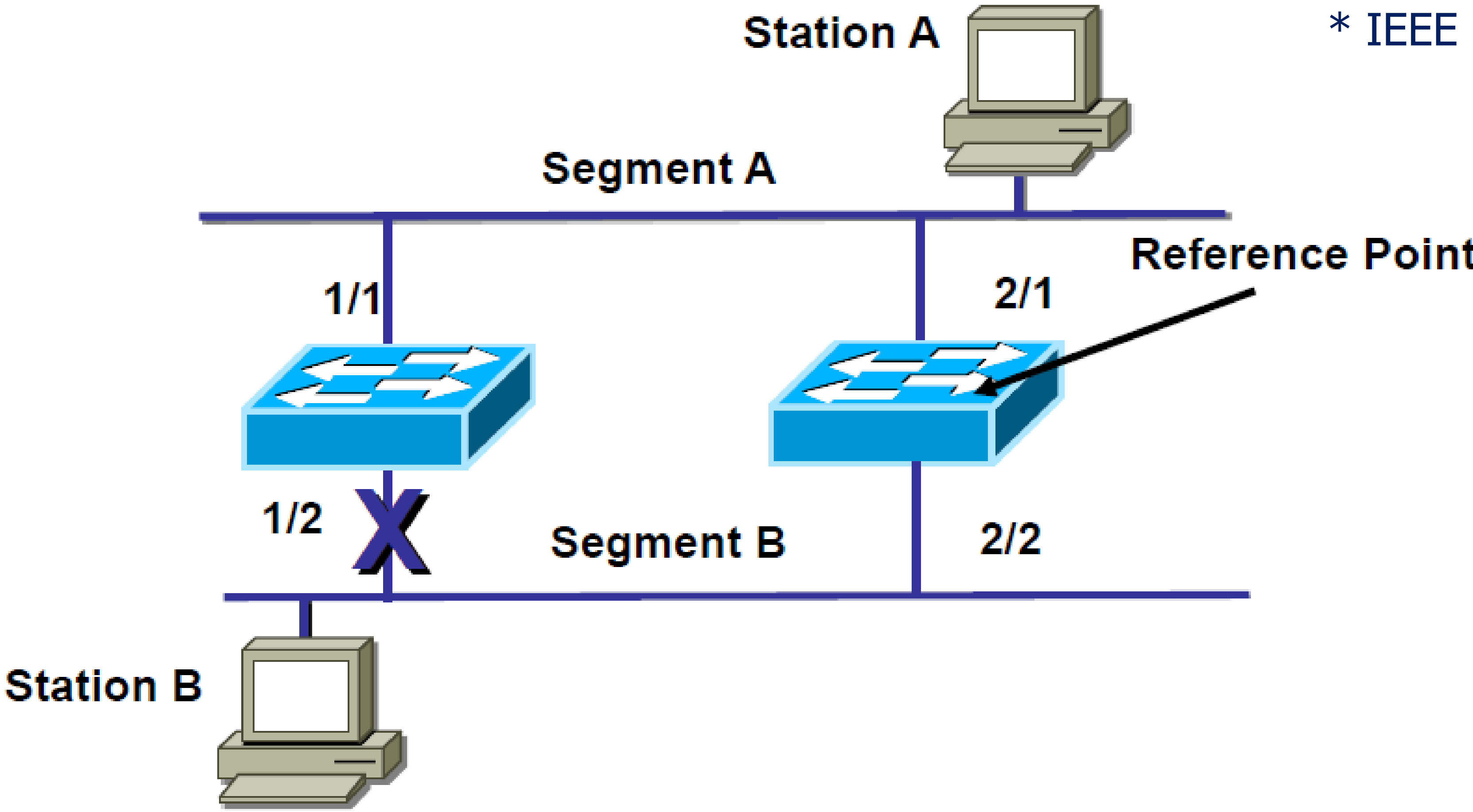
What is a Switching Loop or Bridge Loop?



- Loop will occur any time there is a redundant path or loop in the Layer 2 network

Spanning Tree Protocol (STP)*

* IEEE 802.1D Standard

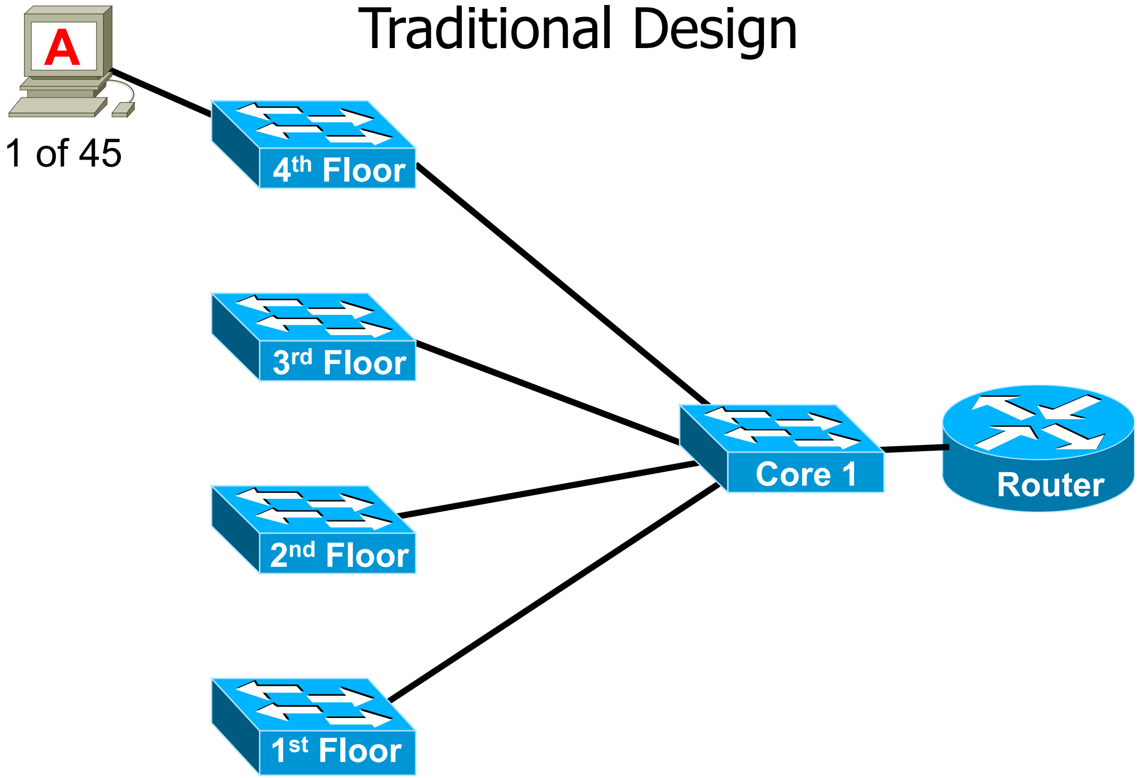


- Loops are prevented by blocking the redundant path
- Blocked link opens up if forwarding link fails

Another Look

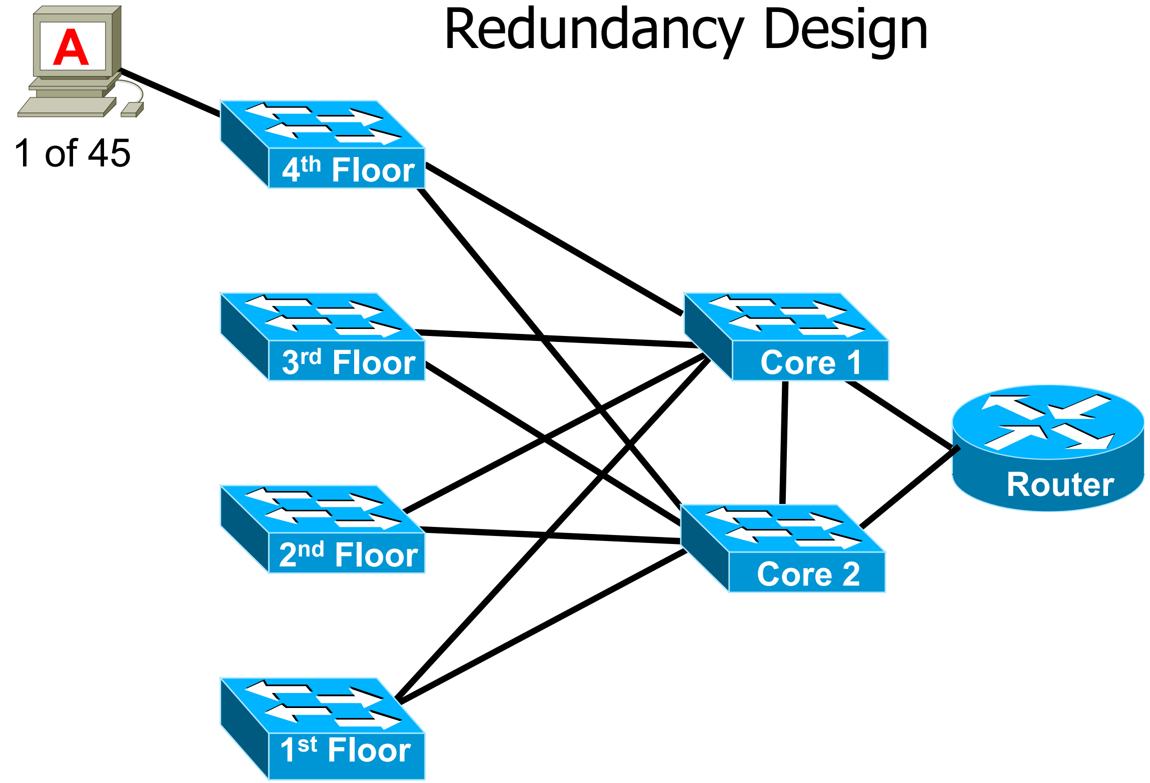
* CAM entries time out after 300 seconds inactive

Traditional Design



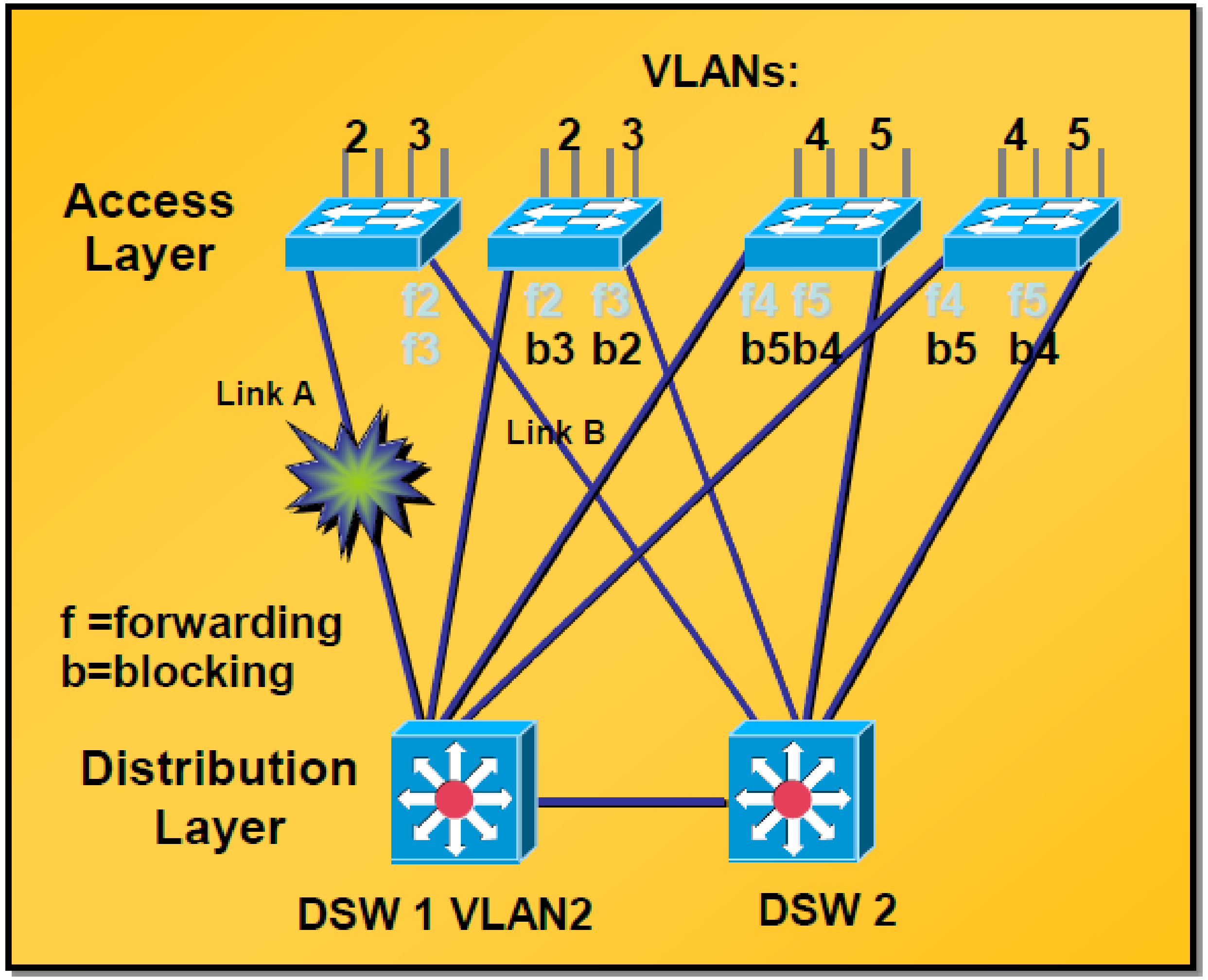
- No loops
- Lots of single point failures

Redundancy Design



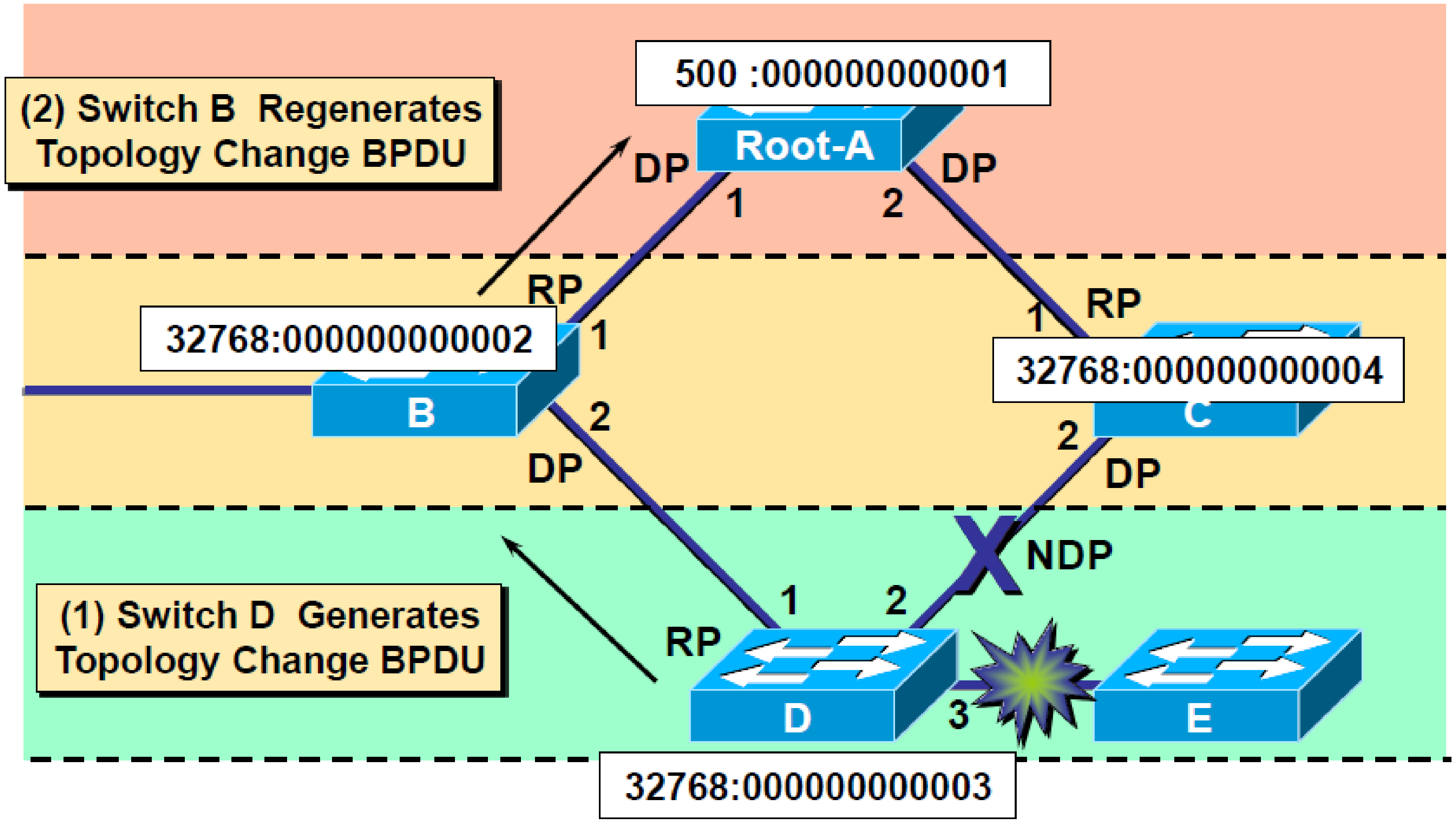
- Lots of loops – looping will occur
- CAM Table or MAC address flapping
- Broadcasts trigger both

Ensuring Network Availability with VLANs



- We want redundancy in LANs
  - To avoid orphan networks
  - To ensure availability
- Spanning Tree
  - Blocks redundant link
- With VLANs
  - Each link can forward one VLAN
    - Block the other

A Network Topology Change



- Topology Change
  - Added device
  - Failed link or device
- STP Election
  - Devices share BPDUs
  - Select blocked link(s)
  - Occurs automatically
  - Can be programmed
    - To control outcome

Bridge Protocol Data Unit (BPDU) – Data message transmitted across a LAN to detect loops in network topologies.

My UW Web Site

Bob Larson, Lecturer

Directory

- Home
- My Background
- Courses I Teach
- Graduate Assistants
- Student Resources
- Career Resources
- Articles and Blog Posts
- Data Visualizations
- Animated Messages
- InfoGraphics
- How Tech Stuff Works
- Check Your Bandwidth
- TED Talks
- Things to Ponder
- MOOC Courses I Liked
- Documents That Changed the World*

* By the iSchools own Joe Janes

Introduction

Bob Larson

Faculty Lecturer in the area of information technology at the Information School since 2005. Holds a MBA from the UW Foster School of Business and a BS from Central Washington University.

My company developed and delivered technology courses at colleges, universities and corporate training centers in seven countries on three continents since 1985. Recent experience includes ten years designing and implementing converged technology networks for businesses and the cruise ship industry. In 2008 designed the technology systems for a new medical university. In 2014 designed the base station network for an ISP for installation in Hong Kong that would serve Southeast Asia.

Interests include the difference between security and security theater, how security and privacy are inter-related, as well as how investment in security theater can reduce real security. Personal interests: history, climate change, equality issues and civil rights.

E-mail: blabob@uw.edu

Email: blabob@uw.edu
Linkedin: https://www.linkedin.com/in/boblarson
Web site: http://faculty.washington.edu/blabob/bob/

Fin...