SCHOOL OF INNOVATIVE TECHNOLOGIES & ENGINEERING

Department of Industrial Systems Engineering jointly with Orange Business Services

Module Information Pack

Postgraduate Diploma in IT

with Specialization in Networking

LAN Switching & Wireless LAN

PDITN4104

October 2018 – Version 1.0

Programme Directors:	Dr. Vinaye Armoogum & Mr. Rishi Heerasing
Module Convenor:	Mr. Rishi Heerasing
Office:	Room G2.14 Level 2 SITE BLOCK
Phone:	207 5250 Ext. 34
E-mail:	rheerasing@umail.utm.ac.mu
Academic Tutoring:	None
Lecture Day and Time:	08:00 – 17:00
Credits & Level:	**4** credits – Level **4**
Pre-requisites (If applicable):	PDITN4102
Co-requisites (If applicable):	None
Method of Delivery & Frequency:	15 x 4 Hrs sessions of lectures, tutorials and practicals.
Method & Criteria of Assessment:	50% Unseen Exam & 50% Coursework

Module Aims:

- Investigate the fundamentals concepts behind LAN switching and forwarding.
- Understand the purpose of different intermediate systems and how they work withing a layered architecture.
- Achieve practical skills with initial switch configuration and IOS Software management.
- Understand basic wireless concepts, configurations and device operations.
- Achieve a theoretical understanding of advanced switching protocols such as VTP and STP.
- Understand and be able to apply theories for design and troubleshooting issues in a switched infrastructure
- Use of simulation software (Packet Tracer/GNS3) and network protocols analyzers (Wireshark)

Learning Objectives and Outcomes:

- Use the command-line interface to configure switches.
- Design an Ethernet switching infastructure.
- Configure Virtual LANs (VLANs)
- Understand Spanning Tree Protocol and VLAN Trunking Protocol
- Configure Inter-VLAN routing
- Understand wireless LAN technologies and be able to configure and troubleshoot issues specific to wireless LANs.
- Understand the types and functions of network interconnect devices.

TENTATIVE LECTURE SCHEDULE

Date	Topics Covered
29/10/18 **DAY 1**	Introduction to Ethernet/802.3 and Token Ring/802.5 LANs. Role of switches and switching in modern computer networks.
	Data Link layer Frame formats; Transparent bridge/switch learning.
30/10/18 **DAY 2**	Fundamental concepts and techniques of layer 2 switching, including Spanning Tree Protocols and Virtual LANs.
	Network Switch management, configuration and security.
31/10/18 **DAY 3**	Output of various commands to verify the status of a switched network. Identification and correcting problems at various OSI layers.
	Configuration, verification and troubleshooting of VLANs, trunking on relevant switches.
01/11/18 **DAY 4**	Inter-VLAN routing, VTP, and RSTP.
	Introduction to 802.11x WLAN.
02/11/18	***Public Holiday***
05/11/18 **DAY 5**	Wireless LAN security.
	Configuring WLAN access. Troubleshooting simple WLAN problems.
06/11/18 **DAY 6**	Introduction to VoIP and components.
	Case -Studies in Network Design & Management
07/11/18	***Public Holiday***
08/11/16 **DAY 7**	***Open book Class Test + Practical Test (20% + 10%)***
	Buffer
09/11/18 **HALF-DAY 8**	***Recap***

READING LIST

RECOMMENDED TEXTS (as per availability in the UTM Resource Centre)**:**

- **Tanenbaum A. (2001)** ***Computer Networks:*** **4th Ed., Prentice-Hall (D4.6TAN)** ⁂
- **Lewis W. (2008)** ***LAN Switching and Wireless, CCNA Exploration Companion Guide:*** **1st Ed., Cisco Press.**
- Stallings W. (2001) *Data and Computer Communications:* 6th Ed., Prentice-Hall (D4.6STA) ⁂
- Lowe D. (2005) *Networking for Dummies:* 7th Ed., Wiley Publishing ⁂

⁂ *You can download a copy of these books in e-book format on Nefertum's Shrine at* **http://www.rishiheerasing.net/download/network.html**

OTHER READING MATERIALS e.g. TEXTS/JOURNALS/ARTICLES/WEBSITES:

- Cisco Academy Website at **http://cisco.netacad.net/**

LECTURE NOTES

The lecture notes are available on **Nefertum's Shrine** at
http://www.rishiheerasing.net/modules/pditn4104/pditn4104.html

The notes are in .pdf format so you will need Adobe Acrobat® Reader to view them. This reader can also be downloaded from the above-mentioned site in the *Downloads* Section.

Introduction to Networks

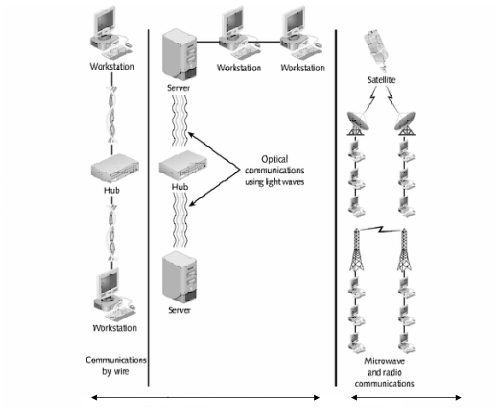
PDITN4104

LAN Switching & Wireless LAN

Network: Definition

- A set of devices (**nodes**) connected by **communication links** (wired or wireless).
- A **node** can be a computer, or any device capable of sending and/or receiving data generated by other nodes on the network.
- A network must be able to meet a certain number of criteria. The most important of those are: **Performance**, **Reliability** and **Security**.

Types of Communication Links



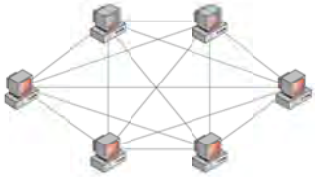
Physical Topology

- The **physical topology** refers to the way a network is laid out physically.
- **2** or more **nodes** connect to a **link. 2** or more **links** form a **topology**. The **topology** is the geometric representation of the relationship of all the links and nodes to one another.
- The are usually **four** basic topologies: **Mesh**, **Star, Bus** and **Ring**.

Mesh Topology

- In a **mesh topology**, every node has a **dedicated point-to-point** link to every other node.

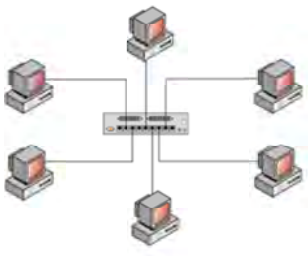
Full-Mesh:



Partial-Mesh:

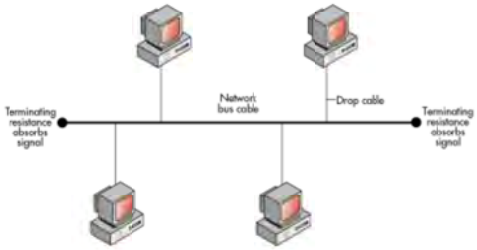
Star Topology

- In a **star topology**, each node has a **dedicated point-to-point** link only to a central controller, usually a **hub** or **switch**.



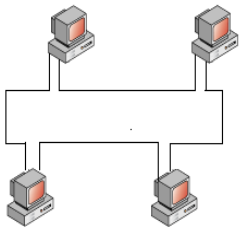
Bus Topology

- In a **bus topology**, a **multipoint** link is used. One long cable acts as a **backbone** to link all the devices in a network.



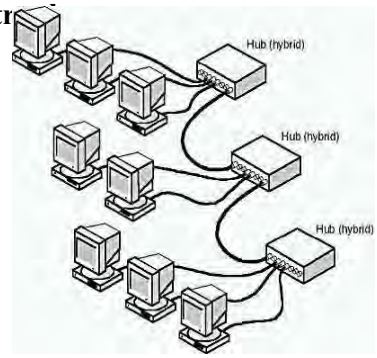
Ring Topology

- In a **ring topology**, each node has a **dedicated point-to-point** link only with the **two** nodes on either side of it.



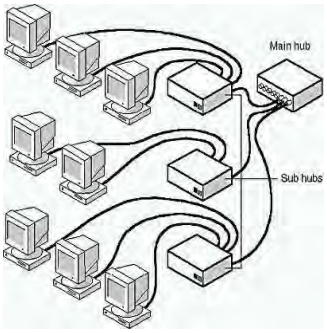
Hybrid: Star Bus Topology

- In a **star bus topology**, **several star topology networks** are linked together with **linear bus tr**



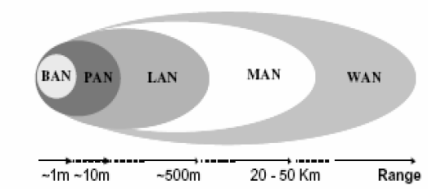
Hybrid: Star Ring Topology

- In a **star ring topology**, **sub hubs** are linked together in a **star pattern** to a **main hub**, rather than to themselves with **linear bus trunks**.



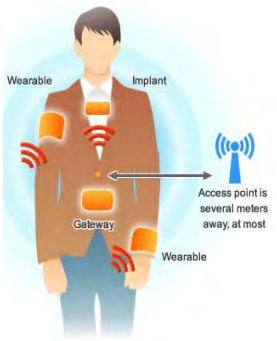
Network Types Defined

- Body Area Network
- Personal Area Network
- Local Area Network
- Metropolitan Area Networks
- Wide Area Networks



Body Area Network (BAN)

- Short range wireless network which consists of wearable or implanted electronic devices that transmit ID or sensor data to gateway device.
- It is also referred to as Wireless Body Area Network (WBAN) or Body Sensor Network (BSN)

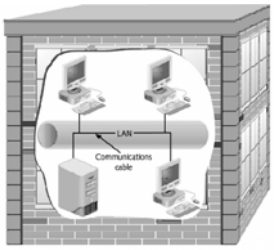


Personal Area Network (PAN)

- A Personal Area Network (PAN) is a computer network used for communication amongst computing devices (Smartphones, PDAs, Tablets) close to one person. The reach of a PAN is typically a few meters.
- Personal area networks may be wired by computer buses such as USB and FireWire. However, a Wireless Personal Area Network (WPAN) is made possible with network technologies such as Infrared (IrDA) and Bluetooth.

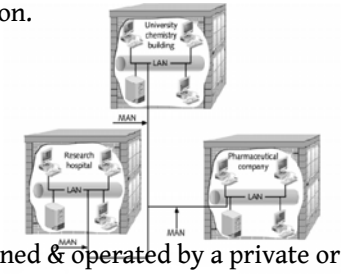
Local Area Network (LAN)

- Series of interconnected computers, printing devices, and other computer equipment that share hardware and software resources
- Service area usually limited to a given office area, floor, or building and is usually privately-owned.



Metropolitan Area Network

- Links **multiple LANs** in a large city or metropolitan region.



- May be wholly owned & operated by a private or public company such as a local telephone company.
- Many **telcos** provide services like **Switched Multi-Megabit Data Services** (SMDS).

Wide Area Network (WAN)

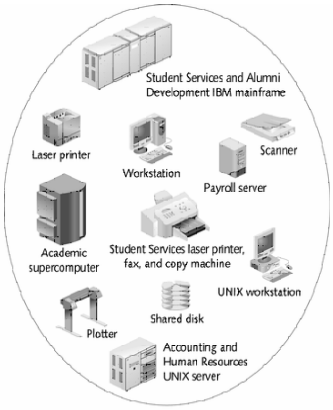
- Provides long-distance transmission of data, voice, image and video information over large geographic areas that may comprise a country, a continent, even the whole world.
- The best example of a WAN is the **Internet**.

Identifying a Network Type

- Communications medium
  - Wire cable, fiber-optic cable, radio waves, microwaves, infrared radiation.
- Protocol
  - How networked data is formatted into discrete units
  - How each unit is transmitted and interpreted
- Topology
  - Physical layout of cable and logical path
- Network type
  - Private versus public

Network Classification

- **Enterprise** network
  - Combination c **LANs**, **MANs** or **WANs** that provides users with an array c computer and network resources to complete different tasks.



Resources in an enterprise network

Events that Led up to LANs and WANs

- **1800s**
  - Oersted
  - Morse
  - Undersea cable
  - Pony Express
  - Bell
- **1900s**
  - Transcontinental and transatlantic calls
  - Voice digitization
  - Electronic digital computers
  - Transistors
  - Sputnik
  - Communications satellites
  - ASCII
  - Mass-produced minicomputers

LAN/WAN History: 1960s

- First WAN
- Hypertext
- Use of fiber optics for phone signals
- Beginning of ARPANET
- Packets and packet switching
- UNIX
- Telecommunications equipment
- First IMP prototype

LAN/WAN History: 1970s

- Ethernet
- ARPANET - 15 sites
- E-mail
- Terminal emulation
- International connections to ARPANET
- Telecommunications conversion from analog to digital
- X.25
- First wireless gateway
- Internet Protocol
- LSI and VLSI chips
- ICCB later IAB

LAN/WAN History: 1980s

- BITNET
- IBM's PC
- Dial-up modem technology
- TCP and IP adopted as protocol suite for ARPANET
- First PC LAN
- Arrival of Internet
- Internetwork hosts
  - 5,000 in 1986
  - 100,000 in 1989
- "Cyberspace"
- T-carrier services
- NFSNET
- Desktop authoring and multimedia
- SNMP

LAN/WAN History: 1990s

- ARPANET retired
- SS7 technology
- NSFNET opened to commercial use
- First cyberbank
- Internet service providers
- Over 16 million Internet hosts

LAN/WAN History: 2000s

- IPv6 used for Internet2 backbone communications
- Video and radio capability
- Prices of 1-Gbps devices fall as competition increases

LAN/WAN History: 2010s

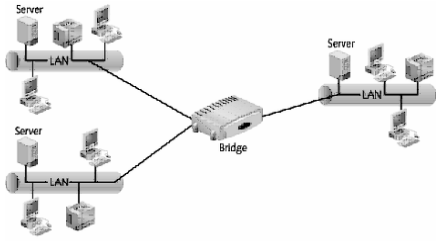
- Cloud Services commonplace
- Internet Of Things (IOT)
- 10G, 25G, 40G and 100G Ethernet has been developed

LAN/WAN Integration

- Becoming more advanced through networking devices
  - Bridges
  - Routers
  - Gateways
  - Switches
  - Firewalls
  - Access Points

Bridges

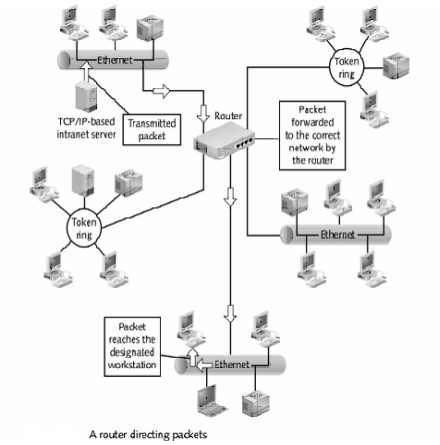
- Connect different LANs or LAN segments using the **same access** method



Routers

- Connect networks having the same or different access methods and media
- Route packets and datagrams to networks by using a decision-making process based on:
  - Routing table data
  - Discovery of most efficient routes
  - Pre-programmed information from network administrator

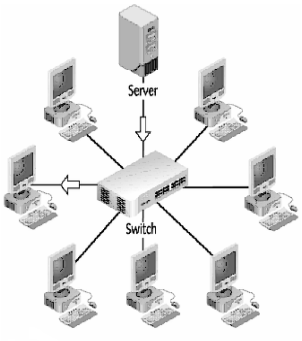
Routers



A router directing packets

Switches

- Link network segments
- Forward and filter frames between segments



A switch in operation

OSI Data Link Layer

Slide Set 1

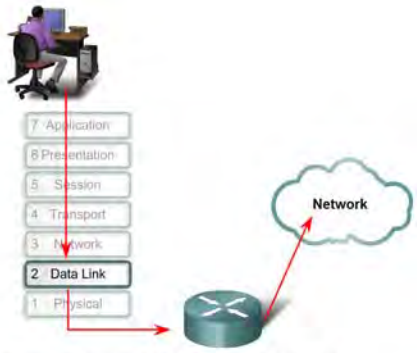
Cisco | Networking Academy®
Mind Wide Open™

Objectives

- Explain the role of Data Link layer protocols in data transmission.
- Describe how the Data Link layer prepares data for transmission on network media.
- Describe the different types of media access control methods.
- Identify several common logical network topologies and describe how the logical topology determines the media access control method for that network.
- Explain the purpose of encapsulating packets into frames to facilitate media access.
- Describe the Layer 2 frame structure and identify generic fields.
- Explain the role of key frame header and trailer fields including addressing, QoS, type of protocol and Frame Check Sequence.

Data Link Layer – Accessing the Media

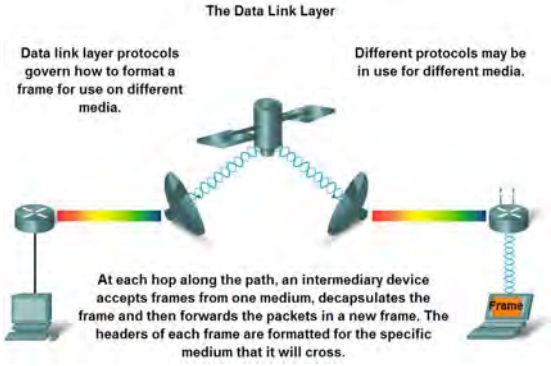
- Describe the service the Data Link Layer provides as it prepares communication for transmission on specific media



The Data Link layer prepares network data for the physical network.

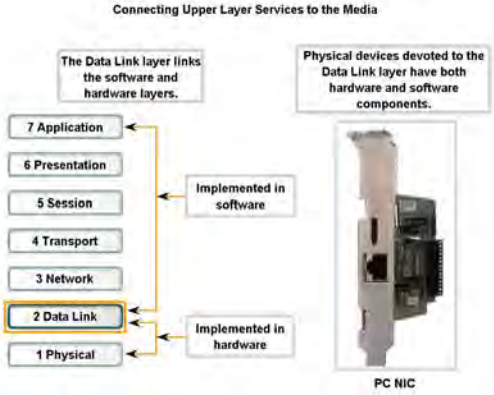
Data Link Layer – Accessing the Media

- Describe why Data Link layer protocols are required to control media access



Data Link Layer – Accessing the Media

- Describe the role the Data Link layer plays in linking the software and hardware layers

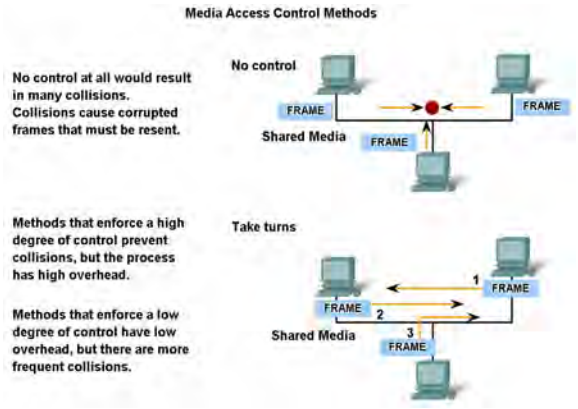


Data Link Layer – Accessing the Media

- Identify several sources for the protocols and standards used by the Data Link layer

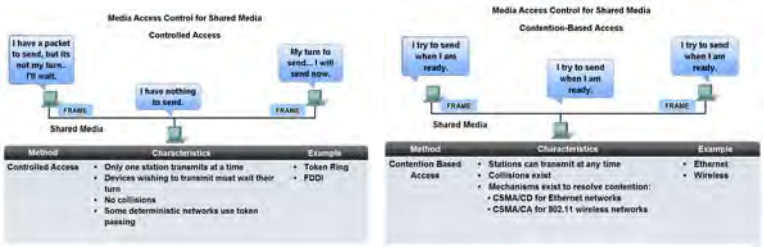
Media Access Control Techniques

- Explain the necessity for controlling access to the media



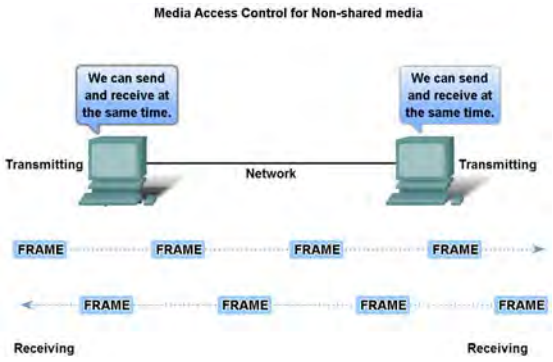
Media Access Control Techniques

- Identify two media access control methods for shared media and the basic characteristics of each



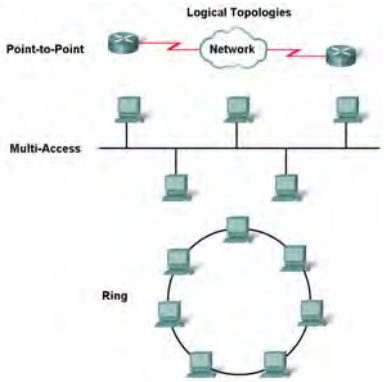
Media Access Control Techniques

- Define Full Duplex and Half Duplex as it relates to Media Access Control for non-shared media



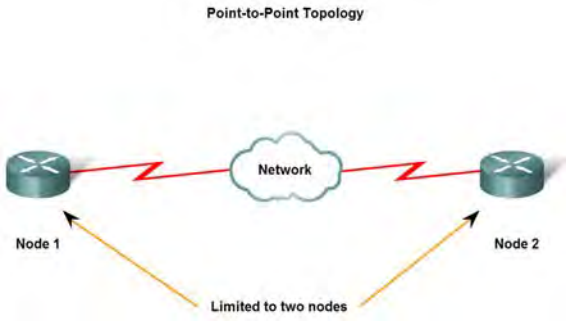
Media Access Control Techniques

- Describe the purpose of a logical topology and identify several common logical topologies



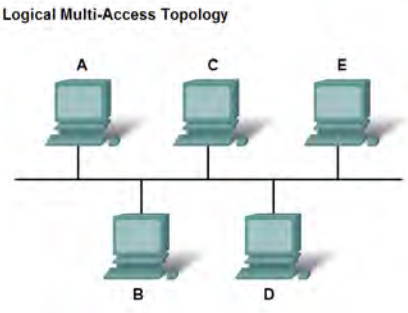
Media Access Control Techniques

- Identify the characteristics of point-to-point topology and describe the implications for media access when using this topology



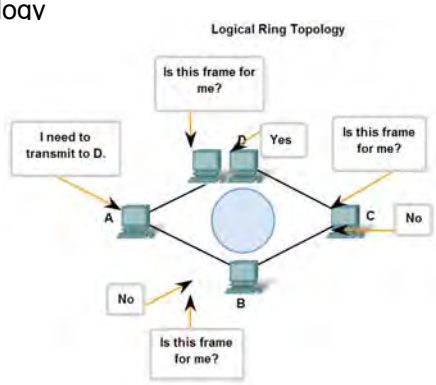
Media Access Control Techniques

- Identify the characteristics of multi-access topology and describe the implications for media access when using this topology



Media Access Control Techniques

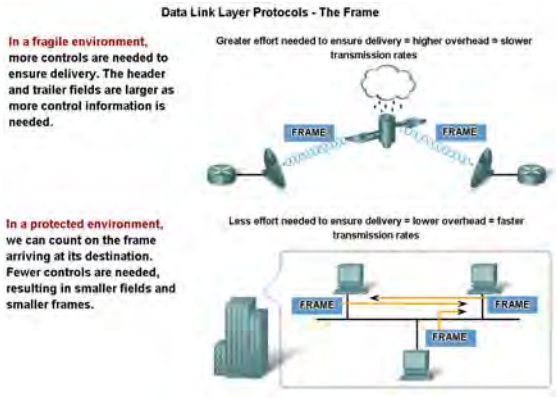
- Identify the characteristics of ring topology and describe the implications for media access when using this topology



13

Media Access Control Addressing and Framing Data

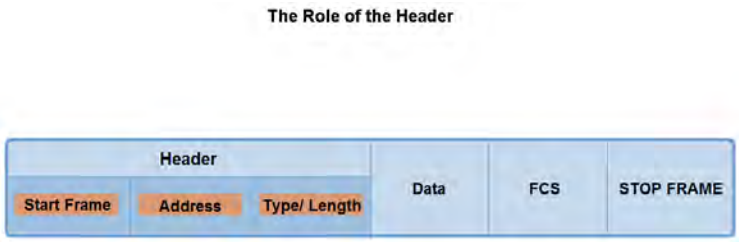
- Describe the purpose of encapsulating packets into frames to facilitate the entry and exit of data on media



14

Media Access Control addressing and framing data

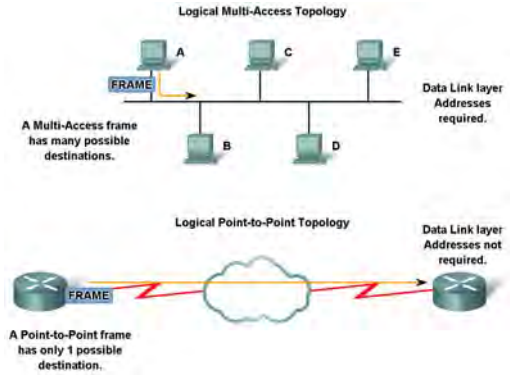
- Describe the role of the frame header in the Data Link layer and identify the fields commonly found in protocols specifying the header structure



15

Media Access Control addressing and framing data

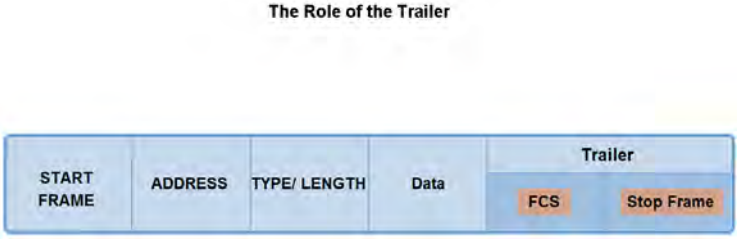
- Describe the role of addressing in the Data Link layer and identify cases where addresses are needed and cases where addresses are not needed



16

Media Access Control addressing and framing data

- Describe the importance of the trailer in the Data Link layer and its implications for use on Ethernet, a "non-reliable" media



17

Summary

In this chapter, you learned to:

- Explain the role of Data Link layer protocols in data transmission.
- Describe how the Data Link layer prepares data for transmission on network media.
- Describe the different types of media access control methods.
- Identify several common logical network topologies and describe how the logical topology determines the media access control method for that network.
- Explain the purpose of encapsulating packets into frames to facilitate media access.
- Describe the Layer 2 frame structure and identify generic fields.
- Explain the role of key frame header and trailer fields, including addressing, QoS, type of protocol, and Frame Check Sequence.

18

Data Link Layer

Slide Set 2

Our goals:

- understand principles behind data link layer services:
  - link layer addressing
- instantiation and implementation of various link layer technologies

1

Outline

Slide Set 2

- **Introduction and services**
- LAN addresses and ARP
- Ethernet
- Hubs, bridges, and switches

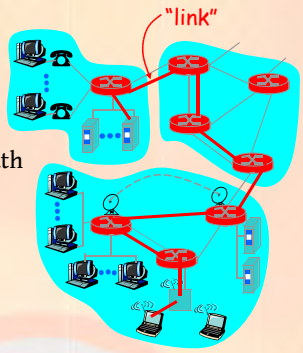
2

Link Layer: Introduction

Slide Set 2

Terminology:

- hosts and routers are **nodes** (bridges and switches too)
- communication channels that connect adjacent nodes along communication path are **links**
  - wired links
  - wireless links
- Layer 2-PDU is a **frame,** encapsulating a datagram



data-link layer has responsibility of transferring datagram from one node to adjacent node over a link

3

Link layer: context

Slide Set 2

- Datagram transferred by different link protocols over different links:
  - e.g., Ethernet on first link, frame relay on intermediate links, 802.11 on last link
- Each link protocol provides different services
  - e.g., may or may not provide reliable data transfer over link

transportation analogy

- trip from Princeton to Lausanne
  - limo: Princeton to JFK
  - plane: JFK to Geneva
  - train: Geneva to Lausanne
- tourist = datagram
- transport segment = communication link
- transportation mode = link layer protocol
- travel agent = routing algorithm

4

Link Layer Services

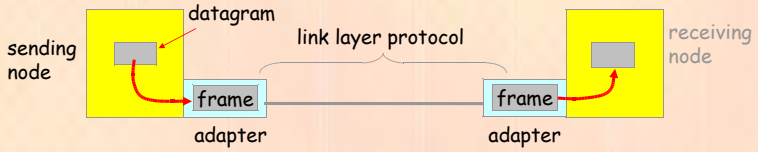
Slide Set 2

- **Framing, link access:**
  - encapsulate datagram into frame, adding header, trailer
  - channel access if shared medium
  - '**physical addresses**' used in frame headers to identify source and destination
    - different from IP address!
- **Reliable delivery between adjacent nodes**
  - seldom used on low bit error link (fibre, twisted pair)
  - wireless links: high error rates
    - Q: why both link-level and end-end reliability?

5

Adaptors Communicating

Slide Set 2



- link layer implemented in "adaptor" (NIC)
  - Ethernet card, PCMCI card, 802.11 card
- sending side:
  - encapsulates datagram in a frame
  - adds error checking bits, rdt, flow control, etc.
- receiving side
  - looks for errors, rdt, flow control, etc
  - extracts datagram, passes to receiving node
- adapter is semi-autonomous
- link & physical layers

6

LAN Addresses and ARP

Slide Set 2

32-bit IP address: (Logical)

- *network-layer* address
- used to get datagram to destination IP network (recall IP network definition)

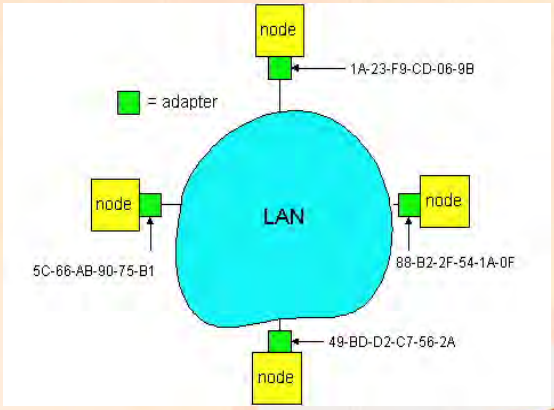
48-bit LAN (or MAC or Physical or Ethernet) address:

- used to get datagram from one interface to another physically-connected interface (same network)
- 48-bit MAC address (for most LANs) burned in the adapter ROM hence cannot be changed.

LAN Addresses and ARP

Slide Set 2

Each adapter on LAN has unique LAN address



LAN Address

Slide Set 2

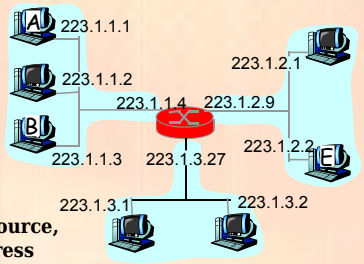
- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- Analogy:
  - (a) MAC address: like NIC Number
  - (b) IP address: like postal address
- MAC flat address => portability
  - can move LAN card from one LAN to another
- IP hierarchical address NOT portable
  - depends on IP network to which node is attached

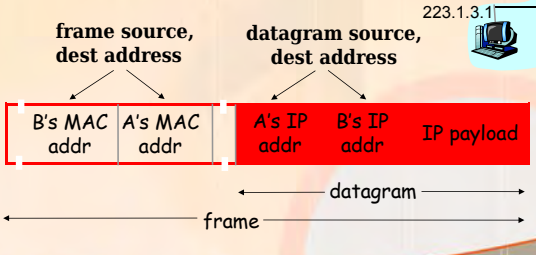
Recall earlier routing discussion

Slide Set 2

Starting at A, given IP datagram addressed to B:

- look up net. address of B, find B on same net. as A
- link layer send datagram to B inside link-layer frame

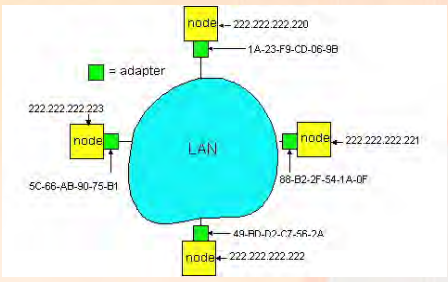




ARP: Address Resolution Protocol

Slide Set 2

Question: *How to determine MAC address of B knowing B's IP address?*



- Each IP node (*host/router*) on LAN has ARP table
- ARP Table: IP/MAC address mappings for some LAN nodes

< IP address; MAC address; TTL>

- TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

ARP protocol

Slide Set 2

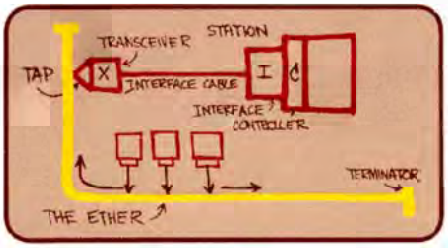
- A wants to send datagram to B, and A knows B's IP address.
- Suppose B's MAC address is not in A's ARP table.
- A broadcasts ARP query packet, containing B's IP address
  - all machines on LAN receive ARP query
- B receives ARP packet, replies to A with its (B's) MAC address
  - frame sent to A's MAC address (*unicast*)
- A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
  - *soft state*: information that times out (goes away) unless refreshed
- ARP is "plug-and-play":
  - nodes create their ARP tables without intervention from net administrator

Ethernet

Slide Set 2

"dominant" LAN technology:

- cheap $20 for 100Mbps !
- first widely used LAN technology
- Simpler, cheaper than token LANs and ATM
- Kept up with speed race: 10,100,1000 Mbps, 10 Gbps

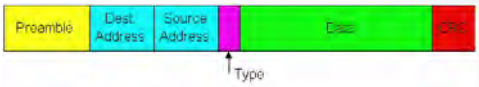


Metcalfe's Ethernet sketch

Ethernet Frame Structure

Slide Set 2

Sending adapter encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame



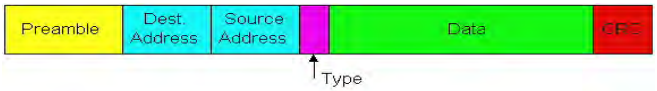
Preamble:

- 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
- used to synchronize receiver, sender clock rates

Ethernet Frame Structure (more)

Slide Set 2

- Addresses: 6 bytes
  - if adapter receives frame with matching destination address, or with broadcast address (e.g. ARP packet), it passes data in frame to network layer protocol
  - otherwise, adapter discards frame
- Type: indicates the higher layer protocol, mostly IP but others may be supported such as Novell IPX and AppleTalk)
- CRC: checked at receiver, if error is detected, the frame is simply dropped



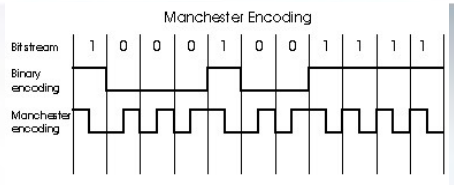
Unreliable, connectionless service

Slide Set 2

- Connectionless: No handshaking between sending and receiving adapter.
- Unreliable: receiving adapter doesn't send *acks* or *nacks* to sending adapter
  - stream of datagrams passed to network layer can have gaps
  - gaps will be filled if app is using TCP
  - otherwise, app will see the gaps

Manchester Encoding

Slide Set 2



- Used in 10BaseT, 100BaseT, 1000 BaseT
- Each bit has a transition
- Allows clocks in sending and receiving nodes to synchronize to each other
  - no need for a centralized, global clock among nodes!
- This is physical-layer stuff !

Gigabit Ethernet

Slide Set 2

- use standard Ethernet frame format
- allows for point-to-point links and shared broadcast channels
- in shared mode, CSMA/CD is used; short distances between nodes to be efficient
- uses hubs, called here "Buffered Distributors"
- Full-Duplex at 1 Gbps for point-to-point links
- 10, 40, 100 Gbps now !!!

Interconnecting LAN segments

Slide Set 2

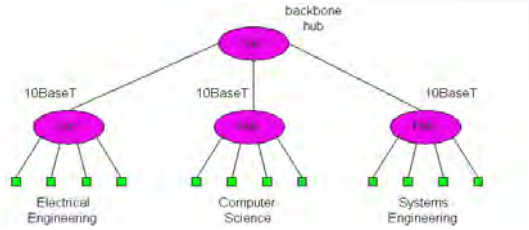
- Hubs
- Bridges
- Switches
  - Remark: switches are essentially multi-port bridges.
  - What we say about **bridges** also holds for **switches**!

19

Interconnecting with hubs

Slide Set 2

- Backbone hub interconnects LAN segments
- Extends max distance between nodes
- But individual segment collision domains become one large collision domain
  - if a node in CS and a node EE transmit at same time: collision
- Can't interconnect 10BaseT & 100BaseT



20

Bridges

Slide Set 2

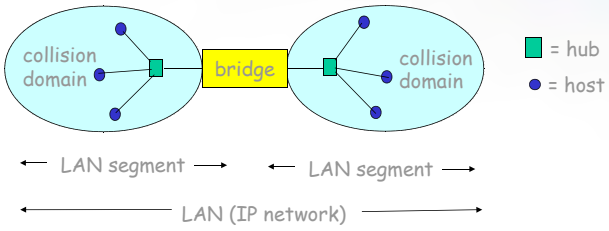
- **Link layer device**
  - stores and forwards Ethernet frames
  - examines frame header and selectively forwards frame based on MAC destination address
  - when frame is to be forwarded on segment, uses CSMA/CD to access segment
- transparent
  - hosts are unaware of presence of bridges
- plug-and-play, self-learning
  - bridges do not need to be configured

21

Bridges: traffic isolation

Slide Set 2

- Bridge installation breaks LAN into LAN segments
- bridges filter packets:
  - same-LAN-segment frames not usually forwarded onto other LAN segments
  - segments become separate collision domains



22

Self learning

Slide Set 2

- A bridge has a bridge or forwarding table
- entry in bridge table:
  - (*Node LAN Address, Bridge Interface, Time Stamp*)
  - stale entries in table dropped (TTL can be 60 min)
- bridges *learn* which hosts can be reached through which interfaces
  - when frame received, bridge "learns" location of sender: incoming LAN segment
  - records sender/location pair in forwarding table

23

Filtering / Forwarding

Slide Set 2

When bridge receives a frame:

index bridge table using MAC dest address
if entry found for destination
then{
if dest on segment from which frame arrived
then drop the frame
else forward the frame on interface indicated
}
else flood

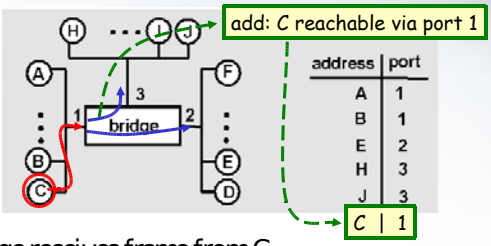
forward on all but the interface on which the frame arrived

24

Slide Set 2

Bridge Learning: example

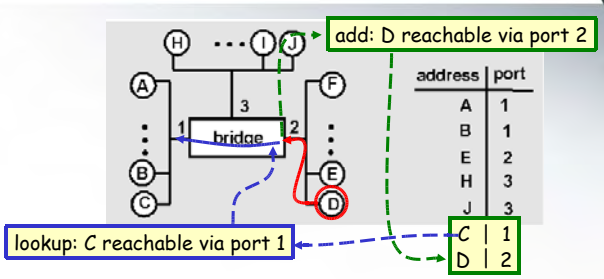
Suppose C sends frame to D and D replies back with frame to C.



- Bridge receives frame from C
  - Insert entry in bridge table that C is on interface 1
  - because D is not in table, bridge sends frame into interfaces 2 and 3 (flooding)
- frame received by D

Slide Set 2

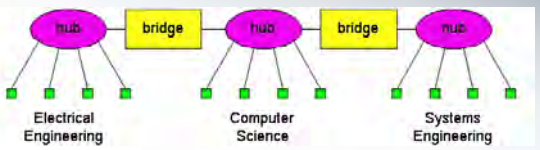
Bridge Learning: example



- D generates frame for C, sends
- bridge receives frame
  - Insert entry in bridge table that D is on interface 2
  - bridge knows C is on interface 1, so *selectively* forwards frame to interface 1

Slide Set 2

Interconnection without backbone

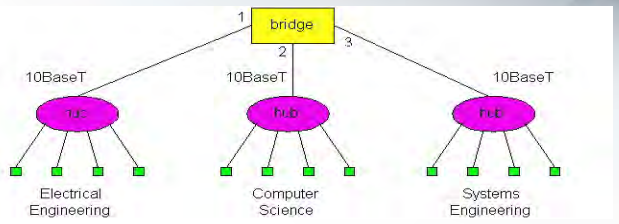


- Not recommended for two reasons:

- single point of failure at Computer Science hub
- all traffic between EE and SE must pass through the CS segment

Slide Set 2

Backbone configuration



Recommended !

Slide Set 2

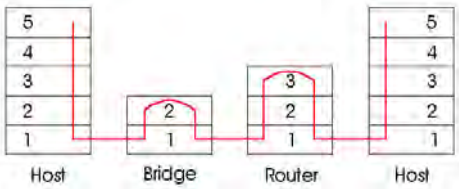
Some Bridge features

- Isolates collision domains resulting in higher total maximum throughput
- limitless number of nodes and geographical coverage
- Can connect different Ethernet types
- Transparent ("plug-and-play"): no configuration necessary

Slide Set 2

Bridges vs. Routers

- ***Both*** store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - bridges are link layer devices
- ***Routers*** maintain routing tables, implement routing algorithms
- ***Bridges*** maintain bridge tables, implement filtering, learning and spanning tree algorithms



Routers vs. Bridges

Bridges + and -

+ Bridge operation is simpler requiring less packet processing
+ Bridge tables are self learning
- All traffic confined to spanning tree, even when alternative bandwidth is available
- Bridges do not offer protection from *broadcast storms*

Routers vs. Bridges

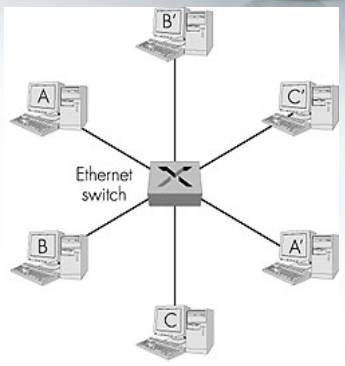
Routers + and -

+ arbitrary topologies can be supported, cycling is limited by TTL counters (and good routing protocols)
+ provide protection against broadcast storms
- require IP address configuration (not plug and play)
- require higher packet processing

- bridges do well in small (few hundred hosts) while routers used in large networks (thousands of hosts)

Ethernet Switches

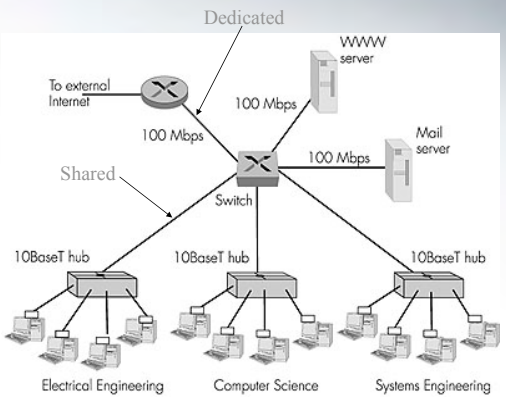
- Essentially a multi-interface bridge
- layer 2 (frame) forwarding, filtering using LAN addresses
- Switching: A-to-A' and B-to-B' simultaneously, no collisions
- large number of interfaces
- often: individual hosts, star-connected into switch
  - Ethernet, but no collisions!



Ethernet Switches

- cut-through switching: frame forwarded from input to output port without awaiting for assembly of entire frame
  - slight reduction in latency
- Store-N-Forward switching: frame buffered completely and error-checked (via CRC) before being forwarded.

A typical LAN (IP network)



Summary comparison

	hubs	bridges	routers	switches
traffic isolation	no	yes	yes	yes
plug & play	yes	yes	no	yes
optimal routing	no	no	yes	no
cut through	yes	no	no	yes

Ethernet

Slide Set 3

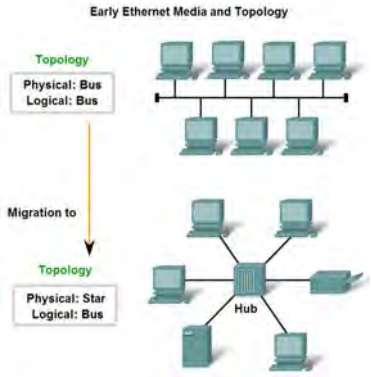
Cisco | Networking Academy®
Mind Wide Open™

Objectives

- Identify the basic characteristics of network media used in Ethernet.
- Describe the physical and data link features of Ethernet.
- Describe the function and characteristics of the media access control method used by Ethernet protocol.
- Explain the importance of Layer 2 addressing used for data transmission and determine how the different types of addressing impacts network operation and performance.
- Compare and contrast the application and benefits of using Ethernet switches in a LAN as apposed to using hubs.
- Explain the ARP process.

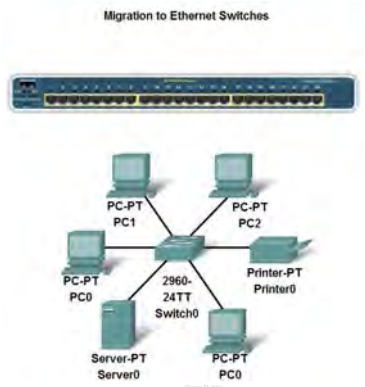
Characteristics of Network Media used in Ethernet

- Identify several characteristics of Ethernet in its early years.



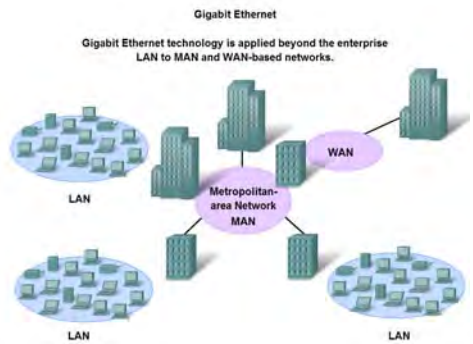
Characteristics of Network Media used in Ethernet

- Describe the emergence of the LAN switch as a key innovation for managing collisions on Ethernet-based networks



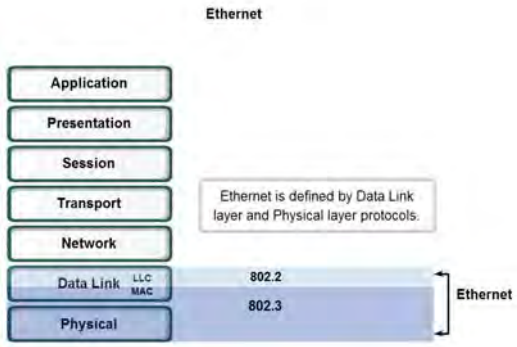
Characteristics of Network Media used in Ethernet

- Identify the characteristics of state-of-the-art Ethernet and describe its utilization of cabling and point-to-point topography



Physical and Data Link Features of Ethernet

- Standards and Implementation



Physical and Data Link Features of Ethernet

- Describe how the Ethernet operates across two layers of the OSI model

Layer 2 Addresses Layer 1 Limitations

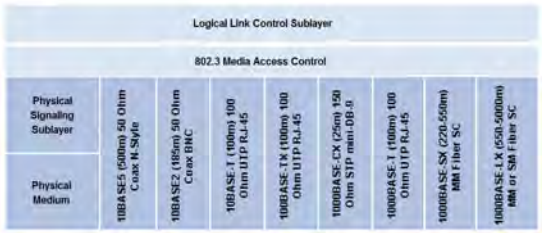
Layer 1 Limitations	Layer 2 Functions
Cannot communicate with upper layers	Connects to upper layers via Logical Link Control (LLC)
Cannot identify devices	Uses addressing schemes to identify devices
Only recognizes streams of bits	Uses frames to organize bits into groups
Cannot determine the source of a transmission when multiple devices are transmitting	Uses Media Access Control (MAC) to identify transmission sources

Physical and Data Link Features of Ethernet

- Logic Link Control – Connecting the Upper Layers

Logical Link Control (LLC)

- Makes the connection with the upper layers
- Frames the Network layer packet
- Identifies the Network layer protocol
- Remains relatively independent of the physical equipment



Physical and Data Link Features of Ethernet

- Media Access Control (MAC)

MAC—Getting Data to the Media

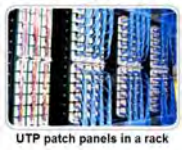
MEDIA ACCESS CONTROL

- Data Encapsulation
  - Frame delimiting
  - Addressing
  - Error detection
- Media Access Control
  - Control of frame placement on and off the media
  - media recovery

Physical and Data Link Features of Ethernet

- Physical Implementations of the Ethernet

Physical Devices Implementing Ethernet


UTP patch panels in a rack


Ethernet switches


Ethernet fiber connectors

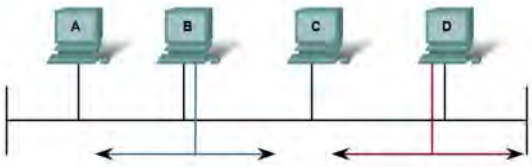

Ethernet switch

Function and Characteristics of the Media Access Control Method

- MAC in Ethernet

Media Access Control in Ethernet

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)



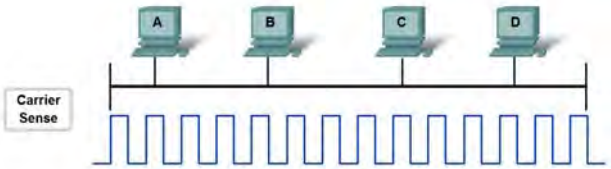
CSMA/CD controls access to the shared media. If there is a collision, it is detected and frames are retransmitted.

Function and Characteristics of the Media Access Control Method

- Carrier Sense Multiple Access with Collision Detection

Media Access Control in Ethernet

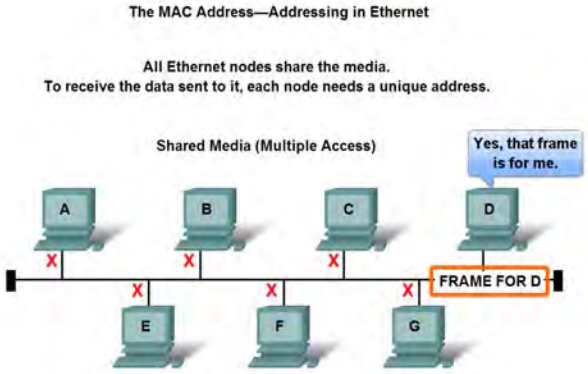
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)



Listen Before Transmitting—Carrier signal detected

Layer 2 addressing and its Impact on Network Operation and Performance

- The Ethernet MAC Address



Layer 2 addressing and its Impact on Network Operation and Performance

- Hexadecimal Numbering and Addressing

Hexadecimal Numbering

Decimal and Binary equivalents of 0 to F Hexadecimal

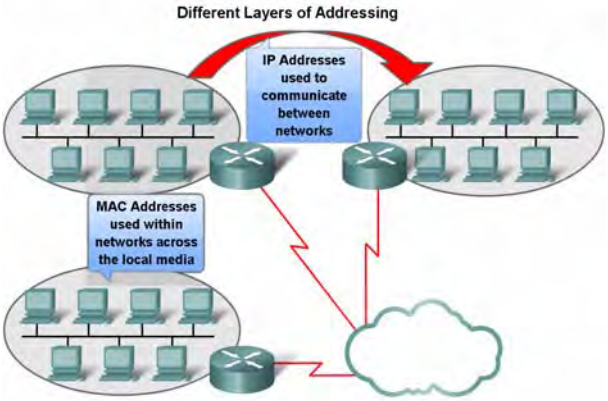
Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Selected Decimal, Binary and Hexadecimal equivalents

Decimal	Binary	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

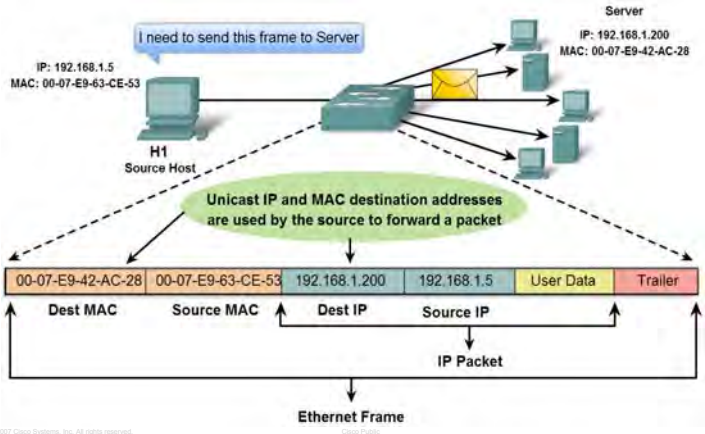
Layer 2 addressing and its Impact on Network Operation and Performance

- Another Layer of Addressing



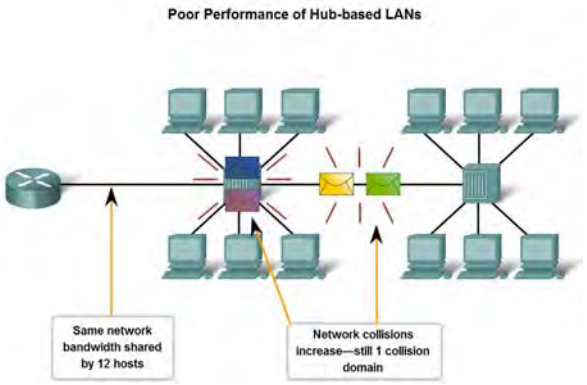
Layer 2 addressing and its Impact on Network Operation and Performance

- Ethernet Unicast, Multicast and Broadcast



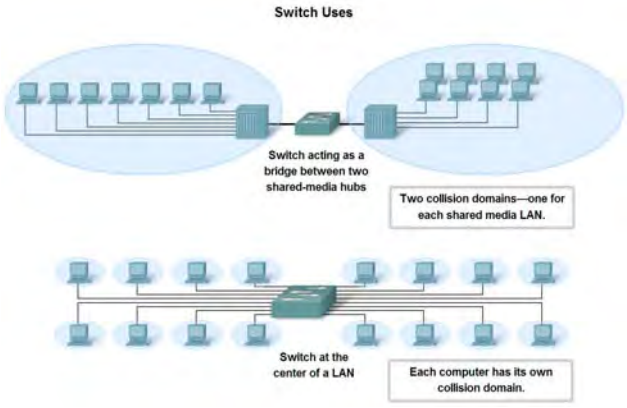
Compare and Contrast the Use of Ethernet Switches versus Hubs in a LAN.

- Legacy Ethernet – Using Hubs



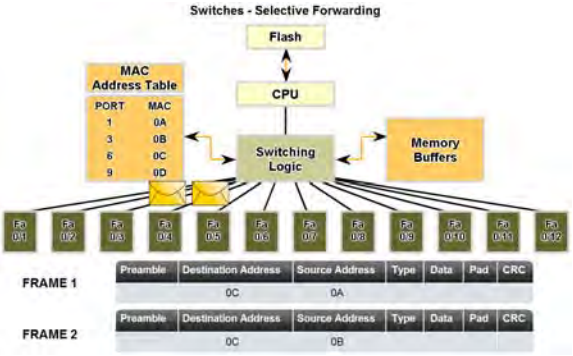
Compare and Contrast the Use of Ethernet Switches versus Hubs in a LAN.

- Ethernet – Using Switches



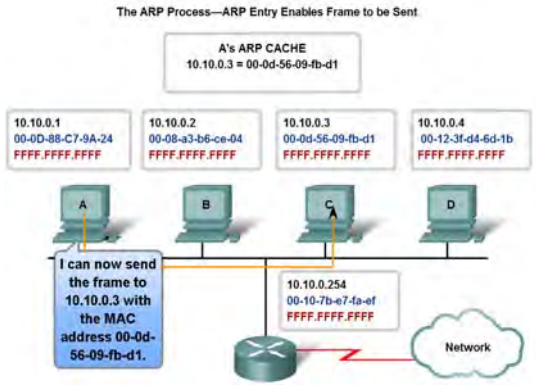
Compare and Contrast the Use of Ethernet Switches versus Hubs in a LAN.

- Describe how a switch can eliminate collisions, backoffs and re-transmissions, the leading factors in reduced throughput on a hub-based Ethernet network



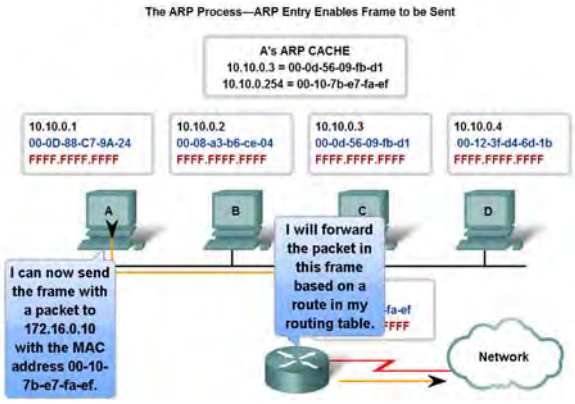
Explain the Address Resolution Protocol (ARP) process.

- Mapping IP to MAC Addresses



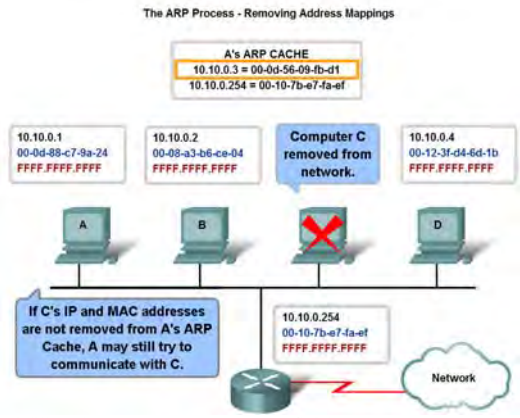
Explain the Address Resolution Protocol (ARP) process.

- ARP – Destinations Outside the Local Network



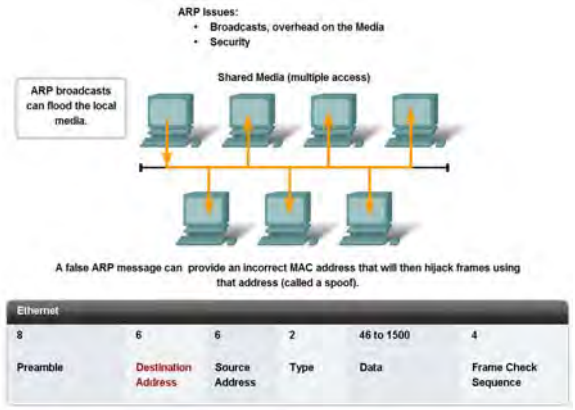
Explain the Address Resolution Protocol (ARP) process.

- ARP – Removing Address Mappings



Explain the Address Resolution Protocol (ARP) process.

- ARP Broadcasts - Issues



Summary

In this chapter, you learned to:

- Identify the basic characteristics of network media used in Ethernet.
- Describe the Physical and Data Link layer features of Ethernet.
- Describe the function and characteristics of the media access control method used by Ethernet protocol.
- Explain the importance of Layer 2 addressing used for data transmission and determine how the different types of addressing impacts network operation and performance.
- Compare and contrast the application and benefits of using Ethernet switches in a LAN as opposed to using hubs.
- Explain the ARP process.

Configuring and Testing Your Network

Slide Set 4

Cisco | Networking Academy®
Mind Wide Open™

Objectives

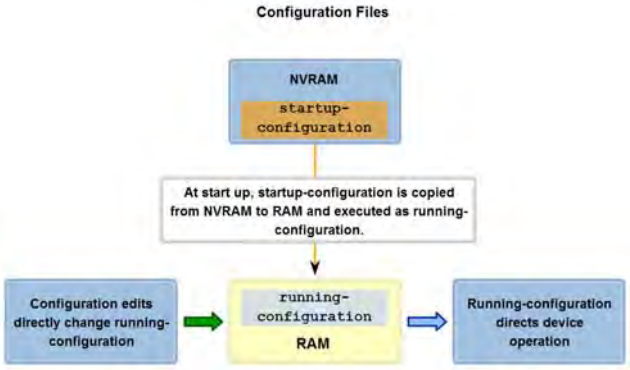
- Define the role of the Internetwork Operating System (IOS)
- Use Cisco CLI commands to perform basic router and switch configuration and verification
- Given a network addressing scheme, select, apply, and verify appropriate addressing parameters to a host
- Use common utilities to verify network connectivity between hosts
- Use common utilities to establish a relative performance baseline for the network

Role of Internetwork Operating System (IOS)

- Identify several classes of devices that have IOS embedded

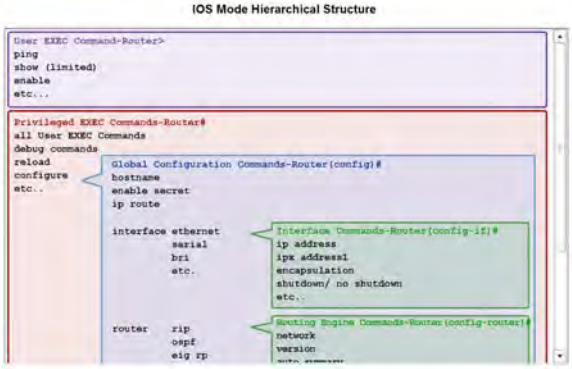
Role of Internetwork Operating System (IOS)

- Identify the relationship between IOS and config



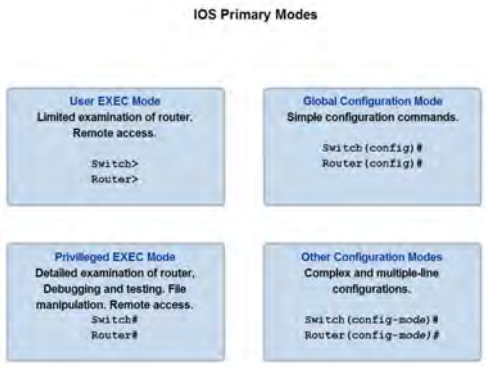
Role of Internetwork Operating System (IOS)

- Recognize that Cisco IOS is modal and describe the implications of modes.



Role of Internetwork Operating System (IOS)

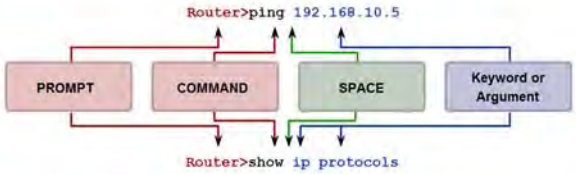
- Define the different modes and identify the mode prompts in the CLI



Role of Internetwork Operating System (IOS)

- Identify the basic command structure for IOS commands

Basic IOS Command Structure



Prompt commands are followed by a space and then the keyword or arguments.

Role of Internetwork Operating System (IOS)

- Identify the types of help and feedback available while using IOS and use these features to get help, take

Context Sensitive Help

Example of a sequence of commands using the CLI context sensitive help

```
Cisco#cl?
clear  clock
Cisco#clock ?
  set  Set the time and date
Cisco#clock set
% Incomplete command.
Cisco#clock set ?
  hh:mm:ss  Current Time
Cisco#clock set 19:50:00
% Incomplete command.
```

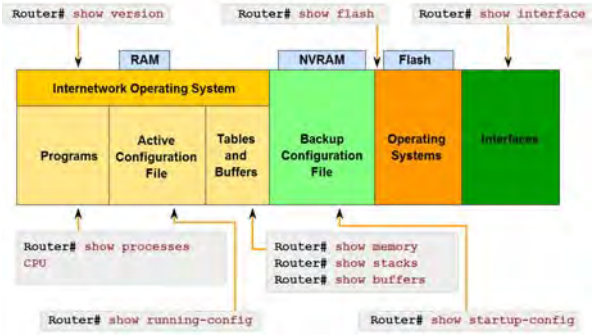
```
Cisco#clock set 19:50:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year
Cisco#clock set 19:50:00 25 6
                           ^
Invalid input detected at '^' marker.
Cisco#clock set 19:50:00 25 June
% Incomplete command.
Cisco#clock set 19:50:00 25 June ?
  <1993-2035>  Year
Cisco#clock set 19:50:00 25 June 2007
Cisco#
```

Command explanations
Incomplete Command messages
Invalid input messages
Variable formats

Role of Internetwork Operating System (IOS)

- Identify the purpose of the show command and several of its variations

IOS show commands can provide information about the configuration, operation and status of parts of a Cisco router.



Role of Internetwork Operating System (IOS)

- Identify several of the configuration modes, their purpose and their associated prompt

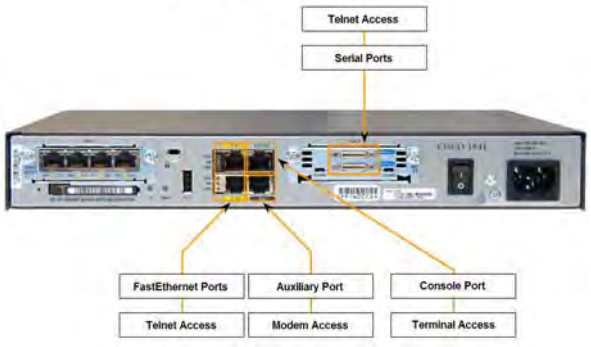
IOS Configuration Modes

Configuration Mode	Prompt
Interface	Router(config-if)#
Line	Router(config-line)#
Routers	Router(config-router)#

Role of Internetwork Operating System (IOS)

- Use the CLI to access various IOS configuration modes on a device

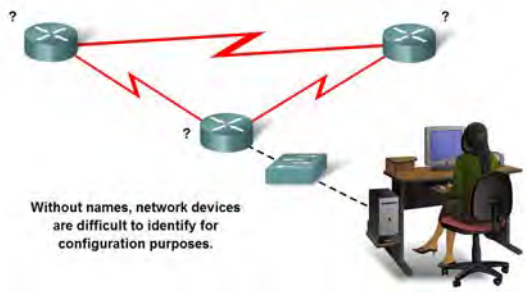
Accessing the Cisco IOS on a Device



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Explain the reasons for naming devices.

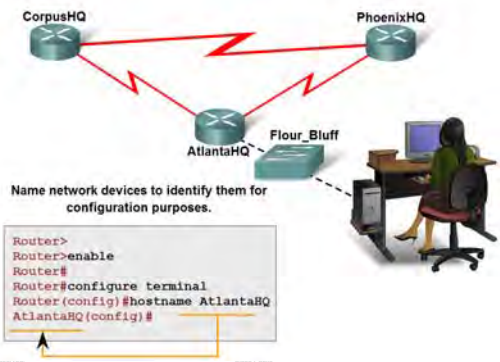
Basic Configuration Using Cisco IOS



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Describe two common approaches to establishing naming conventions

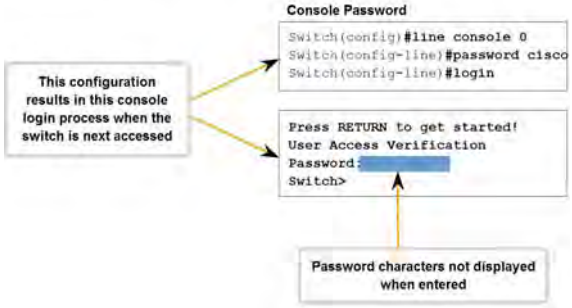
Configuring Device Names



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Describe the role of passwords in limiting access to device configurations

Limiting Device Access - Configuring Console Passwords



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

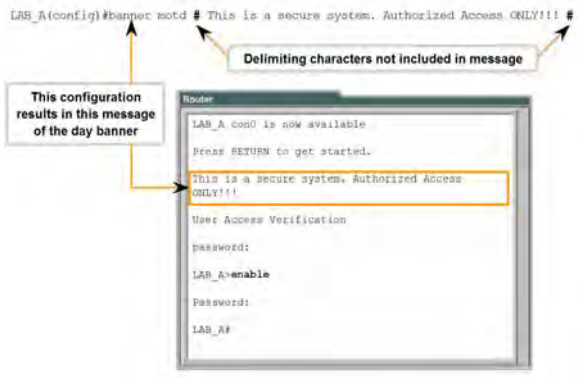
- Describe several ways in which access to a device configuration can be limited

Limiting Device Access
Configuring Telnet and Password Encryption

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Use the CLI to set passwords and add banners to a device

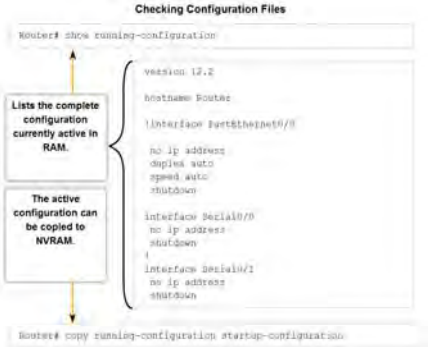
Limiting Device Access – Login Banner



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Trace the steps used to examine the startup config, make changes to config, and replace the startup config with the running config

Checking Configuration Files



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

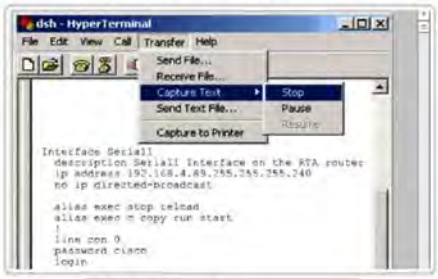
- Use basic IOS config commands to manage a device.

```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm] y
Writing tokyo.2 !!!!!! [OK]
```

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

- Use a text file to backup and restore config settings

Saving to a Text File in Hyperterminal



In the terminal session:

1. Start the text capture process
2. Issue a show running-config command
3. Stop the capture process
4. Save the text file

19

Select, Apply, and Verify Appropriate Addressing Parameters to a Host

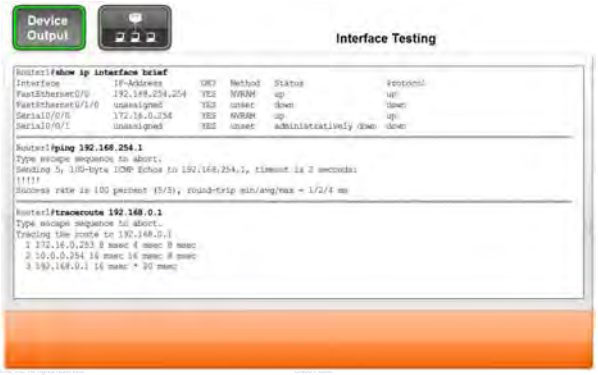
- Given a type of host and a master addressing scheme, trace the steps for assigning host parameters to a host

Testing Local TCP/IP Stack

20

Select, Apply, and Verify Appropriate Addressing Parameters to a Host

- Trace the steps for using ipconfig/ifconfig to verify host parameter assignments and for using ping to test assignments

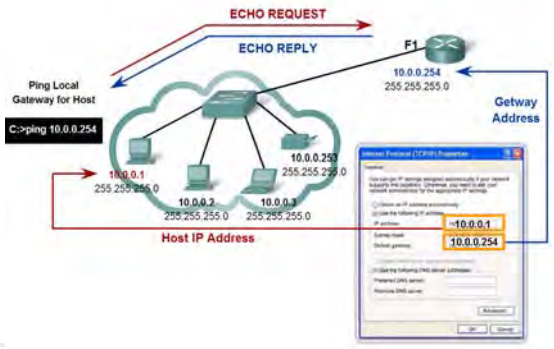


21

Use Common Utilities to Verify Network Connectivity Between Hosts

- Use the ping command in the CLI to determine if the IP protocol is operational on a local host

Testing Gateway Connectivity



22

Use Common Utilities to Verify Network Connectivity Between Hosts

- Use the ping command to determine if the IP protocol is properly bound to an NIC

Testing the Local NIC Assignment

```
IP Address. . . . . . . . . . . . : 10.0.0.5
Subnet Mask . . . . . . . . . . . :
255.255.255.0
```

Verify the host NIC address is bound and ready for transmitting signals across the media by pinging its own IP address

23

Use Common Utilities to Verify Network Connectivity Between Hosts

- Use the ping command to determine if a host can actively communicate across the local network

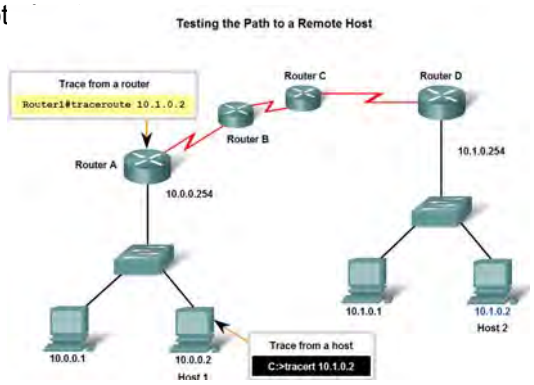
Testing Local Network

Successfully pinging the other host's IPv4 addresses will verify that not only the local host is configured properly but the other hosts are configured correctly as well.

24

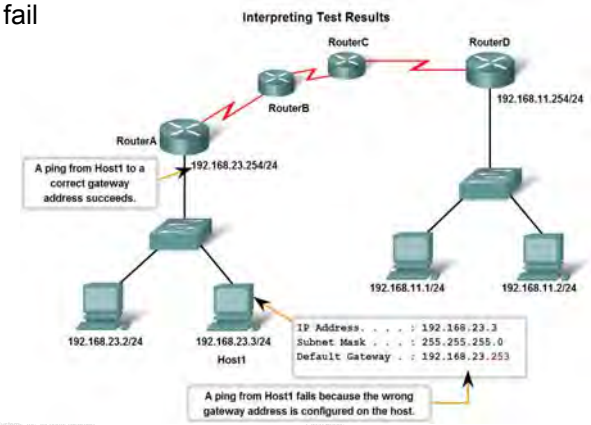
Use Common Utilities to Verify Network Connectivity Between Hosts

- Use the ping command to verify that the local host can communicate across the internetwork to a given remot



Use Common Utilities to Verify Network Connectivity Between Hosts

- Identify several conditions that might cause the test to fail



Use Common Utilities to Establish a Relative Performance Baseline for the Network

- Use the output of the ping command, saved into logs, and repeated over time, to establish relative network performance

Baseline with ping

FEB 2, 2007 08:14:43

```
C:\host1>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.254.159: bytes=32 time<1ms TTL=128
Reply from 10.66.254.159: bytes=32 time<1ms TTL=128
Reply from 10.66.254.159: bytes=32 time<1ms TTL=128
Reply from 10.66.254.159: bytes=32 time<1ms TTL=128
```

MAR 17, 2007 14:41:06

```
C:\host1>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.254.159: bytes=32 time<6ms TTL=128
Reply from 10.66.254.159: bytes=32 time<6ms TTL=128
Reply from 10.66.254.159: bytes=32 time<6ms TTL=128
Reply from 10.66.254.159: bytes=32 time<6ms TTL=128
```


Use Common Utilities to Establish a Relative Performance Baseline for the Network

- Use the output of the traceroute command, saved into logs, and repeated over time, to establish relative network performance

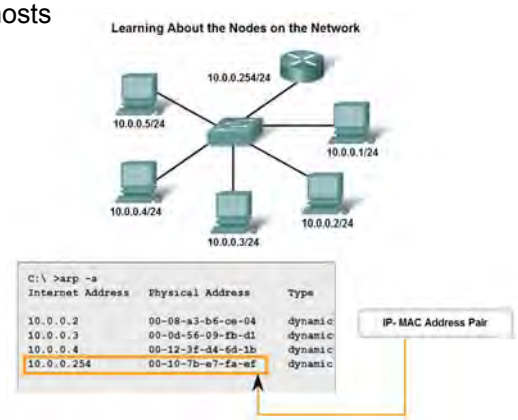
Capturing Trace Route

```
C:\>tracert www.cisco.com

Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.0.1
  2    20 ms    20 ms    20 ms  nexthop.wa.il.net [203.59.14.16]
  3    20 ms    19 ms    20 ms  gi2-4.per-qvl-bdr1.il.net [203.215.4.32]
  4    79 ms    78 ms    78 ms  gi0-14-0-0.syd-ult-core1.il.net [203.215.20.2]
  5    79 ms    81 ms    79 ms  202.139.19.33
  6   227 ms   226 ms   227 ms  203.208.148.17
  7   227 ms   227 ms   227 ms  203.208.149.34
  8   225 ms   225 ms   226 ms  208.30.205.145
  9   236 ms   249 ms   233 ms  sl-bb23-ana-8-0-0.sprintlink.net [144.232.9.23]

 10   241 ms   244 ms   240 ms  sl-bb25-sj-9-0.sprintlink.net [144.232.20.159]
 11   238 ms   238 ms   239 ms  sl-gw8-sj-10-0.sprintlink.net [144.232.3.114]
 12   238 ms   239 ms   240 ms  144.228.44.14
 13   240 ms   242 ms   248 ms  sjce-dmzbb-gw1.cisco.com [128.107.239.89]
```

Sample trace output

Use Common Utilities to Establish a Relative Performance Baseline for the Network

- Trace the steps for verifying the physical addresses of the hosts



Summary

In this chapter, you learned to:

- Define the role of the Internetwork Operating System (IOS).
- Define the purpose of a configuration file.
- Identify several classes of devices that have the IOS embedded.
- Identify the factors contributing to the set of IOS commands available to a device.
- Identify the IOS modes of operation.
- Identify the basic IOS commands.
- Compare and contrast the basic show commands.

Cisco.com

Switching Concepts

Slide Set 5

1

Switches and Bridges

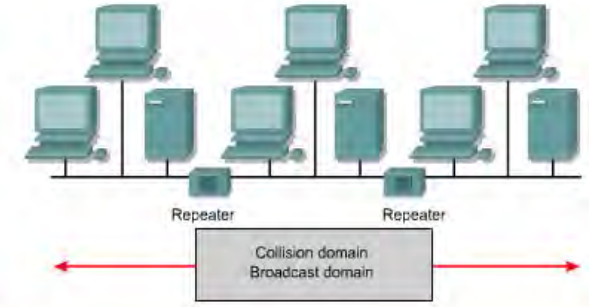
Cisco.com

- Make decisions when frames are received
  - select a path or circuit to send a frame to its destination
- Layer 2 devices
  - increases the number of collision domains
  - hosts connected to the switch are part of the same broadcast domain
- Used to
  - increase available bandwidth
  - reduce network congestion
- Switch segments a LAN into microsegments
  - segments with only a single host
  - creates multiple collision-free domains

2

Repeaters

Cisco.com



- Repeaters are Layer 1 devices that regenerate the signal, and pass it on
- Repeaters allow a longer end-to-end distance
- Repeaters increase the collision domain size
- Repeaters increase the broadcast domain size

3

Hub

Cisco.com

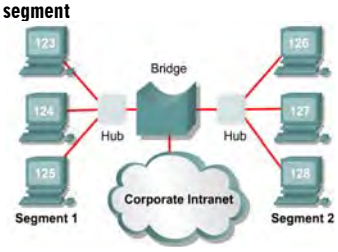
- Layer 1 device (*physical layer*)
- Ethernet concentrator or a multi-port repeater
- No decision made at this level (*no addressing*)
- Takes data signal in one port
  - Regenerates, retimes and amplifies the data signals
  - Sends (*Broadcasts*) data signal out all other ports
- All users connected to the hub compete for the same bandwidth (*shared bandwidth*)
  - 50% – 60% bandwidth available
- Increase collision domains (*extends*)
- Increase broadcast domains (*extends*)
- Only 1 device can transmit at a time

4

Bridge

Cisco.com

- Layer 2 device (*data link layer*)
- Creates 2 network segments
  - 2 collision domains – creates smaller collision domains
  - 2 bandwidth domains
- Do not restrict broadcast traffic – (forwards broadcasts)
- Learns MAC address of all devices on each segment
  - Use this to build bridging table
  - Forwards/blocks traffic based on table
- Makes decisions based on MAC
  - Increase latency by 10 to 30 percent
  - Switching occurs using software
- Store and forward device
- Adds 10% to 30% latency



5

Switch

Cisco.com

- Layer 2 device (*data link layer*)
- Multiport bridge or switching hubs
- Provides microsegmentation (point-to-point link)
  - It isolates traffic among segments
  - creates a collision free environment between the source and destination
  - Each segment uses CSMA/CD (allows multiple communications on different segments)
  - Each port has dedicated bandwidth (100% bandwidth available)
- Makes decisions based on MAC addresses
  - Held in Content Addressable Memory
  - Switching occurs using hardware
- Decreases collision domain
  - 1 collision domain per segment (increases number of collision domains)
- Increases broadcast domain (*Extends*)
  - Broadcasts sent out very port

6

Network Performance

Cisco.com

- LANs are increasingly congested and overburdened
  - Growing population of network users
  - Multitasking environment
    - increased demand for network resources
  - The use of network intensive applications
    - e.g. WWW, multimedia, e-mail
  - Client/server applications
- This has resulted in
  - a need for more bandwidth
  - slower response times
  - longer file transfers
  - network users becoming less productive

7

Elements of Ethernet 802.3

Cisco.com

- Used to transport data between devices on a network (*computers, printers, and file servers*)
- Multi-access broadcast technology
  - Shared media
- Uses CSMA/CD to allows one station transmit at a time
- Latency as frames travel across media
- Repeaters extend distances (*increase latency*)
- Layer 2 devices improve performance

8

Network Latency

Cisco.com

- Latency, or delay, is the time a frame or a packet takes to travel from the source to the final destination
- Latency sources:

Transmit delay and Buffering delay (NIC Delay)

- The time it takes to inject the data (as pulses) on the network at the sender and the time to buffer the data at the receiver
- Transmit delay = Buffering delay = size of data/bandwidth available

Propagation delay

- Signal takes time to travel along the cable = Distance traveled/speed of signal
- About 0.556 microseconds per 100 m for Cat 5 UTP

Networking devices

- Layer 1 no decisions less latency
- Layer 2 devices make layer 2 decisions increased latency
- Layer 3 devices make layer 3 decisions most latency

9

Ethernet X-BaseT Transmission

Cisco.com

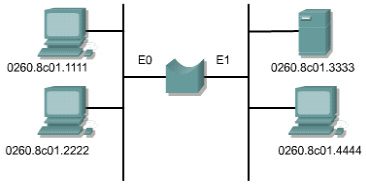
- The time it takes a frame to be transmitted
  - Number of bits being sent * Technology Bit time
- 10 Mbps Ethernet bit has a 100 ns transmission window (bit time of 100 ns)
  - 1 byte is 8bits * 100ns = 800 ns to transmit
- 100Mbps = 10ns
- 1000Mbps = 1 Gbps = 1ns

Frame Size in Bytes	Transmission Time in Microseconds
64	51.2
512	410
1000	800
1518	1214

10

LAN Segmentation with Bridges

Cisco.com



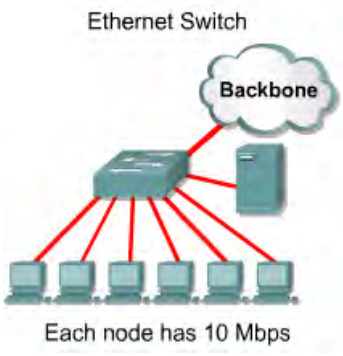
Interface	MAC address
E0	0260.8c01.1111
E0	0260.8c01.2222
E1	0260.8c01.3333
E1	0260.8c01.4444

Operation of a bridge is transparent to other network devices
Bridge increases latency by 10% to 30%
  Due to decision making process
Bridge is a store-and-forward device
  Examine the destination address field
  Calculate the cyclic redundancy check (CRC)
  Forward the frame
Bridge can temporarily store the frame if a port is busy
Forward broadcasts

11

LAN Segmentation with Switches

Cisco.com



Segment LAN into microsegments

Decreases collision domains size

Extends broadcast domain

Virtual network circuit is established within the switch and exists only when the nodes need to communicate

12

How do Switches and Bridges Filter Frames

Cisco.com

- Bridges are capable of filtering frames based on any Layer 2 fields
- Bridge can be programmed to reject/not forward
  - All frames sourced from a particular network
    - Based on upper network layer protocols
  - filters out unnecessary broadcast and multicast packets
- Ignoring a frame is called filtering.
- Copying the frame is called forwarding.

13

Symmetric and Asymmetric Switching

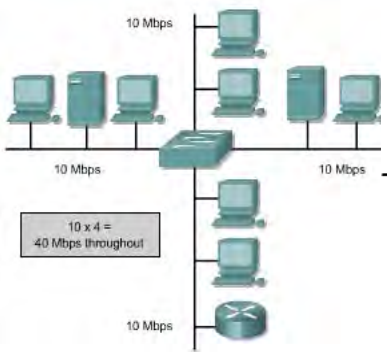
Cisco.com

- based on the way bandwidth is allocated to the switch ports
- Symmetric switch
  - switched connections between ports with the same bandwidth (all 10Mbps or all 100Mbps)
- Asymmetric switch
  - switched connections between ports of unlike bandwidth
  - combination of 10 and 100 Mbps ports
  - Enables more bandwidth to be dedicated to the server switch port in order to prevent a bottleneck
  - Memory buffering is required (keeps the frames contiguous between different data rate ports)

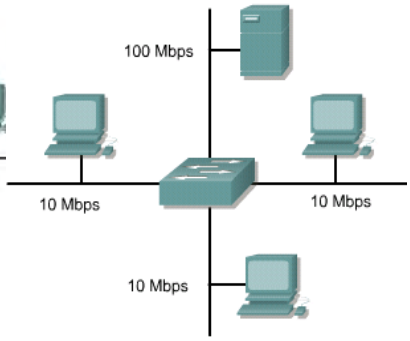
14

Cisco.com

Symmetric Switching



Asymmetric Switching



15

Switching Methods

Cisco.com

1. Store and Forward
   - Entire frame is received before any forwarding
   - Increases latency
   - Filters can be applied to destination and source addresses
   - Frame can be checked for errors and hence discarded if corrupted
2. Cut-Through
   - At least the frame destination address must be read before the frame can be forwarded
   - Decreases latency (Buffer time at switch decreases proportionally)
   - No error detection

16

Types of Cut-Through Switching

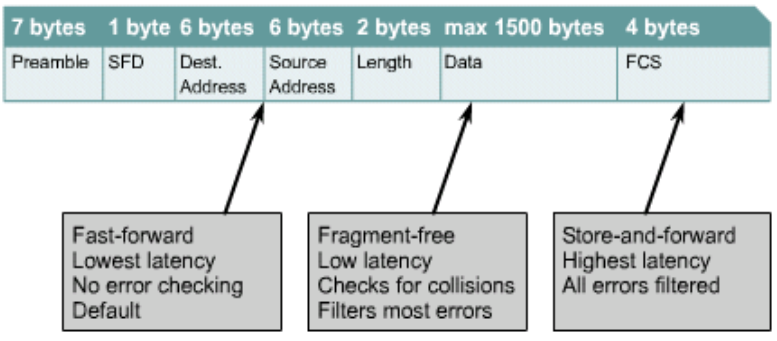
Cisco.com

1. Fast-forward
   - Lowest level of latency
   - Immediately forwards packet after reading destination address
   - No error checking
   - Destination network adapter will discard the faulty packet upon receipt
2. Fragment-free
   - Filter out collision fragments before forwarding begins
   - Reads first 64 bits to identify if a collision occurred

17

Frame Transmission Modes

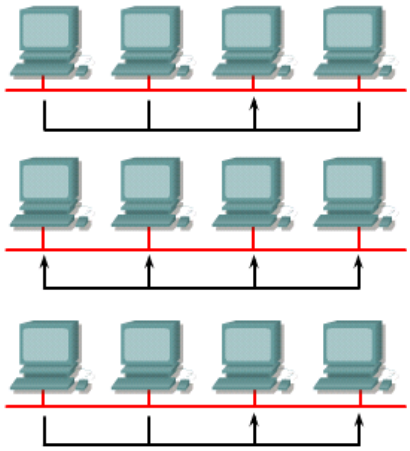
Cisco.com



18

Switches and Broadcast Domains

Cisco.com



one transmitter tries to reach one receiver

one transmitter tries to reach only a subset or a group of the entire segment.

one transmitter tries to reach all receivers in the network

19

Cisco.com

- When a device wants to send out a Layer 2 broadcast
  - Destination MAC address in the frame is set to all ones
  - FF:FF:FF:FF:FF:FF in hexadecimal
  - MAC broadcast domain
- When a switch receives a broadcast
  - it forwards it to each port on the switch except the incoming port
  - Each attached device must process the broadcast frame
- Broadcasts reduce available bandwidth

20

Cisco.com

Switch Configuration

Slide Set 6

1

Switch

Cisco.com

- Switches are dedicated, specialized computers
  - Central processing unit (CPU)
  - Random access memory (RAM)
  - Operating system
- Switch ports for
  - Connecting hosts (for inter-host communication)
  - Management (console port for configuration)

2

Switch LED Indicators

Cisco.com

- If Mode is STAT (default mode)

off No link

Solid green Link operational

Flashing green Port sending/ receiving

Green/Amber Fault on link

Solid Amber Port disabled or Port blocked by STP

- If mode is UTL

Off Reduction by half total b/w

Green All Green – using50% bandwidth

- If mode is FDUP

Off Half-duplex mode

Green Full-duplex mode

- If mode is 100

Off Operating at 10Mbps

Green Operating at 100Mps

3

Verifying Switch LEDs

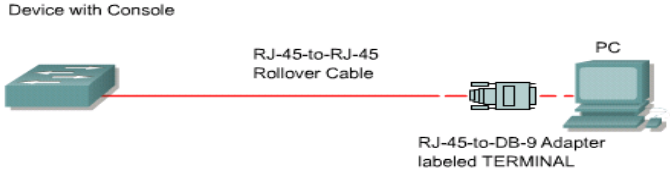
Cisco.com

- **POST**
  - **runs automatically**
  - **verify that the switch functions correctly**
- **The System LED indicates success/failure of POST**
  - **System LED off and switch is plugged in, POST running**
  - **System LED green, POST was successful**
  - **System LED amber, POST failed (fatal error)**
- **The Port Status LEDs changes during switch POST**
  - **Port Status LEDs amber (30 secs) switch discovers network topology and searches for loops**
  - **Port Status LEDs green, Link established between port and PC**
  - **Port Status LEDs off, nothing is plugged into the port**

4

To Configure a Switch

Cisco.com



Set hyperterminal link with Com port Settings

9600bps
8 data bits
No parity
1 stop bit
Hardware flow control

Switch can be configured
Manually or
System Configuration Dialog

5

To Configure a Switch

Cisco.com

- **By default**
  - **Data is in running configuration file**
  - **Hostname is** Switch
  - **No passwords set on the console or vty lines**
  - **Switch ports or interfaces are set to auto mode**
  - **No IP Address**
    - **Switch may be given an IP address for management purposes**
    - **This is configured on the virtual interface, VLAN 1**
  - **All switch ports are in VLAN 1**
    - **default management VLAN**
    - **No VLAN database or configuration file**
  - **IOS image is in flash directory by default**
  - **One broadcast domain**
  - **Spanning-Tree Protocol is enabled and allows the bridge to construct a loop-free topology across an extended LAN**

6

Obtaining help

Cisco.com

- **Command Syntax help**
  - **? List all possible commands**
  - **Command ? List of sub commands for command**

7

Switch Command Modes

Cisco.com

- **User Executive Mode**
  - **Default mode**
  - **Prompt >**
  - **Commands at this level**
    - **change terminal settings**
    - **perform basic tests**
    - **display system information**
    - **Show commands**
  - **>enable change into Privileged Exec Mode**

- **Privileged Exec Mode**
  - **Should be password protected**
    - **Case sensitive**
    - **Does not appear on screen**
  - **Prompt #**
  - **commands**
    - **All allowed in user exec mode**
    - configure **command to access other modes**

8

Switch Configuration

Cisco.com

- **Switch>enable**
- **Switch#delete flash:vlan.dat** *deletes vlan information*
- **Switch#erase startup-config** *erase configuration files*
- **Switch#reload** *reload switch*
- **Switch#config terminal** *enter configuration mode*
- **Switch(config)#hostname newName** *configure hostname*

9

Switch Configuration

Cisco.com

- To configure a console password
  - **Switch(config)#line con 0**
  - **Switch(config-line)#password <password>**
  - **Switch(config-line)#login**
- To configure a telnet password
  - **Switch(config)#line vty 0 4**
  - **Switch(config-line)#password<password>**
  - **Switch(config-line)#login**

10

Switch Configuration

Cisco.com

- **To make switch accessible by Telnet and other TCP/IP applications set**
  - **IP addresses and a default gateway**
- **By default, VLAN 1 is management VLAN**
- **Configuration needed**
  - **To access, configure, and manage all internetworking devices**
  - **Switch(config)#interface VLAN1**
  - **Switch(config-if)#ip address <add> <sub-mask>**
  - **Switch(config-if)#exit**
  - **Switch(config)#ip default-gateway <next hop>**

11

Switch Configuration

Cisco.com

- **Once a switch is configured with an IP address and gateway, it can be accessed through the web browser**
- **This allows you to verify configuration settings**
- **To do this HTTP service must be turned on**
  - **Switch(config)#ip http server**
  - ***Enables a http server***
  - **Switch(config)#ip http port 80**
  - ***Port 80 is the default port for http***

12

Managing the MAC Address Table

Cisco.com

- MAC Address
  - Dynamically learned
  - Held in CAM – MAC address table
  - Switches examines the source address
    - Record or tag mac address
  - MAC Address discarded after 300 seconds of no taging
- To see the MAC Address table
  - show mac-address–table
- To remove all entries from MAC Address table
  - Clear mac-address-table

13

Configuring Static MAC Address

Cisco.com

- Why assign a static mac address
  - MAC address will not be aged out automatically by the switch
  - A specific server or user workstation must be attached to the port and the MAC address is known
  - Security is enhanced
- Configuration
  - Switch(config)#mac-address-table static <mac>
- To remove a static mac address
  - Switch(config)#no mac-address-table static <mac>

14

Configuring Port Security

Cisco.com

- Access layer switch ports are a potential entry point to the network by unauthorized users.
- Port security limits the number of addresses that can be learned on an interface
- Set port security on a switch interface
  - Can be limited to 1
  - Switch(config)#interface fa0/2
  - Switch(config-if)#port security max-mac-count <number>
- switch#show port security

15

What to Configure when Adding a New Switch

Cisco.com

- Switch name
- IP Address form management purposes
- Default gateway
- Passwords for console, aux, vty
- Security
- Access switch ports

16

Moving a MAC Address

Cisco.com

- Add the address to a new port
- Configure port security on new switch
- Remove old port configurations

- Administrator should
  - document and maintain the operational configuration files for networking devices (back up on a server or disk)
  - Backup IOS to a local server

17

Password Recovery

Cisco.com

- Enter the setup program
  - Deleting the switch configuration file
  - Rebooting the switch

18

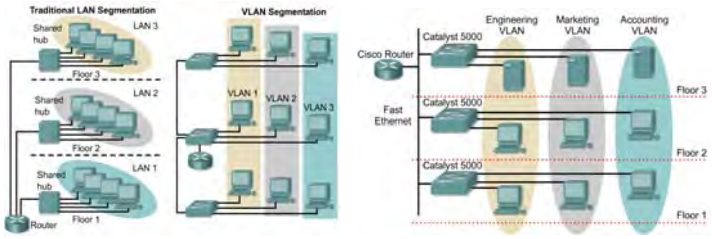
Virtual LAN

Slide Set 7

Overview

- Define VLANs
- List the benefits of VLANs
- Explain how VLANs are used to create broadcast domains
- Explain how routers are used for communication between VLANs
- List the common VLAN types
- Define ISL and 802.1Q
- Explain the concept of geographic VLANs
- Configure static VLANs on 29xx series Catalyst switches
- Verify and save VLAN configurations
- Delete VLANs from a switch configuration

VLAN introduction



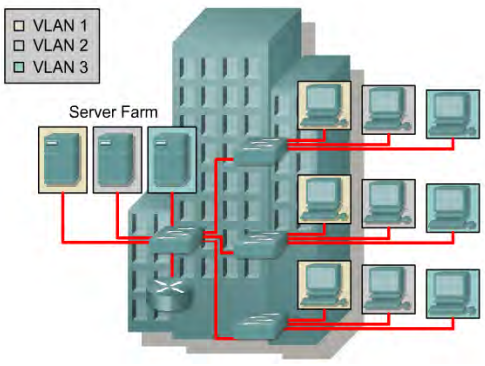
- **VLANs provide segmentation based on broadcast domains.**
- VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.

VLAN introduction

- A group of ports or users in same broadcast domain
- Can be based on port ID, MAC address, protocol, or application
- LAN switches and network management software provide a mechanism to create VLANs
- Frame tagged with VLAN ID

- **VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations.**
- VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain.
- Traffic should only be routed between VLANs.

Broadcast domains with VLANs and routers



- **A VLAN is a broadcast domain created by one or more switches.**
- **The network design above creates three separate broadcast domains.**

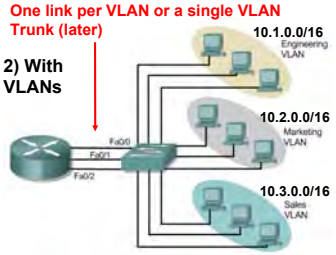
Broadcast domains with VLANs and routers

1) Without VLANs

- 1) Without VLANs, each group is on a different IP network and on a different switch.
- 2) Using VLANs. Switch is configured with the ports on the appropriate VLAN. Still, each group on a different IP network; however, They are all on the same switch.
- What are the broadcast domains in each?

One link per VLAN or a single VLAN Trunk (later)

2) With VLANs



VLAN operation

Configuring VLANs	Description
Statically	Network administrators configure port-by-port. Each Port is associated with a specific VLAN. The network administrator is responsible for keying in the mappings between the ports and VLANs.
Dynamically	The ports are able to dynamically work out their VLAN configuration. Uses a software database of MAC address to VLAN mappings (which the network administrator must set up first).

- Each switch port can be assigned to a different VLAN.
- Ports assigned to the same VLAN share broadcasts.
- Ports that do not belong to that VLAN do not share these broadcasts.

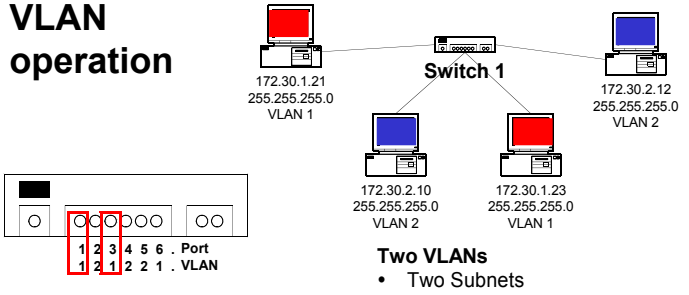
7

VLAN operation

- **Static membership VLANs are called port-based and port-centric membership VLANs.**
- As a device enters the network, it automatically assumes the VLAN membership of the port to which it is attached.
- "The **default VLAN** for every port in the switch is the management VLAN. The management VLAN is always VLAN 1 **and may not be deleted."**
  - ***This statement does not give the whole story. We will examine Management, Default and other VLANs at the end.***
- All other ports on the switch may be reassigned to alternate VLANs.
- More on VLAN 1 later.

8

VLAN operation



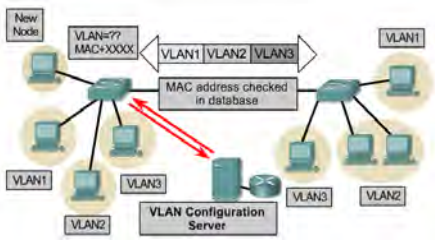
Two VLANs
- Two Subnets

Important notes on VLANs:

1. VLANs are assigned on the switch port. There is no "VLAN" assignment done on the host (usually).
2. In order for a host to be a part of that VLAN, it must be assigned an IP address that belongs to the proper subnet.
   Remember: VLAN = Subnet
3. Assigning a host to the correct VLAN is a 2-step process:
   1. Connect the host to the correct port on the switch.
   2. Assign to the host the correct IP address depending on the VLAN memebership

9

VLAN operation

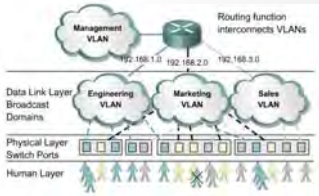


- **Dynamic membership VLANs are created through network management software. (Not as common as static VLANs)**
- **CiscoWorks 2000 or CiscoWorks for Switched Internetworks** is used to create Dynamic VLANs.
- Dynamic VLANs allow for membership based on the MAC address of the device connected to the switch port.
- As a device enters the network, it queries a database within the switch for a VLAN membership.

10

Benefits of VLANs

All users attached to the same switch port must be in the same VLAN.

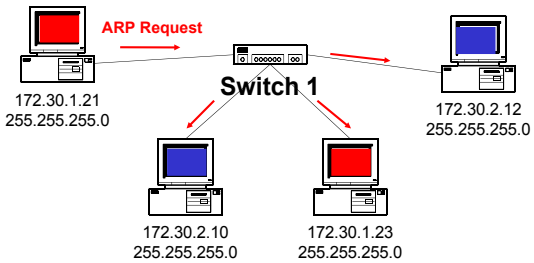


If a hub is connected to VLAN port on a switch, all devices on that hub must belong to the same VLAN.

- The key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically.
- This means that an administrator is able to do all of the following:
  - Easily move workstations on the LAN.
  - Easily add workstations to the LAN.
  - Easily change the LAN configuration.
  - Easily control network traffic.
  - Improve security.

11

Without VLANs – No Broadcast Control

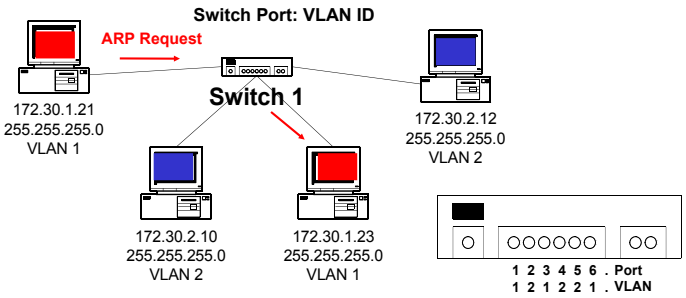


No VLANs
- Same as a single VLAN
- Two Subnets

- Without VLANs, the ARP Request would be seen by all hosts.
- Again, consuming unnecessary network bandwidth and host processing cycles.

12

With VLANs – Broadcast Control

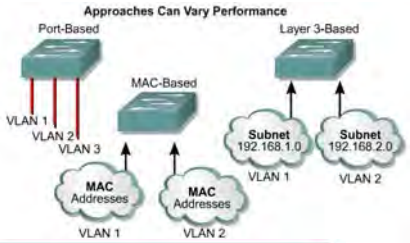


Two VLANs

- Two Subnets

13

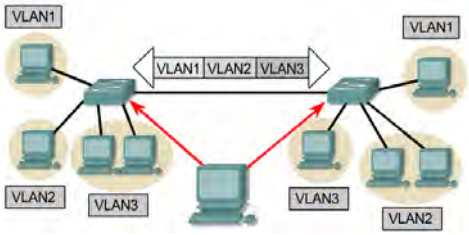
VLAN Types



VLAN Types	Description
Port-based	• Most common configuration method. • Ports assigned individually, in groups, in rows, or across 2 or more switches. • Simple to use. • Often implemented where Dynamic Host Control Protocol (DHCP) is used to assign IP addresses to network hosts.
MAC address	• Rarely implemented today. • Each address must be entered into the switch and configured individually. • Users find it useful. • Difficult to administer, troubleshoot and manage.
Protocol Based	• Configured like MAC addresses, but instead uses a logical or IP address. • No longer common because of DHCP.

14

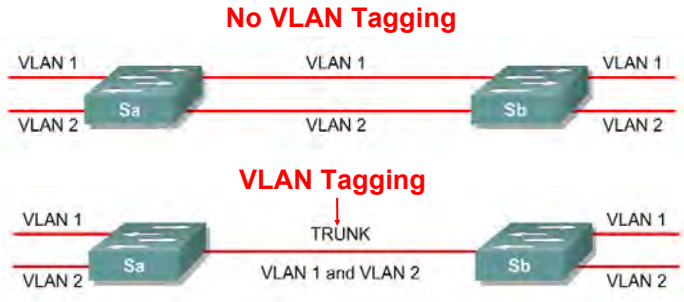
VLAN Tagging



- **VLAN Tagging is used when a link needs to carry traffic for more than one VLAN.**
  - **Trunk link:** As packets are received by the switch from any attached end-station device, a unique packet identifier is added within each header.
- **This header information designates the VLAN membership of each packet.**
- The packet is then forwarded to the appropriate switches or routers based on the VLAN identifier and MAC address.
- Upon reaching the destination node (Switch) the VLAN ID is removed from the packet by the adjacent switch and forwarded to the attached device.
- Packet tagging provides a mechanism for controlling the flow of broadcasts and applications while not interfering with the network and applications.
- This is known as a trunk link or VLAN trunking.

15

VLAN Tagging



- VLAN Tagging is used when a single link needs to carry traffic for more than one VLAN.

16

VLAN Tagging

Tagging	Method	Media	Description
Inter-Switch Link (ISL)	Fast Ethernet	ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header	Frame is lengthened.
802.IQ	Fast Ethernet	IEEE defined Ethernet VLAN protocol	Header is modified.
802.IQ	FDDI	IEEE defined standard: The 802.10 protocol incorporates a mechanism whereby LAN traffic can carry a VLAN identifier	VLAN ID is the essential piece of required header information.
LAN Emulation (LANE)	ATM	No tagging	Virtual connection implies a VLAN ID.

- There are two major methods of frame tagging, Cisco proprietary **Inter-Switch Link (ISL)** and **IEEE 802.1Q**.
- ISL used to be the most common, but is now being replaced by 802.1Q frame tagging.
- Cisco recommends using 802.1Q.
- VLAN Tagging and Trunking will be discussed in the next slide set 8.

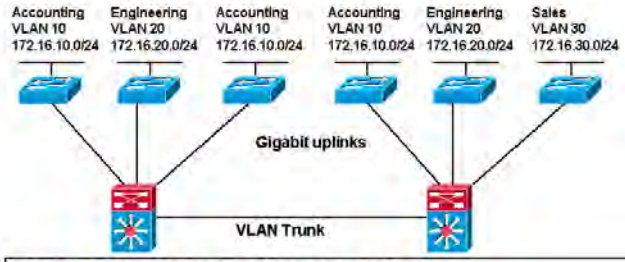
17

Two Types of VLANs

- End-to-End or Campus-wide VLANs
- Geographic or Local VLANs

18

End-to-End or Campus-wide VLANs

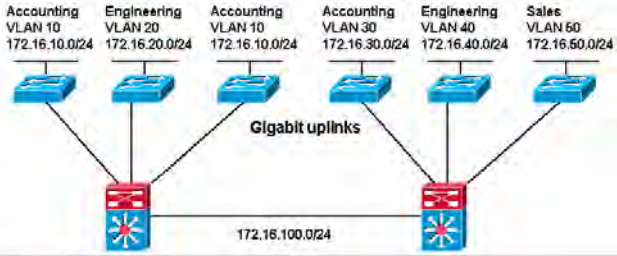


Campus-wide or End-to-End VLAN Model

- VLANs based on functionality
- "VLAN everywhere" model
- VLANs with the same VLAN ID, I.e. Accounting VLAN 10, can be anywhere in the network

19

Geographic or Local VLANs

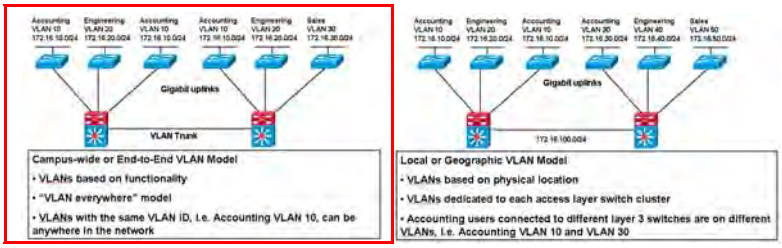


Local or Geographic VLAN Model

- VLANs based on physical location
- VLANs dedicated to each access layer switch cluster
- Accounting users connected to different layer 3 switches are on different VLANs, I.e. Accounting VLAN 10 and VLAN 30

20

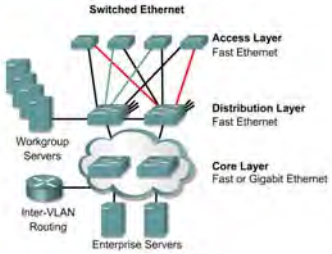
End-to-End or Campus-wide VLANs

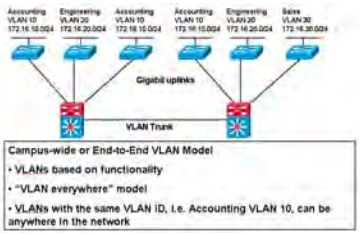


- End-to-End or Campus-wide VLANs
  - Same VLAN/Subnet no matter what the location is on the network
  - Trunking at the Core
  - Usually not recommended by Cisco or other Vendors
  - Adds complexity to network administration
  - Does not resolve Layer 2 Spanning Tree issues

21

End-to-End or Campus-wide VLANs



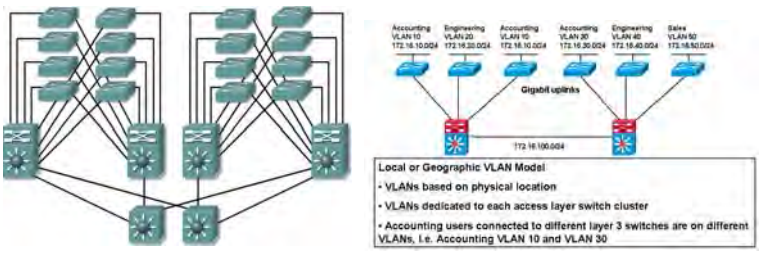


When to use End-to-End?

- Since the core layer router is being used to route between subnets (VLANs), the rule is:
  - **The network is engineered to have 80 percent of the traffic contained within a VLAN.**
  - The remaining 20 percent crosses the router to the enterprise servers and to the Internet and WAN.
  - **Note: This is known as the 80/20 rule. With today's traffic patterns, this rule is becoming obsolete.**

22

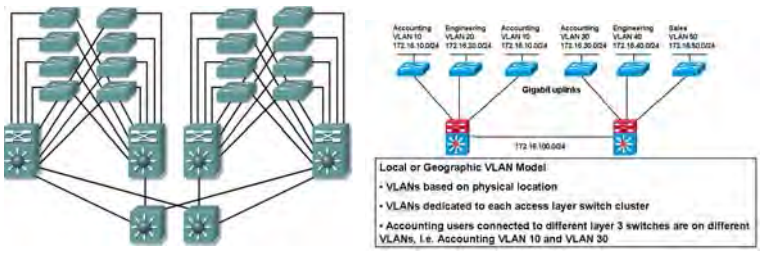
Geographic or Local VLANs



- As many corporate networks have moved to centralize their resources, end-to-end VLANs have become more difficult to maintain.
- Users are required to use many different resources, many of which are no longer in their VLAN.
- Because of this shift in placement and usage of resources, VLANs are now more frequently being created around geographic boundaries rather than commonality boundaries.

23

Geographic or Local VLANs



- This geographic location can be as large as an entire building or as small as a single switch inside a wiring closet.
- **In a VLAN structure, it is typical to find the new 20/80 rule in effect. 80 percent of the traffic is remote to the user and 20 percent of the traffic is local to the user.**
- Although this topology means that the user must cross a Layer 3 device in order to reach 80 percent of the resources, this design allows the network to provide for a deterministic, consistent method of accessing resources.

24

Configuring static VLANs

- The following guidelines must be followed when configuring VLANs on Cisco 29xx switches:
  - The maximum number of VLANs is switch dependent.
    - 29xx switches commonly allow 4,095 VLANs
  - VLAN 1 is one of the factory-default VLANs.
  - VLAN 1 is the default Ethernet VLAN.
  - Cisco Discovery Protocol (CDP) and VLAN Trunking Protocol (VTP) advertisements are sent on VLAN 1.
  - The Catalyst 29xx IP address is in the VLAN 1 broadcast domain by default.
  - "The switch must be in VTP server mode to create, add, or delete VLANs." **(This is not true. Switch could be in VTP Transparent mode. VTP will be discussed in a moment.)**

25

Creating VLANs

- **Assigning access ports (non-trunk ports) to a specific VLAN**

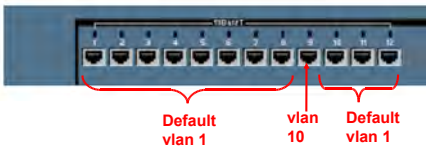
```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan vlan_number
```

- **Create the VLAN:**

```
Switch#vlan database
Switch(vlan)#vlan vlan_number
Switch(vlan)#exit
```

26

Creating VLANs



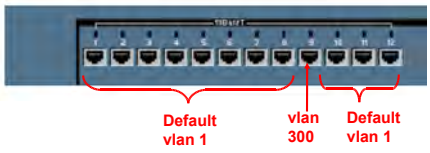
- Assign ports to the VLAN

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan 10
```

- **access** – Denotes this port as an access port and not a trunk link (later)

27

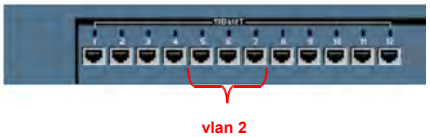
Creating VLANs




```
Cisco
Enter configuration commands, one per line. End with CNTL/Z.

SydneySwitch#config terminal
SydneySwitch(config)#interface fastethernet 0/9
SydneySwitch(config-if)#switchport access vlan 300
SydneySwitch(config-if)#exit
SydneySwitch(config)#exit
```

28

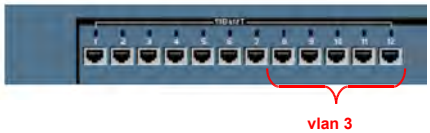
Configuring Ranges of VLANs




```
SydneySwitch(config)#interface fastethernet 0/5
SydneySwitch(config-if)#switchport access vlan 2
SydneySwitch(config-if)#exit
SydneySwitch(config)#interface fastethernet 0/6
SydneySwitch(config-if)#switchport access vlan 2
SydneySwitch(config-if)#exit
SydneySwitch(config)#interface fastethernet 0/7
SydneySwitch(config-if)#switchport access vlan 2
```

29

Configuring Ranges of VLANs

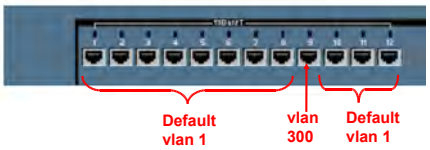



```
SydneySwitch(config)#interface range fastethernet 0/8,
  fastethernet 0/12
SydneySwitch(config-if)#switchport access vlan 3
SydneySwitch(config-if)#exit
```

This command does not work on all 2900 switches, such as the 2900 Series XL. It does work on the 2950.

30

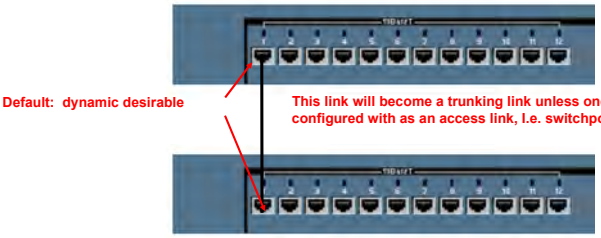
Creating VLANs




```
SydneySwitch(config)#interface fastethernet 0/1
SydneySwitch(config-if)#switchport mode access
SydneySwitch(config-if)#exit
```

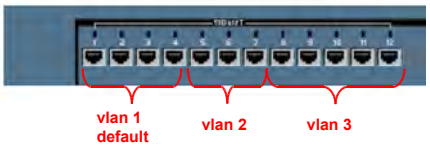
Note: The `switchport mode access` command should be configured on all ports that the network administrator does not want to become a trunk port.

Creating VLANs



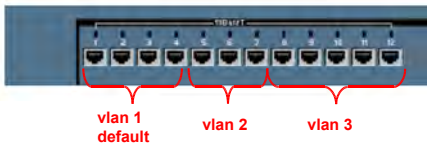
- By default, all ports are configured as **`switchport mode dynamic desirable`**, which means that if the port is connected to another switch with an port configured with the same default mode (or desirable or auto), this link will become a trunking link. (See my article on DTP on my web site for more information.)
- When the `switchport access vlan` command is used, the `switchport mode access` command is not necessary since the `switchport access vlan` command configures the interface as an "access" port (non-trunk port).

Verifying VLANs – show vlan




```
SydneySwitch#show vlan

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------------

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2               active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3               active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                   Fa0/12
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active

VLAN Type SAID MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ---- ---- ---- ------ ------ -------- ---- -------- ------ ------
1    enet 100001 1500  -      -      -        -    -        1002   1003
2    enet 100002 1500  -      -      -        -    -        0      0
```


Verifying VLANs – show vlan brief




```
SydneySwitch#show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2               active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3               active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                   Fa0/12
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active
```


vlan database commands

- Optional Command to add, delete, or modify VLANs.
- VLAN names, numbers, and **VTP** (VLAN Trunking Protocol) information can be entered which "may" affect other switches besides this one. (Discussed in Slide Set 8).
- This does not assign any VLANs to an interface.

```
Switch#vlan database
Switch(vlan)#?
VLAN database editing buffer manipulation commands:
  abort  Exit mode without applying the changes
  apply  Apply current changes and bump revision number
  exit   Apply changes, bump revision number, and exit mode
  no     Negate a command or set its defaults
  reset  Abandon current changes and reread current database
  show   Show database information
  vlan   Add, delete, or modify values associated with a single VLAN
  vtp    Perform VTP administrative functions.
```


Deleting a Port VLAN Membership

```
SydneySwitch#config terminal
SydneySwitch(config)#interface fastethernet 0/9
SydneySwitch(config-if)#switchport access vlan 300
SydneySwitch(config-if)#exit
SydneySwitch(config)#exit
```

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#no switchport access vlan 300
```

`Switch(config-if)#no switchport access vlan` ***`vlan_number`***

Deleting a VLAN

- `Switch#vlan database`
  `Switch(vlan)#No vlan` *`vlan_number`*
  `Switch(vlan)#exit`

VLAN Trunking Protocol

Cisco.com

Slide Set 8

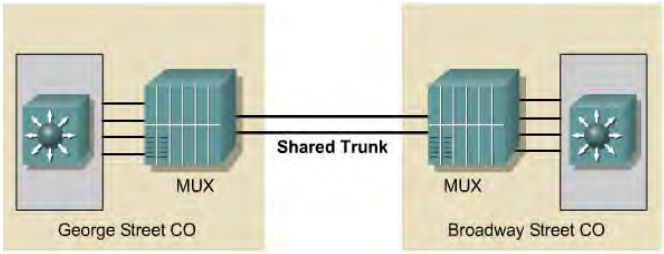
Objectives

Cisco.com

- Trunking
- VTP
- Inter-VLAN routing

History of Trunking

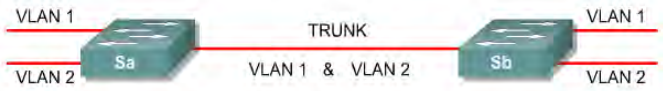
Cisco.com



The telephone industry used multiplexers to carry multiple voice signals on a single trunk between COs.

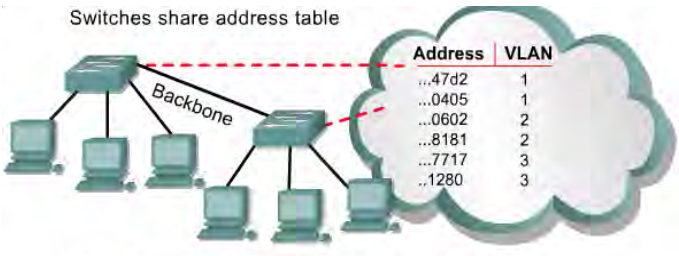
Trunking Concepts

Cisco.com



Frame Filtering

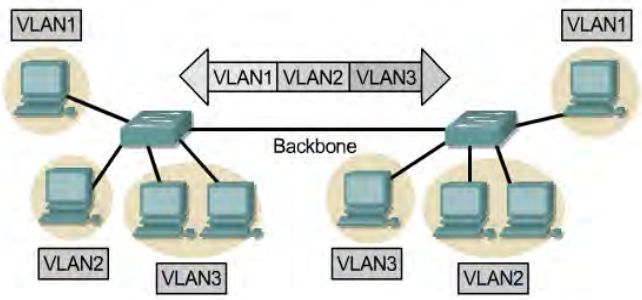
Cisco.com



A filtering table is developed for each switch. Switches share address table information. Table entries are compared with the frames. Switch takes appropriate action

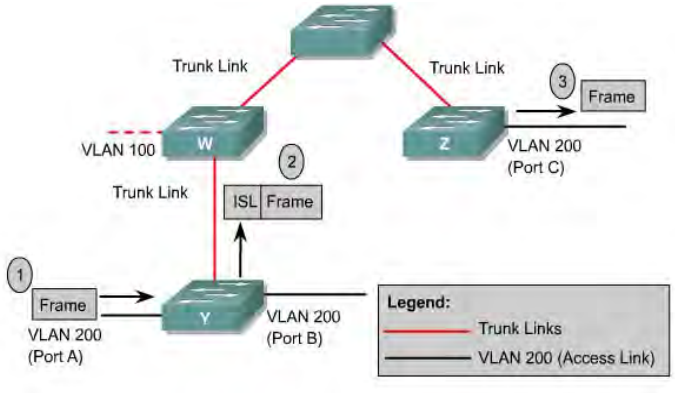
Frame Tagging

Cisco.com



Inter-Switch Link Protocol

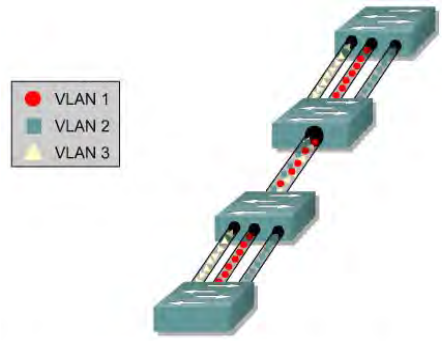
Cisco.com



7

VLANs and Trunking

Cisco.com



Trunking provides effective communication between switches in a network.

8

Frame Tagging and Encapsulation Methods

Cisco.com

Identification Method	Encapsulation	Tagging (insertion into frame)	Media
802.1Q	No	Yes	Ethernet
ISL	Yes	No	Ethernet
802.10	No	No	FDDI
LANE	No	No	ATM

9

VTP Benefits

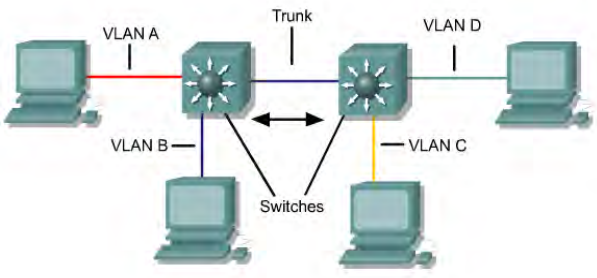
Cisco.com

- VLAN configuration consistency across the network
- VLANs are trunked over mixed media. For example, an Ethernet VLAN is mapped to high-speed ATM LANE or FDDI VLAN
- Accurate tracking and monitoring of VLANs
- Dynamic reporting of added VLANs across the network
- "Plug-and-play" configuration when adding new VLANs

10

VTP Concepts

Cisco.com



The role of VTP is to maintain VLAN configuration consistency across a common network administration domain.

11

VTP Modes

Cisco.com

- **Server**
- **Client**
- **Transparent**

12

VTP Mode Comparison

Cisco.com

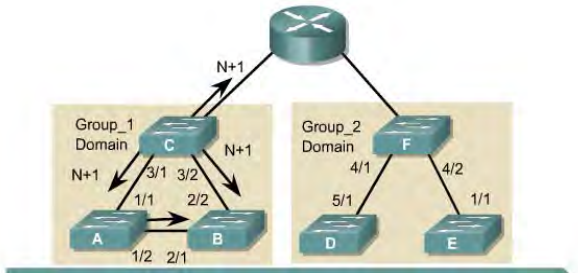
Feature	Server	Client	Transparent
Source VTP Messages	Yes	Yes	No
Listen to VTP Messages	Yes	Yes	No
Create VLANs	Yes	No	Yes*
Remember VLANs	Yes	No	Yes*

*Locally Significant only

13

VTP Operation

Cisco.com



Group_1 Config Rev# N+1	
1	default
2	first-vtp-vlan
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1003	trnet-default

14

VTP Implementation

Cisco.com

- There are two types of VTP advertisements:
  - Requests from clients that want information at bootup
  - Responses from servers
- There are three types of VTP messages:
  - Advertisement requests
  - Summary advertisements
  - Subset advertisements

15

VTP Basic Configuration Steps

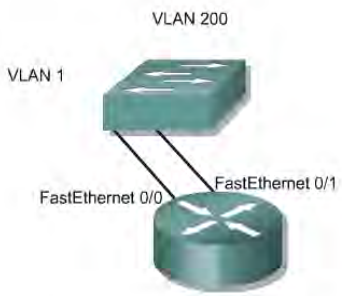
Cisco.com

1. Determine the version number
2. Choose the domain
3. Choose the VTP mode
4. Password protect the domain

16

Inter-VLAN Routing

Cisco.com



To route traffic between VLAN 1 and VLAN 200 in a non-VLAN-trunk environment, a router must be connected to a port in VLAN1 and a port in VLAN 200.

17

Inter-VLAN Issues and Solutions

Cisco.com

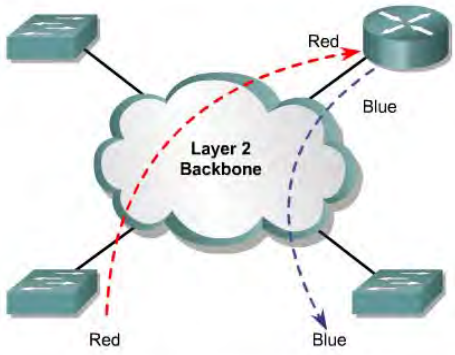
Two of the most common issues that arise in a multiple-VLAN environment are as follows:

- The need for end-user devices to reach non-local hosts
- The need for hosts on different VLANs to communicate

18

Router on a Stick

Cisco.com

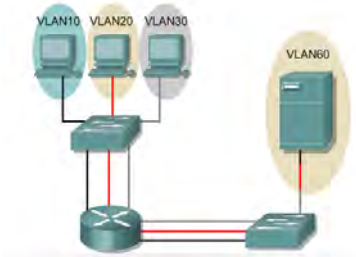


In order for traffic to move from one VLAN to another, it must go through the router.

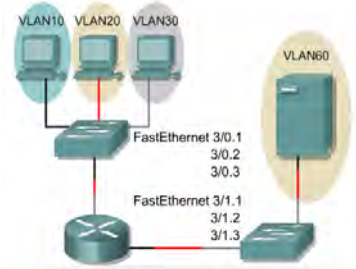
19

Physical and Logical Interfaces

Cisco.com



The router supports one VLAN per interface.

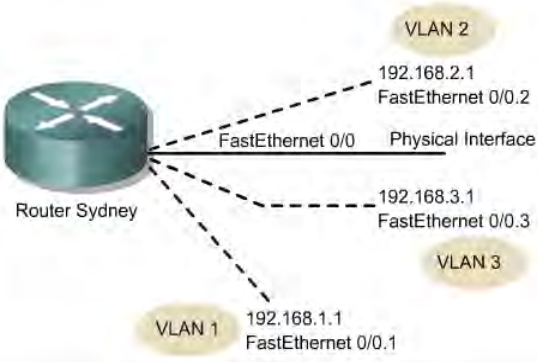


A single ISL link can support multiple VLANs.

20

Dividing Physical Interfaces into Subinterfaces

Cisco.com



Each VLAN is its own IP network or subnet.

21

Configuring Inter-VLAN Routing

Cisco.com

```
Sydney(config)#interface FastEthernet 0/0.1
Sydney(config-subif)#description Management VLAN1
Sydney(config-subif)#encapsulation 802.1q 1
Sydney(config-subif)#ip address 192.168.1.1
255.255.255.0
oSydney(config)#interface FastEthernet 0/0.2
Sydney(config-subif)#description Accounting VLAN 20
Sydney(config-subif)#encapsulation 802.1q 20
Sydney(config-subif)#ip address 192.168.2.1
255.255.255.0
Sydney(config)#interface FastEthernet 0/0.3
Sydney(config-subif)#description Sales VLAN 30
Sydney(config-subif)#encapsulation 802.1q 30
Sydney(config-subif)#ip address 192.168.3.1
255.255.255.0
```

22

Spanning Tree Protocol

Slide Set 8.5

1

Overview

- Define redundancy and its importance in networking
- Describe the key elements of a redundant networking topology
- Define broadcast storms and describe their impact on switched networks
- Define multiple frame transmissions and describe their impact on switched networks
- Identify causes and results of MAC address database instability
- Identify the benefits and risks of a redundant topology
- Describe the role of spanning tree in a redundant-path switched network
- Identify the key elements of spanning tree operation
- Describe the process for root bridge election
- List the spanning-tree states in order
- Compare Spanning-Tree Protocol and Rapid Spanning-Tree Protocol

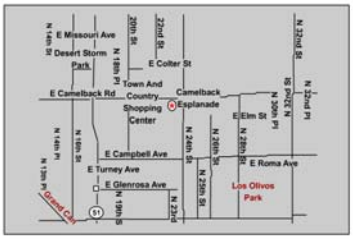
2

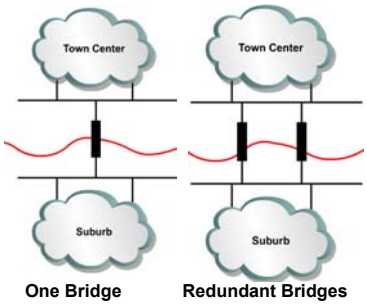
Redundancy

- Achieving such a goal requires extremely reliable networks.
- Reliability in networks is achieved by reliable equipment and by designing networks that are tolerant to failures and faults.
- The network is designed to reconverge rapidly so that the fault is bypassed.
- Fault tolerance is achieved by redundancy.
- Redundancy means to be in excess or exceeding what is usual and natural.

3

Redundant topologies



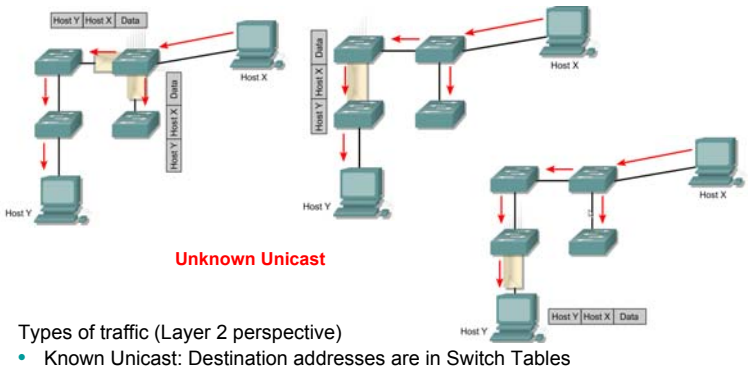


One Bridge **Redundant Bridges**

- A network of roads is a global example of a redundant topology.
- If one road is closed for repair there is likely an alternate route to the destination

4

Types of Traffic

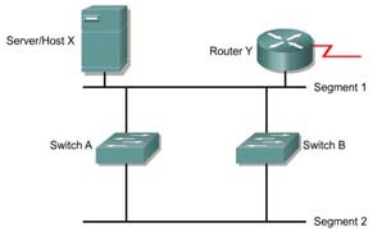


Types of traffic (Layer 2 perspective)

- Known Unicast: Destination addresses are in Switch Tables
- Unknown Unicast: Destination addresses are <u>not</u> in Switch Tables
- Multicast: Traffic sent to a group of addresses
- Broadcast: Traffic forwarded out all interfaces except incoming interface.

5

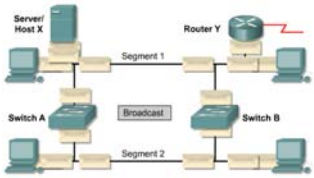
Redundant switched topologies



- Switches learn the MAC addresses of devices on their ports so that data can be properly forwarded to the destination.
- Switches will flood frames for unknown destinations until they learn the MAC addresses of the devices.
- Broadcasts and multicasts are also flooded. (Unless switch is doing Multicast Snooping or IGMP)
- A redundant switched topology ***may*** (STP disabled) cause broadcast storms, multiple frame copies, and MAC address table instability problems.

6

Broadcast Storm

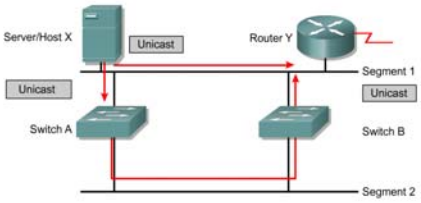


A state in which a message that has been broadcast across a networkresults in even more responses, and each response results in still more responses in a snowball effect. www.webopedia.com

- Broadcasts and multicasts can cause problems in a switched network.
- If Host X sends a broadcast, like an ARP request for the Layer 2 address of the router, then Switch A will forward the broadcast out all ports.
- Switch B, being on the same segment, also forwards all broadcasts.
- Switch B sees all the broadcasts that Switch A forwarded and Switch A sees all the broadcasts that Switch B forwarded.
- Switch A sees the broadcasts and forwards them.
- Switch B sees the broadcasts and forwards them.
- The switches continue to propagate broadcast traffic over and over.
- This is called a broadcast storm.

7

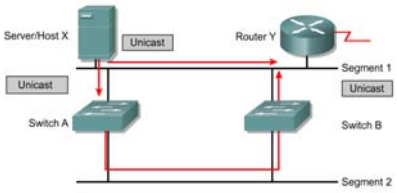
Multiple frame transmissions



- In a redundant switched network it is possible for an end device to receive multiple frames.
- Assume that the MAC address of Router Y has been timed out by both switches.
- Also assume that Host X still has the MAC address of Router Y in its ARP cache and sends a unicast frame to Router Y.

8

Multiple frame transmissions

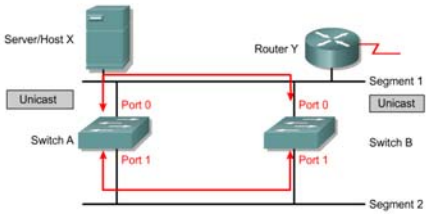


(Some changes to curriculum)

- The router receives the frame because it is on the same segment as Host X.
- Switch A does not have the MAC address of the Router Y and will therefore flood the frame out its ports. (Segment 2)
- Switch B also does not know which port Router Y is on.
- Note: Switch B will forward the the unicast onto Segment 2, creating multiple frames on that segment.
- After Switch B receives the frame from Switch A , it then floods the frame it received causing Router Y to receive multiple copies of the same frame.
- This is a causes of unnecessary processing in all devices.

9

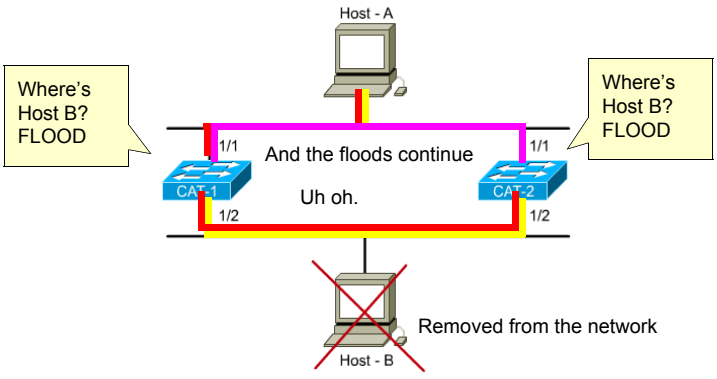
Media access control database instability



- In a redundant switched network it is possible for switches to learn the wrong information.
- A switch can incorrectly learn that a MAC address is on one port, when it is actually on a different port.
- Host X sends a frame directed to Router Y.
- Switches A and B learn the MAC address of Host X on port 0.
- The frame to Router Y is flooded on port 1 of both switches.
- Switches A and B see this information on port 1 and incorrectly learn the MAC address of Host X on port 1.

10

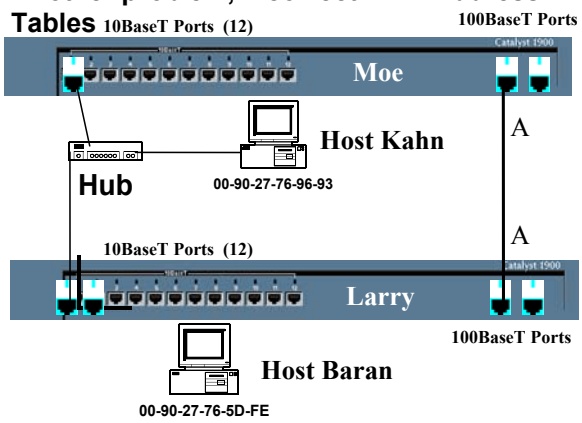
Layer 2 Loops - Flooded unicast frames



11

Redundant Paths and No Spanning Tree

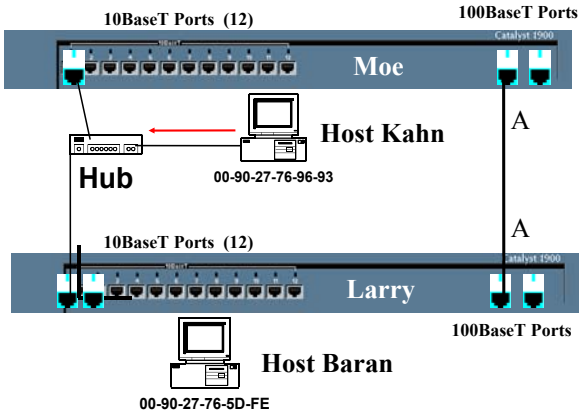
Another problem, incorrect MAC Address Tables



12

Redundant Paths and No Spanning Tree

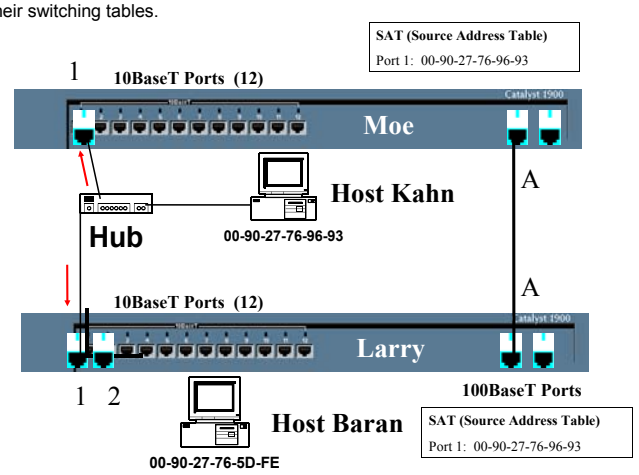
Host Kahn sends an Ethernet frame to Host Baran. Both Switch Moe and Switch Larry see the frame and record Host Kahn's Mac Address in their switching tables.



13

Redundant Paths and No Spanning Tree

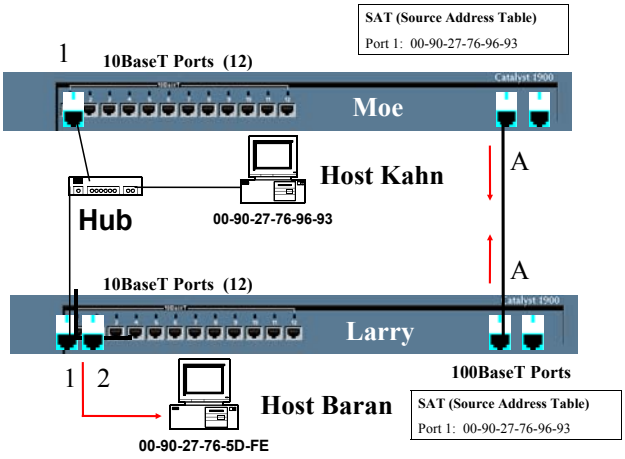
Both Switch Moe and Switch Larry see the frame and record Host Kahn's Mac Address in their switching tables.



14

Redundant Paths and No Spanning Tree

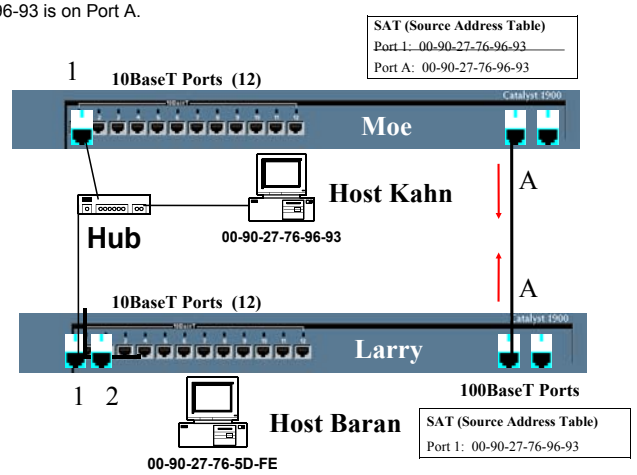
Both Switches do not have the **destination MAC address** in their table so they **both flood** it out all ports. Host Baran receives the frame.)



15

Redundant Paths and No Spanning Tree

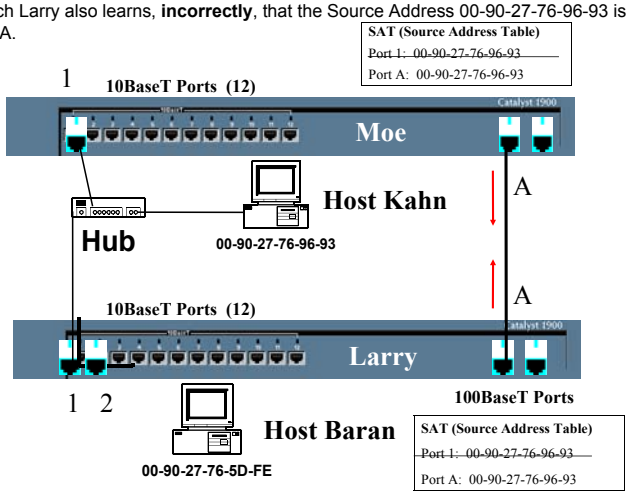
Switch Moe now learns, **incorrectly**, that the Source Address 00-90-27-76-96-93 is on Port A.



16

Redundant Paths and No Spanning Tree

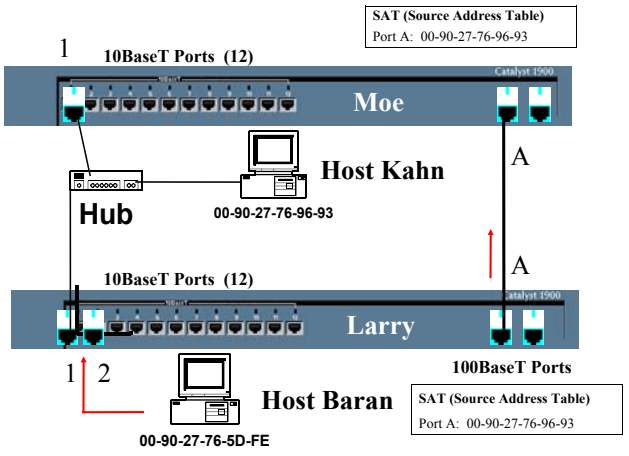
Switch Larry also learns, **incorrectly**, that the Source Address 00-90-27-76-96-93 is on Port A.



17

Redundant Paths and No Spanning Tree

Now, when Host Baran sends a frame to Host Kahn, it will be sent the longer way, through Switch Larry's port A.



18

Redundant Paths and No Spanning Tree

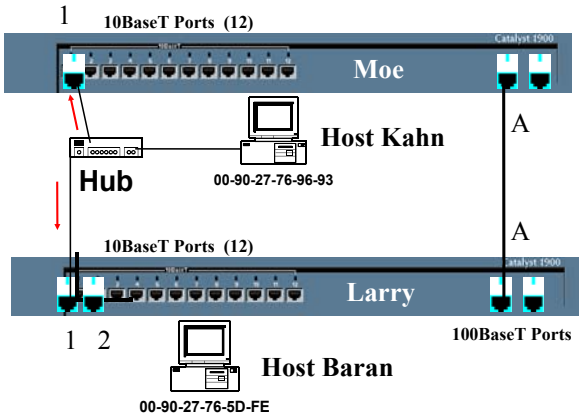
- Then, the same confusion happens, but this time with Host Baran.
- Okay, maybe not the end of the world.
- Frames will just take a longer path and you may also see other “unexpected results.”

- But what about broadcast frames, like ARP Requests?

19

Broadcasts and No Spanning Tree

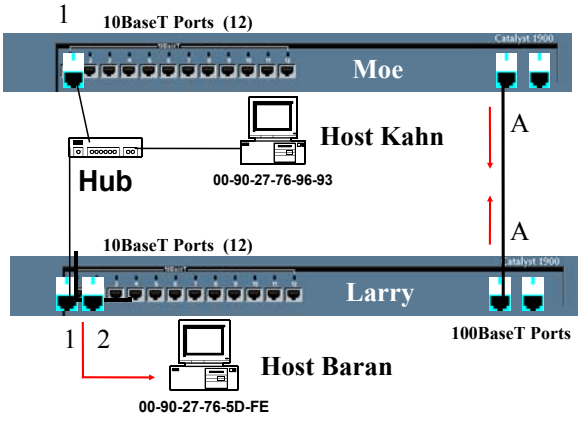
Lets, leave the switching tables alone and just look at what happens with the frames. Host Kahn sends out a layer 2 broadcast frame, like an ARP Request.



20

Broadcasts and No Spanning Tree

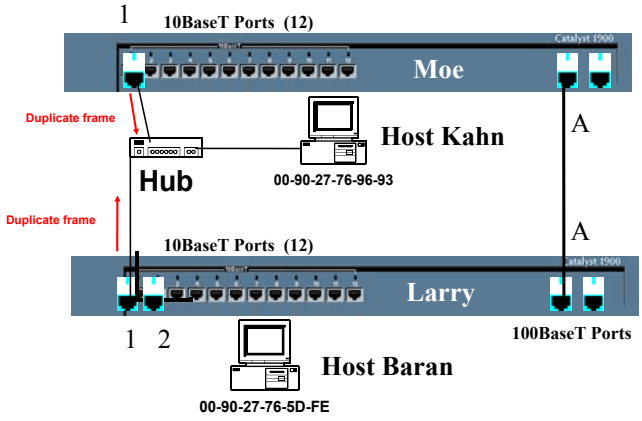
Because it is a layer 2 broadcast frame, both switches, Moe and Larry, **flood the frame out all ports**, including their port A’s.



21

Broadcasts and No Spanning Tree

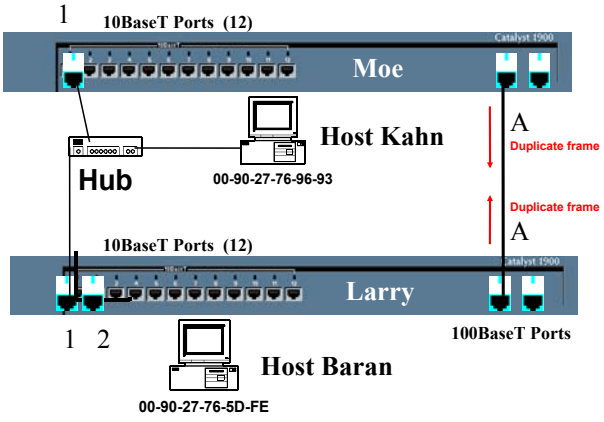
Both switches receive the same broadcast, but on a different port. Doing what switches do, **both switches flood the duplicate broadcast frame** out their other ports.



22

Broadcasts and No Spanning Tree

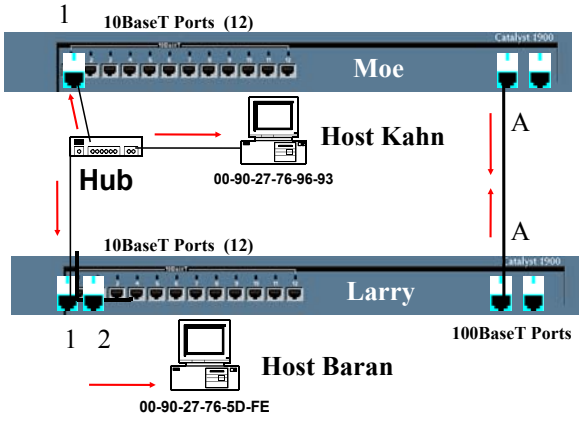
Here we go again, with the switches flooding the same broadcast again out its other ports. This results in duplicate frames, known as a ***broadcast storm***!



23

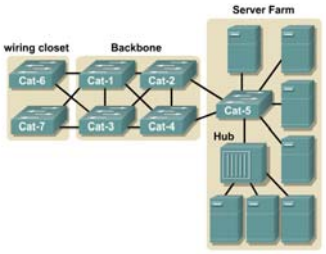
Broadcasts and No Spanning Tree

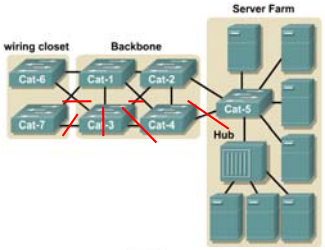
Remember, that layer 2 broadcasts not only take up network bandwidth, but must be processed by each host. This can severely impact a network, to the point of making it unusable.



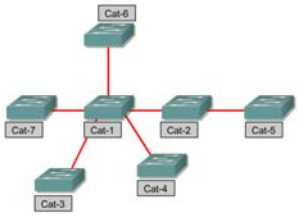
24

Redundant topology and spanning tree



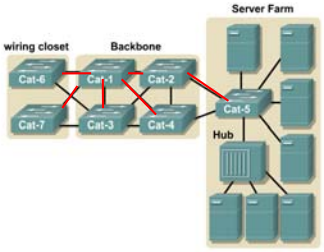


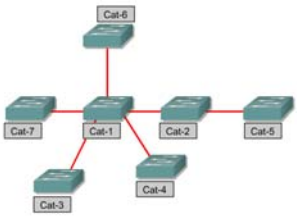
- Unlike IP, in the Layer 2 header there is no Time To Live (TTL).
- The solution is to allow physical loops, but create a loop free logical topology.
- The loop free logical topology created is called a tree.
- This topology is a star or extended star logical topology, the spanning tree of the network.



25

Redundant topology and spanning tree



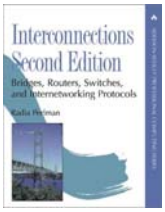


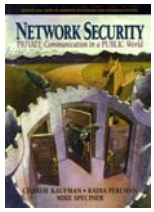
- It is a spanning tree because all devices in the network are reachable or spanned.
- The algorithm used to create this loop free logical topology is the **spanning-tree algorithm**.
- This algorithm can take a relatively long time to converge.
- A new algorithm called the **rapid spanning-tree algorithm** is being introduced to reduce the time for a network to compute a loop free logical topology. (later)

26

Spanning-Tree Protocol (STP)

Radia Perlman, networking hero!



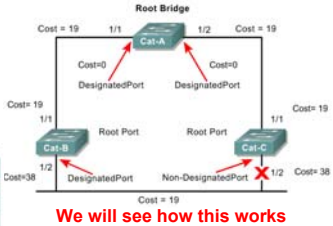


- Ethernet bridges and switches can implement the **IEEE 802.1D Spanning-Tree Protocol** and use the spanning-tree algorithm to **construct a loop free shortest path network**.
- Radia Perlman "is the inventor of the spanning tree algorithm used by bridges (switches), and the mechanisms that make link state routing protocols such as IS-IS (which she designed) and OSPF (which adopted many of the ideas) stable and efficient. Her thesis on sabotage-proof networks is well-known in the security community." http://www.equipecom.com/radia.html

27

Spanning-Tree Protocol (STP)

Link Speed	Cost(Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

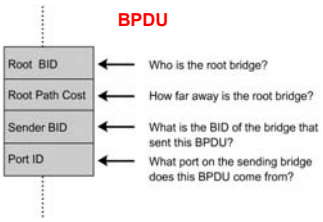


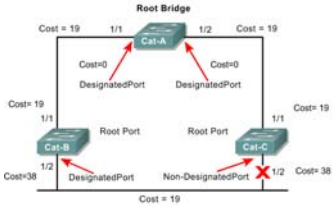
We will see how this works in a moment.

- Shortest path is based on cumulative link costs.
- Link costs are based on the speed of the link.
- The Spanning-Tree Protocol establishes a root node, called the root bridge.
- The Spanning-Tree Protocol constructs a topology that has one path for reaching every network node.
- The resulting tree originates from the **root bridge**.
- **Redundant links** that are not part of the shortest path tree are **blocked**.

28

Spanning-Tree Protocol (STP)

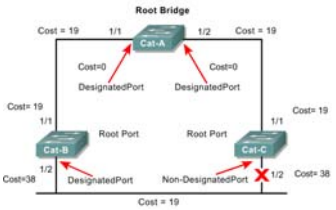




- It is because certain paths are blocked that a loop free topology is possible.
- Data frames received on blocked links are dropped.
- The Spanning-Tree Protocol requires network devices to exchange messages to detect bridging loops.
- Links that will cause a loop are put into a blocking state.
- topology, is called a **Bridge Protocol Data Unit (BPDU).**
- BPDUs continue to be received on blocked ports.
- This ensures that if an active path or device fails, a new spanning tree can be calculated.

29

Spanning-Tree Protocol (STP)



BPDUs contain enough information so that all switches can do the following:

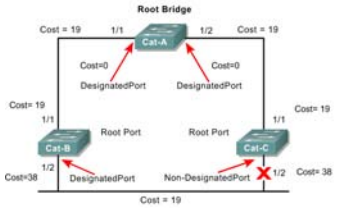
- Select a **single switch that will act as the root** of the spanning tree
- Calculate the **shortest path from itself to the root switch**
- **Designate one of the switches as the closest one to the root**, for each LAN segment. This bridge is called the "**designated switch**".
  - The designated switch handles all communication from that LAN towards the root bridge.
- Choose one of its ports as its root port, for each non-root switch.
  - This is the interface that gives the best path to the root switch.
- Select ports that are part of the spanning tree, the designated ports. Non-designated ports are blocked.

30

Let's see how this is done!

Some of this is extra information or information explained that is not explained fully in the curriculum.

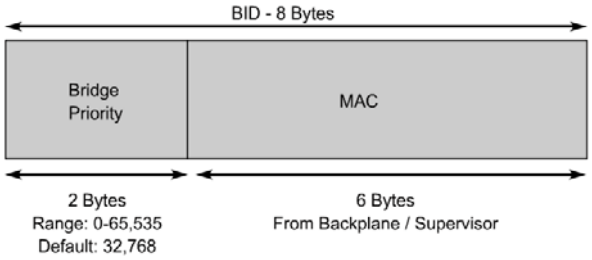
Two Key Concepts: BID and Path Cost



- STP executes an algorithm called Spanning Tree Algorithm (STA).
- STA chooses a reference point, called a root bridge, and then determines the available paths to that reference point.
  - If more than two paths exists, STA picks the best path and blocks the rest
- STP calculations make extensive use of two key concepts in creating a loop-free topology:
  - **Bridge ID**
  - **Path Cost**

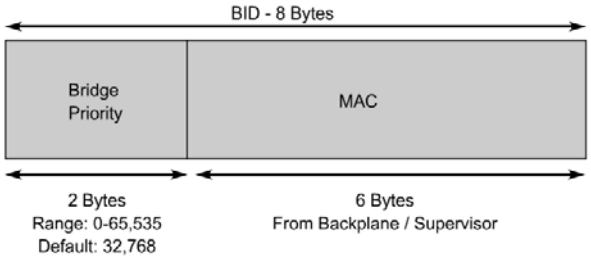
Rick Graziani graziani@cabrillo.edu

Bridge ID (BID)



- **Bridge ID (BID)** is used to identify each bridge/switch.
- The BID is used in determining the center of the network, in respect to STP, known as the root bridge.
- Consists of two components:
  - **A 2-byte Bridge Priority**: Cisco switch defaults to **32,768** or 0x8000.
  - **A 6-byte MAC address**

Bridge ID (BID)



- **Bridge Priority** is usually expressed in **decimal format** and the **MAC address** in the BID is usually expressed in **hexadecimal format**.
- BID is used to elect a root bridge (coming)
- **Lowest Bridge ID is the root.**
- If all devices have the same priority, the bridge with the lowest MAC address becomes the root bridge. (Yikes!)

Path Cost

Link Speed	Cost(Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

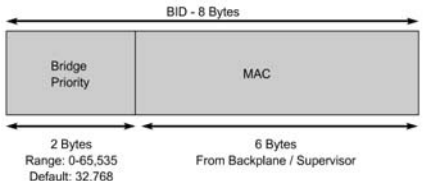
- Bridges use the concept of cost to evaluate how close they are to other bridges.
- This will be used in the STP development of a loop-free topology .
- **Originally, 802.1d** defined cost as 1000/bandwidth of the link in Mbps.
  - Cost of 10Mbps link = 100 or 1000/10
  - Cost of 100Mbps link = 10 or 1000/100
  - Cost of 1Gbps link = 1 or 1000/1000
- Running out of room for faster switches including 10 Gbps Ethernet.

Path Cost

Link Speed	Cost(Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

- IEEE modified the most to use a non-linear scale with the new values of:
  - 4 Mbps 250 (cost)
  - 10 Mbps 100 (cost)
  - 16 Mbps 62 (cost)
  - 45 Mbps 39 (cost)
  - 100 Mbps 19 (cost)
  - 155 Mbps 14 (cost)
  - 622 Mbps 6 (cost)
  - 1 Gbps 4 (cost)
  - 10 Gbps 2 (cost)

Path Cost



Link Speed	Cost(Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

- You can modify the path cost by modifying the cost of a port.
  - Exercise caution when you do this!
- BID and Path Cost are used to develop a loop-free topology .
- Coming very soon!
- But first the **Four-Step STP Decision Sequence**

Four-Step STP Decision Sequence

- When creating a loop-free topology, STP always uses the same four-step decision sequence:

Four-Step decision Sequence

Step 1 - Lowest BID
Step 2 - Lowest Path Cost to Root Bridge
Step 3 - Lowest Sender BID
Step 4 - Lowest Port ID

- Bridges use Configuration BPDUs during this four-step process.
  - There is another type of BPDU known as Topology Change Notification (TCN) BPDU.

Four-Step STP Decision Sequence

BPDU key concepts:

- Bridges save a copy of only the best BPDU seen on every port.
- When making this evaluation, it considers all of the BPDUs received on the port, as well as the BPDU that would be sent on that port.
- As every BPDU arrives, it is checked against this four-step sequence to see if it is more attractive (lower in value) than the existing BPDU saved for that port.
- Only the lowest value BPDU is saved.
- Bridges send configuration BPDUs until a more attractive BPDU is received.
- Okay, lets see how this is used...

Four-Step STP Decision Sequence

BPDU key concepts:

- Bridges save a copy of only the best BPDU seen on every port.
- When making this evaluation, it considers all of the BPDUs received on the port, as well as the BPDU that would be sent on that port.
- As every BPDU arrives, it is checked against this four-step sequence to see if it is more attractive (lower in value) than the existing BPDU saved for that port.
- Only the lowest value BPDU is saved.
- Bridges send configuration BPDUs until a more attractive BPDU is received.
- Okay, lets see how this is used...

Three Steps of Initial STP Convergence

- The STP algorithm uses three simple steps to converge on a loop-free topology.
- Switches go through three steps for their initial convergence:

STP Convergence
Step 1 Elect one Root Bridge
Step 2 Elect Root Ports
Step 3 Elect Designated Ports

- All STP decisions are based on a the following predetermined sequence:

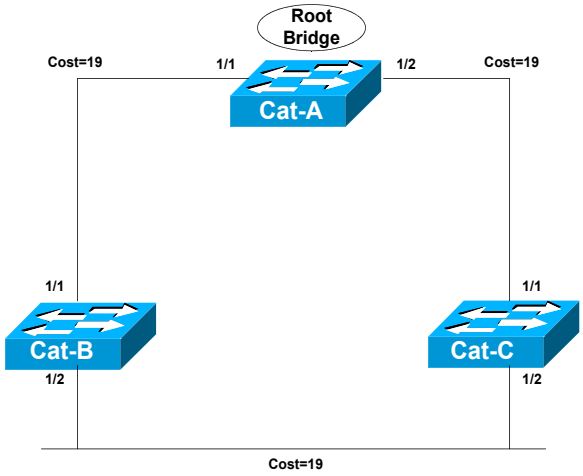
Four-Step decision Sequence
Step 1 - Lowest BID
Step 2 - Lowest Path Cost to Root Bridge
Step 3 - Lowest Sender BID
Step 4 - Lowest Port ID

Three Steps of Initial STP Convergence

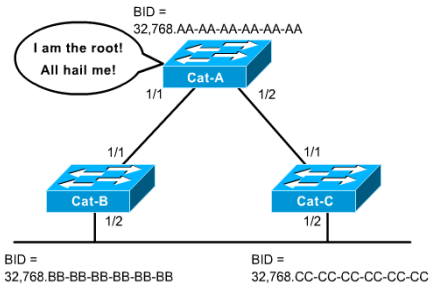
STP Convergence

Step 1 Elect one Root Bridge
Step 2 Elect Root Ports
Step 3 Elect Designated Ports

Step 1 Elect one Root Bridge



Step 1 Elect one Root Bridge



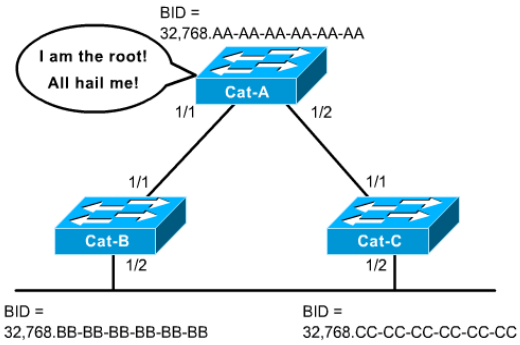
- When the network first starts, all bridges are announcing a chaotic mix of BPDUs.
- All bridges immediately begin applying the four-step sequence decision process.
- Switches need to elect a single Root Bridge.
- Switch with the **lowest BID** wins!

Note: Many texts refer to the term “highest priority” which is the “lowest” BID value.

- This is known as the “Root War.”

Step 1 Elect one Root Bridge

Cat-A has the lowest Bridge MAC Address, so it wins the Root War!



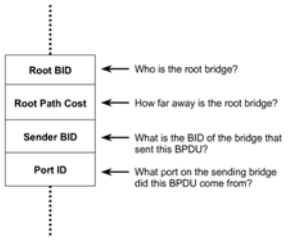
All 3 switches have the same default Bridge Priority value of 32,768

Step 1 Elect one Root Bridge

BPDU

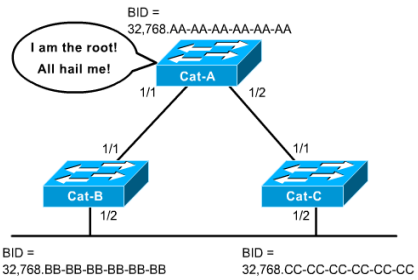
Its all done with BPDUs!

```
802.3 Header
  Destination:    01:80:C2:00:00:00  Mcast 802.1d Bridge group
  Source:         00:D0:C0:F5:18:D1
  LLC Length:     38
802.2 Logical Link Control (LLC) Header
  Dest. SAP:      0x42  802.1 Bridge Spanning Tree
  Source SAP:     0x42  802.1 Bridge Spanning Tree
  Command:        0x03  Unnumbered Information
802.1 - Bridge Spanning Tree
  Protocol Identifier:  0
  Protocol Version ID:  0
  Message Type:         0  Configuration Message
  Flags:                %00000000
  Root Priority/ID:     0x8000/ 00:D0:C0:F5:18:C0
  Cost Of Path To Root: 0x00000000  (0)
  Bridge Priority/ID:   0x8000/ 00:D0:C0:F5:18:C0
  Port Priority/ID:     0x80/ 0x1D
  Message Age:          0/256 seconds (exactly 0  seconds)
  Maximum Age:          5120/256 seconds (exactly 20  seconds)
  Hello Time:           512/256 seconds (exactly 2  seconds)
  Forward Delay:        3840/256 seconds (exactly 15  seconds)
```



Configuration BPDUs are sent every 2 seconds by default.

Step 1 Elect one Root Bridge



- At the beginning, all bridges assume they are the center of the universe and declare themselves as the Root Bridge, by placing its own BID in the Root BID field of the BPDU.
- Once all of the switches see that Cat-A has the lowest BID, they are all in agreement that Cat-A is the Root Bridge.

Three Steps of Initial STP Convergence

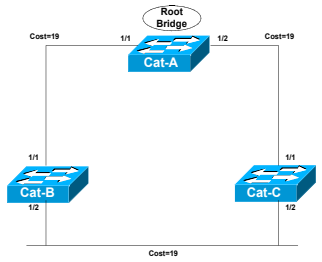
STP Convergence

Step 1 Elect one Root Bridge

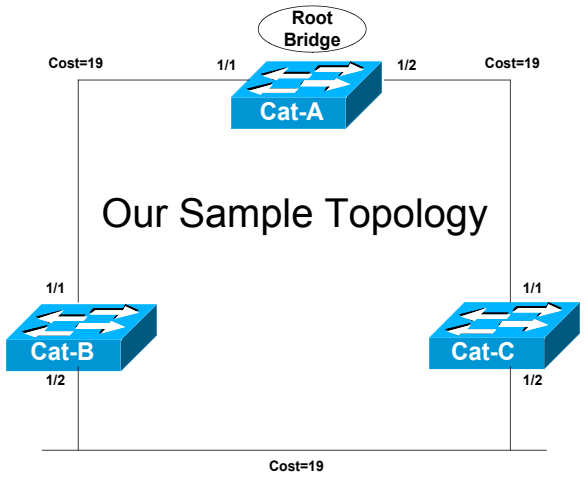
Step 2 Elect Root Ports

Step 3 Elect Designated Ports

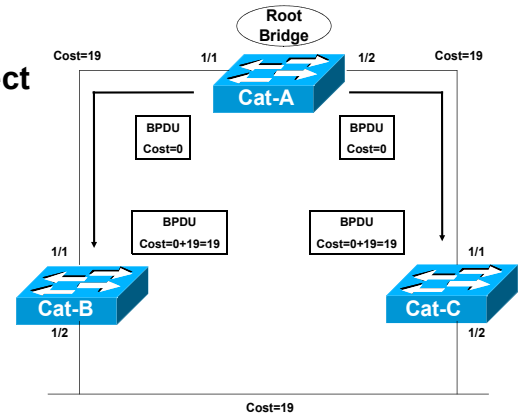
Step 2 Elect Root Ports



- Now that the Root War has been won, switches move on to selecting **Root Ports**.
- A bridge's **Root Port** is the ***port closest to the Root Bridge***.
- Bridges use the **cost** to determine closeness.
- **Every non-Root Bridge will select one Root Port!**
- Specifically, bridges track the **Root Path Cost**, the cumulative cost of all links to the Root Bridge.



Step 2 Elect Root Ports



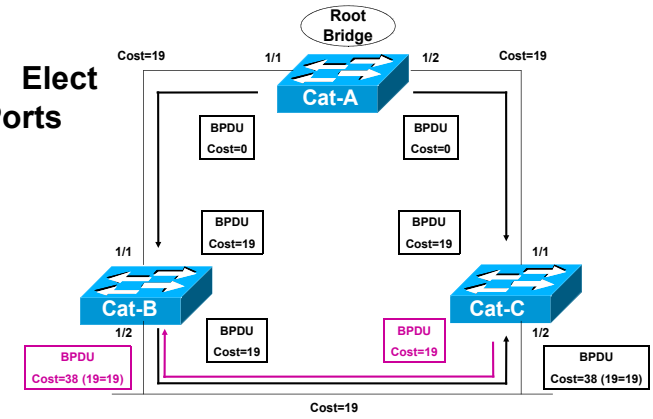
Step 1

- Cat-A sends out BPDUs, containing a Root Path Cost of 0.
- Cat-B receives these BPDUs and adds the Path Cost of Port 1/1 to the Root Path Cost contained in the BPDU.

Step 2

- Cat-B adds Root Path Cost 0 PLUS its Port 1/1 cost of 19 = 19

Step 2 Elect Root Ports



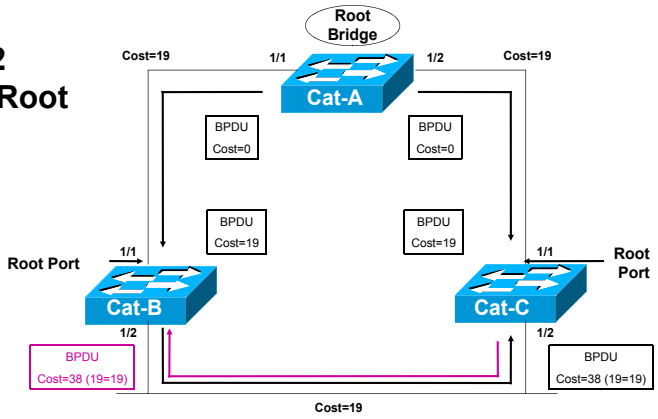
Step 3

- Cat-B uses this value of 19 internally and sends BPDUs with a Root Path Cost of 19 out Port 1/2.

Step 4

- Cat-C receives the BPDU from Cat-B, and increased the Root Path Cost to 38 (19+19). (Same with Cat-C sending to Cat-B.)

Step 2 Elect Root Ports



Step 5

- Cat-B calculates that it can reach the Root Bridge at a cost of 19 via Port 1/1 as opposed to a cost of 38 via Port 1/2.
- Port 1/1 becomes the Root Port for Cat-B, the port closest to the Root Bridge.
- Cat-C goes through a similar calculation. Note: Both Cat-B:1/2 and Cat-C:1/2 save the best BPDU of 19 (its own).

Three Steps of Initial STP Convergence

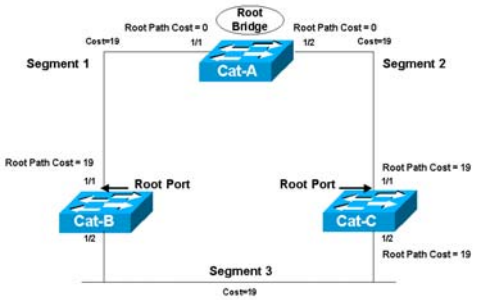
STP Convergence

Step 1 Elect one Root Bridge

Step 2 Elect Root Ports

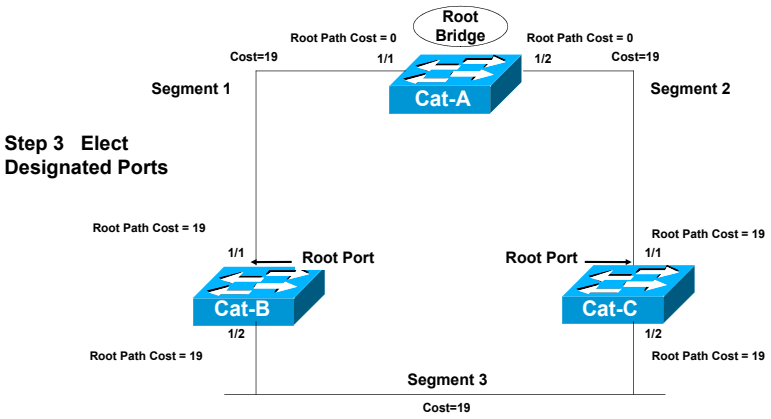
Step 3 Elect Designated Ports

Step 3 Elect Designated Ports



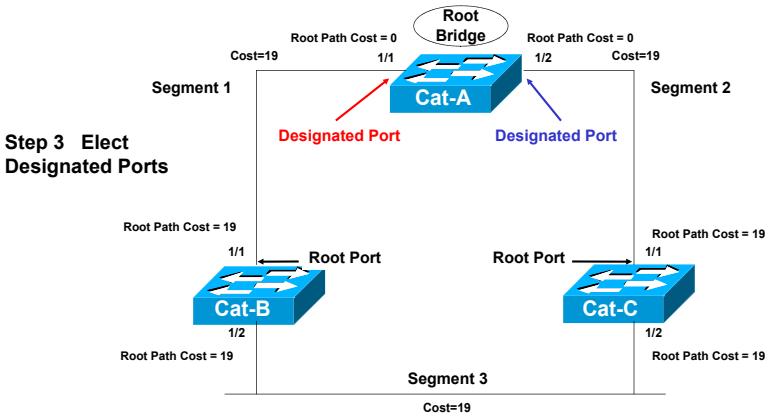
- The loop prevention part of STP becomes evident during this step, electing designated ports.
- A **Designated Port** functions as ***the single bridge port that both sends and receives traffic to and from that segment and the Root Bridge.***
- **Each segment in a bridged network has one Designated Port, chosen based on cumulative Root Path Cost to the Root Bridge.**
- The switch containing the Designated Port is referred to as the **Designated Bridge** for that segment.
- To locate Designated Ports, lets take a look at each segment.
- **Root Path Cost**, the cumulative cost of all links to the Root Bridge.

55



- **Segment 1**: Cat-A:1/1 has a Root Path Cost = 0 (after all it has the Root Bridge) and Cat-B:1/1 has a Root Path Cost = 19.
- **Segment 2**: Cat-A:1/2 has a Root Path Cost = 0 (after all it has the Root Bridge) and Cat-C:1/1 has a Root Path Cost = 19.
- **Segment 3**: **Cat-B:1/2** has a **Root Path Cost = 19** and **Cat-C:1/2** has a **Root Path Cost = 19**. ***It's a tie!***

56



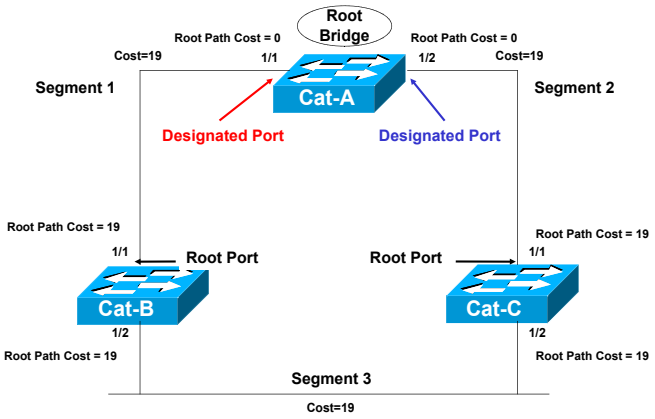
Segment 1

- Because Cat-A:1/1 has the lower Root Path Cost it becomes the **Designate Port for Segment 1**.

Segment 2

- Because Cat-A:1/2 has the lower Root Path Cost it becomes the **Designate Port for Segment 2**.

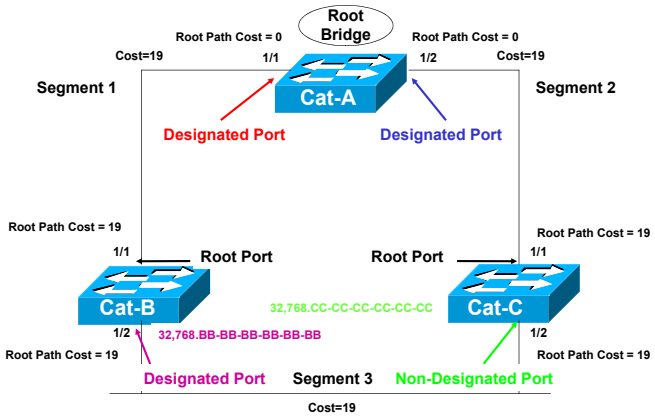
57



Segment 3

- **Both Cat-B and Cat-C** have a **Root Path Cost of 19**, a tie!
- When faced with a tie (or any other determination) STP always uses the four-step decision process:
  1. Lowest Root BID; 2. Lowest Path Cost to Root Bridge;
  3. Lowest Sender BID; 4. Lowest Port ID

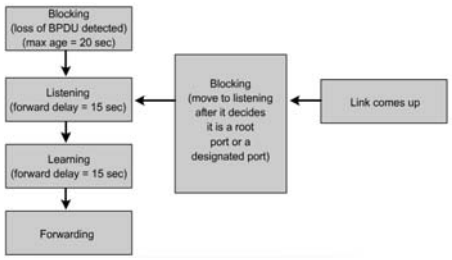
58



Segment 3 (continued)

- 1) All three switches agree that Cat-A is the Root Bridge, so this is a tie.
- 2) Root Path Cost for both is 19, also a tie.
- 3) The sender's BID is lower on Cat-B, than Cat-C, so Cat-B:1/2 becomes the **Designated Port for Segment 3**.
- Cat-C:1/2 therefore becomes the **non-Designated Port for Segment 3**.

Stages of spanning-tree port states



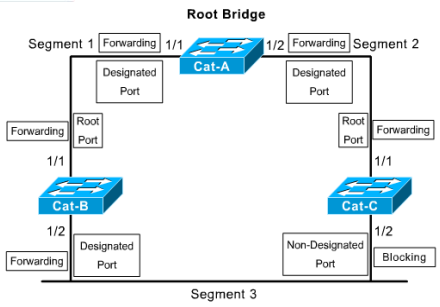
- Time is required for (BPDU) protocol information to propagate throughout a switched network.
- Topology changes in one part of a network are not instantly known in other parts of the network.
- There is propagation delay.
- A switch should not change a port state from inactive (Blocking) to active (Forwarding) immediately, as this may cause data loops.
- Each port on a switch that is using the Spanning-Tree Protocol has one of five states,

60

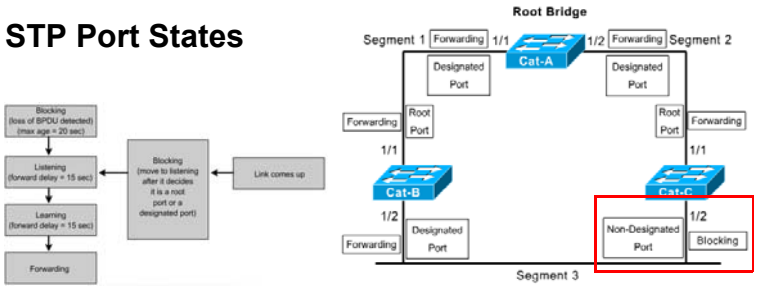
State	Purpose
Forwarding	Sending / receiving user data
Learning	Building bridging table
Listening	Building "active" topology
Blocking	Receives BPDUs only
Disabled	Administratively down

Designated Ports & Root Ports

Non-Designated Ports

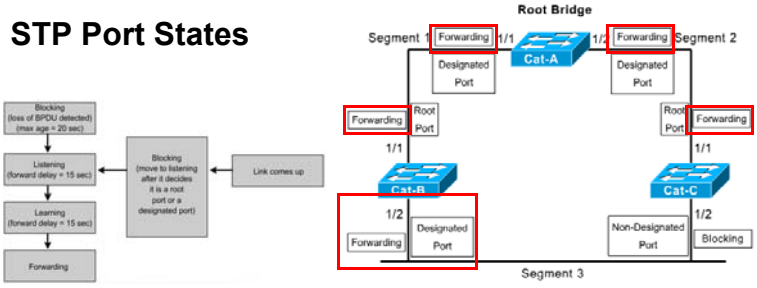


STP Port States



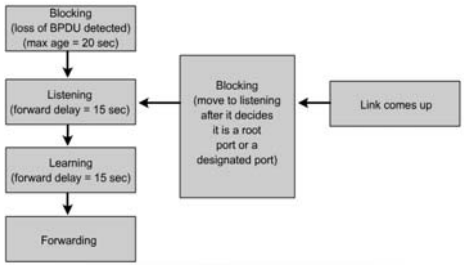
- In the **blocking state**, ports can only receive BPDUs.
  - Data frames are discarded and no addresses can be learned.
  - It may take up to 20 seconds to change from this state.
- Ports go from the blocked state to the **listening state**.
  - Switch **determines if there are any other paths to the root bridge**.
  - The **path that is not the least cost path to the root bridge goes back to the blocked state**.
  - The listening period is called the forward delay and lasts for 15 seconds.
  - In the listening state, user data is not being forwarded and MAC addresses are not being learned.
  - BPDUs are still processed.

STP Port States

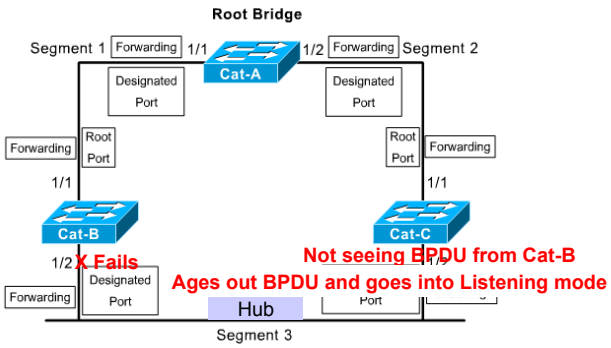


- Ports transition from the listening to the **learning state**.
  - In this state **user data is not forwarded, but MAC addresses are learned** from any traffic that is seen.
  - The learning state lasts for 15 seconds and is also called the forward delay.
  - BPDUs are still processed.
- A port goes from the learning state to the **forwarding state**.
  - In this state user data is forwarded and MAC addresses continue to be learned.
  - BPDUs are still processed.

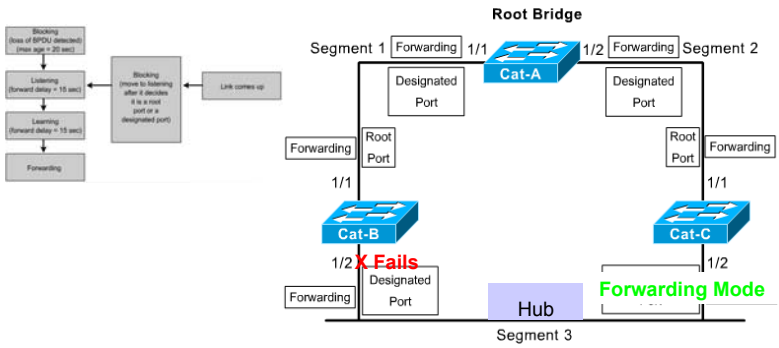
STP Timers



- Some details have been left out, such as timers, STP FSM, etc.
- The time values given for each state are the default values.
- These values have been calculated on an assumption that there will be a maximum of seven switches in any branch of the spanning tree from the root bridge.

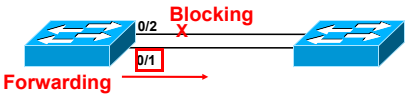


- Cat-B:1/2 fails.
- Cat-C has no immediate notification because it's still receiving a link from the hub.
- Cat-C notices it is not receiving BPDUs from Cat-B.
- **20 seconds (max age)** after the failure, Cat-C ages out the BPDU that lists Cat-B as having the DP for segment 3.
- This causes **Cat-C:1/2 to transition into the Listing state (15 seconds)** in an effort to become the DP.



- Because Cat-C:1/2 now offers the most attractive access from the Root Bridge to this link, it **eventually transitions to Learning State (15 seconds), then all the way into Forwarding mode.**
- In practice this will take **50 seconds (20 max age + 15 Listening + 15 Learning)** for Cat-C:1/2 to take over after the failure of Cat-B:1/2.

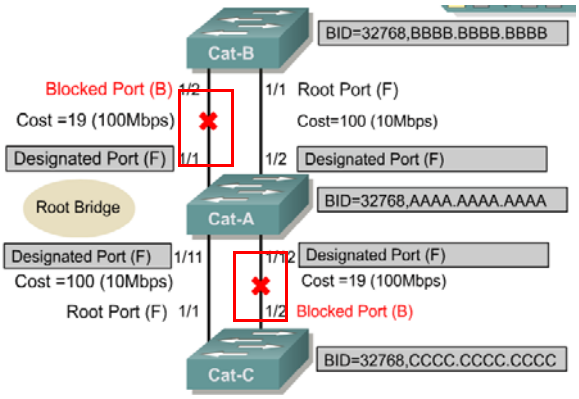
Port Cost/Port ID



Assume path cost and port priorities are default (32). Port ID used in this case. Port 0/1 would forward because it's the lower than Port 0/2.

- If the path cost and bridge IDs are equal (as in the case of parallel links), the switch goes to the port priority as a tiebreaker.
- Lowest port priority wins (all ports set to 32).
- You can set the priority from 0 – 63.
- If all ports have the same priority, the port with the lowest port number forwards frames.

Port Cost/Port ID



- If all ports have the same priority, the port with the lowest port number forwards frames.

STP Convergence Recap

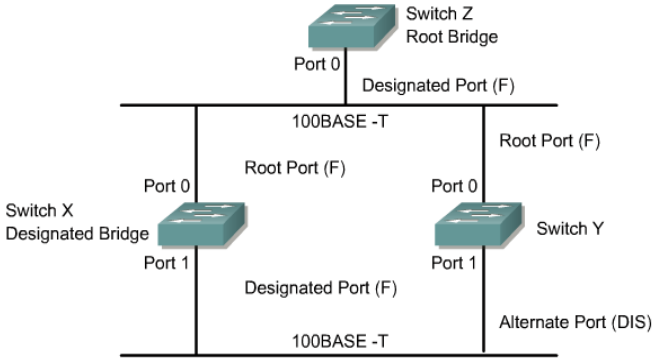
- Recall that switches go through three steps for their initial convergence:

STP Convergence
Step 1 Elect one Root Bridge
Step 2 Elect Root Ports
Step 3 Elect Designated Ports

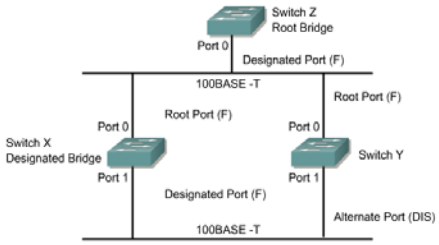
- Also, all STP decisions are based on a the following predetermined sequence:

Four-Step decision Sequence
Step 1 - Lowest BID
Step 2 - Lowest Path Cost to Root Bridge
Step 3 - Lowest Sender BID
Step 4 - Lowest Port ID

Rapid Spanning Tree Protocol (RSTP)

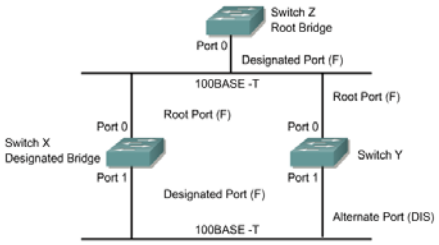


Rapid Spanning Tree Protocol (RSTP)



- The Rapid Spanning-Tree Protocol is defined in the IEEE 802.1w LAN standard. The standard and protocol introduce the following:
  - Clarification of port states and roles
  - Definition of a set of link types that can go to forwarding state rapidly
  - Concept of allowing switches, in a converged network, to generate their own BPDUs rather than relaying root bridge BPDUs
- The "blocked" state of a port has been renamed as the "discarding" state.

RSTP Link Types



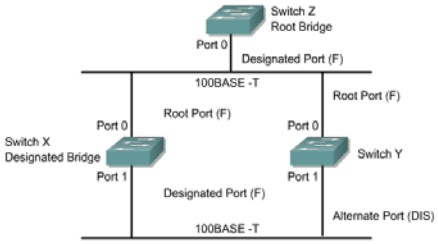
- Link types have been defined as point-to-point, edge-type, and shared.
- These changes allow failure of links in switched network to be learned rapidly.
- Point-to-point links and edge-type links can go to the forwarding state immediately.
- Network convergence does not need to be any longer than 15 seconds with these changes.
- The Rapid Spanning-Tree Protocol, IEEE 802.1w, will eventually replace the Spanning-Tree Protocol, IEEE 802.1D

RSTP Port States

STP (802.1D) Port State	RSTP (802.1w) Port State	Is Port Included in Active Topology?	Is Port Learning Mac Addresses?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	No	No
Learning	Learning	No	Yes
Forwarding	Forwarding	Yes	Yes

73

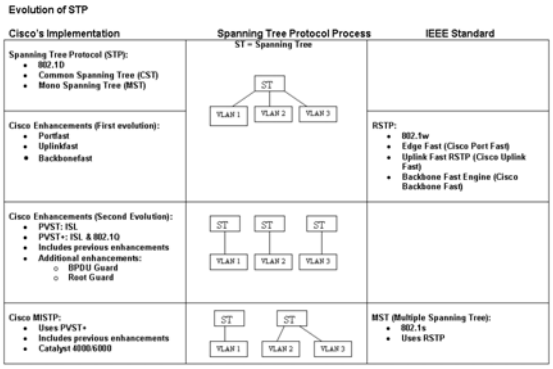
RSTP Port Roles



- The role is now a variable assigned to a given port.
- The root port and designated port roles remain.
- The blocking port role is now split into the **backup** and **alternate** port roles.
- The Spanning Tree Algorithm (STA) determines the role of a port based on Bridge Protocol Data Units (BPDUs).
- To keep things simple, the thing to remember about a BPDU is that there is always a way of comparing any two of them and deciding whether one is more useful than the other.
- This is based on the value stored in the BPDU and occasionally on the port on which they are received.

74

Rapid Spanning Tree Protocol (RSTP)



- RSTP adds features to the standard similar to vendor proprietary features including Cisco's Port Fast, Uplink Fast and Backbone Fast.
- Cisco recommends that administrators upgrade to the IEEE 802.1w standard when possible.

75

Cisco's Port Fast and RSTP's Edge Fast

- A common problem is with DHCP and STP Port States.
- The workstation will power up and start looking for a DHCP servers before its port has transitioned to Forwarding State.
- The workstation will not be able to get a valid IP address, and may default to an IP address such as 169.x.x.x.
- Spanning-tree PortFast causes a port to enter the spanning-tree forwarding state immediately, bypassing the listening and learning states.
- You can use PortFast on switch ports connected to a single workstation or server to allow those devices to connect to the network immediately, instead of waiting for the port to transition from the listening and learning states to the forwarding state.
- **Caution** PortFast should be used *only* when connecting a single end station to a switch port.
  - If you enable PortFast on a port connected to another networking device, such as a switch, you can create network loops.

76

Algorithm by Radia Perlman

I think I shall never see
A graph more lovely than a tree.

A tree whose crucial property
Is loop-free connectivity

A tree that must be sure to span
So packets can reach every LAN.

First the root must be elected.
By ID is is elected.

Least-cost paths from root are traced.
In the tree, these paths are placed.

A mesh is made by folks like me,
Then bridges find a spanning tree.

77

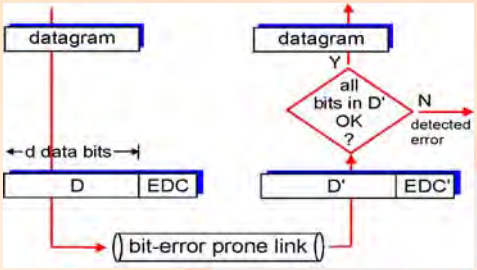
Error Control: Detection and Correction

Slide Set 9

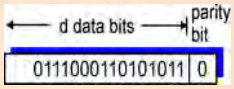
Error Detection

EDC = Error Detection and Correction bits (redundancy)
D = Data protected by error checking, may include header fields

- **Error detection not 100% reliable!**
  - **protocol may miss some errors, but rarely**
  - **larger EDC field yields better detection and correction**



Single Bit Parity Checking (Detect Only)



This is an example of odd parity: The parity bit is chosen (0) in such a way that the total number of 1s is odd (9)

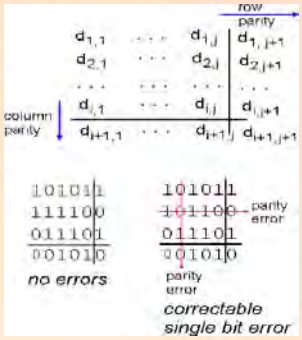
Even Parity Scheme:
Parity bit chosen so that total number of 1s including the parity bit is **EVEN.**

Odd Parity Scheme:
Parity bit chosen so that total number of 1s including the parity bit is **ODD.**

IMPORTANT
A single bit parity check will only be able to detect 1 or and odd number of bits in error.

It is highly efficient since a single parity bit is needed for any length of data bits (Message M).

2-D Bit Parity Checking (Detect & Correct)



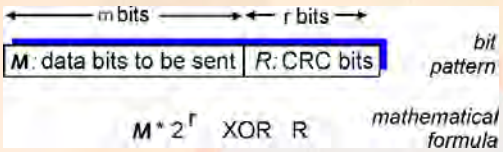
This is an example of even parity: The parity bits are chosen in such a way that the total number of 1s is either a column or row is even

In this technique, the data bits are rearranged in an nxm matrix. Ideally a square matrix for higher efficiency. The parity bit is chosen for each row and column in the matrix. An additional parity bits can be used for checking the parity bits themselves but this is optional.

IMPORTANT
A 2-D bit parity check will only be able to detect 1 or and odd number of bits in error in either a column or a row but can also correct single bit errors if they occur in different rows and columns.

Cyclic Redundancy Check (Detect Only)

- view Message bits, M, as a binary number
- choose r+1 bit pattern divisor (generator), G
- goal: choose r CRC bits, R, such that
  - <M,R> exactly divisible by G (modulo 2)
  - receiver knows G, divides <M,R> by G. If non-zero remainder occurs: error detected!



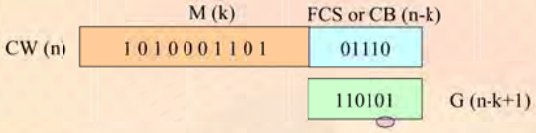
Example of CRC in an Ethernet frame

CRC appends **redundant** bits to the frame trailer called Frame Check Sequence (FCS)
The FCS bits are used at Receiver for error detection
In a given frame containing a total of n bits, we define:
k = the number of original data bits (Message M)
(n – k) = the number of added bits as the FCS field or Code Bits (CB)
So, the total frame length is k + (n – k) = n bits or Code Word (CW)

	M (k)	CB (n-k)
CW(n)	1 0 1 0 0 0 1 1 0 1	01110

CRC Generation

CRC generation at the sender is all about finding the FCS, given the data (M) and a divisor (G) that makes CW exactly divisible by G (i.e. with 0 remainder)



There are three equivalent ways to see how the CRC code is generated:
Modulo-2 Arithmetic Method
Polynomial Method (not covered)
Digital Logic Method (not covered)

What is F that makes T divide P exactly? i.e. with no remainder

Modulo-2 Arithmetic

- *In modulo 2 arithmetic addition and substruction are identical to EXCLUSUVE OR (XOR) operation.*
- *Multiplication and division are the same as in base-2 arithmetic without carries in addition or borrows in substraction.*

0 XOR 0 = 0
0 XOR 1 = 1
1 XOR 0 = 1
1 XOR 1 = 0

Examples:
1011 XOR 0101 = 1110
1001 XOR 1101 = 0100

CRC Error Detection Process

Given k-bit data (M), the Sender generates an (n – k)-bit FCS field (CB) such that the *total* n-bit frame (CW) is exactly divisible by a predefined (n-k+1) bit divisor (G) (i.e. gives a zero remainder)

In general, the received frame (CW') may or may not be identical to the sent frame (CW).
Let the received frame be (CW')
Only in error-free transmissions that we have CW' = CW
Receiver divides (CW') by the same known divisor (G) and checks if there is any remainder, if division yields a remainder then the frame is erroneous
If the division yields zero remainder then the frame is error-free unless many erroneous bits in CW' resulted in a new exact division by G.

This is extremely unlikely but possible, causing an undetected error!

Example – Modulo-2 Arithmetic Method

- Given
  - M = 1 0 1 0 0 0 1 1 0 1
  - G = 1 1 0 1 0 1 (i.e. $x^5+x^4+x^2+1$)

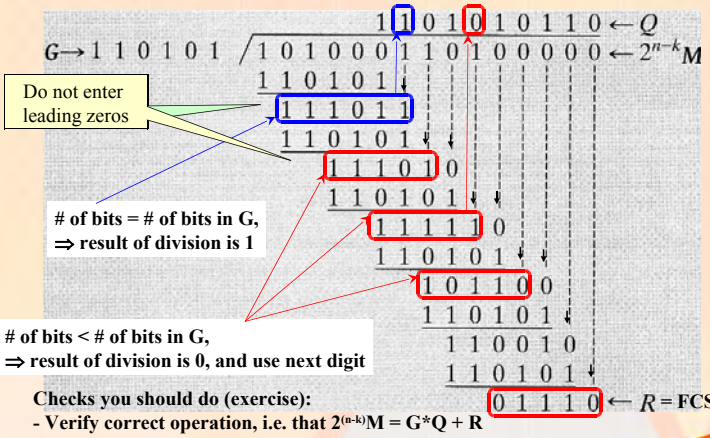
  At the Sender (source) side
- Find the FCS field
- Solution:
  - First we note that:
    - The size of the data block M is k = 10 bits
    - The size of G is (n – k + 1) = 6 bits
      - Hence the FCS length is n – k = 5
      - Total size of the CW is n = 15 bits

Example – Modulo-2 Arithmetic Method

- Solution (continued):
  - Multiply $2^{(n-k)}$ x M
    - $2^{(5)}$ x 1 0 1 0 0 0 1 1 0 1 = 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0
    - This is a simple shift to the left by five positions and inserting (n-k) zeroes.
  - Divide $2^{(n-k)}$ x M / G (see next slide for details)
    - 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0 ÷ 1 1 0 1 0 1 yields:
      - **Quotient Q = 1 1 0 1 0 1 0 1 1 0**
      - **Remainder R = 0 1 1 1 0**
  - So, FCS = R = 0 1 1 1 0: Append it to M to get the full frame CW to be transmitted
  - CW = 1 0 1 0 0 0 1 1 0 1 0 1 1 1 0

    M FCS

Example – Modulo-2 Arith. Method



Checks you should do (exercise):
- Verify correct operation, i.e. that $2^{(n-k)}M = G*Q + R$
- Verify that the obtained CW(1010001101 01110) divides G (110101) exactly (i.e. with zero remainder)

Example – Modulo-2 Arith. Method

For G = 110011 & M = 11100011, find the CRC

```
          10110110
      ____________
110011 | 11100011000000
         110011
         -------
          101111
          110011
          ------
           111000
           110011
           ------
            101100
            110011
            ------
             111110
             110011
             ------
CRC =        11010
```

CW to transmit is? Answer: 11100011**11010**

Hamming Code (Detect & Correct)

Hamming Code is an error control technique where the redundant bits (CB) are spread at strategic position within the message bits (M).

- The position of these redundant bits are always at position 2^n (where n =0,1,2,3,...) i.e. position 1,2,4,8,...
- The number of redundant bits needed depends on the number of bits in the message (M).
- It is usually expressed as a function ***H(CW,M)*** e.g **H(11,7)** i.e. 7 message bits and 4 Code Bits (CB) yielding an 11-bit Codeword (CW)

Hamming Code: Code Bits Generation

At the SENDER:

Suppose M = 101000001 (9 bits)

13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	0	?	0	0	0	?	1	?	?

We reserve **4 boxes**: 1,2,4 and 8 for the code bits, and insert the message bits in the remaining boxes. There are 13 boxes in all that will represent the 13 bits in the codeword.

- To obtain the values of the code bits (the 4 boxes with interrogation marks), we perform a **modulo-2 addition** of all the box positions containing a '1' bit.
- In modulo-2 addition, we count the number of '1's in each column respectively. If the number of '1's is even, the addition yield 0 else if the number of '1's is odd, the addition yields 1.

Hamming Code: Code Bits Generation

Modulo-2 addition yields:

```
13:  1101
11:  1011
3 :  0011
     ----
     0101   = Code Bits
```

These become the code bits and are substituted back in the interrogation mark boxes. The transmitted codeword therefore becomes:

13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	0	0	0	0	0	1	1	0	1

Hamming Code: Error Checking

At the RECEIVER:

13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	0	0	0	0	0	1	1	0	1

A modulo-2 addition is performed on the received codeword with all the box positions containing a '1':

```
13:  1101
11:  1011
 4:  0100
 3:  0011
 1:  0001
     ----
     0000
```

Since addition is 0, it implies that no errors have taken place.

Hamming Code: Error Correction

Assume that at the RECEIVER, bit number 11 is in error:

13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	0	0	0	0	0	0	0	1	1	0	1

A modulo-2 addition is performed on the received codeword with all the box positions containing a '1':

```
13:  1101
 4:  0100
 3:  0011
 1:  0001
     ----
     1011
```

Since addition is NOT 0, it implies that a error has taken place. The bit position in error is given by the result of the addition **i.e. 1011 = 11th bit.** So to correct, we simply invert the bit value

Hamming Code

- It is always assumed that the code bits are not corrupted during transmission.
- Hamming code can only detect and correct **1 bit** in error in the message M.
- The efficiency of Hamming Code increases as the number of bits in the message becomes larger.

Summary

- Single parity bit checking can **only detect** 1 or an odd number of bits in error in the message M. It has the highest efficiency as it needs only one code bit irrespective of the length of the message M.
- 2-Dimensional parity bit checking can **detect and correct** 1 or more errors as long as 1 or an odd number of bits in error occur in different rows and/or columns.
- CRC can **only detect** any number of bits in error in the message M. The number of code bits needed is always one bit less than the divisor irrespective of the length of the message M.
- Hamming code can **detect and correct** a single bit in error in the message M. The number of code bits needed increases with the the length of the message M.

Wireless LANs

Slide Set 10

Characteristics of wireless LANs

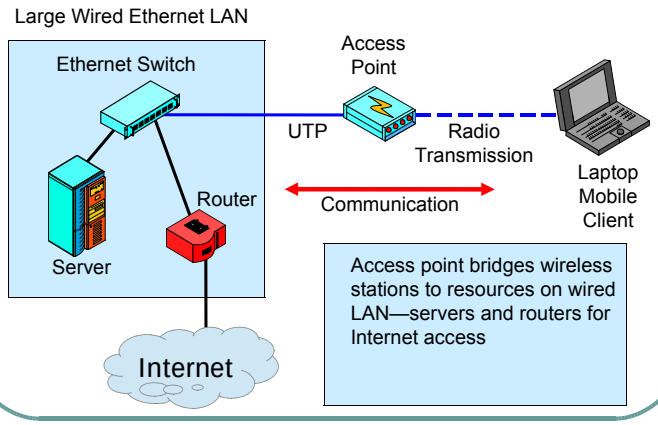
Advantages

Flexibility and Mobility: very flexible within the reception area
Planning: *Ad-hoc* networks without previous planning possible
Design: (almost) no wiring difficulties (e.g. historic buildings, harzardous media, firewalls)
Robustness: more robust against disasters like, e.g., earthquake, fire or flood...
Cost: Adding additional users to a wireless network will not increase the cost. Cheap Hardware.

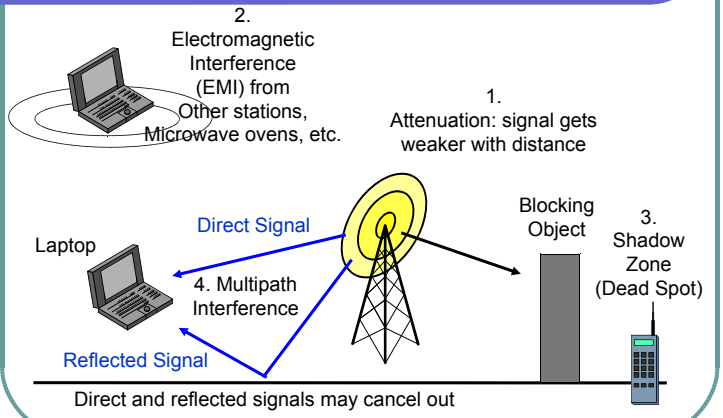
Disadvantages

Throughput: typically lower speed compared to wired networks but increasing everyday.
Proprietary solutions: many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11). Now, 802.11n is a popular solution.
Legal Restrictions: Have to conform to many national restrictions if working with wireless.
Safety and Security: Precautions have to be taken to prevent safety hazards and interference. Confidentiality and integrity must be enforced.

Wireless LAN (WLAN) Access Point



Wireless Propagation Problems

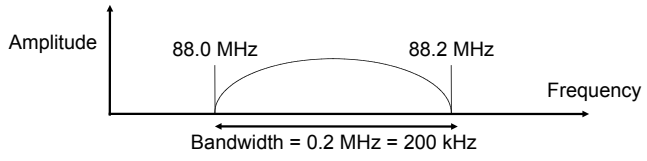


Wireless Propagation Problems

- Some problems are Frequency-Dependent
  - Higher-frequency signals attenuate faster
    - Absorbed more rapidly by moisture in the air
  - Higher-frequency signals blocked more by obstacles
    - At lower frequencies, signal refract (bend) around obstacles like an ocean wave hitting a buoy
    - At higher frequencies, signals do not refract; leave a complete shadow behind obstacles

Channel Bandwidth

- Channel Bandwidth
  - An 88.0 MHz to 88.2 MHz channel (FM radio) has a bandwidth of 0.2 MHz (200 kHz)
  - Higher-speed signals need wider bandwidths



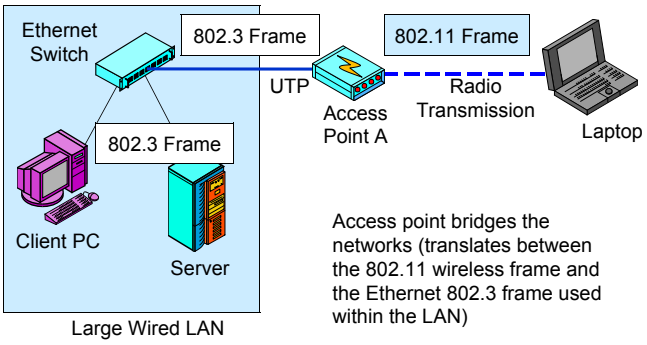
Transmission Speed

- Shannon Capacity Theorem
  - C=B Log_2 (1+S/N)
    - C = Maximum possible transmission speed in the channel (bps)
    - B = Bandwidth (Hz) (Like thickness of a hose)
    - S/N = Signal-to-Noise power
  - Note that doubling the bandwidth (B) doubles the maxir transmission speed
  - More generally, increasing the bandwidth by X increases the maximum possible speed by X
  - Increasing S/N helps slightly but usually cannot be done to any significant extent

The Golden Zone

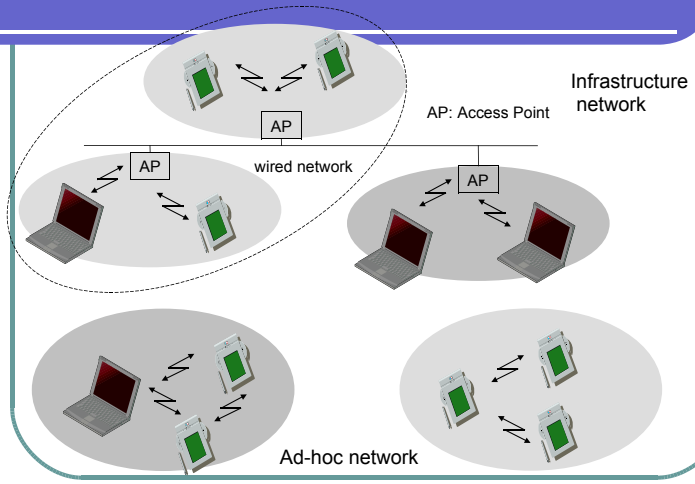
- The Golden Zone
  - Most organizational radio technologies operate in the "golden zone"
  - High megahertz to low gigahertz range
  - At higher frequencies, there is more available bandwidth
  - At lower frequencies, signals propagate better.
  - Frequencies should be high enough for there to be large total bandwidth
  - Frequencies should be low enough to allow fairly good propagation characteristics.

Typical 802.11 Wireless LAN Operation with Access Points

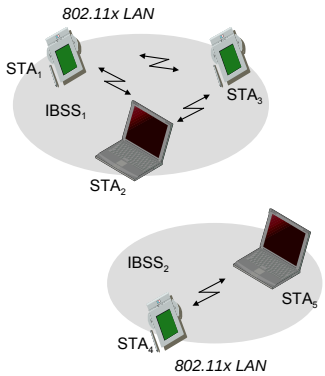


Access point bridges the networks (translates between the 802.11 wireless frame and the Ethernet 802.3 frame used within the LAN)

Infrastructure Mode vs. Ad-hoc Mode



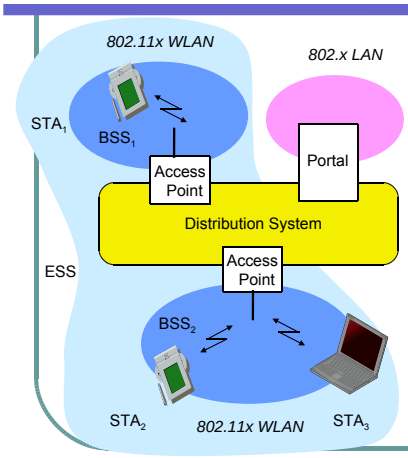
802.11 - Architecture of an *ad-hoc* network



Direct communication within a limited range:

- Station (STA): terminal with access mechanisms to the wireless medium
- Independent Basic Service Set (IBSS): group of stations using the same radio frequency

Architecture of an infrastructure network



Station (STA)
- terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)
- group of stations using the same radio frequency

Access Point (AP)
- station integrated into the wireless LAN and the distribution system

Portal
- bridge to other (wired) networks

Distribution System
- interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

802.11x Wireless Access Point and Wireless LAN Adapters (PCMCIA, PCI & USB)

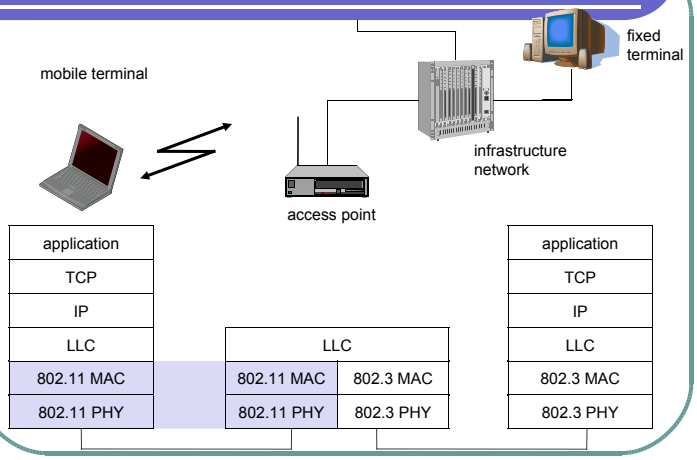
A 802.11g Access Point with two antennas

USB: Most popular and portable. Works with any device with USB ports

PCMCIA: used in old laptops with no built-in WLAN Adapter

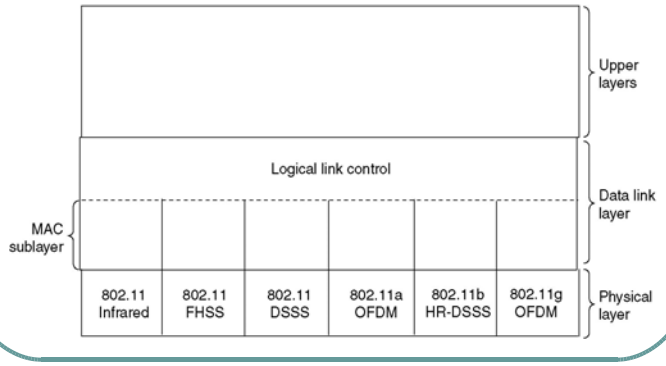
PCI: used in Desktop PCs

IEEE standard 802.11



The 802.11 Protocol Stack

Part of the 802.11 protocol stack.



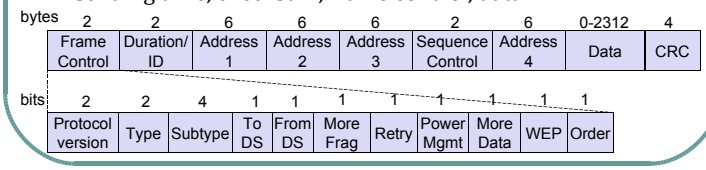
802.11 - Frame format

Types
- control frames, management frames, data frames

Sequence numbers
- important against duplicated frames due to lost ACKs

Addresses
- receiver, transmitter (physical), BSSID, sender (logical)

Miscellaneous
- sending time, checksum, frame control, data



MAC address Configurations

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

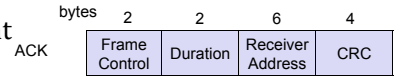
DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address

BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

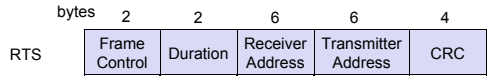
- *Ad-hoc* network: packet exchanged between two wireless nodes without a distribution system
- Infrastructure network, from AP: a packet sent to the receiver via the access point
- Infrastructure network, to AP: a station sends a packet to another station via the access point
- Infrastructure network, within DS: packets transmitted between two access points over the distribution system.

Special Frames: ACK, RTS, CTS

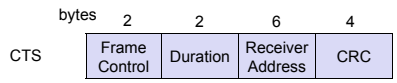
Acknowledgement



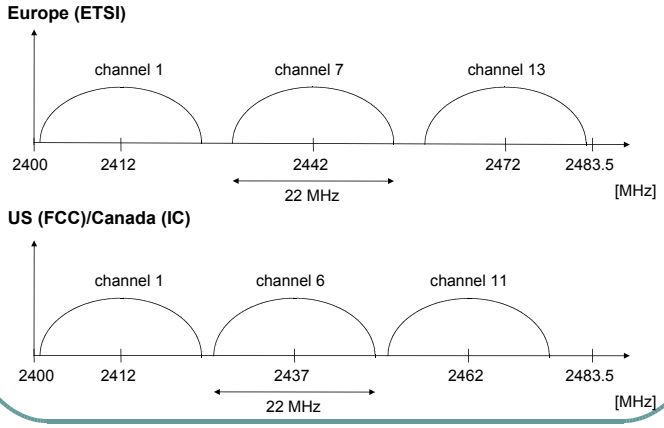
Request To Send



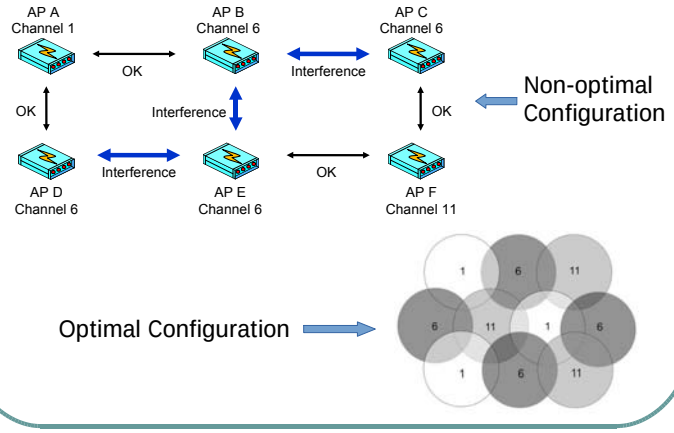
Clear To Send



Channel selection (non-overlapping)



4 or more AP Configuration for minimal Interference in close vicinity



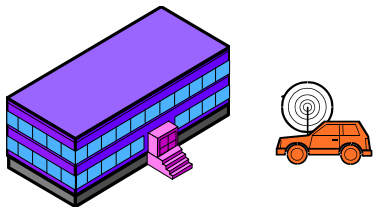
802.11 Wireless LAN Standards

802.11-Standard	Standard Year	Frequency (GHz)	Bandwidth (MHz)	Modulation Type	Max. Data Rate (Mbit/s)
802.11a	1999	5 GHz	20 MHz	OFDM	54 Mbit/s
802.11ac	2013	5 GHz	40/80/160	OFDM	6,93 Gbit/s
802.11ad	2012	60 GHz	2160	SC-OFDM	6,76 Gbit/s
802.11b	1999	2,4 GHz	20	DSSS	11 Mbit/s
802.11g	2003	2,4 GHz	20	DSSS/OFDM	54 Mbit/s
802.11n	2009	2,4/5 GHz	20/40	OFDM	600 Mbit/s

DSSS, direct sequence spread spectrum
FHSS, frequency hopping spread spectrum
OFDM, orthogonal frequency division multiplex
SC-OFDM, single carrier orthogonal frequency division multiplex

802.11x Security

- Automated Drive-By Hacking (War Driving)
  - Can read traffic from outside the corporate walls
  - Can also send malicious traffic into the network



802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Initial flawed security method developed by the 802.11 Working Group for 802.11 devices
  - All stations share the same encryption key with the access point
  - This key is cannot be changed
  - This is a shared static key

802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Shared static keys means that a large volume of traffic is encrypted with the same key
  - With so much traffic generated with one unchanging key, cryptanalysts (code-breakers) can crack the key by collecting data for a few days
  - Once the key is cracked, the attacker can read all messages and send attack messages into the network without going through a firewall filter

802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Software that automates the hacking process is widely available e.g. AirSnort
    - Locate vulnerable access points by driving around (war driving)
    - Collect traffic and crack the key
    - **No longer recommended to use WEP nowadays**

802.11 Security, Continued

- 802.11i Security
  - Products started becoming available in late 2003
- WiFi Protected Access (WPA)
  - Stopgap security method introduced before full 802.11i security could be developed
  - Introduced some parts of 802.11i in 2002 and 2003
  - It was often possible to upgrade older WEP products to WPA

802.11 Security, Continued

- 802.11i Security (WPA2) (Stronger than WPA)
  - Later, 802.11 Working Group introduced strong security
    - 802.11i
  - 802.11i specifies the Temporal Key Integrity Protocol (TKIP)
    - Each station gets a separate key for confidentiality
    - This key can be changed frequently

802.11 Security, Continued

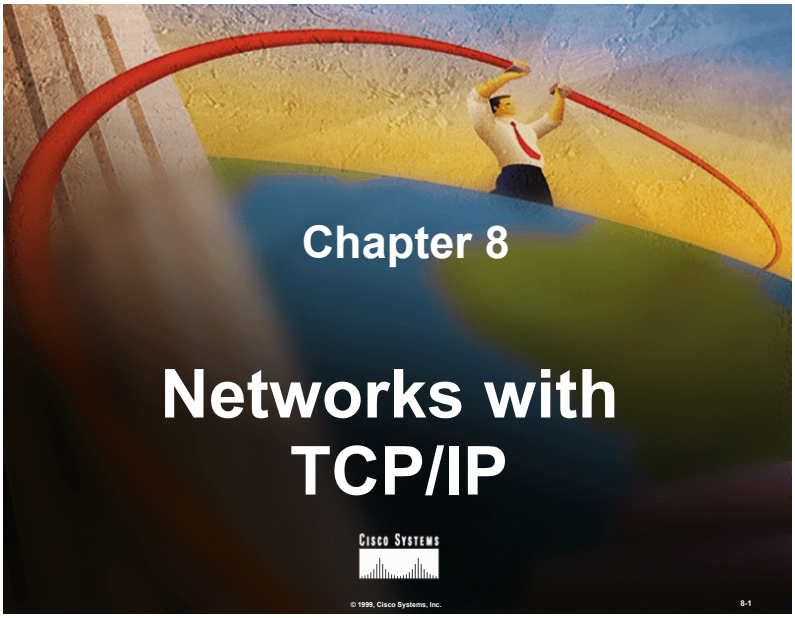
- Ways to strengthen your Wireless LAN
  - Do not use WEP. Use WPA or WPA2 instead
  - Enforce MAC address Association (i.e only allowed wireless adapters can join your wireless network)
  - Disable BSSID broadcast once all permitted stations have been allowed to join the wireless network.
  - Enable Access Point firewall features to prevent potential attacks.

802.11 Security, Continued

- The Transition to Strong Security
  - We will soon have a mix of no security, WEP, 802.11i, WPA, and other security protocols
  - Only as strong as the weakest link
  - Legacy equipment that cannot be upgraded to 802.11i will have to be discarded
  - (802.11i is sometimes called WPA2)

802.11 Security, Continued

- Rogue Access Points
  - Unauthorized access points set up by department or individual
  - Often have very poor security, leaving a big opening for hackers
  - Often operate at high power, attracting many clients to these access points with weak security

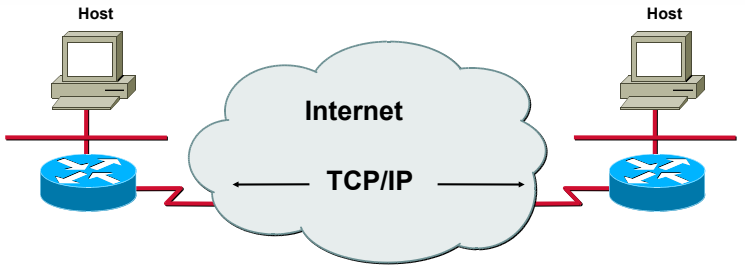


Chapter 8

Networks with TCP/IP

Cisco Systems

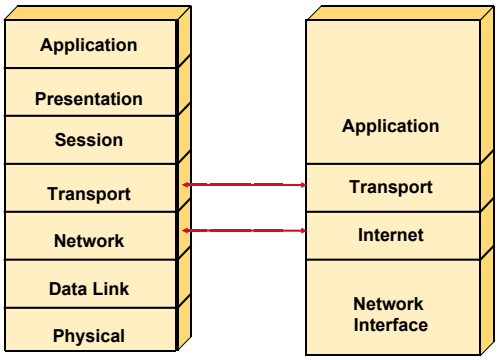
Introduction to TCP/IP



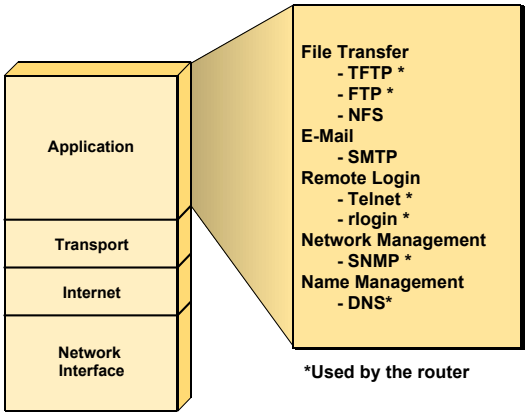
Early protocol suite

Universal

TCP/IP Protocol Stack

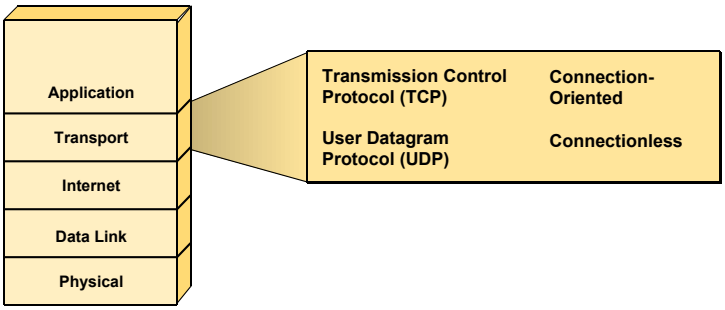


Application Layer Overview

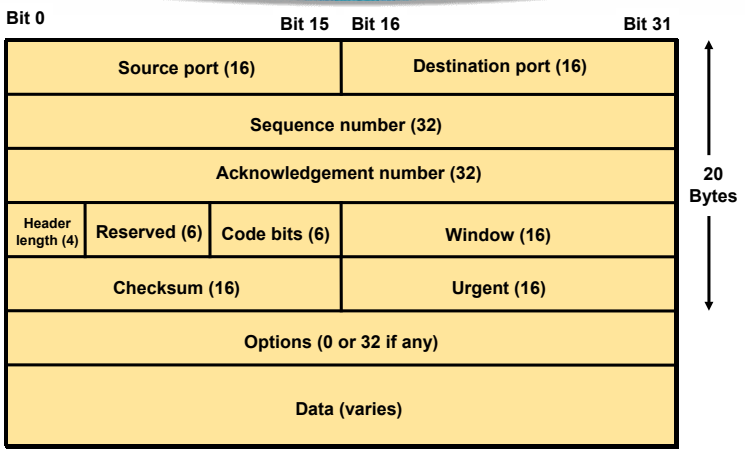


*Used by the router

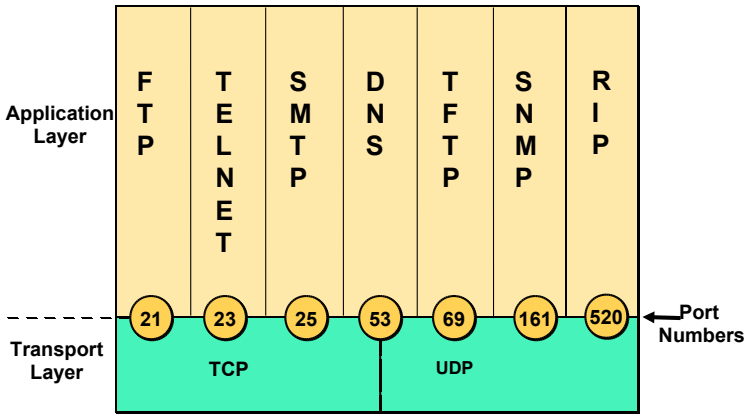
Transport Layer Overview



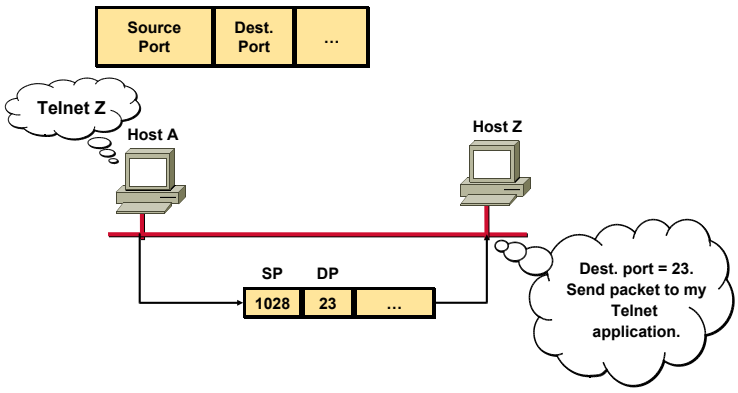
TCP Segment Format



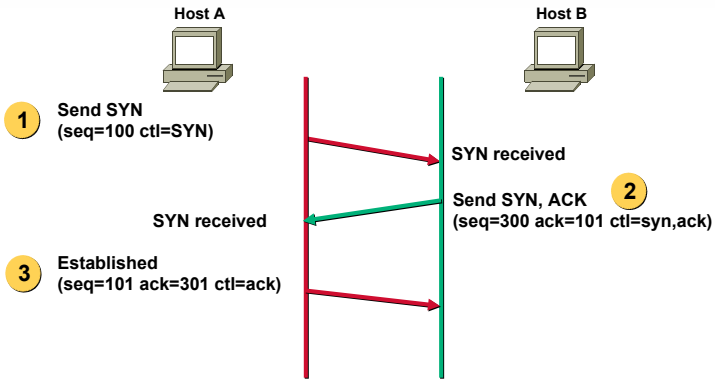
Port Numbers



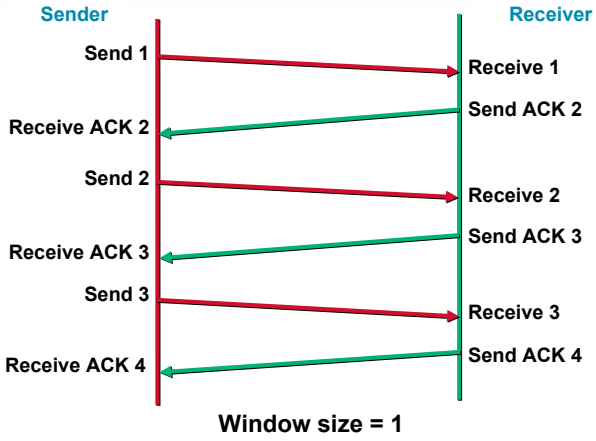
TCP Port Numbers



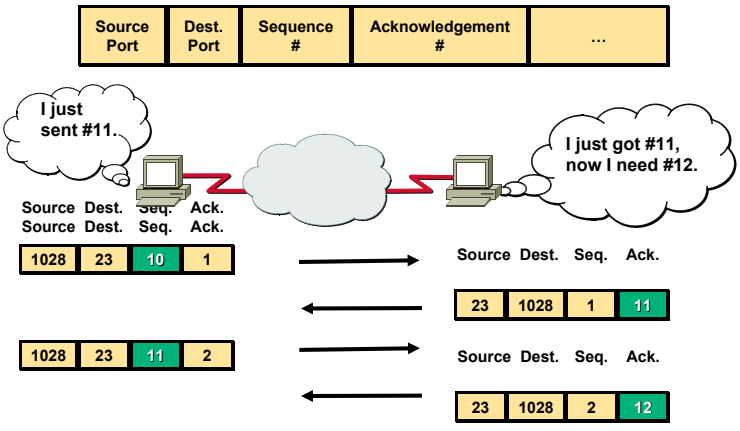
TCP Three Way Handshake/ Open Connection



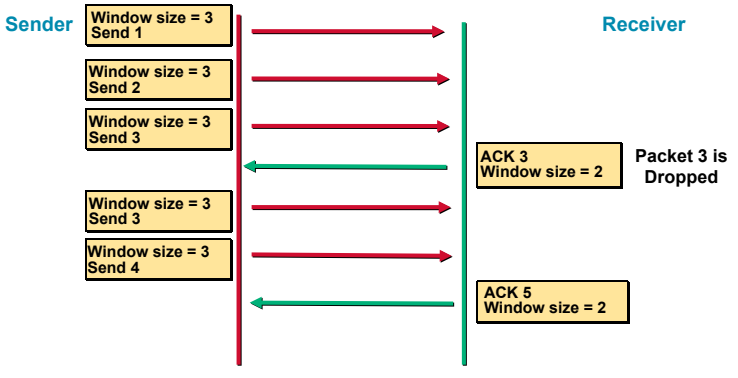
TCP Simple Acknowledgment



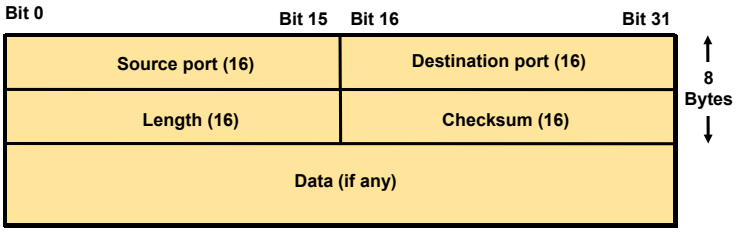
TCP Sequence and Acknowledgment Numbers



TCP Windowing

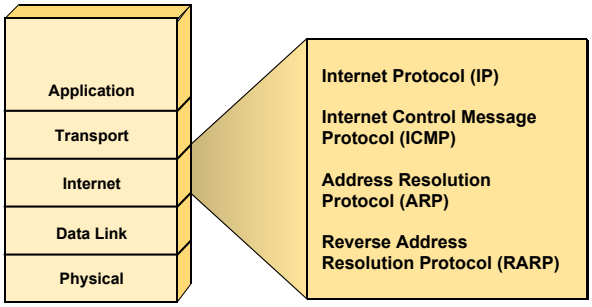


UDP Segment Format



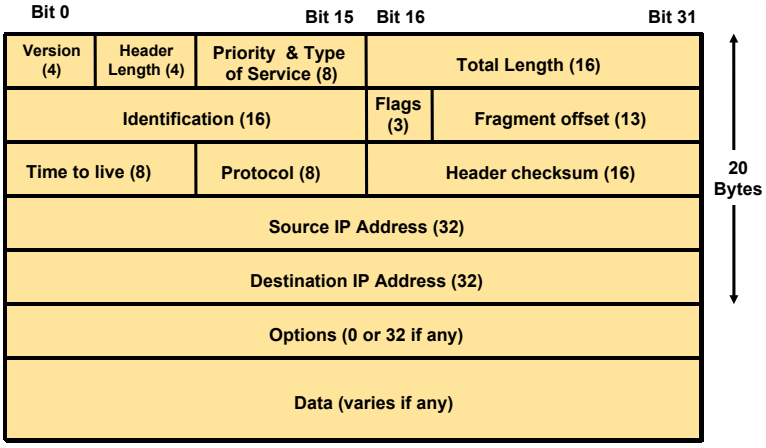
No sequence or acknowledgment fields

Internet Layer Overview

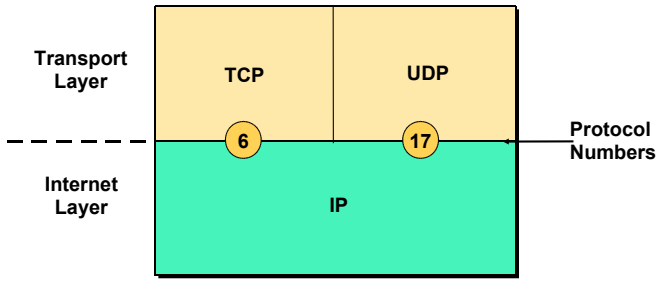


OSI network layer corresponds to the TCP/IP internet layer

IP Datagram

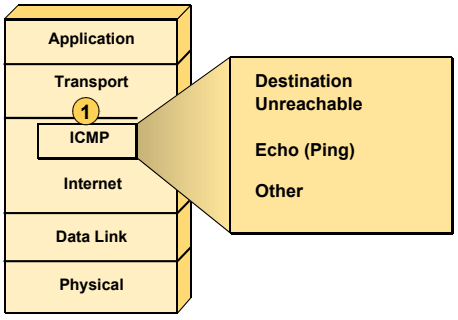


Protocol Field

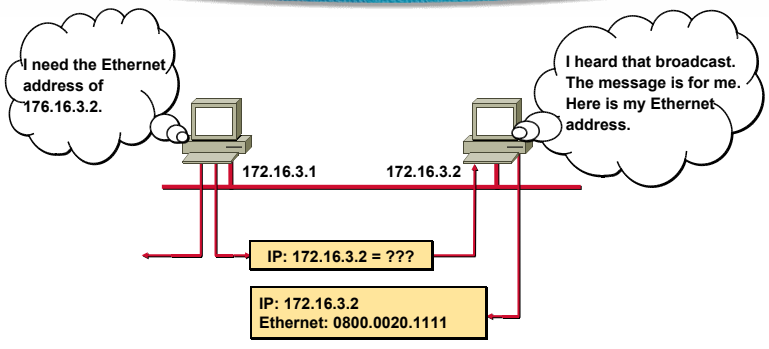


Determines destination upper-layer protocol

Internet Control Message Protocol



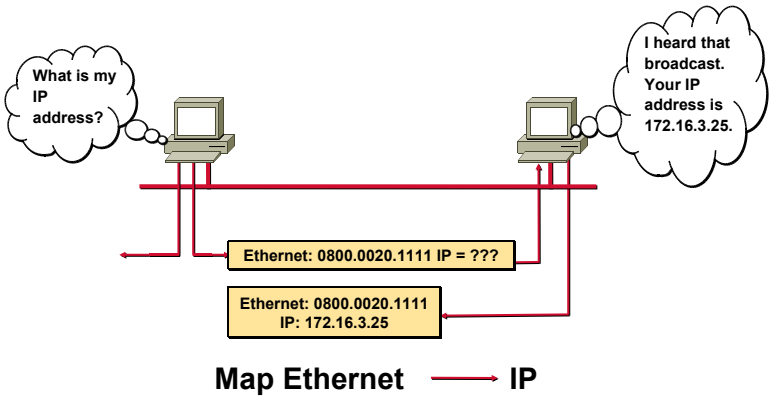
Address Resolution Protocol



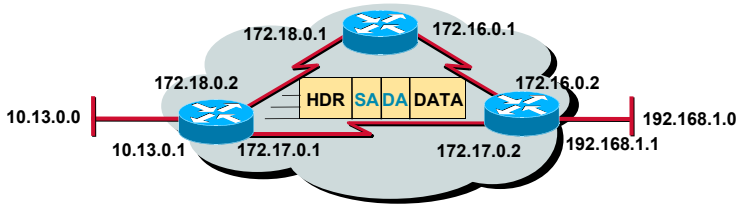
Map IP — Ethernet

Local ARP

Reverse ARP

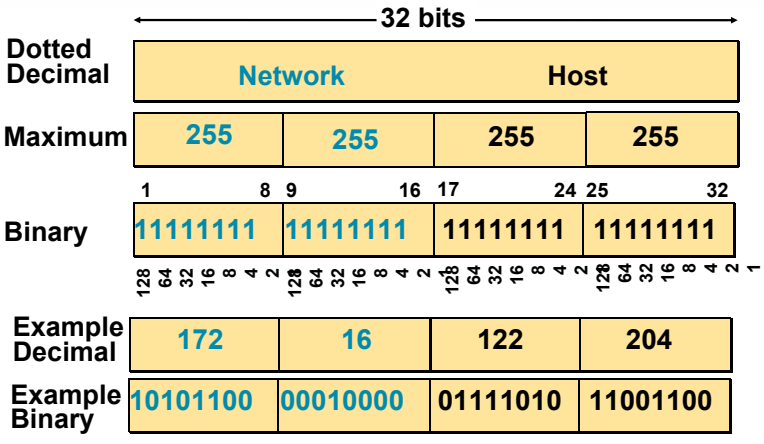


Introduction to TCP/IP Addresses

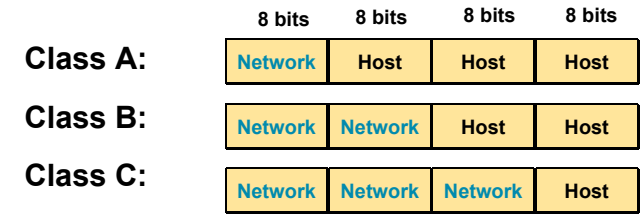


- Unique addressing allows communication between end stations
- Path choice is based on location

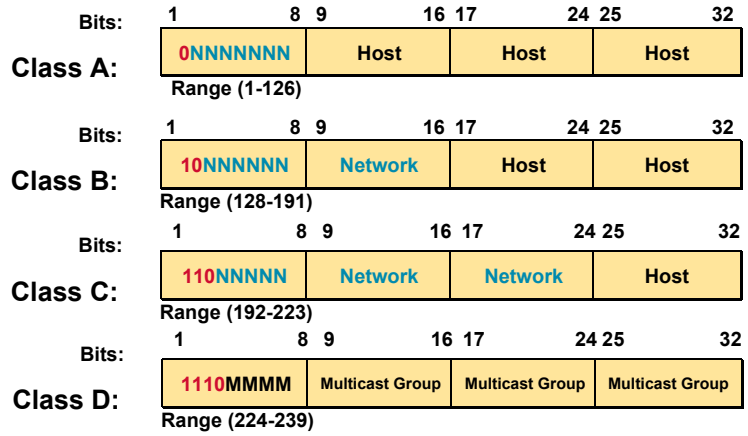
IP Addressing



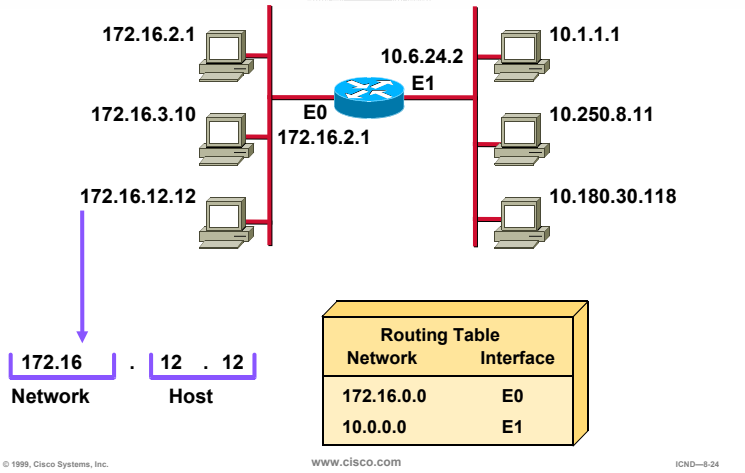
IP Address Classes



IP Address Classes



Host Addresses



Determining Available Host Addresses

Network		Host	
172	16	0	0
10101100	00010000	00000000	00000000

16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 N

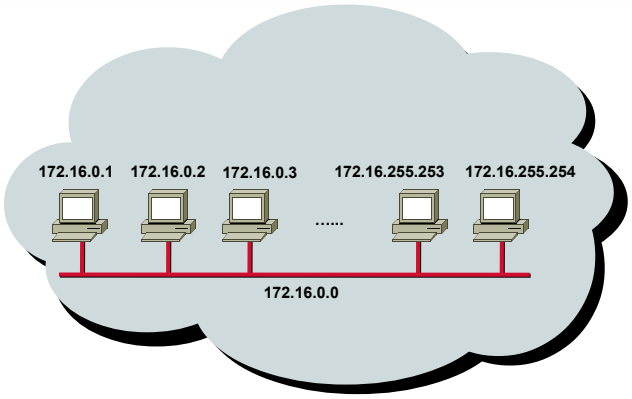
00000000	00000000	1
00000000	00000001	2
00000000	00000011	3
⋮	⋮	⋮
11111111	11111101	65534
11111111	11111110	65535
11111111	11111111	65536
		- 2
		65534

$2^N-2 = 2^{16}-2 = 65534$

IP Address Classes Exercise Answers

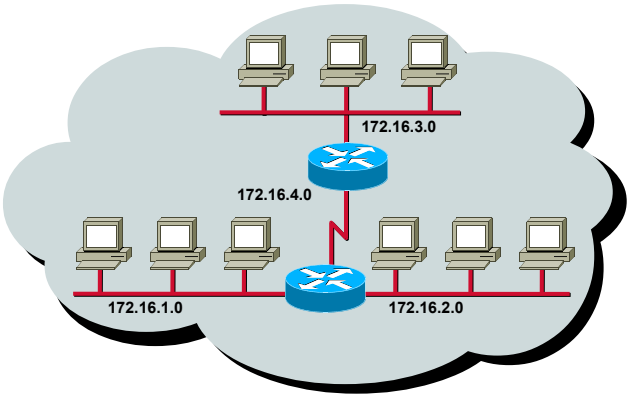
Address	Class	Network	Host
10.2.1.1	A	10.0.0.0	0.2.1.1
128.63.2.100	B	128.63.0.0	0.0.2.100
201.222.5.64	C	201.222.5.0	0.0.0.64
192.6.141.2	C	192.6.141.0	0.0.0.2
130.113.64.16	B	130.113.0.0	0.0.64.16
241.256.201.10	Nonexistent		

Addressing without Subnets



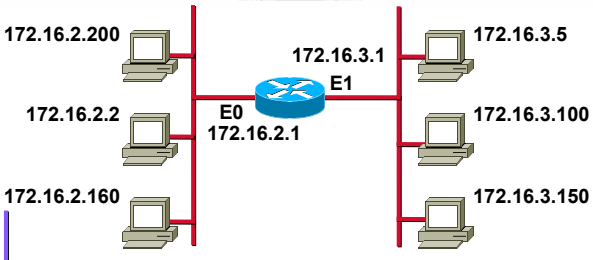
Network 172.16.0.0

Addressing with Subnets



Network 172.16.0.0

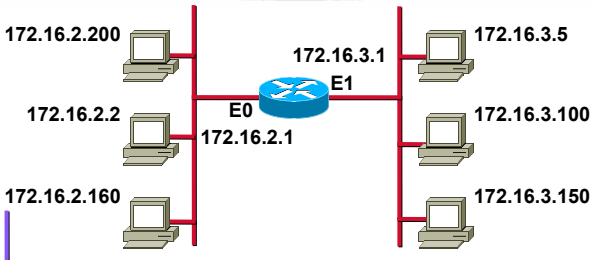
Subnet Addressing



172.16 . 2 . 160
Network Host

New Routing Table	
Network	Interface
172.16.0.0	E0
172.16.0.0	E1

Subnet Addressing



172.16 . 2 . 160
Network Subnet Host

New Routing Table	
Network	Interface
172.16.2.0	E0
172.16.3.0	E1

Subnet Mask

	Network		Host	
IP Address	172	16	0	0
	Network		Host	
Default Subnet Mask	255 11111111	255 11111111	0 00000000	0 00000000

Also written as "/16" where 16 represents the number of 1s in the mask.

	Network	Subnet	Host
8-bit Subnet Mask	255	255	255	0

Also written as "/24" where 24 represents the number of 1s in the mask.

Decimal Equivalents of Bit Patterns

128	64	32	16	8	4	2	1		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

Subnet Mask without Subnets

	Network		Host	
172.16.2.160	10101100	00010000	00000010	10100000
255.255.0.0	11111111	11111111	00000000	00000000
	10101100	00010000	00000000	00000000
Network Number	172	16	0	0

Subnets not in use—the default

Subnet Mask with Subnets

	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.0	11111111	11111111	11111111	00000000
	10101100	00010000	00000010	00000000
Network Number	172	16	2	0

128 192 224 240 248 252 254 255

Network number extended by eight bits

Subnet Mask with Subnets (cont.)

	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.192	11111111	11111111	11111111	11000000
	10101100	00010000	00000010	10000000
Network Number	172	16	2	128

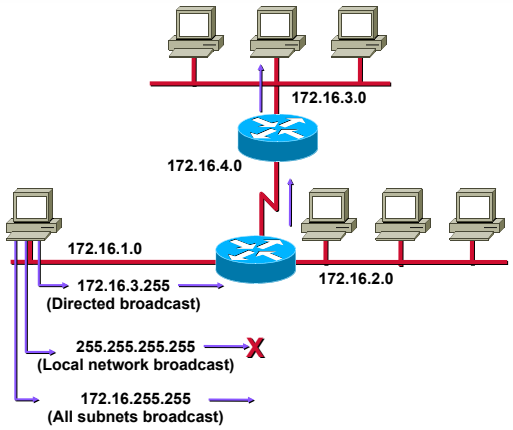
128 192 224 240 248 252 254 255 128 192 224 240 248 252 254 255

Network number extended by ten bits

Subnet Mask Exercise Answers

Address	Subnet Mask	Class	Subnet
172.16.2.10	255.255.255.0	B	172.16.2.0
10.6.24.20	255.255.240.0	A	10.6.16.0
10.30.36.12	255.255.255.0	A	10.30.36.0

Broadcast Addresses



Addressing Summary Example

	172	16	2	160	
172.16.2.160	10101100	00010000	00000010	10 100000	Host 1
255.255.255.192	11111111	11111111	11111111	11 000000	Mask 2
172.16.2.128 8	10101100	00010000	00000010	10 000000	Subnet 4
172.16.2.191 9	10101100	00010000	00000010	10 111111	Broadcast 5
172.16.2.129	10101100	00010000	00000010	10 000001	First 6
172.16.2.190	10101100	00010000	00000010	10 111110	Last 7

3

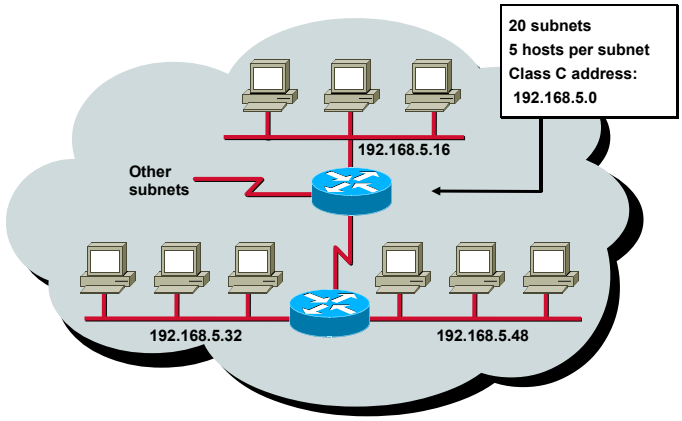
Class B Subnet Example

IP Host Address: 172.16.2.121
Subnet Mask: 255.255.255.0

	Network	Network	Subnet	Host
172.16.2.121:	10101100	00010000	00000010	01111001
255.255.255.0:	11111111	11111111	11111111	00000000
Subnet:	10101100	00010000	00000010	00000000
Broadcast:	10101100	00010000	00000010	11111111

Subnet Address = 172.16.2.0
Host Addresses = 172.16.2.1–172.16.2.254
Broadcast Address = 172.16.2.255
Eight bits of subnetting

Subnet Planning



Class C Subnet Planning Example

IP Host Address: 192.168.5.121
Subnet Mask: 255.255.255.248

	Network	Network	Network	Subnet	Host
192.168.5.121:	11000000	10101000	00000101	01111001	
255.255.255.248:	11111111	11111111	11111111	11111000	
Subnet:	11000000	10101000	00000101	01111000	
Broadcast:	11000000	10101000	00000101	01111111	

Subnet Address = 192.168.5.120
Host Addresses = 192.168.5.121–192.168.5.126
Broadcast Address = 192.168.5.127
Five Bits of Subnetting

Answers

Address	Subnet Mask	Class	Subnet	Broadcast
201.222.10.60	255.255.255.248	C	201.222.10.56	201.222.10.63
15.16.193.6	255.255.248.0	A	15.16.192.0	15.16.199.255
128.16.32.13	255.255.255.252	B	128.16.32.12	128.16.32.15
153.50.6.27	255.255.255.128	B	153.50.6.0	153.50.6.127

WireShark Lab 0 – Getting Started

One's understanding of network protocols can often be greatly deepened by "seeing protocols in action" and by "playing around with protocols" – observing the sequence of messages exchanged between two protocol entities, delving down into the details of protocol operation, and causing protocols to perform certain actions and then observing these actions and their consequences. You'll be running various network applications in different scenarios using a computer on your desk, at home, or in a lab. You'll observe the network protocols in your computer "in action," interacting and exchanging messages with protocol entities executing elsewhere in the Internet. Thus, you and your computer will be an integral part of these "live" labs. You'll observe, and you'll learn, by doing.

The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer**. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer(s); it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a *copy* of packets that are sent/ received from/by application and protocols executing on your machine.

Fig. 1 shows the structure of a packet sniffer. At the right of Fig. 1 are the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client) that normally run on your computer. The packet sniffer, shown within the dashed rectangle in Fig. 1 is an addition to the usual software in your computer, and consists of two parts. The **packet capture library** receives a copy of every link-layer frame that is sent from or received by your computer. Recall that messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable. In Fig. 1, the assumed physical media is an Ethernet, and so all upper layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you all messages sent/received from/by all protocols and applications executing in your computer.

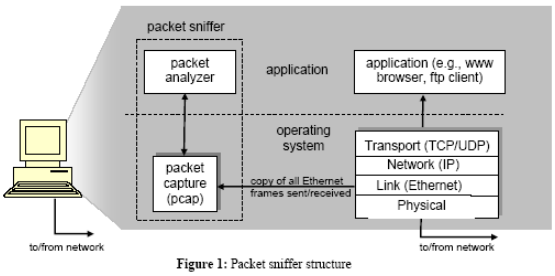


Figure 1: Packet sniffer structure

The second component of a packet sniffer is the **packet analyzer**, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must "understand" the structure of all messages exchanged by protocols. For example, suppose we are interested in displaying the various fields in messages exchanged by HTTP in Fig. 1. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It understands the IP datagram format, so that it can extract the TCP segment within the IP datagram. It understands the TCP segment structure, so it can extract the HTTP message contained in the TCP segment. Finally, it understands HTTP and so, knows that the first bytes of an HTTP message will contain the string "GET," "POST," or "HEAD," headers.

We will use the WireShark packet sniffer (*www.wireshark.org*) for these labs, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack. WireShark is a free network protocol analyzer that runs on Windows, Linux, and Mac computers. It's an ideal packet analyzer for these labs – it is stable, has a large user base and good support with a user guide (*www.wireshark.org/docs/wsug_html*), man pages (*www.wireshark.org/docs/man-pages/*), FAQ (*www.wireshark.org/faq.html*), rich functionality that includes the capability to analyze over 500 protocols, and a well-designed user interface. It operates in computers using Ethernet to connect to the Internet, as well as so-called point-to-point protocols such as PPP.

Getting WireShark

Download WireShark from http://www.rishiheerasing.net/Network.Tools/WireShark/Wireshark-win64-1.10.5.exe on your computer.
Note: Ensure that you install the WinPcap 4.0 packet capture library if it is not already present on your machine. Please start WinPcap NPF as a service as well.

Running WireShark

When you run the WireShark program, the WireShark graphical user interface shown in Figure 2 will be displayed. Initially, no data will be displayed in the various windows.

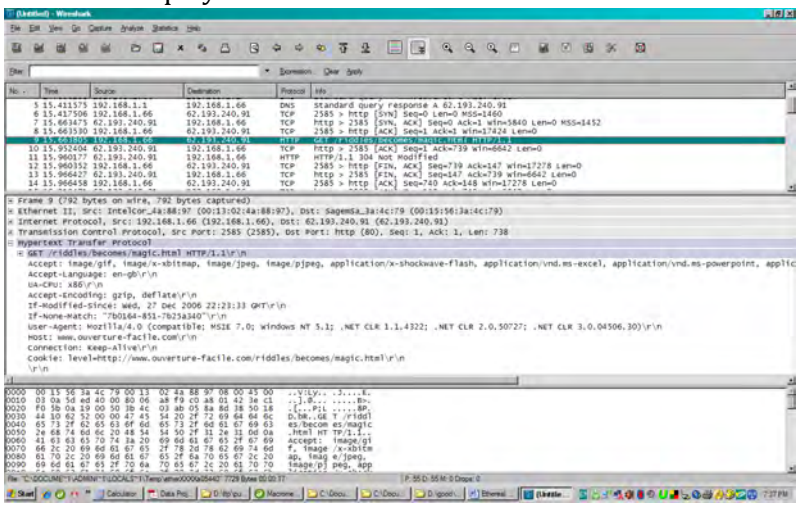


Figure 2

The WireShark interface has 5 major components:

• The **command menus** are standard pull-down menus located at the top of the window. The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exit the WireShark application. The Capture menu allows you to begin packet capture.

• The **packet-listing window** displays a one-line summary for each packet captured, including the packet number (assigned by WireShark; this is *not* a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest level protocol that sent or received this packet.

• The **packet-header details window** provides details about the packet selected (highlighted) in the packet listing window. (To select a packet in the packet listing window, place the cursor over the packet's one-line summary in the packet listing window and click with the left mouse button.). These details include information about the Ethernet frame and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the crosshairs to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, these can similarly be expanded or minimized. Finally, details about the highest level protocol that sent or received this packet are also provided.

• The **packet-contents window** displays the contents of the captured frame in ASCII & Hex.

• Towards the top of the WireShark graphical user interface, is the **packet display filter field,** into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have WireShark hide (not display) packets except those that correspond to HTTP messages.

Taking WireShark for a Test Run

The best way to learn about any new piece of software is to try it out! Do the following:

1. Start up your favorite web browser, which will display your selected homepage.

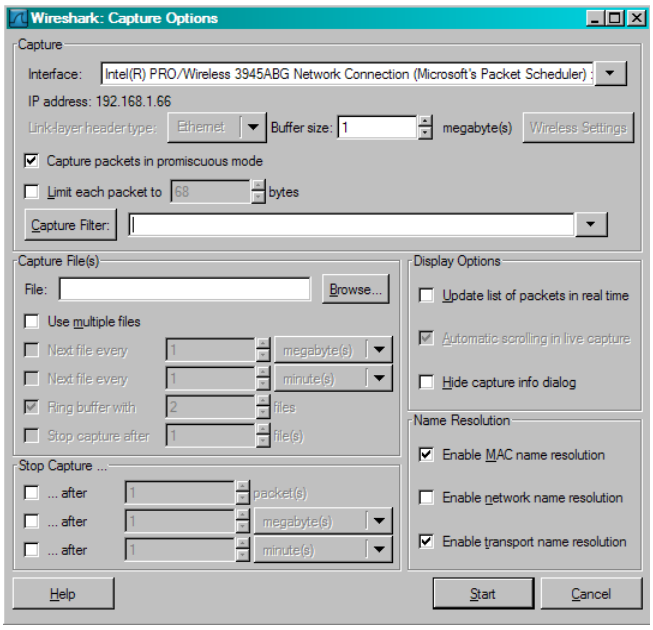


Figure 3

2. Start up the WireShark software.

3. To begin packet capture, select the *List the available capture interfaces…* icon on the far-left menu bar and choose the interface (usually there will only be one interface with an IP address like 172.16.x.x) and Click on *Capture*.

4. You can also the select the second-most icon to the left of the menu bar. This will cause the "WireShark: Capture Options" window to be displayed, as shown in the Fig. 3. You then select the appropriate interface (in case your computer has got 2 network cards) and click on *Start*. Please uncheck the first and last *Display Options* checkboxes.

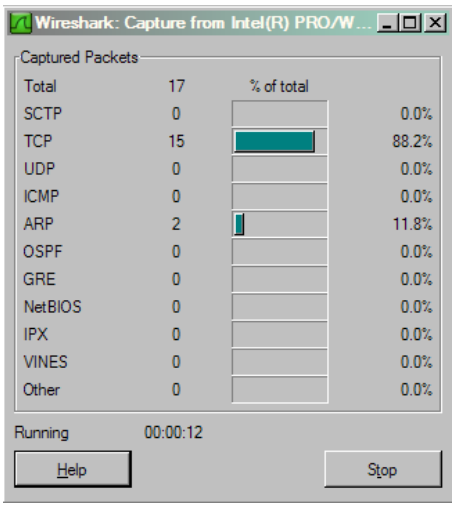


Figure 4

5. Once you begin packet capture, a packet capture summary window will appear, as shown in Figure 4. This window summarizes the number of packets of various types that are being captured, and contains the *Stop* button that will allow you to stop packet capture. Don't stop packet capture yet.

6. While WireShark is running, enter the URL: http://www.fscmauritius.org and have that page displayed in your browser. In order to display this page, your browser will contact the "HTTP" server at www.fscmauritius.org and exchange HTTP messages with the server in order to download this page. The Ethernet frames containing these HTTP messages will be captured by WireShark.

7. After your browser has displayed the FSC homepage, stop WireShark packet capture by selecting ***Stop*** in the WireShark capture window. This will cause the WireShark capture window to disappear and the main WireShark window to display all packets captured since you began packet capture. The main WireShark window should now look similar to Fig. 2. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanged with the "FSC web server" should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well (e.g., the many different protocol types shown in the *Protocol* column in Fig. 2). Even though the only action you took was to download a web page, there were evidently many other protocols running on your computer that are unseen by the user.
8. Type in "http" (without the quotes, and in lower case – all protocol names are in lower case in WireShark) into the display filter specification window at the top of the main WireShark window. Then select *Apply* (to the right of where you entered "http"). This will cause only HTTP message to be displayed in the packet-listing window.

9. Select the first http message shown in the packet-listing window. This should be the HTTP GET message that was sent from your computer to the "www.fscmauritius.org" HTTP server. When you select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window. By clicking on the crosshairs to the left side of the packet details window, *minimize* the amount of Frame, Ethernet, Internet Protocol, and Transmission Control Protocol information displayed. *Maximize* the amount information displayed about the HTTP protocol. Your WireShark display should now look roughly as shown in Fig. 2 (Note, in particular, the minimized amount of protocol information for all protocols except HTTP, and the maximized amount of protocol information for HTTP in the packet-header window).

10. Exit WireShark.

Congratulations! You've now completed the first lab.

What to hand in

The goal of this first lab was primarily to introduce you to WireShark. The following questions will demonstrate that you've been able to get WireShark up and running, and have explored some of its capabilities.

Answer the following questions, based on your WireShark experimentation:

1. Screen-capture the HTTP protocols that appear in the protocol column in the filtered packet-listing window in step 8 above.

2. How long did it take from when the first HTTP GET message was sent until the respective HTTP response was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since WireShark tracing began. To display the Time field in time-of-day format, select the WireShark *View* pull-down menu, then select Time *Display Format*, then select *Time-of-day)*.

3. Why is the HTTP response code not "200 OK" as you would expect?

4. What is the actual HTTP response code received and what does this code mean?

5. What is therefore the Internet address of the actual server where the FSC homepage resides?

6. What is the Internet address of your computer?

7. What did your browser do before the first HTTP GET message was sent to the web server?

8. Why were more GET messages needed to display the FSC homepage?

WireShark Lab 1 – HTTP

Having gotten our feet wet with the WireShark packet sniffer in the introductory lab, we're now ready to use WireShark to investigate protocols in operation. In this lab, we'll explore several aspects of the HTTP protocol: the basic GET response interaction, HTTP message formats, retrieving large HTML files, retrieving HTML files with embedded objects, and HTTP authentication and security.

1. The Basic HTTP GET response interaction

Let's begin our exploration of HTTP by downloading a very simple HTML file - one that is very short, and contains no embedded objects. Do the following:
1. Start up your web browser.
2. Start up the WireShark packet sniffer, as described in the introductory lab (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
3. Enter the following to your browser *http://pages.intnet.mu/rhh/wireshark/file1.html*
Your browser should display the very simple, one-line HTML file.
5. Stop WireShark packet capture.
Your WireShark window should look similar to the window shown in Fig. 1.

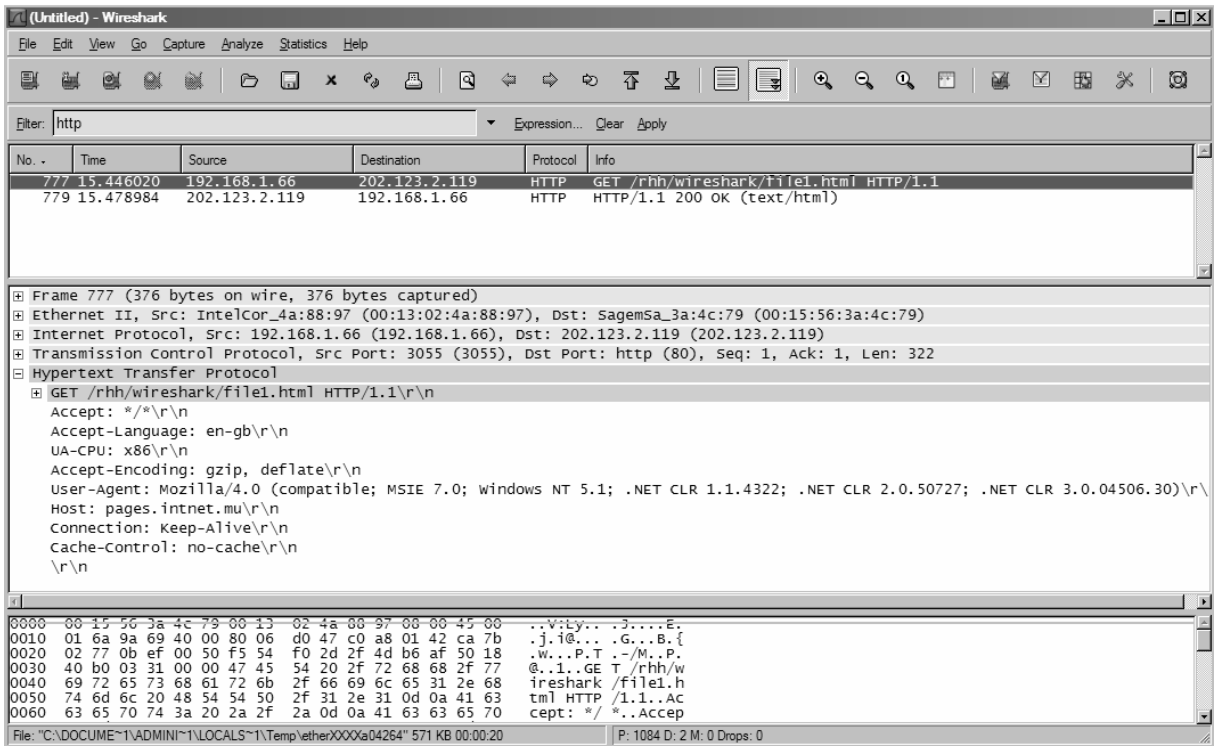


Fig. 1

The example in Fig. 1 shows in the packet-listing window that two HTTP messages were captured: the GET message (from your browser to the *pages.intnet.mu* web server) and the response message from the server to your browser. The packet-contents window shows details of the selected message (in this case the HTTP GET message, which is highlighted in the packet-listing window). Recall that since the HTTP message was carried inside a TCP segment, which was carried inside an IP datagram, which was carried within an Ethernet frame, WireShark

displays the Frame, Ethernet, IP, and TCP packet information as well. We want to minimize the amount of non-HTTP data displayed (we are interested in HTTP here, and will be investigating the other protocols is later labs), so make sure the boxes at the far left of the Frame, Ethernet, IP and TCP information have an crosshair (meaning there is hidden, not displayed information), and the HTTP line has a minus (all information about the HTTP message is displayed).
By looking at the information in the HTTP request/response messages, **answer the following questions**. When answering the following questions, you should print out the request/response messages (see the WireShark Lab 0 for an explanation of how to do this) and indicate where in the message you've found the information.

1. Is your browser running HTTP version 1.0 or 1.1?

2. Which version of HTTP is the server running?

3. What languages (if any) does your browser indicate that it can accept to the server?

4. What is the IP address of your computer? Of the *pages.intnet.mu* server?

5. What is the status code returned from the server to your browser?

6. When was the HTML file you just retrieved last modified on the server?

7. How many bytes of content are being returned to your browser?

2. The HTTP CONDITIONAL GET/response interaction

Recall that most web browsers perform object caching and thus perform a conditional GET when retrieving an HTTP object. Before performing the steps below, make sure your browser's cache is empty. (For Internet Explorer, select *Tools->Internet Options->Delete File;* these actions will remove cached files from your browser's cache.) Now do the following:

• Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
• Start up the WireShark packet sniffer
• Enter the following URL into your browser *http://pages.intnet.mu/rhh/wireshark/file2.html*
Your browser should display a very simple one line HTML file.
• Quickly enter the same URL into your browser again (or simply select the Refresh button on your browser or press F5).
• Stop WireShark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

Answer the following questions:

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

3. Retrieving Long Documents

In our examples thus far, the documents retrieved have been simple and short HTML files. Let's next see what happens when we download a long HTML file. Do the following:
• Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
• Start up the WireShark packet sniffer
• Enter the following URL into your browser *http://pages.intnet.mu/rhh/WireShark/file3.html*
Your browser should display the rather lengthy UTM Act 2002.
• Stop WireShark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.
In the packet-listing window, you should see your HTTP GET message, followed by a multiple-packet response to your HTTP GET request. This multiple-packet response deserves a bit of explanation. Recall that the HTTP response message consists of a status line, followed by header lines, followed by a blank line, followed by the entity body. In the case of our HTTP GET, the entity body in the response is the *entire* requested HTML file. In our case here, the HTML file is rather long, and at 45,652 bytes is too large to fit in one TCP packet. The single HTTP response message is thus broken into several pieces by TCP, with each piece being contained within a separate TCP segment. Each TCP segment is recorded as a separate packet by WireShark, and the fact that the single HTTP response was fragmented across multiple TCP packets is indicated by the "Continuation" phrase displayed by WireShark.

Answer the following questions:

12. How many HTTP GET request messages were sent by your browser?

13. How many data-containing TCP segments were needed to carry the single HTTP response?

14. What is the status code and phrase associated with the response to the HTTP GET request?

15. Are there any HTTP status lines in the data associated with a TCP induced "Continuation"?

4. HTML Documents with Embedded Objects

Now that we've seen how WireShark displays the captured packet traffic for large HTML files, we can look at what happens when your browser downloads a file with embedded objects, i.e., a file that includes other objects (e.g. image files) that are stored on another server(s).
Do the following:
• Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
• Start up the WireShark packet sniffer.
• Enter the following URL into your browser *http://pages.intnet.mu/rhh/index.htm*
Your browser should display my website with an external link to *www.mauritiustopsites.com*.
The two images themselves are not contained in the HTML; instead the URLs for the images are contained in the *style.css* file. Your browser will get these two gifs from the indicated web sites.
• Stop WireShark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.
(*Note:* You should ignore any HTTP GET and response for myicon.ico. If you see a reference to this file, it is your browser automatically asking the server if it has a small icon file (Nefertum) that is displayed next to the URL in the address bar).

Answer the following question:

16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?

5 HTTP Authentication

Finally, let's try visiting a web page that is password-protected and examine the sequence of HTTP message exchanged for such a site. The URL *http://172.16.16.66/wireshark/file4.aspx* is password protected. The username is "CNDM" (without the quotes), and the password is "wiresh@rk" (again, without the quotes). So let's access this "secure" password-protected page.

Do the following:
• Make sure your browser's cache is cleared, as discussed above, and close down your browser. Then, start up your browser
• Start up the WireShark packet sniffer
• Enter the following URL into your browser *http://172.16.16.66/WireShark/file4.aspx*
Type the requested user name and password into the form. You will be brought to the *file4.aspx* page otherwise an error message will appear if you type the username/password incorrectly.
• Stop WireShark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.
Now let's examine the WireShark output.

Answer the following questions:

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

19. Why and where does your browser send the second HTTP GET message?

20. Why are 3 HTTP GET messages needed while requesting only a single page with no external referencing objects?

The username (CNDM) and password (wiresh@rk) that you entered can be found in the HTTP POST message sent to my server. If you scroll down in the contents window at the bottom, you will find the username and password in CLEAR !!!

Wireshark Lab 2 – Ethernet ARP

In this lab, we'll investigate the Ethernet protocol and the ARP protocol. Before beginning this lab, you'll probably want to review details of the ARP protocol, which is used by a device to determine the Ethernet address of a remote interface whose IP address is known.

1. Capturing and analyzing Ethernet frames

Let's begin by capturing a set of Ethernet frames to study. Do the following:
• First, make sure your browser's cache is empty. (Select *Tools->Internet Options->Delete Files)*
• Start up the Wireshark packet sniffer
• Enter the following URL into your browser *http://pages.intnet.mu/rhh/wireshark/file3.html*
• Stop Wireshark packet capture. First, note down the packet numbers (the leftmost column in the upper Wireshark window) of the HTTP GET message that was sent from your computer to *pages.intnet.mu*, as well as the first of the HTTP response message sent back to you. You should see a screen like Fig. 1 (where packet 5 in ***my screenshot*** contains the HTTP GET message).

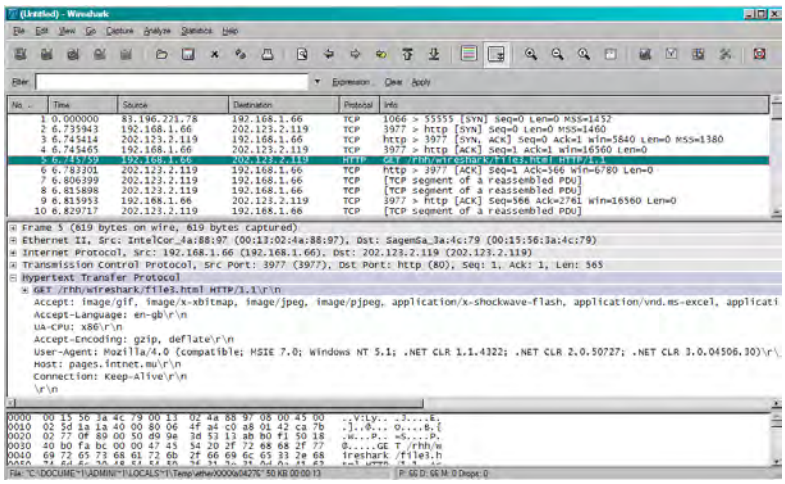


Fig. 1

Since this lab is about Ethernet and ARP, we're not interested in IP or higher layer protocols. So let's change Wireshark's "listing of captured packets" window so that it shows information only about protocols below IP. To have Wireshark do this, select *Analyze->Enabled Protocols.* Then uncheck the IP box and select *OK*. You should now see a Wireshark window that looks like this:

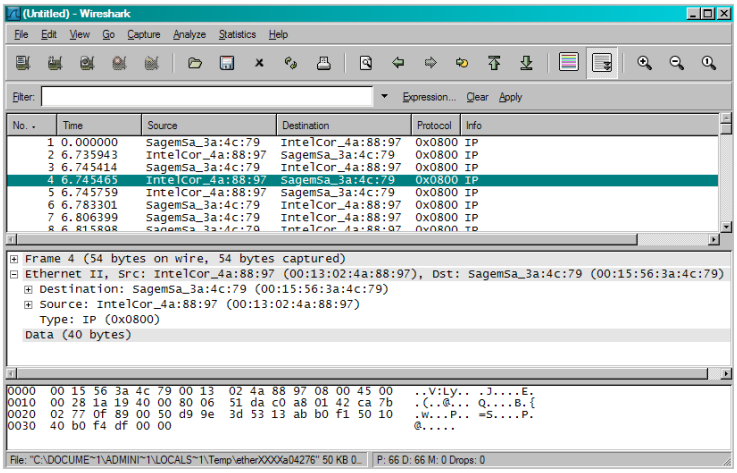


Fig. 2

In order to answer the following questions, you'll need to look into the packet details and packet contents windows (the middle and lower display windows in Wireshark).

Select the Ethernet frame containing the HTTP GET message. (Recall that the HTTP GET message is carried inside of a TCP segment, which is carried inside of an IP datagram, which is carried inside of an Ethernet frame). Expand the Ethernet II information in the packet details window. Note that the contents of the Ethernet frame (header as well as payload) are displayed in the packet contents window.

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message. Whenever possible, when answering a question you should include a screenshot of the packets captured that you used to answer the question asked.

1. What is the 48-bit Ethernet address of your computer?

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of *pages.intnet.mu*? (Hint: the answer is *No*). Which device has this as its Ethernet address? [Note: this is an important question and one that students sometimes get wrong]

3. Give the hexadecimal value for the two-byte Frame type field. What does this value mean?

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

5. What is the value of the Ethernet source address? Is this the address of your computer, or of *pages.intnet.mu*? (Hint: the answer is *No*). What device has this as its Ethernet address?

6. What is the Ethernet destination address? Is this the Ethernet address of your computer?

7. Give the hexadecimal value for the two-byte Frame type field. What does this mean?

8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

2. The Address Resolution Protocol

In this section, we'll observe the ARP protocol in action. I strongly recommend that you refresh yourself on this topic before proceeding.

ARP Caching

Recall that the ARP protocol typically maintains a cache of IP-to-Ethernet address translation pairs on your comnputer The *arp* command (in both MSDOS and Linux/Unix) is used to view and manipulate the contents of this cache. Since the *arp* command and the ARP protocol have the same name, it's understandably easy to confuse them. But keep in mind that they are different - the *arp* command is used to view and manipulate the ARP cache contents, while the ARP protocol defines the format and meaning of the messages sent and received, and defines the actions taken on message transmission and receipt.

Let's take a look at the contents of the ARP cache on your computer:
• **MS-DOS.** Open a Command Prompt Window by typing *File->Run* and enter *cmd* then at the prompt enter *arp –a* and press Enter.
The *arp –a* command will display the contents of the ARP cache on your computer.

11. Write down the contents of your computer's ARP cache. What is the meaning of each column value?

In order to observe your computer sending and receiving ARP messages, we'll need to clear the ARP cache, since otherwise your computer is likely to find a needed IP-Ethernet address translation pair in its cache and consequently not need to send out an ARP message.

• **MS-DOS.** The MS-DOS *arp –d ** command will clear your ARP cache. The *–d* flag indicates a deletion operation, and the * is the wildcard that says to delete all table entries.

Observing ARP in action

Do the following:
• Clear your ARP cache, as described above.
• Next, make sure your browser's cache is empty. (select *Tools->Internet Options->Delete Files.)*
• Start up the Wireshark packet sniffer
• Enter the following URL into your browser *http://pages.intnet.mu/rhh/wireshark/file3.html*
Your browser should again display the rather lengthy UTM Act 2002.
• Stop Wireshark packet capture. Again, we're not interested in IP or higher-layer protocols, so change Wireshark's "listing of captured packets" window so that it shows information only about protocols below IP. To have Wireshark do this, select *Analyze->Enabled Protocols.* Then uncheck the IP box and select *OK*. You should now see a Wireshark window that looks like:

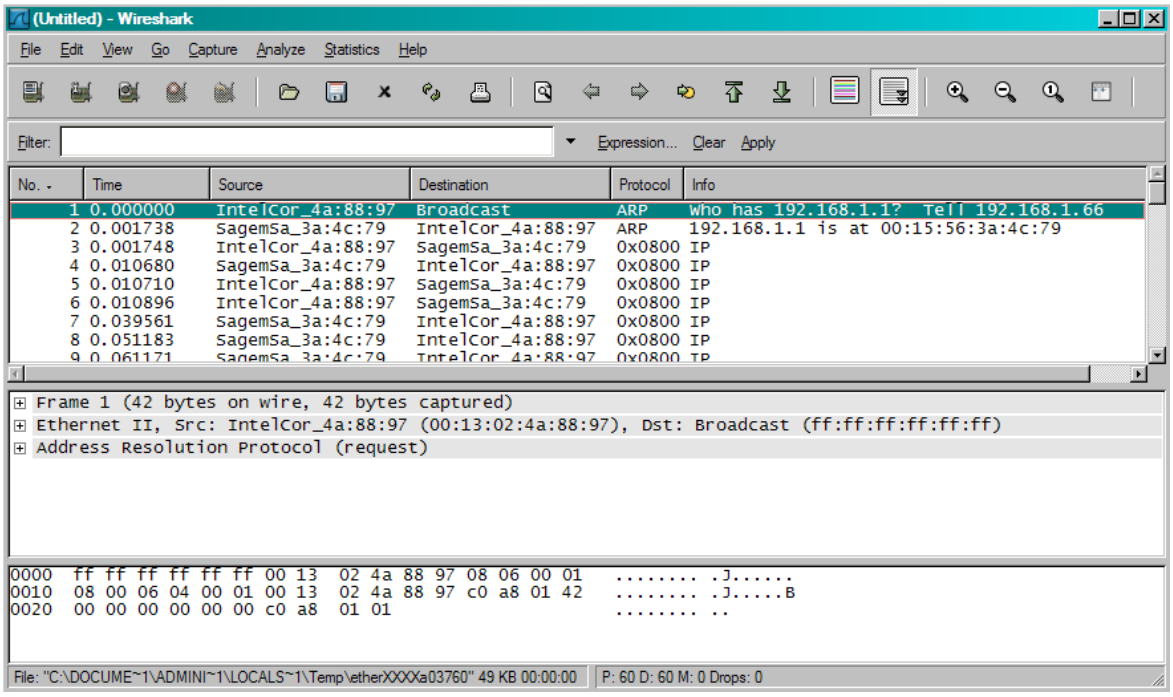


Fig. 3

In the example above, the first two frames in the capture contain ARP messages.

Answer the following questions:

12. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

13. Give the hexadecimal value for the two-byte Ethernet Frame type field. What does this mean?

14. Download the ARP specification from http://www.networksorcery.com/enp/protocol/arp.htm

a) How many bytes from the beginning of the Ethernet frame does the ARP *opcode* field begin?

b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

c) Does the ARP message contain the IP address of the sender?

d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

15. Now find the ARP reply that was sent in response to the ARP request.

a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

c) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

16. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

Extra Credit

EX-1. The *arp* command:

arp -s InetAddr EtherAddr

allows you to manually add an entry to the ARP cache that resolves the IP address *InetAddr* to the physical address *EtherAddr*. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

EX-2. What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.

LAB 3 – Basic Switch Configuration Commands

This lab explains basic switch configuration commands in detail with examples. Configuration and commands explained in this tutorial are essential commands to manage a Cisco switch effectively.

Packet tracer network simulator software will be used to explain basic switch configuration commands. You can use any network simulator software like GNS3 or can use a real Cisco switch to follow this lab. There is no difference in output as long as your selected software contains the commands explained in this tutorial.

Create a practice lab as shown in following figure:

In this topology

- Two 2960 Series switches are used.
- Switch1 (Interface Gig1/1) is connected with Switch2 (Interface Gig1/1) via cross cable.
- Switch1 has two PCs connected on interfaces Eth0/1 and Eth0/2 via straight through cable.
- Same as switch1, Switch2 also has two PCs connected on its interfaces Eth0/1 and Eth0/2.
- IP address is configured on all PCs PC0 (192.168.1.1/24), PC1 (192.168.1.2/24), PC2 (192.168.1.3/24), PC3 (192.168.1.4/24).

Click *Switch1* and click *CLI* menu item and press *Enter Key.*

Cisco Switch command modes

Cisco switch runs on proprietary OS known as Cisco IOS. IOS is a group of commands used for monitoring, configuring and maintaining Cisco devices. For security and easy administration, IOS commands are divided in the set of different command modes. Each command mode has its own set of commands. Which commands are available to use, depend upon the mode we are in.

Mode	Purpose	Prompt	Command to enter	Command to exit
User EXEC	Allow you to connect with remote devices, perform basic tests, temporary change terminal setting and list system information	Router >	Default mode after booting. Login with password, if configured.	Use **exit** command
Privileged EXEC	Allow you to set operating parameters. It also includes high level testing and list commands like show, copy and debug.	Router #	Use **enable** command from user exec mode	Use **exit** command
Global Configuration	Contain commands those affect the entire system	Router(config)#	Use **configure terminal** command from privileged exec mode	Use **exit** command
Interface Configuration	Contain commands those modify the operation of an interface	Router(config-if)#	Use **interface *type number*** command from global configuration mode	Use **exit** command to return in global configuration mode

Mode	Purpose	Prompt	Command to enter	Command to exit
Sub-Interface Configuration	Configure or modify the virtual interface created from physical interface	Router(config-subif)	Use **interface *type sub interface*** number command from global configuration mode or interface configure mode	Use **exit** to return in previous mode. Use **end** command to return in privileged exec mode.
Setup	Used by router to create initial configuration, if running configuration is not present	Parameter[Parameter value]:	Router will automatically insert in this mode if running configuration is not present	Press `CTRL+C` to abort. Type `Yes` to save configuration, or `No` to exit without saving when asked in the end of setup.
ROMMON	If router automatically enter in this mode, then it indicates that it fails to locate a valid IOS image. Manual entrance in this mode Allow you to perform low-level diagnostics.	ROMMON>	Enter **reload** command from privileged exec mode. Press `CTRL + C` key combination during the first 60 seconds of booting process	Use **exit** command.

How to get help on Cisco Switch command mode

Switch provides two types of context sensitive help, word help and command syntax help.

Word help

Word help is used to get a list of available commands that begin with a specific letter. For example if we know that our command begins with letter **`t`**, we can hit enter key after typing **`t?`** at command prompt. It will list all possible commands that begin with letter **`t`**.

```
Switch>t?
telnet  terminal  traceroute
Switch>t
```

We can list all available commands, if we don't know the initials of our command. For example to list all available commands at User exec mode, just type **`?`** at command prompt and hit enter key.

```
Switch>?
Exec commands:
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
Switch>
```

Command syntax help

Command syntax help can be used to get the list of keyword, commands, or parameters that are available starting with the keywords that we had already entered. Enter **`?`** (Question mark) after hitting Space key and

prompt will return with the list of available command options. For example to know the parameters required by show ip command type **`show ip ?`** and prompt will return with all associate parameters. If prompt returns with **`<CR>`** only as an option, that means switch does not need any additional parameters to complete the command. You can execute the command in current condition.

```
Switch>show ip ?
  arp         IP ARP table
  dhcp        Show items in the DHCP database
  interface   IP interface status and configuration
  ssh         Information on SSH
Switch>show ip arp ?
  <cr>
Switch>show ip arp
```

How to set name on switch

Switch name can be set from global configuration mode. Use **`hostname [`*`desired hostname`*`]`** command to set name on switch. TAB key can be pressed to auto-complete possible command.

```
Switch>enable
Switch#conf
Switch#configure ter
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#
SW1(config)#
```

How to set password on a Catalyst switch

Passwords are used to restrict physical access to switch. Cisco switch supports console line for local login and VTYs for remote login. All supported lines need be secure for User Exec mode. For example if you have secured VTYs line leaving console line unsecure, an intruder can take advantage of this situation in connecting with device. Once you are connected with device, all remaining authentication are same. No separate configuration is required for further modes.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line console 0
Switch(config-line)#password con1234
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line vty 0 15
Switch(config-line)#password telnet1234
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#
```

CONSOLE

VTY

Password can be set from their respective line mode. Enter in line mode from global configuration mode. VTY term stand for virtual terminal such as telnet or SSH. Switch may support up to thousand VTYs lines. By default, the first five (0 - 4) lines are enabled. If we need more lines, we have to enable them manually. 2960 Series switch supports 16 lines. We can set a separate password for each line, for that we have to specify the number of the line. In the example above, we have set a common password `"telnet1234"` for all lines.

Above method is good for small companies, where there are a few network administrators. In above method, a password is shared among all administrators. The switch supports both local and remote server authentication. Remote server authentication is a complex process. In local database authentication method, the switch allows us to set a separate password for each user. Two global configuration commands are used to set local user database.

```
Switch(config)#username [Username] password[test123]
```

Or

```
Switch(config)#username [Username] secret[test123]
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#username rishi password test123
Switch(config)#line console 0
Switch(config-line)#login local
Switch(config-line)#exit
Switch(config)#exit
```

Both commands do same job. Advantage of using **secret** option over **password** option is that in **secret** option password is stored in MD5 encryption format while in **password** option password is stored in plain text format.

Along with User Exec mode we can also secure Privilege Exec mode. Two commands are available for it.

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

Again as mentioned earlier, password stored with **secret** command is encrypted while password stored with **password** command remains in plain text. You only need to use single command. If you would use both commands as above, **enable secret** command would automatically replace the **enable password** command.

How to reset switch to factory defaults

During the practice several times we have to reset switch to factory defaults. Make sure you don't runfollowing commands in production environment unless you understand their effect clearly. Following commands will erase all configurations. In production environment you should always takes backup before removing configurations. In LAB environment we can skip backup process.

```
Switch>enable
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?              [Press Enter Key]
Delete flash:vlan.dat? [confirm]         [Reconfirm by pressing enter key]
Switch#erase startup-config
Switch#reload
```

How to set IP address in Switch

IP address is the address of device in network. Switch allows us to set IP address on interface level. IP address assigned on interface is used to manage that particular interface. To manage entire switch we have to assign IP address to **`VLAN1`** (Default VLAN of switch). We also have to set default gateway IP address from global configuration mode. In following example we would assign **`IP 172.16.10.2 255.255.255.0`** to **`VLAN1`** and set default gateway to **`172.16.10.1`**.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip address 172.16.10.2 255.255.255.0
Switch(config-if)#exit
Switch(config)#ip default-gateway 172.16.10.1
```

How to set interface description

Switches have several interfaces. Adding description to interface is a good habit. It may help you in finding correct interface. In following example we would add description *Development VLAN* to interface *FastEthernet 0/1*.

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#description Development VLAN
```

How to clear mac address table

Switch stores MAC addresses in MAC address table. Gradually it could be full. Once it full, switch automatically starts removing old entries. You can also clear these tables manually from privileged exec mode. To delete all entries use following command:

```
switch# clear mac address-table
```

To delete only dynamic entries, type s**witch# clear mac address-table dynamic**

How to add static MAC address in CAM table

For security purpose sometime we have to add mac address in CAM table manually. To add static MAC address in CAM table use following command

```
Switch(config)#mac address-table static aaaa.aaaa.aaaa vlan 1 interface
fastethernet 0/1
```

In the above command we entered an entry for static MAC address **aaaa.aaaa.aaaa** assigned to **FastEnternet 0/1** with default **VLAN1**.

How to save running configuration in switch

Switch keeps all running configuration in RAM. All data from RAM is erased when we turned off the device. To save running configuration use following command

```
Switch# copy running-config startup-config
```

How to set duplex mode

Switch automatically adjust duplex mode depending upon remote device. We could change this mode with any of other supported mode. For example to force switch to use full duplex mode use

```
Switch(config)# #interface fastethernet 0/1
Switch(config-if)# duplex full
```

To use half duplex use

```
Switch(config)# #interface fastethernet 0/1
Switch(config-if)#duplex half
```

show version

`show version` command provides general information about device including its model number, type of interfaces, its software version, configuration settings, location of IOS and configuration files and available memories.

```
Switch>show version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE
SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
Image text-base: 0x80010000, data-base: 0x80562000

ROM: Bootstrap program is is C2950 boot loader
Switch uptime is 27 minutes, 33 seconds
System returned to ROM by power-on

Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of memory.
Processor board ID FHK0610Z0WC
Last reset from system-reset
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 0004.9A69.4C0A
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: FOC061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0610Z0WC
Configuration register is 0xF

Switch>
```

show mac-address-table

Switch stores MAC address of devices those are attached with its interfaces in CAM table. We can use *show mac-address-table* command to list all learned devices. Switch uses this table to make forward decision.

```
Switch>show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0c2d.7635    DYNAMIC     Fa0/2
   1    0000.0c6d.ceb1    DYNAMIC     Fa0/3
   1    0004.9ab1.4326    DYNAMIC     Fa0/4
   1    0060.5c62.ced0    DYNAMIC     Fa0/1
Switch>
```

show flash

Switch stores IOS image file in flash memory. **`show flash`** command will list the content of flash memory. This command is useful to get information about IOS file and available memory space in flash.


```
Switch>enable
Switch#show flash
Directory of flash:/

    1  -rw-     3058048          <no date>  c2950-i6q412-mz.121-22.EA4.bin

64016384 bytes total (60958336 bytes free)
Switch#
```

show running-config

Configuration parameter values are created, stored, updated and deleted from running configuration. Running configuration is stored in RAM. We can use **`show running-config`** command to view the running configuration.

```
Switch>enable
Switch#show running-config
Building configuration...

Current configuration : 990 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 duplex half
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
```

show startup-config

Any configuration stored in RAM is erased when devices is turned off. We can save running configuration in NVRAM. If we have saved running configuration in NVRAM, it would be automatically loaded back in RAM from NVRAM during the next boot. As switch load this configuration back in RAM in startup of device, at NVRAM it is known as startup-config.

show vlan

show vlan command will display the VLANs. For administrative purpose, switch automatically create VLAN 1 and assign all its interfaces to it. You can create custom VLANs from global configuration mode and then assign them to interfaces.

```
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
17   Outcast                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```


show interface

`show interface` command displays information about interfaces. Without argument it would list all interfaces. To get information about specific interface we need to pass its interface number as an argument. For example to view details about **`FastEthernet 0/1`**, use **`show interface fastethernet 0/1`**.

```
Switch#show interface fastethernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0010.11dc.8101 (bia 0010.11dc.8101)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
```

First line from output provides information about the status of interface.

FastEthernet0/1 is up, line protocol is up (connected)

The first up indicates the status of the physical layer, and second up indicates the status of the data link layer.

Possible interface status

- **up and up :-** Interface is operational.
- **up and down :-** Data link layer problem.
- **down and down :-** Physical layer problem.
- **Administratively down and down :-** Interface is disabled with shutdown command.

Possible values for physical layer status

- **Up :-** Switch is sensing physical layer signal.
- **Down :-** Switch is not sensing physical layer signal. Possible reasons could be cable is not connected, wrong cable type is used and remote end device is turned off.
- **Administratively down :-** Interface is disabled by using shutdown command.

Possible values for data link layer status

- **Up :-** The data link layer is operational.
- **Down :-** The data link layer is not operational. Possible reasons could be a disabled physical layer, missed keep alives on a serial link, no clocking or an incorrect encapsulation type.

show ip interface brief

```
Switch>enable
Switch#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/1        unassigned      YES manual up                    up

FastEthernet0/2        unassigned      YES manual up                    up

FastEthernet0/3        unassigned      YES manual up                    up

FastEthernet0/4        unassigned      YES manual up                    up

FastEthernet0/5        unassigned      YES manual down                  down

FastEthernet0/6        unassigned      YES manual down                  down

FastEthernet0/7        unassigned      YES manual down                  down

FastEthernet0/8        unassigned      YES manual down                  down
```

show ip interface brief is a extremely useful command to get quick overview of all interfaces on switch. It lists their status including IP address and protocol.

LAB 3 – VLAN : VTP : DTP : STP

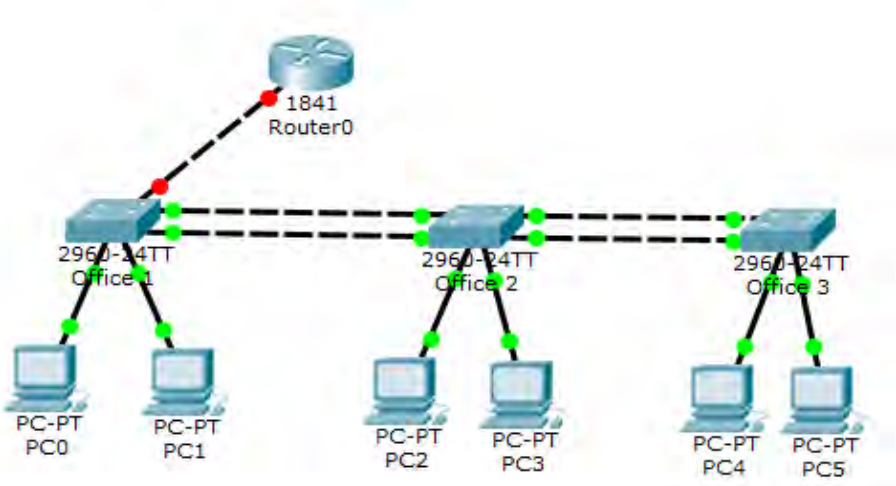
This lab explains how to use Packet Tracer for the practice of VLAN Configuration, VTP Server and Client configuration, DTP configuration, STP Configuration, Intra VLAN communication and Router on Stick Configuration.

Section A

Scenario and Initial Setup

A company has three offices which are all connected via layer 2 links. For redundancy purpose, each office has one more layer 2 link. The company has two departments: Sales & Management. In each office, we have one PC from each department. The Ethernet port of a router is used for inter VLAN communication.

Create a topology in packet tracer, as shown below:



PCs Configuration

Device	IP Address	Subnet Mask	Gateway	VLAN	Connected With
PC0	10.0.0.2	255.0.0.0	10.0.0.1	VLAN 10	Office 1 Switch on F0/1
PC1	20.0.0.2	255.0.0.0	20.0.0.1	VLAN 20	Office 1 Switch on F0/2
PC2	10.0.0.3	255.0.0.0	10.0.0.1	VLAN 10	Office 2 Switch on F0/1
PC3	20.0.0.3	255.0.0.0	20.0.0.1	VLAN 20	Office 2 Switch on F0/2
PC4	10.0.0.4	255.0.0.0	10.0.0.1	VLAN 10	Office 3 Switch on F0/1
PC5	20.0.0.4	255.0.0.0	20.0.0.1	VLAN 20	Office 3 Switch on F0/2

Office 1 Switch Configuration

Port	Connected To	VLAN	Link	Status
F0/1	With PC0	VLAN 10	Access	OK
F0/2	With PC1	VLAN 20	Access	OK
Gig0/1	With Router	VLAN 10,20	Trunk	OK
Gig0/2	With Switch2	VLAN 10,20	Trunk	OK
F0/24	With Switch2	VLAN 10,20	Trunk	STP - Blocked

Office 2 Switch Configuration

Port	Connected To	VLAN	Link	Status
F0/1	With PC0	VLAN 10	Access	OK
F0/2	With PC1	VLAN 20	Access	OK
Gig 0/2	With Switch1	VLAN 10,20	Trunk	OK
Gig 0/1	With Switch3	VLAN 10,20	Trunk	OK
F0/24	With Switch1	VLAN 10,20	Trunk	STP - Blocked
F0/23	With Switch3	VLAN 10,20	Trunk	STP - Blocked

Office 3 Switch Configuration

Port	Connected To	VLAN	Link	Status
F0/1	With PC0	VLAN 10	Access	OK
F0/2	With PC1	VLAN 20	Access	OK
Gig 0/1	With Switch2	VLAN 10,20	Trunk	OK
F0/24	With Switch1	VLAN 10,20	Trunk	STP - Blocked

Router Configuration

Port	Connected To	VLAN	Link	Status
Fa0/0	Office 1 Switch Gig 0/1	VLAN 10, 20	Trunk	Ok

VLAN Configuration

VLAN Number	VLAN Name	Gateway IP	PCs
10	Sales	10.0.0.1	PC0,PC2,PC4
20	Management	20.0.0.1	PC1,PC3,PC5

Assign IP Addresses to PCs

Assigning IP addresses is bit easy task in packet tracer. Just double Click on **PC-PT** and Click **Desktop** menu item and Click **IP Configuration** Select **Static** from radio option and fill IP address, subnet mask and default gateway IP in given input boxes. Use PC Configuration table above to assign correct IP address.

Section B

Configuring VTP Server and Client in Switch

This section explains basic concepts of VTP Protocol, VTP Domain, VTP Messages and VTP modes (Server mode, Transparent mode and Client mode) and how to configure VTP Server and VTP Clients.

VLAN Trunk Protocol (VTP) is a Cisco proprietary protocol used to share VLAN configuration across the network. Cisco created this protocol to share and synchronize their VLAN information throughout the network. Main goal of VTP is to manage all configured VLANs across the network.

In our scenario, we have only **3** switches. We can easily add or remove VLAN manually on all three switches. However this process could be more tedious and difficult if we have **50** switches. In a large network, we might make a mistake in VLAN configuration. We might forget to add a VLAN in one of the switch, or we may assign a wrong VLAN number. We may forget to remove a VLAN on one of the switch, whilst removing VLANs.

VTP is a life-saver protocol in this situation. With VTP, we can add or remove VLANs on one switch and this switch will propagate VLAN information to all other switches in network.

VTP Messages

VTP share VLANs information via VTP messages. VTP messages can only be propagate through the **trunk** connections. So we need to set up trunk connection between switches. VTP messages are propagated as layer 2 **multicast** frames.

VTP Domain

VTP domain is a group of switches that share same VLAN information. A switch can have a single domain. VTP messages include domain name. Switch only update VLAN information if it receive VTP message from same domain.

VTP can be configured in three different modes.

1. Server
2. Transparent
3. Client

VTP Server Mode

VTP Server can add, modify, and delete VLANs. It will propagate a VTP message containing all the changes from all of its trunk ports. If server receives a VTP message, it will incorporate the change and forward the message from all remaining trunk ports.

VTP Transparent Mode

VTP Transparent switch can also make change in VLANs but it will not propagate these changes to other switches. If transparent switch receives a VTP message, it will not incorporate the change and forward the message as it receives, from all remaining trunk ports.

VTP Client Mode

VTP client switch cannot change the VLAN configurations itself. It can only update its VLAN configuration through the VTP messages that it receive from VTP server. When it receives a VTP message, it incorporates the change and then forwards it to the remaining trunk ports.

Configuring VTP Server

We will configure **Office 1 Switch** as VTP Server. Double click on **Office 1 Switch** and Click **CLI** menu item and press **Enter key** to start CLI session.

By default all switches work as VTP server so we only need few commands to configure it. In the following commands we will:

- Set hostname to **`S1`**

- Set domain name to **pditn18b**
- Set password to **test1234**. (Password is case-sensitive)

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname S1
S1(config)# vtp mode server
Device mode already VTP SERVER.
S1(config)# vtp domain pditn18b
Changing VTP domain name from NULL to pditn18b
S1(config)# vtp password test1234
Setting device VLAN database password to test1234
```

Configure VTP Client

We will configure Office 2 Switch and Office 3 Switch as VTP client switch. Access **CLI** prompt of **Office 2 Switch** and execute following commands

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname S2
S2(config)# vtp mode client
Setting device to VTP CLIENT mode.
S2(config)# vtp domain pditn18b
Changing VTP domain name from NULL to pditn18b
S2(config)# vtp password test1234
Setting device VLAN database password to test1234
S2(config)#
```

Now access **CLI** prompt of **Office 3 Switch** and enter following commands

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname S3
S3(config)# vtp mode client
Setting device to VTP CLIENT mode.
S3(config)# vtp domain pditn18b
Changing VTP domain name from NULL to pditn18b
S3(config)# vtp password test1234
Setting device VLAN database password to test1234
S3(config)#
```

We have configured VTP server and VTP client. At this moment, VTP client will not receive VTP messages from server. We need to configure DTP between switches.

Section C

This section explains VLAN Tagging, VLAN Trunking protocols (ISL & 802.1Q), DTP Modes (ON, DTP Mode Desirable, Auto, No-Negotiate & OFF) and VLAN Trunk configuration in detail.

In VLAN configuration, a switch port can operate in two mode; access and trunk. In access mode it can carry only single VLAN information while in trunk mode it can carry multiple VLANs information. **Access mode** is used to connect the port with **end devices** while **trunk mode** is used to connect two **switching devices**.

Access Link and Trunk Link

An access link can carry single VLAN information while trunk link can carry multiple VLANs information. Configuring VLANs on single switch does not require trunk link. It is required only when you configure VLANs across the multiple switches.

For example if we do not connect all switches in our network, we do not require to configure the trunk link. In this case PC0, PC2 and PC4 cannot communicate with each other. Although they all belongs to same VLAN group but they have no link to share this information.

Trunk link connections are used to connect multiple switches sharing same VLANs information.

You may think why we cannot use access link to connect these switches. We can use access links to connect switches but we will need to use one separate link for each VLAN. If we have 2 VLANs, we need 2 links.

With this implementation, we need links equal to VLANs that does not scale very well. For example if our design require 30 VLANs, we will have to use 30 links to connect switches.

Summary

- An access link can carry single VLAN information.
- Theoretically, we can use access link to connect switches.
- If we use access link to connect switches, we have to use links equal to VLANs.
- Due to scalability we do not use access link to connect the switches.
- A trunk link can carry multiple VLAN information.
- Practically we use trunk links to connect switches or switches to routers.

VLAN Tagging

Trunk links use VLAN tagging to carry the multiple VLANs traffic separately.

In VLAN tagging process, sender switch add a VLAN identifier header to the original Ethernet frame. Receiver switch read VLAN information from this header and remove it before forwarding to the associate ports. Thus original Ethernet frame remains unchanged. Destination PC receives it in its original shape.

VLAN Tagging process with example

- PC1 generates a broadcast frame.
- Office1 switch receives it and know that it is a broadcast frame for VLAN20.
- It will forward this frame from all of its port associated with VLAN20 including trunk links.
- While forwarding frame from access links, switch does not make any change in original frame. So any other port having same VLAN ID in switch will receive this frame in original shape.
- While forwarding frame from trunk links, switch adds a VLAN identifier header to the original frame. In our case switch will add a header indicating that this frame belongs to VLAN20 before forwarding it from trunk link.
- Office2 switch will receive this frame from trunk link.
- It will read VLAN identifier header to know the VLAN information.
- From header it will learn that this is a broadcast frame and belong to VLAN20.
- It will remove header after learning the VLAN information.
- Once header is removed, switch will have original broadcast frame.
- Now office2 switch has original broadcast frame with necessary VLAN information.
- Office2 Switch will forward this frame from all of its ports associated with VLAN20 including trunk links. For trunk link same process will be repeated.
- Any device connected in ports having VLAN20 ID in Office2 switch will receive original frame.

Now we know that in VLAN tagging process sender switch adds VLAN identifier header to the original frame while receive switch removes it after getting necessary VLAN information. Switches use VLAN trunking protocol for VLAN tagging process.

VLAN Trunking Protocol

Cisco switches supports two types of trunking protocols **ISL** and **802.1Q**.

ISL

ISL (Inter-Switch Link) is a Cisco proprietary protocol. It was developed a long time before the 802.1Q. It adds a 26-byte header (containing a 15-bit VLAN identifier) and a 4-byte CRC trailer to the frame.

802.1Q

It is an open standard protocol developed by IEEE. It inserts 4 byte tag in original Ethernet frame. Over time, 802.1Q has become the most popular trunking protocols.

Key difference between ISL and 802.1Q

- ISL was developed Cisco while 802.1Q was developed by IEEE.
- ISL is a proprietary protocol. It will works only in Cisco switches. 802.1Q is an open standard based protocol. It will works on all switches.
- ISL adds 26 bytes header and 4 byte trailer to the frame.
- 802.1Q inserts 4 byte tag in original frame.

802.1Q is a lightweight and advanced protocol with several enhanced security features. Even Cisco has adopted it as a standard protocol for tagging in newer switches. 2960 Switch supports only 802.1Q tagging protocol.

VLAN Trunk Configuration

We can configure trunking in Cisco switches by two ways: statically or dynamically. In static method, we need to configure trunking in interface statically; while in dynamic mode it automatically done by a DTP trunking protocol.

Dynamic Trunking Protocol

DTP [Dynamic Trunking Protocol] is a Cisco proprietary protocol. It automatically configures trunking on necessary ports. It operates in five modes.

DTP Modes

DTP Mode ON

In ON mode, interface is set to trunk, regardless whether remote end supports trunking or not. ON mode cause interface to generate DTP messages and tag frames based on trunk type.

DTP Mode Desirable

In Desirable mode, interface will generate the DTP messages and send them to other end. Interface will work as access link until it get replies from remote end. If reply messages indicate that remote device is trunking capable, DTP will change connection link from access link to Trunk. If the other end does not respond to DTP message, the interface will work as access link connection.

DTP Mode Auto

In auto mode interface works as access link and passively listen for DTP messages. Interface will change connection link to trunk, if it receives a DTP message from remote end.

DTP Mode No-Negotiate

In No-Negotiate mode, interface is set as trunk connection. Interface will tag frames but it will not generate DTP messages. DTP is a Cisco's proprietary protocol, thus a non Cisco device will not understand it. This mode is used to trunk connection between **Cisco device and a non Cisco device**.

DTP Mode OFF

In off mode interface is configured as access-link. No DTP message will be generated nor frames will be tagged. In our topology, we need to configure trunk on following interfaces:

Switch	Interfaces
Office 1	Gig0/1, Gig0/2, F0/24
Office 2	Gig0/1, Gig0/2, F0/23, F0/24
Office 3	Gig0/1, Gig0/2

By default, all interface on a switch starts as access link. **`switchport mode trunk`** command is used to change connection link in trunk. Run this command from interface mode. We will now change all necessary interfaces (given in above table) connection link in trunk.

Office 1 Switch

```
S1(config)# interface fastEthernet 0/24
S1(config-if)# switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24,changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24,changed state to up
S1(config-if)# exit
S1(config)# interface gigabitEthernet 0/1
S1(config-if)# switchport mode trunk
S1(config-if)# exit
S1(config)# interface gigabitEthernet 0/2
S1(config-if)# switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2,changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2,changed state to up
S1(config-if)# exit
S1(config)#
```

Office 2 Switch

```
S2(config)# interface gigabitEthernet 0/1
S2(config-if)# switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,changed state to up
S2(config-if)# exit
S2(config)# interface gigabitEthernet 0/2
S2(config-if)# switchport mode trunk
S2(config-if)# exit
S2(config)# interface fastEthernet 0/23
S2(config-if)# switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23,changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23,changed state to up
S2(config-if)# exit
S2(config)# interface fastEthernet 0/24
S2(config-if)# switchport mode trunk
S2(config-if)# exit
```

Office 3 Switch

```
S3(config)#  interface fastEthernet 0/24
S3(config-if)# switchport mode trunk
S3(config-if)# exit
S3(config)# interface gigabitEthernet 0/1
S3(config-if)# switchport mode trunk
S3(config-if)# exit
```

That's all the configurations we need. Now our trunk links are ready to move multiple VLANs traffic.

Section D

This final section explains how to create and assign VLAN, VLAN Membership (Static and Dynamic), Router on Stick and Spanning Tree Protocol (STP) in detail.

Creating VLAN

In Section B, Switch S1 was configured as VTP Server. S2 and S3 were configured as VTP clients. We only need to create VLANs in VTP Server. VTP Server will propagate this info to all VTP clients automatically.

`vlan` ***`vlan number`*** command is used to create the VLAN.

Office 1 Switch

```
S1(config)# vlan 10
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# exit
S1(config)#
```

Assigning VLAN Membership

VLAN can be assigned statically or dynamically but at our level, we only need to use the static method to assign VLAN membership. **`switchport access vlan [`*`vlan number`*`]`** command is used to assign VLAN to the interface. Following commands will assign VLANs to the interfaces.

Office 1 Switch

```
S1(config)# interface fastEthernet 0/1
S1(config-if)# switchport access vlan 10
S1(config-if)# interface fastEthernet 0/2
S1(config-if)# switchport access vlan 20
```

Office 2 Switch

```
S2(config)# interface fastEthernet 0/1
S2(config-if)# switchport access vlan 10
S2(config-if)# interface fastEthernet 0/2
S2(config-if)# switchport access vlan 20
```

Office 3 Switch

```
S3(config)# interface fastEthernet 0/1
S3(config-if)# switchport access vlan 10
S3(config-if)# interface fastEthernet 0/2
S3(config-if)# switchport access vlan 20
```

We have successfully assigned VLAN membership. It's time to test our configuration. To test this configuration, we will use *`ping`* command. *`ping`* command is used to test connectivity between two devices. As per our configuration, devices from same VLAN can communicate. Devices from different VLANs must not be able to communicate with each other without router.

Testing VLAN configuration

Access PC(X) command prompt by Double click **PC(X)-PT** and click **Command Prompt**

We have two VLAN configurations VLAN 10 and VLAN 20. Let's test VLAN 10 first. In VLAN 10 we have three PCs with IP addresses: `10.0.0.2`, `10.0.0.3` and `10.0.0.4`. These PCs must be able to communicate with each other's. At this point, PCs from VLAN 10 should not be allowed to access PCs from VLAN 20. VLAN 20 also has three PCs `20.0.0.2`, `20.0.0.3` and `20.0.0.4`.

```
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::210:11FF:FEED:A6C7
   IP Address.....: 10.0.0.3
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: 10.0.0.1

PC>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=2ms TTL=128
Reply from 10.0.0.2: bytes=32 time=0ms TTL=128
Reply from 10.0.0.2: bytes=32 time=0ms TTL=128
Reply from 10.0.0.2: bytes=32 time=0ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time=0ms TTL=128
Reply from 10.0.0.4: bytes=32 time=0ms TTL=128
Reply from 10.0.0.4: bytes=32 time=0ms TTL=128
Reply from 10.0.0.4: bytes=32 time=11ms TTL=128

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms

PC>
```

```
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::20D:BDFF:FE87:D003
   IP Address.....: 10.0.0.4
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: 10.0.0.1

PC>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 20.0.0.2:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
PC>ping 20.0.0.3

Pinging 20.0.0.3 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 20.0.0.3:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

Control-C
^C
PC>
```

We have successfully implemented VLAN 10 now test VLAN 20.

Same as VLAN 10, PCs from VLAN 20 must be able to communicate with other PCs of same VLAN while they should not be able to access VLAN 10.

```
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::206:2AFF:FE0C:5A43
   IP Address.....: 20.0.0.4
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: 20.0.0.1

PC>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time=0ms TTL=128
Reply from 20.0.0.2: bytes=32 time=0ms TTL=128
Reply from 20.0.0.2: bytes=32 time=0ms TTL=128
Reply from 20.0.0.2: bytes=32 time=10ms TTL=128

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

PC>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 10.0.0.4:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

Control-C
^C
PC>
```

```
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::201:43FF:FE88:5781
   IP Address.....: 20.0.0.3
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: 20.0.0.1

PC>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time=2ms TTL=128
Reply from 20.0.0.2: bytes=32 time=3ms TTL=128
Reply from 20.0.0.2: bytes=32 time=0ms TTL=128
Reply from 20.0.0.2: bytes=32 time=0ms TTL=128

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

PC>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 10.0.0.2:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
PC>
```

Configure Router on Stick

Typically routers are configured to receive data on one physical interface and forward that data from another physical interface based on its configuration. Each VLAN has a layer 3 address that should be configured as default gateway address on all its devices. In our scenario we reserved IP address 10.0.0.1 for VLAN 10 and 20.0.0.1 for VLAN 20.

With default configuration, we need two physical interfaces on router to make intra-VLAN communication. Due to the high price of a router, it's not a cost effective solution to use a physical interface of router for each VLAN. Usually a router has one or two Ethernet interface. For example, if we have 50 VLANs, we would need nearly 25 routers in order to make intra-VLANs communication. To deal with situation, we use Router on Stick.

Router on Stick is router that supports trunk connection and has an ability to switch frames between the VLANs on this trunk connection. On this router, a single physical interface is sufficient to make communication between both VLANs.

Access command prompt of Router

To configure Router on Stick we have to access CLI prompt of Router. Click **Router** and Click **CLI** from menu items and Press **Enter key** to access the CLI

Run following commands in same sequence to configure Router on Stick

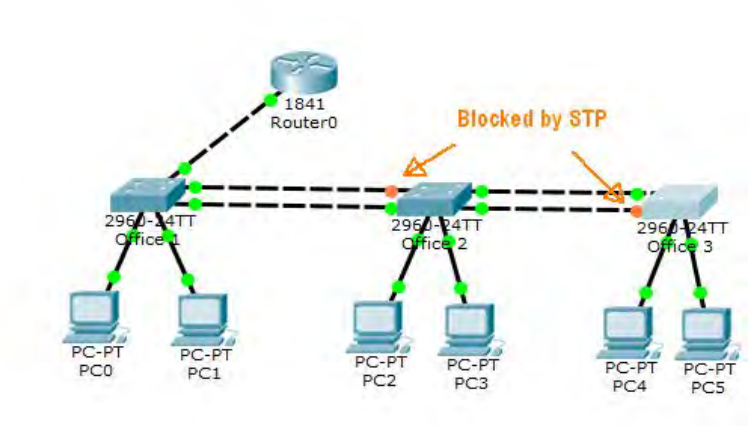
```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastEthernet 0/0
Router(config-if)# no ip address
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface fastEthernet 0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 10.0.0.1 255.0.0.0
Router(config-subif)# exit
Router(config)# interface fastEthernet 0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 20.0.0.1 255.0.0.0
Router(config-subif)# exit
```

- In above configuration, we broke up single physical interface [FastEthernet 0/0] into two logical interfaces, known as sub-interfaces. A router can support up to 1000 interfaces
- By default interface link works as access link. We need to change it into trunk link. encapsulation commands specify the trunk type and associate VLAN with sub-interface.
- In next step we assigned IP address to our sub-interface.

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::210:11FF:FEED:A6C7
   IP Address.....: 10.0.0.3
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: 10.0.0.1

PC>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time=0ms TTL=127
Reply from 20.0.0.2: bytes=32 time=1ms TTL=127
Reply from 20.0.0.2: bytes=32 time=15ms TTL=127
Reply from 20.0.0.2: bytes=32 time=10ms TTL=127

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 6ms

PC>
```

That's all configuration we need to switch VLANs. Now we can test different VLAN communications. To test intra VLANs communication open command prompt of PC and ping the PC of other VLAN. PC2 [10.0.0.3] from VLAN 10 can now access PC1 [20.0.0.2] from VLAN 20.

Spanning Tree Protocol (STP)

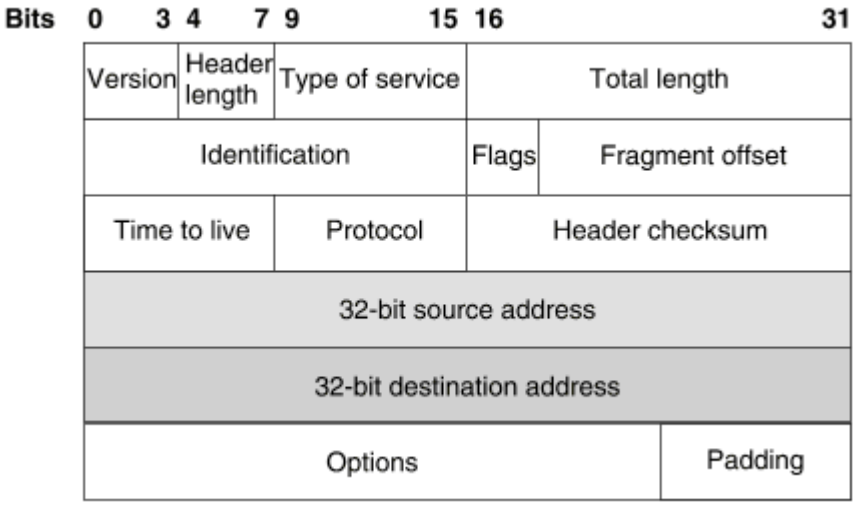


STP is a layer 2 protocol, used for removing loops. For backup purpose we typically create backup links for important resources. In our scenario, all offices have backup links that create loops in topology. STP automatically removes layer 2 loops. STP multicasts frame that contain information about switch interfaces. These frames are called BPDU (Bridge Protocol Data Units). Switch use BPDUs to learn network topology. If it found any loop, it will automatically remove that. To remove loop, STP disables port or ports that are causing it. *(may differ to yours)*

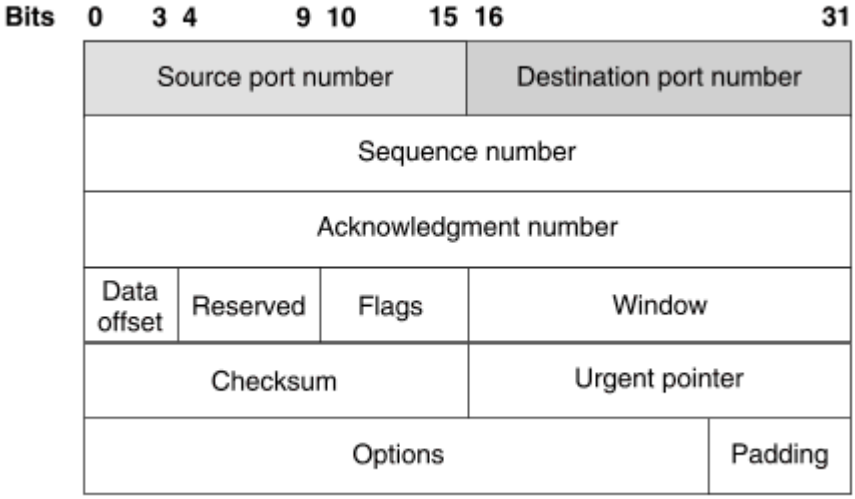
APPENDIX: VLAN VTP DTP commands cheat sheet

Command	Description
`Switch(config)# vtp mode server`	Configure Switch as VTP Server
`Switch(config)# vtp mode client`	Configure Switch as VTP Client
`Switch(config)# vtp mode transparent`	Configure Switch as VTP Transparent
`Switch(config)# no vtp mode Configure`	Switch to default VTP Server Mode
`Switch(config)# vtp domain domain-name`	Set VTP Domain name.
`Switch(config)# vtp password password`	Set VTP password. Password is case sensitive
`Switch# show vtp status`	Display VTP status including general information
`Switch# show vtp counters`	Show VTP counters of switch
`Switch(config-if)# switchport mode trunk`	Change interface mode in Trunk
`Switch(config)# vlan 10`	Create VLAN and associate number ID 10 with it
`Switch(config-vlan)# name Sales`	Assign name to VLAN
`Switch(config-vlan)# exit`	Return in Global configuration mode from VLAN configuration mode
`Switch(config)# interface fastethernet 0/1`	Enter in interface configuration mode
`Switch(config-if)# switchport mode access`	Set interface link type to access link
`Switch(config-if)# switchport access vlan 10`	Assign this interface to VLAN 10
`Switch# show vlan`	Displays VLAN information
`Switch# show vlan brief`	Displays VLAN information in short
`Switch# show vlan id 10`	Displays information VLAN ID 10 only
`Switch# show vlan name sales`	Displays information about VLAN named sales only
`Switch(config)# interface fastethernet 0/8`	Enter in Interface configuration mode
`Switch(config-if)# no switchport access vlan 10`	Removes interface from VLAN 10 and reassigns it to the default VLAN - VLAN 1
`Switch(config-if)# exit`	Move back to Global configuration mode
`Switch(config)# no vlan 10`	Delete VLAN 10 from VLAN database
`Switch# copy running-config startup-config`	Saves the running configuration in NVRAM

IPv4 (RFC 791) format



TCP (RFC 793) format



Ethernet II format