Murdoch
UNIVERSITY

Unit Review

ICT169

Foundations of Data Communications

Last Week

- A look at some new(er) trends in networking
- Software-Defined Networks, Whitebox switches, Orchestration, and the Internet of Things
- This topic will not feature in the final exam

https://medium.com/thrive-global/use-technology-in-a-thoughtful-way-that-improves-your-life-3e22fb3372a4

Lecture Overview

- Details about the Final Exam
    - Tips on preparing for the exam
    - Resources to help you study
- A reminder about Cisco certifications
- A look back at the topics we've covered this semester (including some example questions)

7. Application

6. Presentation

5. Session

4. Transport

3. Network

2. Data Link

1. Physical

Final Exam

- Online (LMS-based) closed book exam, 90 minutes
- No aids allowed except note paper (provided)
- Exam covers all topics (from lectures, labs, and readings) from this unit
- Consists of 30 questions (total of 40 marks)
    - 22 Multiple choice / matching
    - 2 Short answer
    - 6 Long answer
- Contributes 50% of your overall grade

Final Exam – When is it?

- Currently scheduled for Friday, 16 November
- Two sessions due to number of students:
  - Session 1 – 9:30—11:00
  - Session 2 – 11:30—13:00
- Five different venues (assigned by surname **as listed in MyInfo**)
- You must attend your assigned session and venue!
- Check the exam timetable (available online) for most up-to-date times and venues
  - http://www.murdoch.edu.au/admin/timetables/exams/

Passing ICT169

To pass this unit, you must:

- Achieve an overall score of 50% or above

For higher grades:

- Credit - aggregate score of ≥ 60%
- Distinction - an aggregate score of ≥ 70%
- High distinction - aggregate score of ≥ 80%

Supplementary assessments are granted at the discretion of unit coordinator in-line with University policy

Studying for the Exam

- Focus on key concepts for the unit rather than reading every slide and chapter
    - Lecture objectives are useful to identifying these (re-listed in today's lecture)
- Sample questions are also helpful in guiding your study
    - This lecture
    - Review questions from previous lectures
    - Participation quizzes
    - Mid-Semester Test
    - NetAcad quizzes and exams
    - Practice Exam (listed under Topic 12)

Studying for the Exam (cont.)

- If you get a question wrong, refer to other resources
    - Review relevant lecture slides / Echo360 recording
    - Refer to appropriate reading(s)
    - Make use of other online resources (like Google)
    - If all else fails, email your tutor or myself
- Keep in mind that the goal should be to understand concepts, rather than simply remembering answers
- Remember that PASS will also be running an exam preparation session
    - Thursday, 8 November 12:30-2:30PM in 235.4.008

Cisco Certification – The CCENT

- Cisco certifications are some of the most popular and industry-recognised IT certifications
- This unit has covered (most of) two modules from the Cisco Networking Academy curriculum:
  - Introduction to Networks
  - Routing and Switching Essentials
- These modules make up the Cisco Certified Entry Networking Technician (CCENT)
- Topics for further certifications covered in later units from the Internetworking and Network Security major
- Cisco certifications are frequently listed as essential or desirable when applying for jobs
- Contact me if you'd like more information

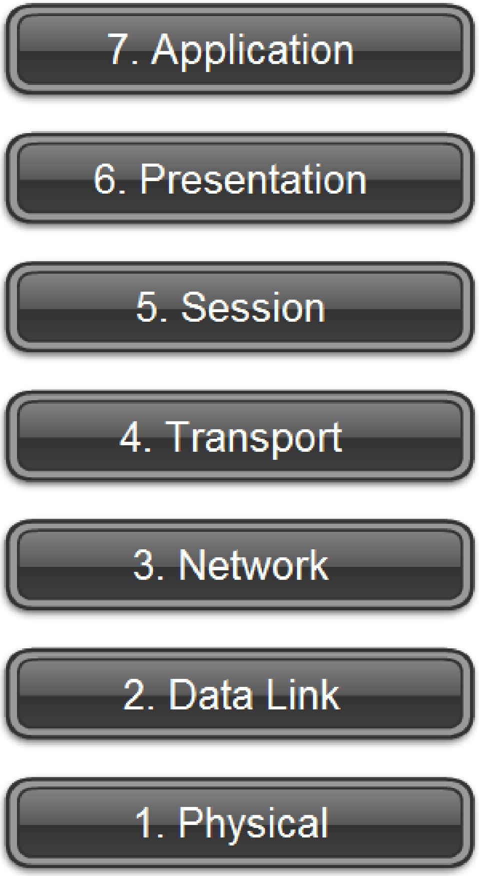
Topic 1 – Introduction to Networks

You should now be able to:

- Describe the difference between packet switched and circuit switched networks
- Describe why data networks break communications into packets
- Define network convergence, and identify problems associated with it
- Describe a communications medium, giving three examples
- Differentiate between a LAN and a WAN
- Describe the purpose of the OSI model
- Name the layers of the OSI model
- Name some networking devices, and identify which layer of the OSI model they operate at
- Define the term ‘protocols’ and describe their purpose in data communications.
- Differentiate between units used to define network speeds and data storage
- Convert between units used to define network speeds and data storage

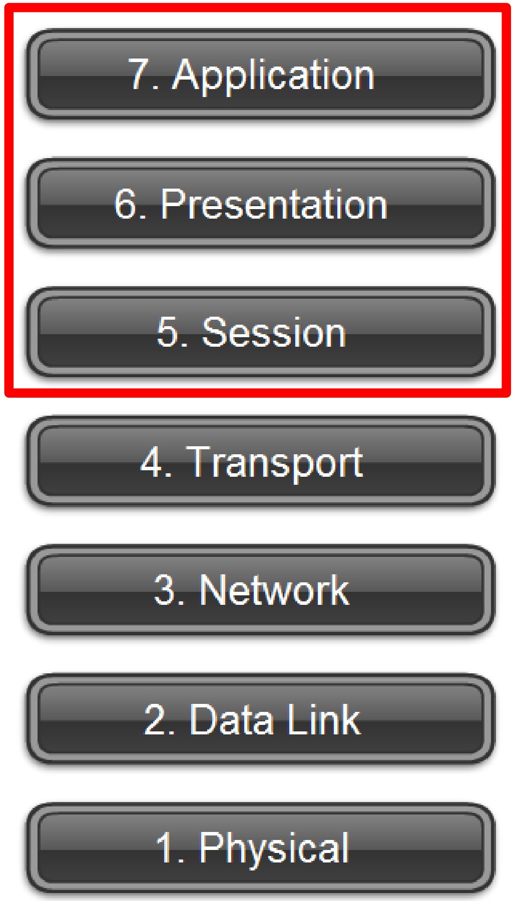
The ISO OSI Model

- Open Systems Interconnection model
- Reference model for communication networks
- Models communication into layers
  - A Layer serves the layers above
  - A Layer is served by the layers below
- Layers are independent with standardised interfaces between layers; changes in one layer don’t affect other layers
- Makes protocol design much easier



Application, Presentation, and Session Layers

- Application protocols
- Data encoding
- Session handling
- **Examples:** Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP)



7. Application

6. Presentation

5. Session

4. Transport

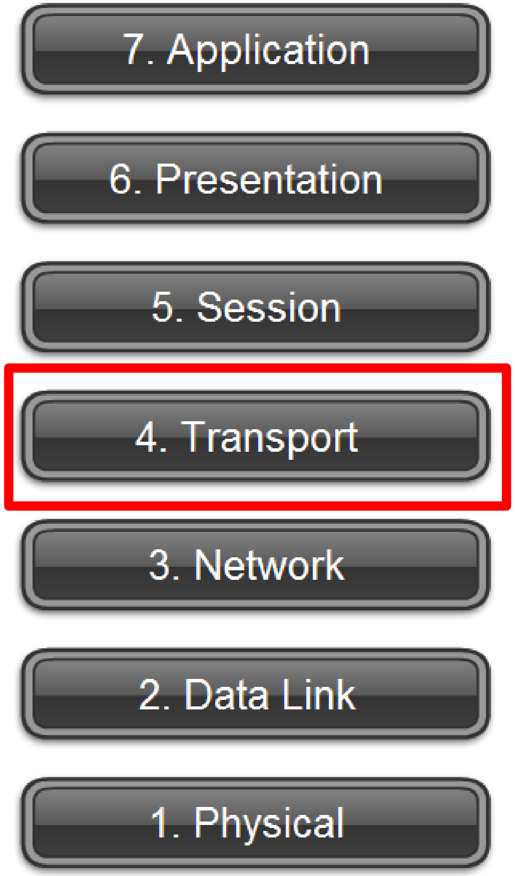
3. Network

2. Data Link

1. Physical

Transport Layer

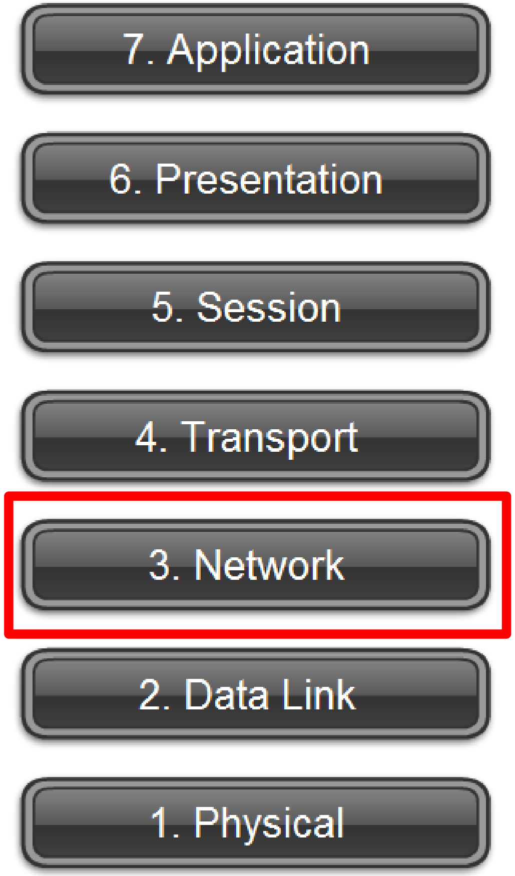
- Defines protocols for end-to-end delivery of application data
  - Controls amount of data to send
  - Provides error detection and correction
  - Defines application addressing
- **Examples:** Transmission Control Protocol (TCP) , User Datagram Protocol (UDP)



Murdoch UNIVERSITY

Network Layer

- Defines the packetisation and end-to-end transport of data
  - Logical device addressing (IP addresses)
  - Routing of packets from source to destination
- **Examples:** Internet Protocol (IP)



7. Application

6. Presentation

5. Session

4. Transport

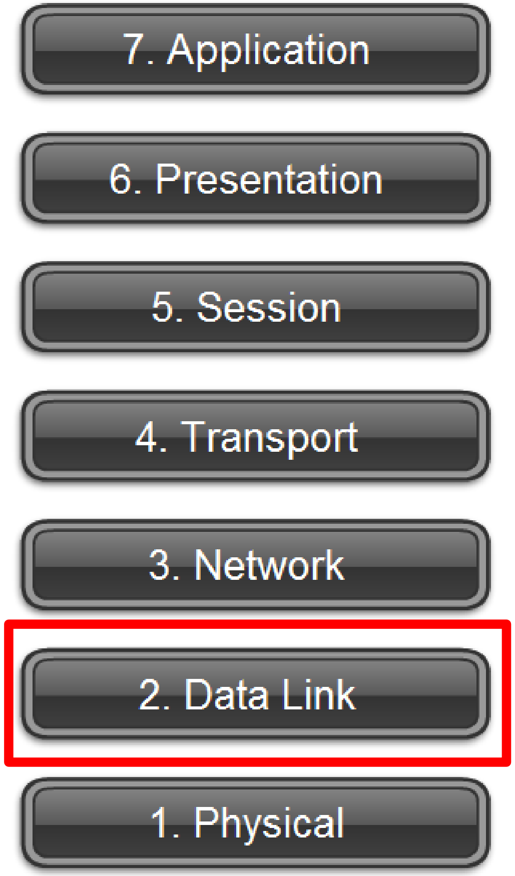
3. Network

2. Data Link

1. Physical

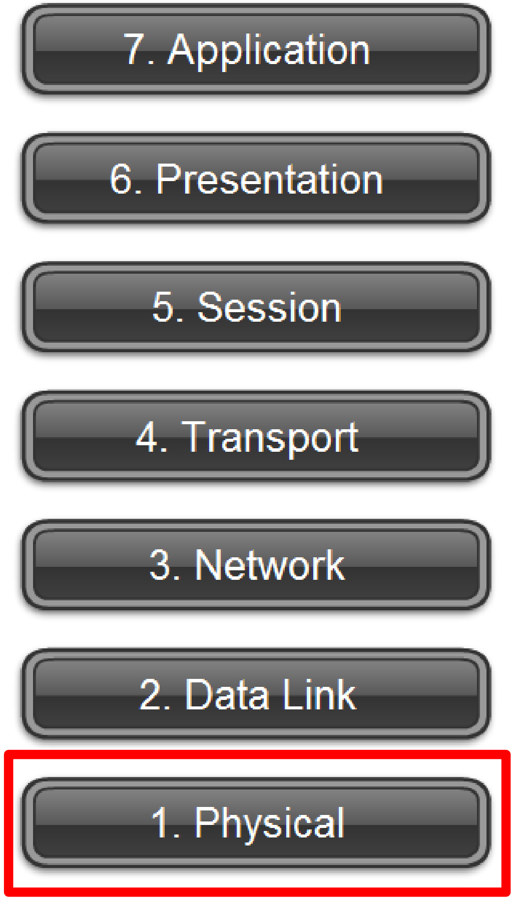
Data Link Layer

- Controls data transport over single link or network segment
  - Division of data into frames
  - Medium access control
  - Physical device addressing
- **Examples:** Ethernet, IEEE 802.11



Physical Layer

- Defines encoding of signals on the medium, including:
    - Voltages, amplitudes, frequencies, wave lengths
    - Connectors
- Closely related to the data link layer
- Examples: Ethernet, IEEE 802.11



7. Application

6. Presentation

5. Session

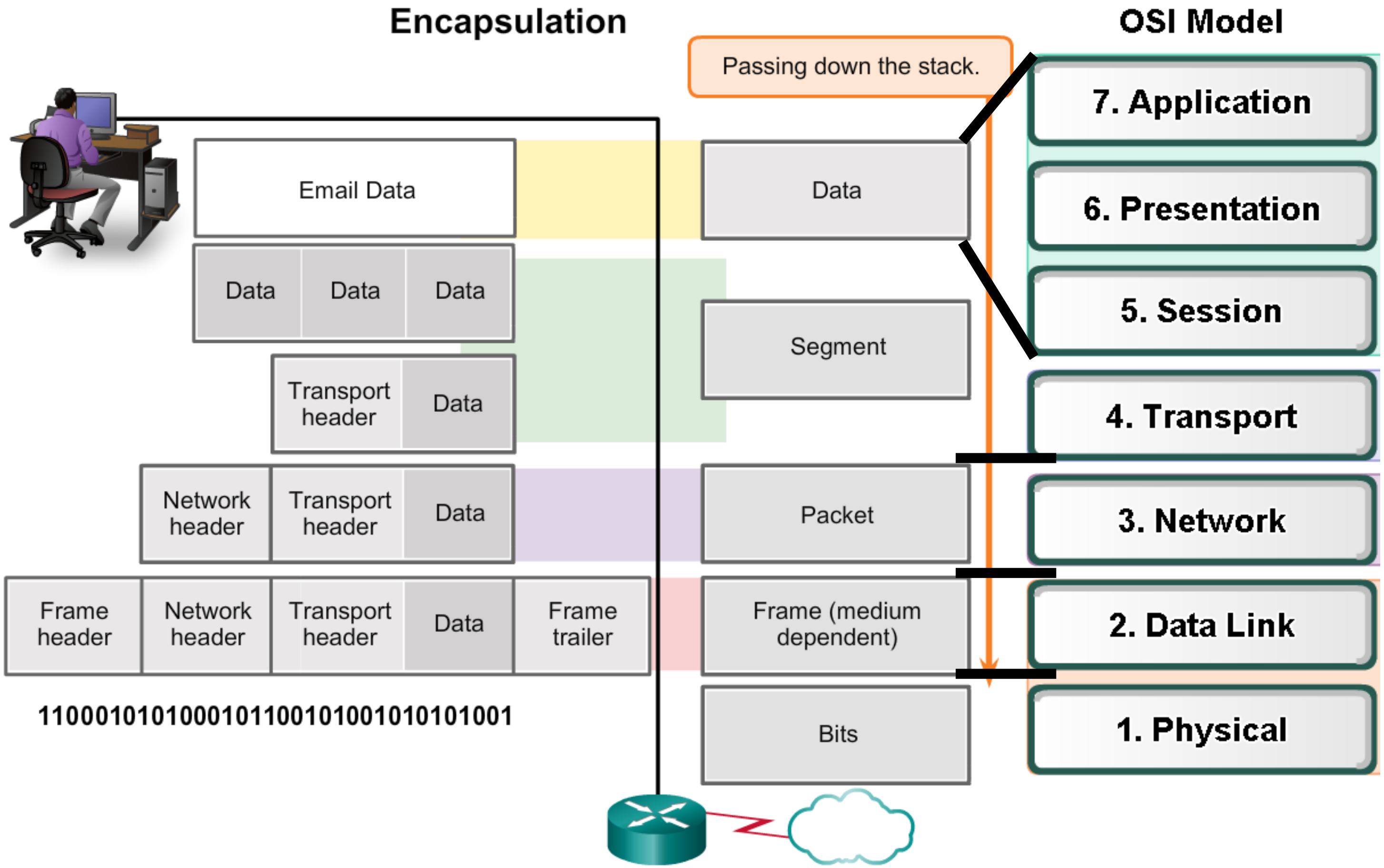
4. Transport

3. Network

2. Data Link

1. Physical

The Encapsulation Process



Data comes from application

Transport header inc. ports added

Network header inc. IP addresses added

MAC header inc. MAC addresses added

Topic 2 – The Application and Transport Layers

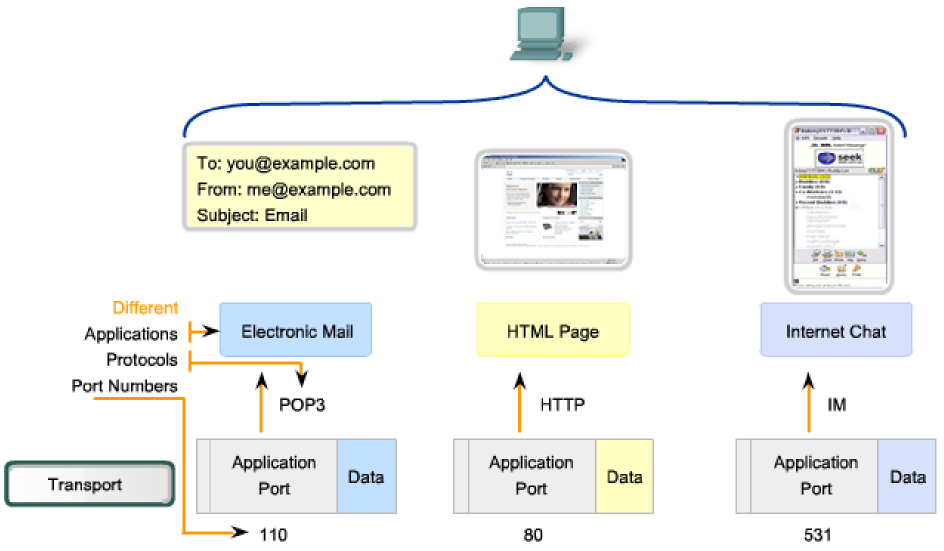
You should now be able to:

- Describe the role of the OSI Application, Presentation, and Session layers
- Describe the Client/Server and Peer-to-Peer architectures
- Describe the purpose and operation of the Domain Name System
- Describe the purpose and operation of Hypertext Transfer Protocol
- Describe the purpose and operation of File Transfer Protocol
- Describe the purpose and operation of Dynamic Host Configuration Protocol
- Describe the purpose of the OSI Transport layer
- Define ports with respect to the transport layer
- Differentiate between the reliable and unreliable delivery of data
- Describe the operation of the Transmission Control Protocol and User Datagram Protocol
- Identify when it is appropriate to use each transport layer protocol

Ports – Addressing at the Transport Layer

- Don’t exist physically; ports are a logical concept used by operating systems for identification of different applications
- Ports are identical, but some are ‘recognised’ for use by specific applications (eg. TCP port 80 is recognised as HTTP)
- Some applications can have multiple port numbers (eg. HTTP can also used port 8080)

Port Addressing

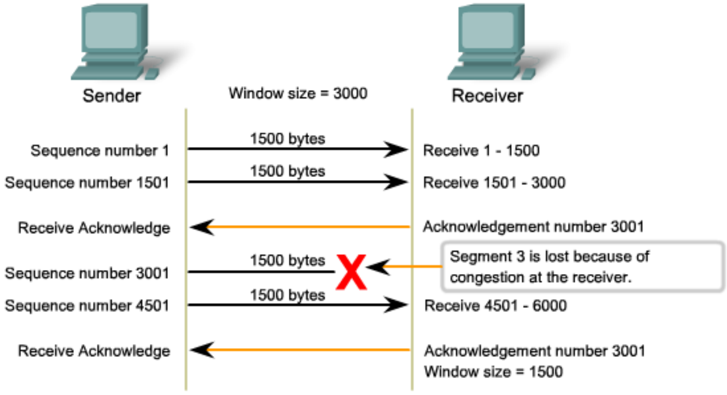


Data for different applications is directed to the correct application because each application has a unique port number.

Transmission Control Protocol (TCP)

- TCP is a **connection-oriented protocol**; connections must be explicitly initiated and terminated
- Provides in-order delivery of segments to application by using **sequence numbers**
- All data transmitted using TCP must be acknowledged
- TCP uses congestion control and flow control to manage the rate of transmission

TCP Congestion and Flow Control



If segments are lost because of congestion, the Receiver will acknowledge the last received sequential segment and reply with a reduced window size.

Murdoch UNIVERSITY

User Datagram Protocol (UDP)

- UDP is a **connectionless** protocol; just send datagrams as needed
- ‘Best effort’ protocol, and has no equivalent to TCP acknowledgements
  - Not necessarily less reliable, just not guaranteed
- Datagrams may also arrive out of order
- No congestion or flow control
- Low per-packet overhead (simpler and smaller header)
- UDP is used when data must arrive in a timely manner

Review Question

Which of the following is not a property of TCP?

a) Reliable end-to-end delivery of data

b) Rate-limiting of transmission to avoid congestion

c) Low latency transmission of data

d) Re-ordering of data to ensure in-order delivery

e) Explicit setup and termination of connections

Review Question

Which of the following is not a property of TCP?

a) Reliable end-to-end delivery of data

b) Rate-limiting of transmission to avoid congestion

c) Low latency transmission of data

d) Re-ordering of data to ensure in-order delivery

e) Explicit setup and termination of connections

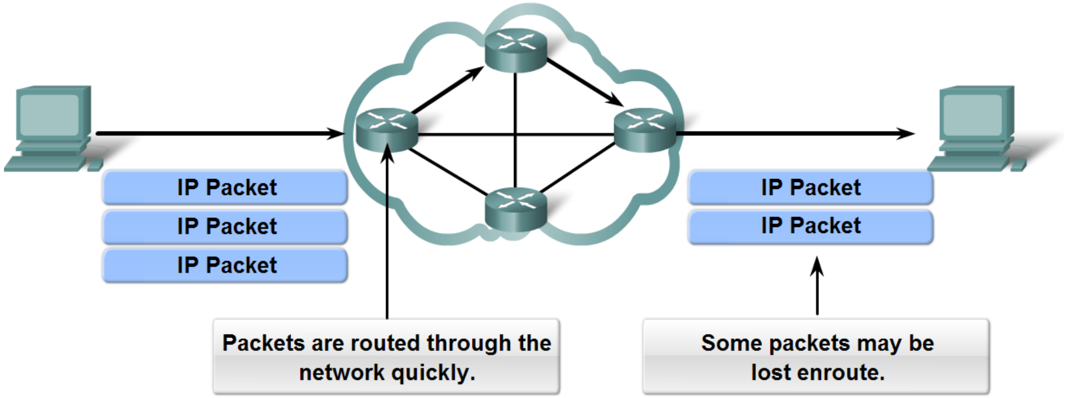
Topic 3 – The Network Layer

You should be able to:

- Describe the purpose of the network layer
- Describe the encapsulation process
- Identify network layer protocols
- Identify an IP version 4 address
- Describe the components of an IP version 4 address
- Describe the different types of IP transmissions
- Represent binary numbers in decimal
- Represent decimal numbers in binary
- Describe the purpose of the subnet mask
- Differentiate between classful and classless IP addressing

Internet Protocol (IP)

- IP communications are **connectionless**; no setup required
- Like UDP, IPv4 is a ‘best effort’ protocol;
  - Like UDP, this doesn’t mean that IP is unreliable
  - Reliability must come from another layer of the networking stack
- IPv4 is also media independent; it can function over copper, fiber, air (or any combination of the three)


IP Packet
IP Packet
IP Packet
IP Packet
IP Packet
Packets are routed through the network quickly.
Some packets may be lost enroute.

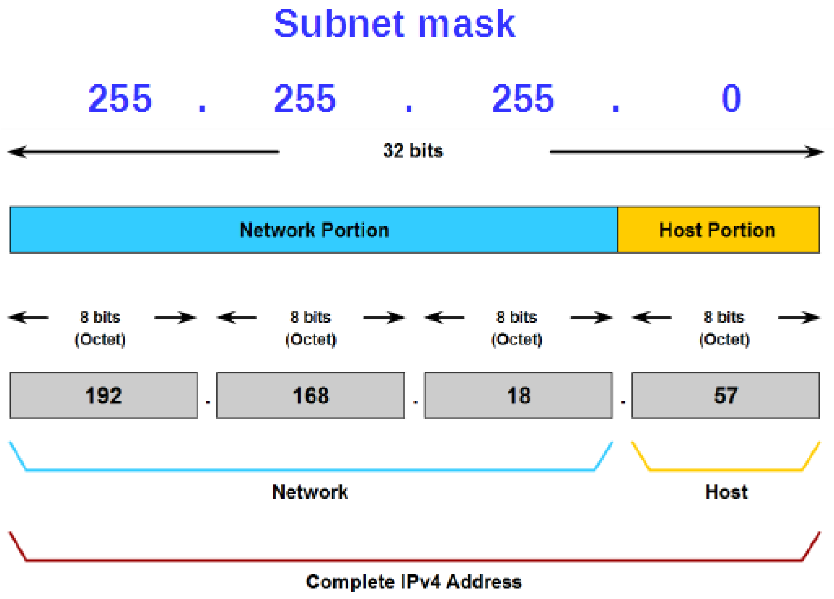
As an unreliable Network layer protocol, IP does not guarantee that all sent packets will be received.

Public and Private IP Addressing

- Some address blocks are reserved for private networks:
  - 10.0.0.0 – 10.255.255.255
  - 169.254.0.0 – 169.254.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
- These address ranges are used inside private networks, and packets addressed to these ranges cannot be routed on the Internet
- Packets originating from a private IP address must undergo Network Address Translation (NAT) to be routed over the Internet (more on this in a later lecture)

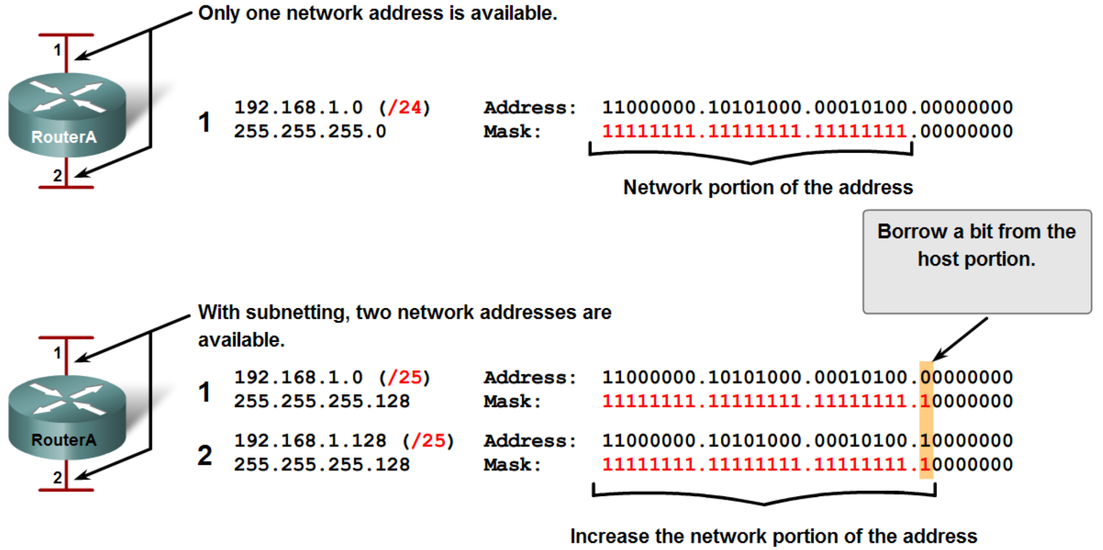
Hierarchical IP Addressing

- IP uses the **subnet mask** to provide hierarchy by dividing addresses into a **network** and **host** portion
- The subnet mask uses bits set to 1 to represent the network portion of an address
- Each host is only aware of other hosts within its own subnet
- Hosts pass packets to the **default gateway** to be routed outside of the local network



Subnetting using VLSM

- We borrow bits from the host portion to create subnets
- Traditionally subnets were all the same size, but this approach is wasteful
- Instead, we now use an approach called **Variable Length Subnet Masks (VLSM)**
  - Allows each subnet to be provisioned to the most appropriate size



Only one network address is available.

```
1  192.168.1.0 (/24)      Address:  11000000.10101000.00010100.00000000
   255.255.255.0          Mask:     11111111.11111111.11111111.00000000
```

Network portion of the address

Borrow a bit from the host portion.

With subnetting, two network addresses are available.

```
1  192.168.1.0 (/25)      Address:  11000000.10101000.00010100.00000000
   255.255.255.128        Mask:     11111111.11111111.11111111.10000000
2  192.168.1.128 (/25)    Address:  11000000.10101000.00010100.10000000
   255.255.255.128        Mask:     11111111.11111111.11111111.10000000
```

Increase the network portion of the address

Review Question

Which of the following IP addresses are private IP addresses?

a) 134.148.0.1

b) 10.12.10.1

c) 192.168.0.10

d) 172.16.16.16

e) 201.201.201.100

Review Question

Which of the following IP addresses are private IP addresses?

a) 134.148.0.1

b) 10.12.10.1

c) 192.168.0.10

d) 172.16.16.16

e) 201.201.201.100

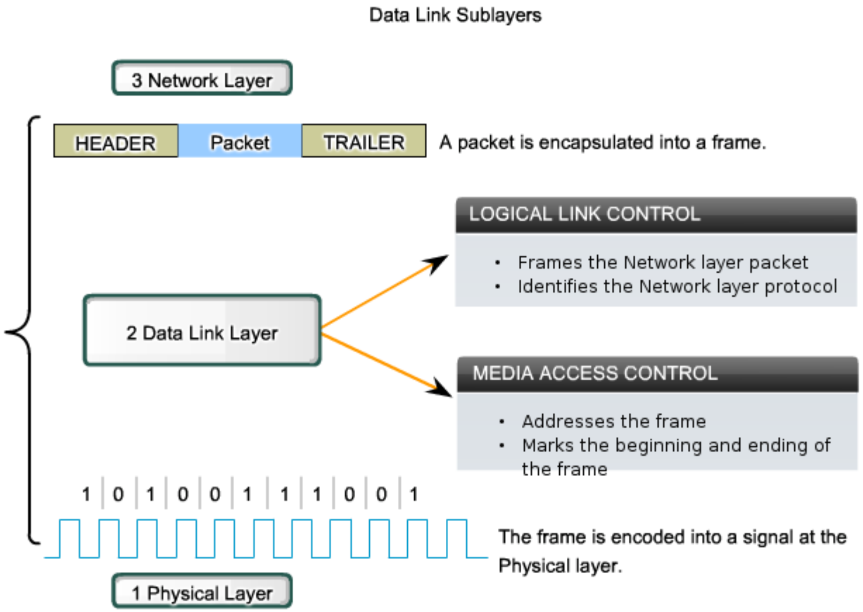
Topic 4 – The Data Link and Physical Layers

You should now be able to:

- Describe the role of the Data Link layer
- Discuss the division of Data Link layer functions between Logical Link Control (LLC) and Media Access Control (MAC)
- Describe the difference between Point-to-Point and Multi-Access links
- Describe the role of MAC addressing in data communications
- Describe data link layer protocols
- Differentiate between different approaches to MAC
- Describe the purpose of the physical layer
- Identify different forms of physical media
- Describe the effects of attenuation and interference

Data Link Sub-Layers

- Data link layer is divided into two sub layers known as Logical Link Control (LLC) and Media Access Control (MAC)
- LLC is the upper half of the link layer, which interacts with the network layer
- MAC is the lower half of the link layer, which interacts with the physical layer



Data Link Sublayers
3 Network Layer
HEADER
Packet
TRAILER
A packet is encapsulated into a frame.
LOGICAL LINK CONTROL
• Frames the Network layer packet
• Identifies the Network layer protocol
2 Data Link Layer
MEDIA ACCESS CONTROL
• Addresses the frame
• Marks the beginning and ending of the frame
1 0 1 0 0 1 1 1 0 0 1
The frame is encoded into a signal at the Physical layer.
1 Physical Layer

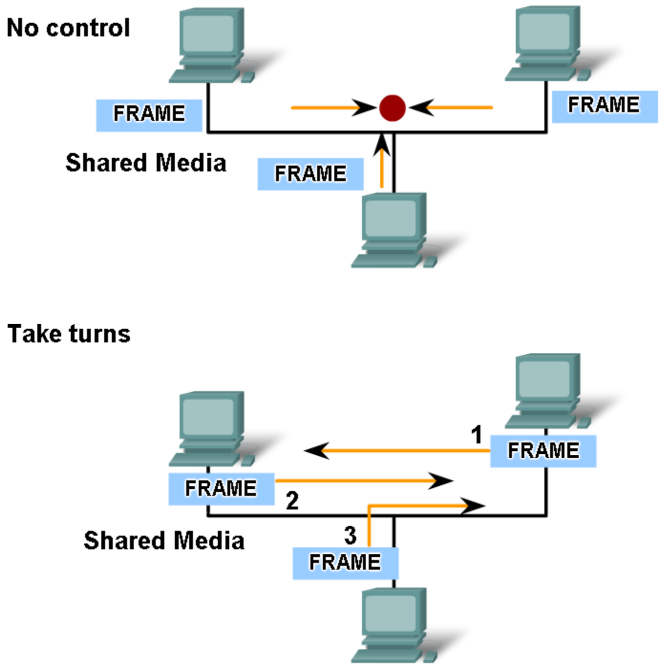
Collisions

- Two devices transmitting at the same time causes a collision, requiring the message to be re-sent
- Similar to a conversation between two people; when two people speak at once, you can't understand either of them
- Transmitting devices must take turns, but how?

No control at all would result in many collisions. Collisions cause corrupted frames that must be resent.

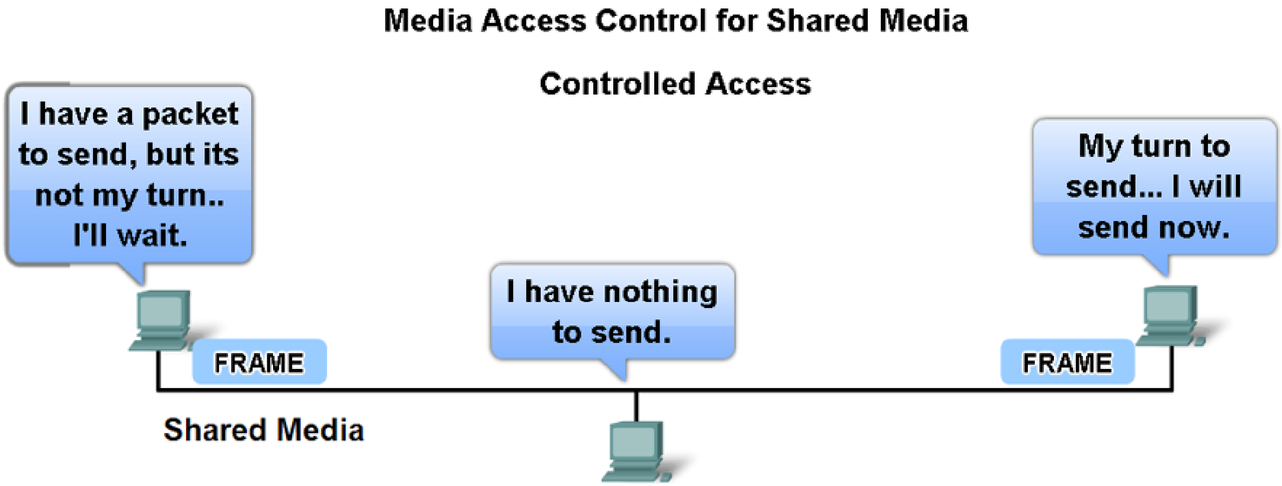
Methods that enforce a high degree of control prevent collisions, but the process has high overhead.

Methods that enforce a low degree of control have low overhead, but there are more frequent collisions.



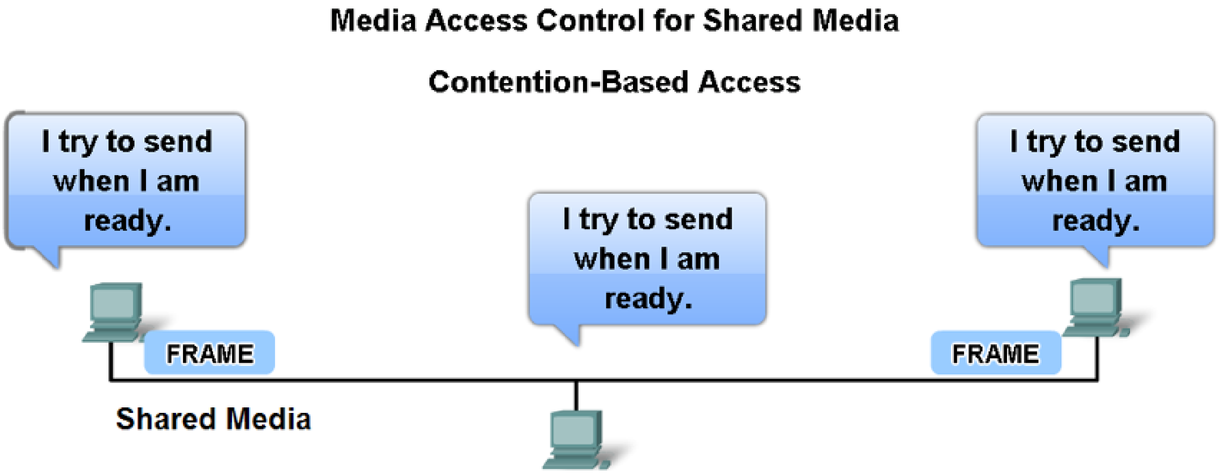
Controlled Access

- Controlled Access MAC avoids collisions entirely by ensuring that only one device can transmit at any given time
- This is usually achieved by having devices pass a **token** or sharing time slices
- Controlled Access can be viewed as fairer than Contention-based MAC as each device gets a predictable ‘turn’


Media Access Control for Shared Media
Controlled Access
I have a packet to send, but its not my turn.. I'll wait.
FRAME
I have nothing to send.
My turn to send... I will send now.
FRAME
Shared Media

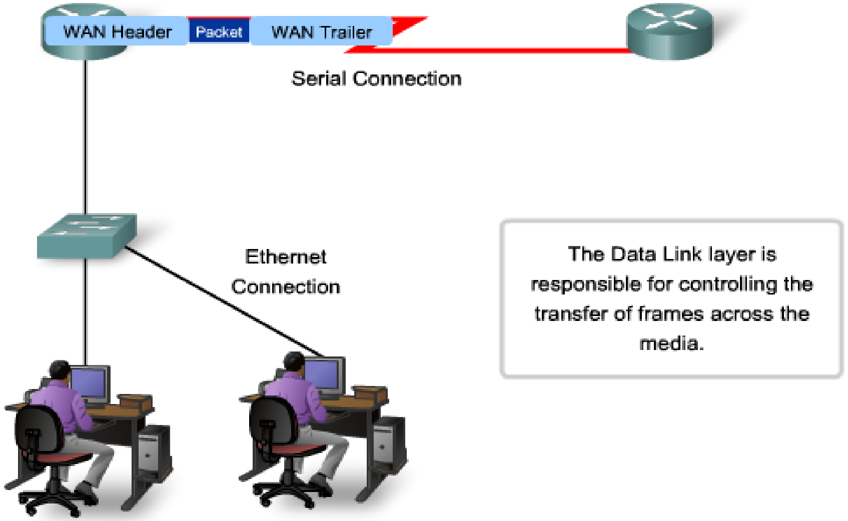
Contention-based Access

- In contention-based media access control, devices can transmit at (almost) any time
- Usually requires that devices listen for other transmissions before transmitting
- If a device hears an ongoing transmission, it should wait until that transmission is complete before transmitting


Media Access Control for Shared Media
Contention-Based Access
I try to send when I am ready.
I try to send when I am ready.
I try to send when I am ready.
FRAME
FRAME
Shared Media

Link Layer Addressing

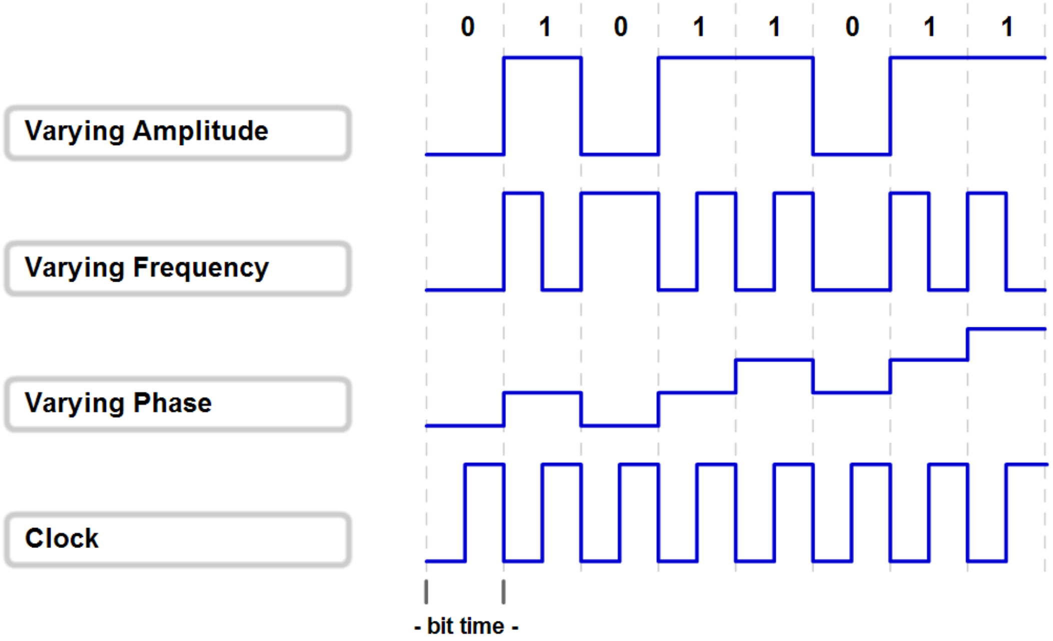
- Recall that the network and transport layers deal with end-to-end delivery of data
  - IP addresses and ports don't change
- Given differences between link layer protocol headers, this wouldn't be practical at the link layer
- Link layer headers and trailers are re-written at every hop



The Data Link layer is responsible for controlling the transfer of frames across the media.

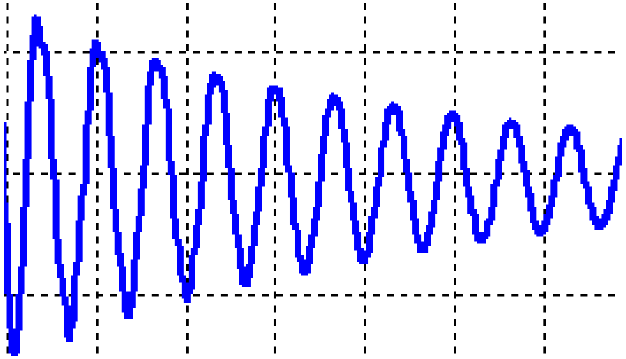
Encoding Techniques

- Bits can be encoded on the physical medium in different ways:
  - Amplitude
  - Frequency
  - Phase



Attenuation

- Signals in all media attenuate with distance
  - LAN speeds (e.g. Ethernet) are always going to be faster than WAN speeds (e.g. ADSL)
  - Ethernet has maximum distance of 100m and must run on Cat5 cable or better while ADSL must work over many kilometers using 40 year old telephone cable
- Attenuation also depends on medium
  - Highest for wireless, followed by copper, followed by fibre
- Attenuation also depends on frequency
  - Higher for higher frequencies



Review Question

Which of the following statements about broadcast and collision domains is true?

a) Broadcast domains represent a network segment in which hosts compete for bandwidth

b) Collision domains are extended by Ethernet switches

c) Broadcast domains are extended by routers

d) Collision domains represent a network segment in which hosts can communicate using link layer addresses

e) Collision domains are extended by Ethernet hubs

Review Question

Which of the following statements about broadcast and collision domains is true?

a) Broadcast domains represent a network segment in which hosts compete for bandwidth

b) Collision domains are extended by Ethernet switches

c) Broadcast domains are extended by routers

d) Collision domains represent a network segment in which hosts can communicate using link layer addresses

e) Collision domains are extended by Ethernet hubs

Topic 5 – Ethernet and VLANs

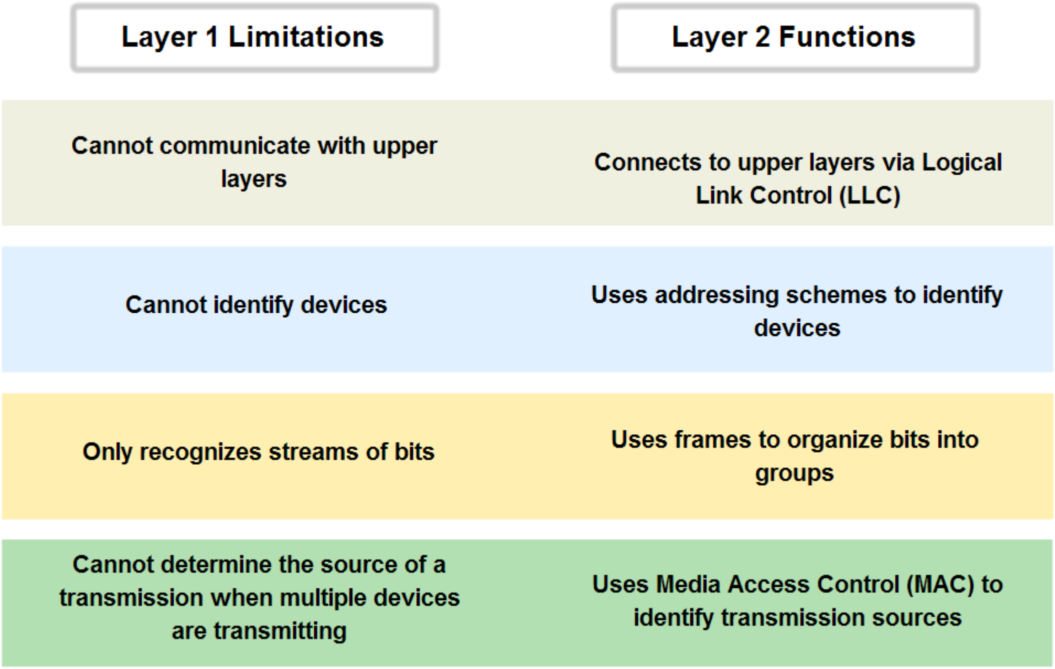
You should now be able to:

- List different topologies used by Ethernet networks
- Describe the operation of CSMA/CD
- Describe the role of MAC addresses in Ethernet networks
- Describe the operation of Ethernet switches
- Describe the role and operation of ARP
- Define and identify Collision and Broadcast domains
- Differentiate between a straight-through and crossover cable
- Identify the suitable cable type for connecting network devices
- Describe the role of Virtual Local Area Networks (VLANs) in switched networks
- Describe how traffic from different VLANs is identified and isolated
- Describe the purpose of a trunk link
- Describe the purpose of Spanning Tree Protocol

Murdoch UNIVERSITY

Ethernet Protocols

- Actually consists of two protocols: IEEE 802.2 and IEEE 802.3
- 802.2 is the specification for the Logical Link Control (LLC)
- 802.3 is the “Ethernet” specification, defining the MAC sub-layer functions as well as cables and connectors



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

CSMA/CD

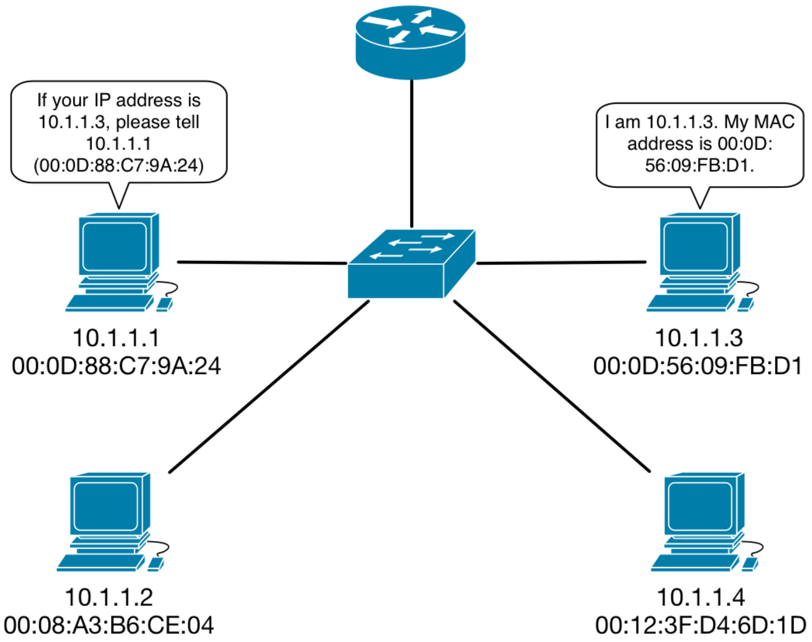
- Contention-based media access control used by Ethernet
- CSMA/CD process is:
  - Listen for other transmissions before transmitting
  - If no other transmissions heard, send data
  - Otherwise, wait for current transmission to end
  - Collisions generate a JAM signal, which prompts devices to back-off and wait for a random period of time
  - Once the timer expires, try to resend
- Now unnecessary in modern networks because of prevalence of switches

MAC Addresses

- Ethernet is a multi-access network and uses **MAC addresses** as its addressing scheme
- 48-bit address represented in hexadecimal (0—9, A—F)
- MAC Addresses only significant within the local network segment
- Flat structure (not hierarchical like IP)
- Common representations of MAC addresses:
    - 12:34:56:78:9A:BC
    - 12-34-56-78-9A-BC
    - 1234.5678.9ABC

Address Resolution Protocol (ARP)

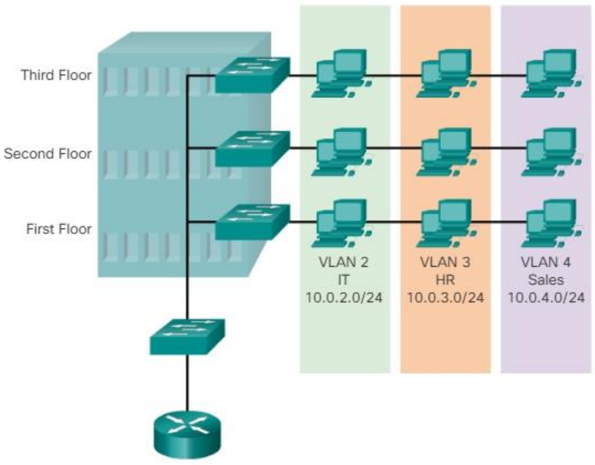
- ARP creates and maintains a list of mappings between IP and MAC addresses in the **ARP table**
- Hosts check their ARP table before transmitting packets bound for the local network
- If no mapping exists, an **ARP request** will be generated


If your IP address is 10.1.1.3, please tell 10.1.1.1 (00:0D:88:C7:9A:24)
I am 10.1.1.3. My MAC address is 00:0D: 56:09:FB:D1.
10.1.1.1
00:0D:88:C7:9A:24
10.1.1.3
00:0D:56:09:FB:D1
10.1.1.2
00:08:A3:B6:CE:04
10.1.1.4
00:12:3F:D4:6D:1D

Virtual LANs

- Logical networks allow networks to be extended between different physical locations
- Using VLANs enables the network administrator to create a number of smaller networks on a single switch
- Each VLAN becomes a different logical network (and its own broadcast domain)
- Distinguish between VLANs using a VLAN ID

Defining VLAN Groups



Break

When we return: A look back at Topics 6—10

Topic 6 – IPv6 and Network Address Translation

You should now be able to:

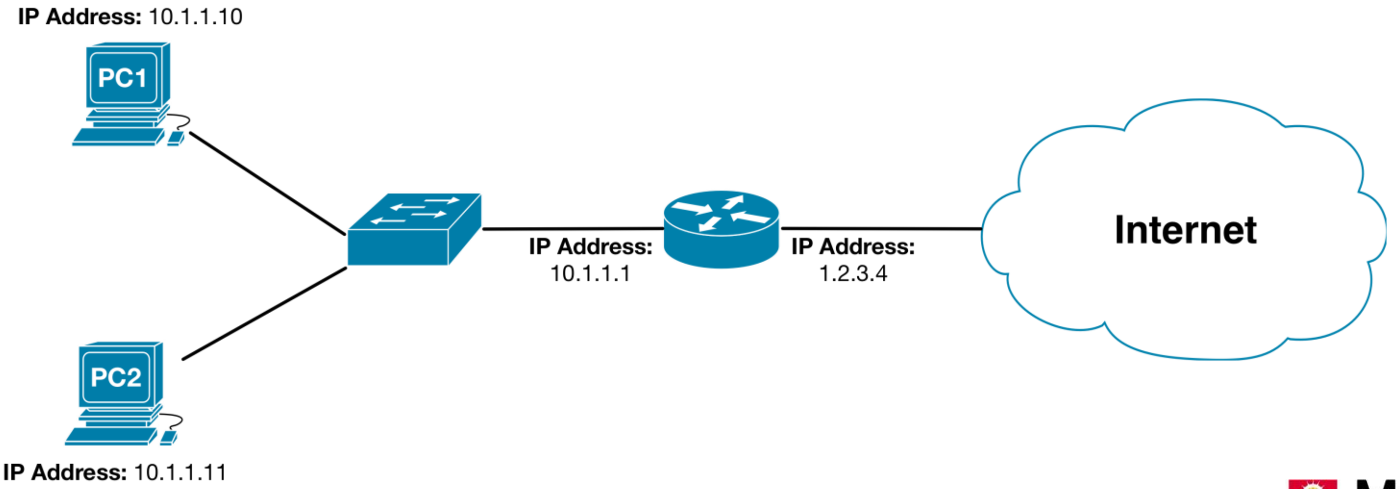
- Describe IP version 4 address exhaustion
- Discuss the causes and consequences of IP version 4 address exhaustion
- Describe the purpose of Network Address Translation
- Describe the operation of Network Address Translation
- Identify challenges posed by the use of Network Address Translation
- Differentiate between IP version 4 and version 6
- Identify an IPv6 address
- Describe components of an IP version 6 address
- Describe IPv6 anycast transmission
- Identify approaches to transitioning from IP version 4 to IP version 6

IPv4 Address Exhaustion

- 32 bit addresses allowed for 2^{32} (4,294,967,296) addresses
- Requirements for IP addresses have changed since 1980 and early allocation practices were very inefficient
- AFRINIC the only RIR to still have IPv4 addresses
- Some organisations are returning unused IPv4 addresses, allowing RIRs to reallocate them
- Classess Inter-Domain Routing (CIDR) was adopted
  - Think VLSM
- Network Address Translation (NAT) became commonplace

NAT Operation

- NAT creates mappings between private IP address and port number combination (eg. 10.1.1.10:32453) to a public IP address and port combination
- Allows multiple devices with private IP addresses to share a single Internet connection
- Breaks the end-to-end nature of the Network layer

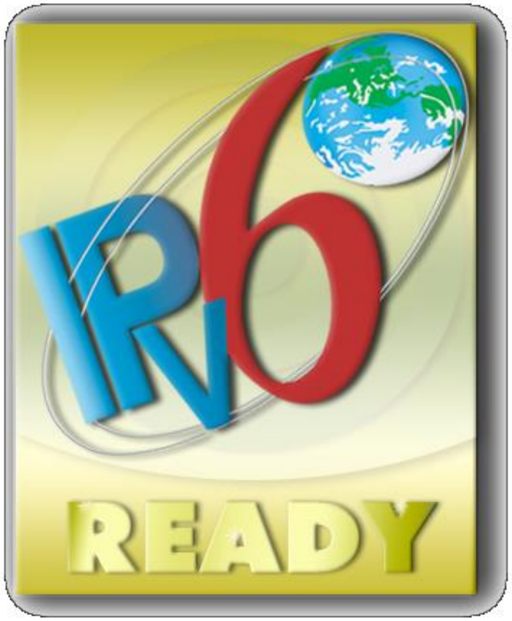


Internet Protocol version 6 (IPv6)

- Increase address length to 128 bits represented as eight 16 bit hexadecimal numbers separated by colons (:)
    - Example: 2001:0db8:0031:0001:020a:95ff:fef5:246e
    - Each hexadecimal digit is 4 bits long
- Simplified packet headers
- Automatic address configuration (without requiring DHCP)
- Mobility; devices to be always reachable
- Integrated IP Security (IPSec)

The Road to IPv6

- So IPv6 sounds great on a technical level, so why are we still stuck with IPv4?
  - Lack of economic incentives for organisations
  - Lack of backwards compatibility with IPv4
  - Lack of perceived urgency (NAT and IPv4 markets exist)



http://blogs.technet.com/b/ipv6/archive/2007/11/13/windows-vista-earns-ipv6-ready-logo-phase-2.aspx

Review Question

Which of the following IPv6 addresses is in its most condensed form? (Choose two.)

a) aaaa:0000:0450:0000::acdc:0210

b) aaaa:0:0450::acdc:0210

c) aaaa:0:450::acdc:210

d) aaaa::450:0:0:acdc:210

e) aaaa::0450:0000:acdc:210

f) aaaa::450:0:0:0:acdc:210

Review Question

Which of the following IPv6 addresses is in its most condensed form? (Choose two.)

a) aaaa:0000:0450:0000::acdc:0210

b) aaaa:0:0450::acdc:0210

c) aaaa:0:450::acdc:210

d) aaaa:0000:450:0:0:acdc:210

e) aaaa::0450:0000:acdc:210

f) aaaa::450:0:0:0:acdc:210

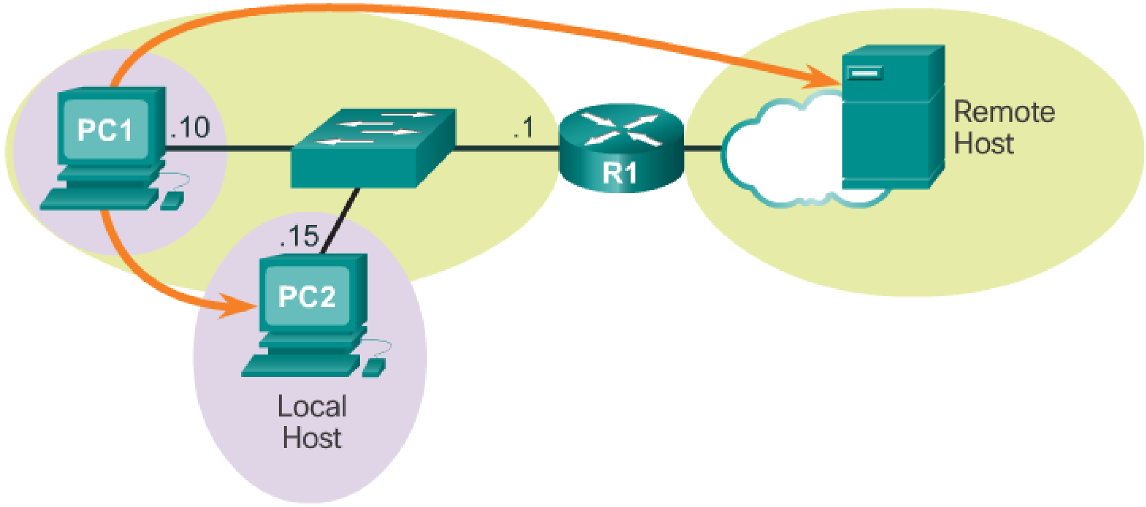
Topic 7 – Interior Routing

You should now be able to:

- Describe the packet forwarding process
- Describe the purpose of the default gateway
- Describe the process of routing packets between networks
- Describe the role of the routing table in routing packets between networks
- Identify key attributes of the routing table
- Differentiate between static and dynamic routing
- Describe the purpose of default routes
- Describe the characteristics of distance vector routing protocols
- Describe the characteristics of link-state routing protocols
- Differentiate between distance vector and link-state routing protocols

Packet Forwarding

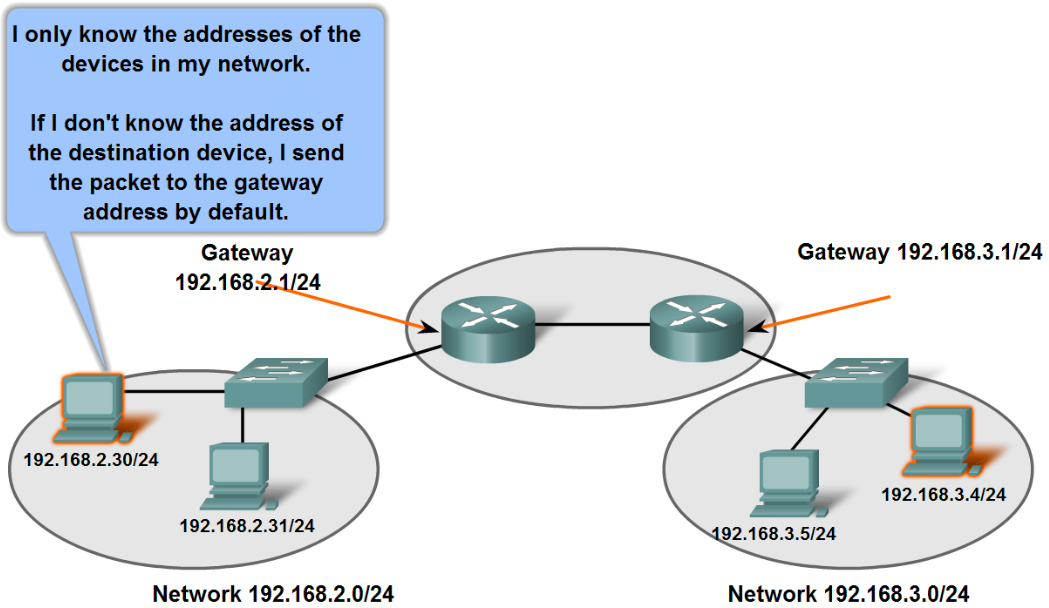
- When a device is readying a packet for submission, it first checks whether the destination is in its local subnet
- If the destination is in the local subnet, the devices will use Layer 2 addressing
- Otherwise, the packet will be forwarded to the default gateway



The Default Gateway

- The default gateway is the router responsible for forwarding traffic outside of the local subnet
- As the gateway exists within the local subnet, packets are forwarded to the gateway using its Layer 2 address

Gateways Enable Communications between Networks

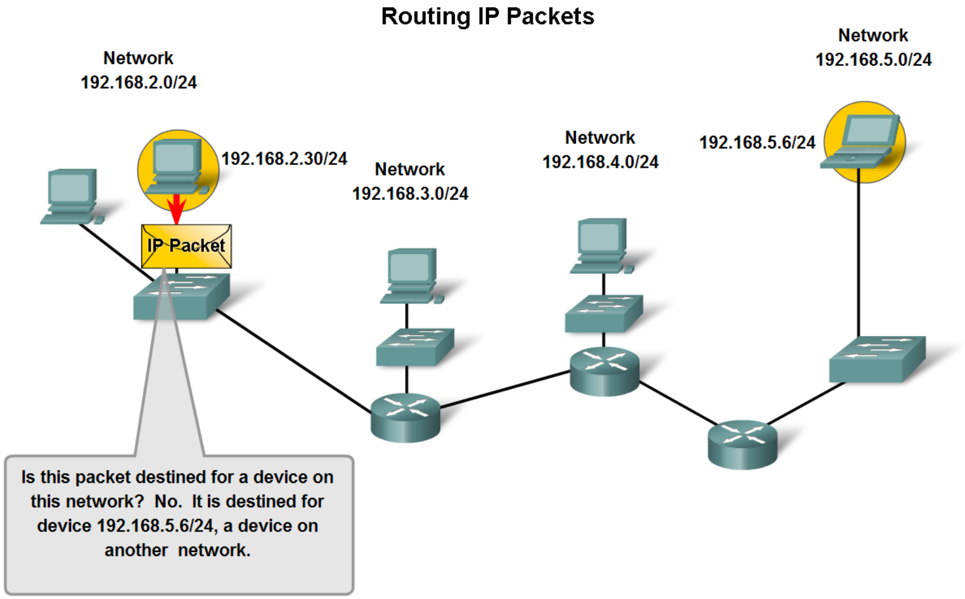


I only know the addresses of the devices in my network.

If I don't know the address of the destination device, I send the packet to the gateway address by default.

Routers and the Routing Process

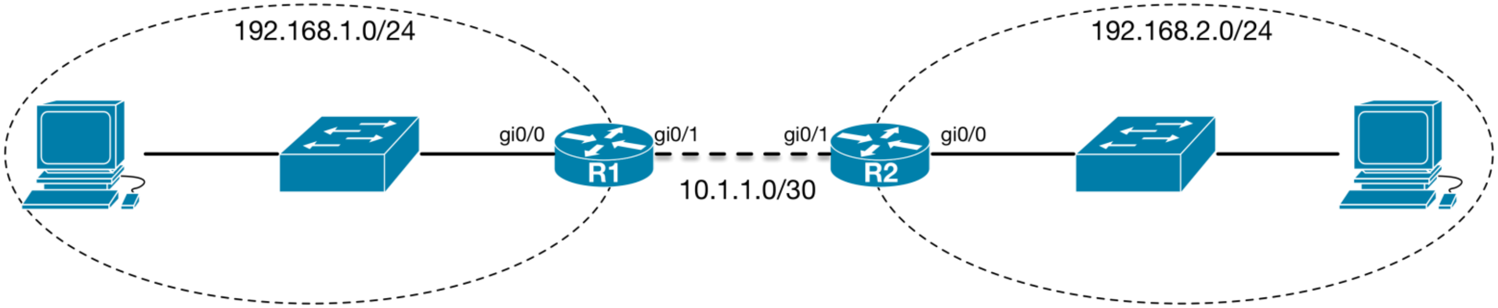
- Routers are used to forward packets from one network to another
- Routers interfaces must belong to different IP networks
- Decision to forward the packet made based on the destination IP address



Is this packet destined for a device on this network? No. It is destined for device 192.168.5.6/24, a device on another network.

Establishing Routes

- Routers are able to acquire knowledge of remote networks using two techniques:
    - A network engineer may manually enter a **static route**
    - **Routing protocols** may be used to propagate information between routers



Dynamic Routing Protocols

- Routing protocols can be divided into two categories
- **Interior Gateway Protocols (IGPs)** are used to route within an administrative domain (eg. a single organisation)
    - Some examples include: Router Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF)
- **Exterior Gateway Protocols (EGPs)** are used for routing packets between autonomous systems (eg. between organisations)
    - Only one EGP in common use: Border Gateway Protocol (BGP)
    - Used to route Internet traffic

Comparing Routing Protocols

	Distance Vector	Link-State
Message complexity	Exchange entire routing table between neighbours	Flood link-state advertisements throughout network
Robustness / Accuracy of path cost	Errors by one router can propagate throughout network	Each router computes its own table
Resource requirements	Low (just use advertised routing tables)	High memory and CPU requirements (compute own routing table)
Convergence	Slow (unless triggered updates available	Fast

Review Question

Which of the following statements regarding dynamic routing protocols is false?

a) Distance vector routing protocols propagate routing information by transmitting the entire routing table

b) Link-state routing protocols send updates periodically

c) Link-state routing protocols send updates only when the network topology changes

d) Distance vector routing protocols can propagate erroneous information throughout the network

Review Question

Which of the following statements regarding dynamic routing protocols is false?

a) Distance vector routing protocols propagate routing information by transmitting the entire routing table

b) Link-state routing protocols send updates periodically

c) Link-state routing protocols send updates only when the network topology changes

d) Distance vector routing protocols can propagate erroneous information throughout the network

Topic 8 – Exterior Routing and the Internet

You should now be able to:

- Describe the operation of Open Shortest Path First (OSPF)
- Describe the purpose of Neighbour Adjacencies in OSPF
- Describe the purpose of Link-State Advertisements
- Describe the role of the Link-State Database in computing routes
- Describe the metric used by OSPF in determining the best path
- Identify the role of the Designated and Backup Designated Routers
- Describe the purpose of areas in OSPF
- Describe the role of the backbone area in OSPF operation
- Differentiate between interior and exterior gateway routing
- Describe the operation of the Border Gateway Protocol
- Differentiate between the BGP and interior gateway routing protocols

Murdoch UNIVERSITY

Dynamic Routing Protocols

- Routing protocols can be divided into two categories
- **Interior Gateway Protocols (IGPs)** are used to route within an administrative domain (eg. a single organisation)
    - Some examples include: Router Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF)
- **Exterior Gateway Protocols (EGPs)** are used for routing packets between autonomous systems (eg. between organisations)
    - Only one EGP in common use: Border Gateway Protocol (BGP)
    - Used to route Internet traffic

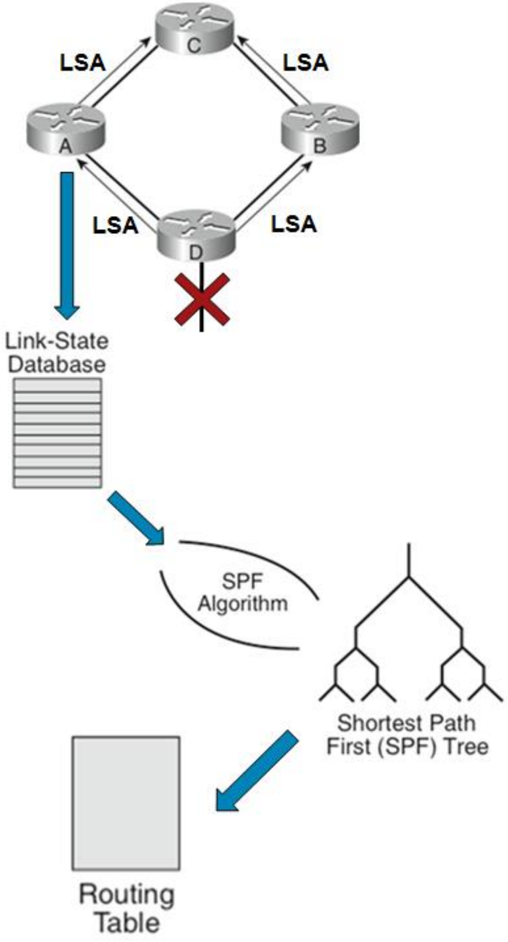
Open Shortest Path First (OSPF)

- Implements the key properties of link-state routing protocols:
  - Routers construct individual shortest path trees
  - Updates are triggered when network topology changes
    - Less bandwidth use (no periodic updates)
    - Faster notification of changes to network
- Uses cost as a routing metric to make more intelligent decisions about routing
  - Link cost takes speed into account
- Allows for routers to be grouped into multiple areas for scalability

OSPF Operation

So how does this all work?

1. Routers form neighbour adjacencies with neighbouring routers
2. Flood **Link State Advertisements (LSAs)** to all neighbouring routers
3. Add information from received LSAs to **Link-State Database (LSDB)**
4. Compute best routes based on Dijkstra’s algorithm
5. Install best routes into the **routing table**



Border Gateway Protocol (BGP)

- The only exterior gateway protocol currently available and in use
- Designed to allow routing **between autonomous systems** and manage large numbers of routes
- Can also be used internally (usually only for very large networks)
- Path vector routing protocol
  - Similar to distance-vector routing algorithm
  - Includes a list of AS along the path to destination
- Only routing protocol to use TCP (most IGPs use IP)

Review Question

Which of the following is a property of exterior gateway routing protocols?

a) Calculates the best path to all destinations based on a routing metric

b) Constructs a map of the entire network before making routing decisions

c) Used to propagate routing information within a single administrative domain

d) Designed to propagate routing information between multiple administrative domains

Review Question

Which of the following is a property of exterior gateway routing protocols?

a) Calculates the best path to all destinations based on a routing metric

b) Constructs a map of the entire network before making routing decisions

c) Used to propagate routing information within a single administrative domain

d) Designed to propagate routing information between multiple administrative domains

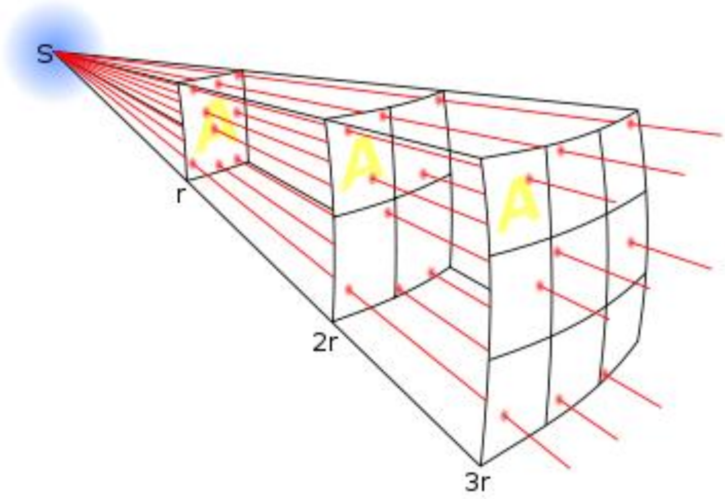
Topic 9 – Wireless Networks

You should now be able to:

- Describe the motivation for using wireless technologies
- Describe common wireless technologies and their applications
- Differentiate between Personal Area, Local Area and Wide Area wireless networks
- Differentiate between different wireless media access control techniques
- Differentiate between CSMA/CA and CSMA/CD
- Describe the relationship between spectrum use, transmission power and range in relation to wireless networks
- Differentiate between different 802.11 standards
- Describe the limitations of 802.11 performance
- Differentiate between infrastructure and ad-hoc networking in relation to 802.11
- Describe the purpose of the Service Set Identifier in relation to 802.11 networks
- Differentiate between the security mechanisms available to protect 802.11 networks

Wireless Range

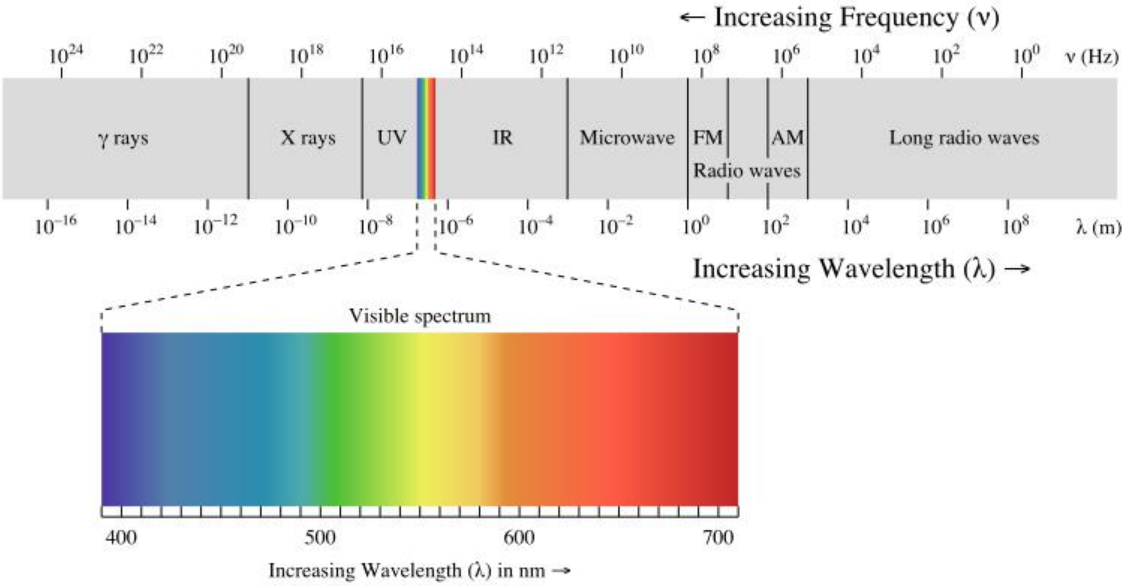
- Wireless technologies suffer the most attenuation of any transmission media
- Every time the distance doubles, the energy from a wireless transmission is spread over four times the area; this is known as the **inverse square law**
- The result is that the signal strength is reduced to ¼



http://en.wikipedia.org/wiki/Inverse-square_law

Frequency

- Wireless transmissions are transmitted using electromagnetic spectrum
- Radio communications operate at frequencies between 30KHz and 300GHz
- Lower frequencies propagate further (and usually penetrate solid objects better) than higher ones



← Increasing Frequency (ν)
10^{24} 10^{22} 10^{20} 10^{18} 10^{16} 10^{14} 10^{12} 10^{10} 10^{8} 10^{6} 10^{4} 10^{2} 10^{0} ν (Hz)
γ rays
X rays
UV
IR
Microwave
FM
AM
Radio waves
Long radio waves
10^{-16} 10^{-14} 10^{-12} 10^{-10} 10^{-8} 10^{-6} 10^{-4} 10^{-2} 10^{0} 10^{2} 10^{4} 10^{6} 10^{8} λ (m)
Increasing Wavelength (λ) →
Visible spectrum
400
500
600
700
Increasing Wavelength (λ) in nm →

http://en.wikipedia.org/wiki/File:EM_spectrum.svg

802.11 (WiFi)

- Most common wireless technology used to provide LAN connectivity in homes and enterprise
- Original version of 802.11 provided data rates of 1—2Mbps
- Latest standard (802.11ac) allows for speeds up to 2.34Gbps
- Operates on 2.4GHz or 5GHz spectrum

Review Question

802.11n (WiFi 5) operates over which frequencies? (Choose all that apply)

a) 700MHz

b) 900MHz

c) 1.8GHz

d) 2.4GHz

e) 5GHz

f) 5.8GHz

g) 60GHz

Review Question

802.11n (WiFi 5) operates over which frequencies? (Choose all that apply)

a) 700MHz

b) 900MHz

c) 1.8GHz

d) 2.4GHz

e) 5GHz

f) 5.8GHz

g) 60GHz

Topic 10 – Internet Security

You should now be able to:

- Describe motivations for hacking
- Differentiate between white hat and black hat hackers
- Describe confidentiality, integrity, and availability in relation to computer security
- Differentiate between types of cyberattacks
- Differentiate between active and passive reconnaissance in relation to computer security
- Identify tools and techniques that can be used in cyberattacks
- Describe a denial of service attack
- Differentiate between denial of service and distributed denial of service attacks
- Describe defence in depth in relation to computer security
- Describe the concept of ‘security through obscurity’
- Describe methods for securing the network
- Describe methods for securing endpoint devices
- Describe the tradeoff between security and convenience

The CIA Triangle

- Three primary principles and goals used in security:
  - Confidentiality – keep the data secure from unauthorized people
  - Integrity – prevent tampering with the data
  - Availability – make sure the data and services are always available
- Referred to as the **CIA triangle** (or sometimes triad)

Types of Attacks

- **Reconnaissance** – Find information regarding a potential victim (usually to help plan another attack)
  - Passive – use existing information sources
  - Active – make direct contact with the target
- **Access and Intrusion** – Aim to gain unauthorised access to a system or network
- **Denial of Service** – Aim to impact the availability of a system or network and prevent legitimate access
- **Data Manipulation** – intercept and modify communications between the victim and their destination

Review Question

Which of the following statements regarding the CIA triangle are true?

a) Data modified without authorisation constitutes a breach of confidentiality

b) Availability describes the ability to prevent unauthorised persons from accessing data

c) Data modified in transit has been subject to a breach of integrity

d) Rendering a system or resource inaccessible constitutes a breach of integrity

Review Question

Which of the following statements regarding the CIA triangle are true?

a) Data modified without authorisation constitutes a breach of confidentiality

b) Availability describes the ability to prevent unauthorised persons from accessing data

c) Data modified in transit has been subject to a breach of integrity

d) Rendering a system or resource inaccessible constitutes a breach of integrity

Don’t Forget the Labs

- Content from the lab exercises are also examinable
    - Ensure that you’re familiar with the protocols we’ve examined and configured
    - Parameters used for commands
- Identify, describe, and interpret output from key tools used (eg. ping, traceroute, Wireshark, Nmap)
- Determine possible causes of issues based on a description
    - What steps would you take to identify a problem?
    - What layer is the issue likely to be occurring at?
    - What could go wrong with key protocols?

Unit Summary

- Throughout this semester, you should have gained a solid understanding of the fundamental concepts involved in networking
  - Networking models, key protocols, amongst others
- Also gained some specialised skills like configuring networking devices, subnetting, and examining network traffic
- You may not use all these skills again, but hopefully some of the knowledge will be valuable

Murdoch UNIVERSITY

My feedback

Have your say.
Unit and Teaching Surveys now open.

moss.murdoch.edu.au

Best of luck with the Final Exam

I will still be contactable during the study break