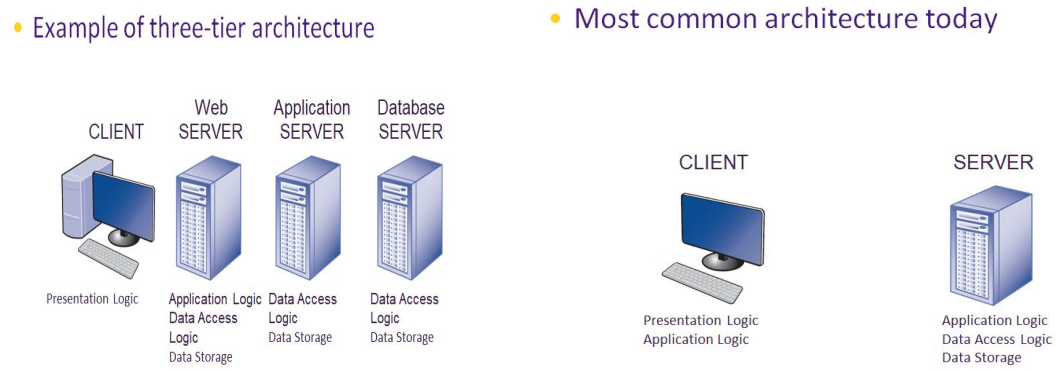
ISDS 4120
Exam 2

Exam 2 will be a closed note, closed book, closed Internet Moodle based exam. The exam will consist of multiple choice, matching, short answer, and scenarios and you will have 50 minutes to complete the exam.
The content will cover lectures 6 to 9 and chapters 4 to 10 of the Fitzgerald book.
What follows is a list of the concepts and models on the exam. It is not enough to simply memorize the definitions or concepts – the key will be your ability to take the concepts and models and apply them to information presented to you.
If you cannot locate a concept, reach out to your colleagues for assistance – I highly recommend forming study groups to assist you.

Concept Questions

- **What does an application layer address using TCP look like?**
  Example of application layer address: www.indiana.edu
- **The functions of the application layer**
  - Presentation Logic
  - Application Logic
  - Data Access Logic
  - Data Storage
- **The division of software on clients versus servers for three tier and two-tier architecture**



- **Where server name resolution is done**
  - Network Layer
- **What does TCP use to reassemble packets in the correct order?**
  - Sequence Numbers (protocols)

- **The attributes of a sound wave**
  - **Amplitude:** height of wave (decibels)
  - **Frequency:** waves per second (hertz)
    Wavelength is the inverse of frequency
  - **Phase:** wave direction (degrees) or the point at which the wave begins

- **What routing means; the three fundamental approaches to routing; and different types of dynamic routing**
  - **Routing:** Process of identifying what path to have a packet take through a network from sender to receiver

    - **Centralized Routing:** Routing decisions made by one computer; *not common these days*. Centralized routing is commonly used in host-based networks (see Chapter 2), and in this case, routing decisions are rather simple. All computers are connected to the central computer, so any message that needs to be routed is simply sent to the central computer, which in turn retransmits the message on the appropriate circuit to the destination.
    - **Static Routing-**Static routing is *decentralized*, which means that all computers or routers in the network make their own routing decisions following a formal routing protocol.With static routing, routing decisions are made in a fixed manner by individual computers or routers. The routing table is developed by the network manager, and it changes only when computers are added to or removed from the network.
      - For example, if the computer recognizes that a circuit is broken or unusable (e.g., after the data link layer retry limit has been exceeded without receiving an acknowledgment), the computer will update the routing table to indicate the failed circuit. If an alternate route is available, it will be used for all subsequent messages. Otherwise, messages will be stored until the circuit is repaired. *Static routing is commonly used in networks that have few routing options that seldom change.*
    - **Dynamic Routing-** With dynamic routing (or adaptive routing), routing decisions are made in a decentralized

manner by individual computers. This approach is used when there are multiple routes through a network, and it is important to select the best route.

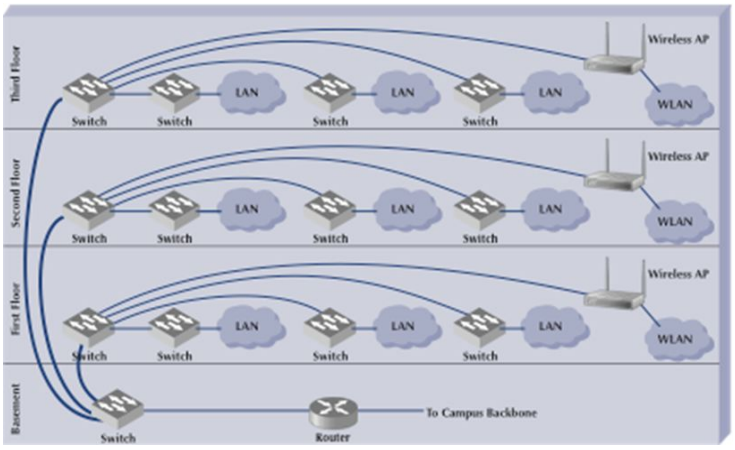
        - **Two Types of Dynamic Routing:**
            - **<u>Distance vector:</u>** based on the number of “hops” between two devices
            - **<u>Link state</u>**: based on the number of hops, circuit speed, and traffic congestion
- **What does the transport layer do to the messages?**
    - Link to the application layer
    - Segment
    - Session Management
- **How the capacity of a circuit is determined**
    - Bandwidth
- **The different types of data**
    - *Digital transmission* involves discrete binary values (i.e., 0 or 1)
    - *Analog transmission* involves continuous waves
- **The factors to consider when selecting media to be used in a network**
    - Type of network
    - Cost
    - Transmission distance
    - Security
    - Error rates
    - Transmission speeds
- **How contention and collision work and which is better for different types of networks**
    - **Contention**- Transmit whenever circuit is available with no centralized control. With low traffic, the high overhead of controlled access makes contention more efficient**.**
    - **Collision:** is the result of two devices on the same Ethernet network attempting to transmit data at exactly the same time. The network detects the "collision" of the two transmitted packets and discards them both.
    - **Devices must be “polite” and follow these steps:**
        - “Listen” for traffic
        - If another device is transmitting, wait to transmit
        - Otherwise, transmit (and keep listening)
        - If another device begins to transmit, stop and wait

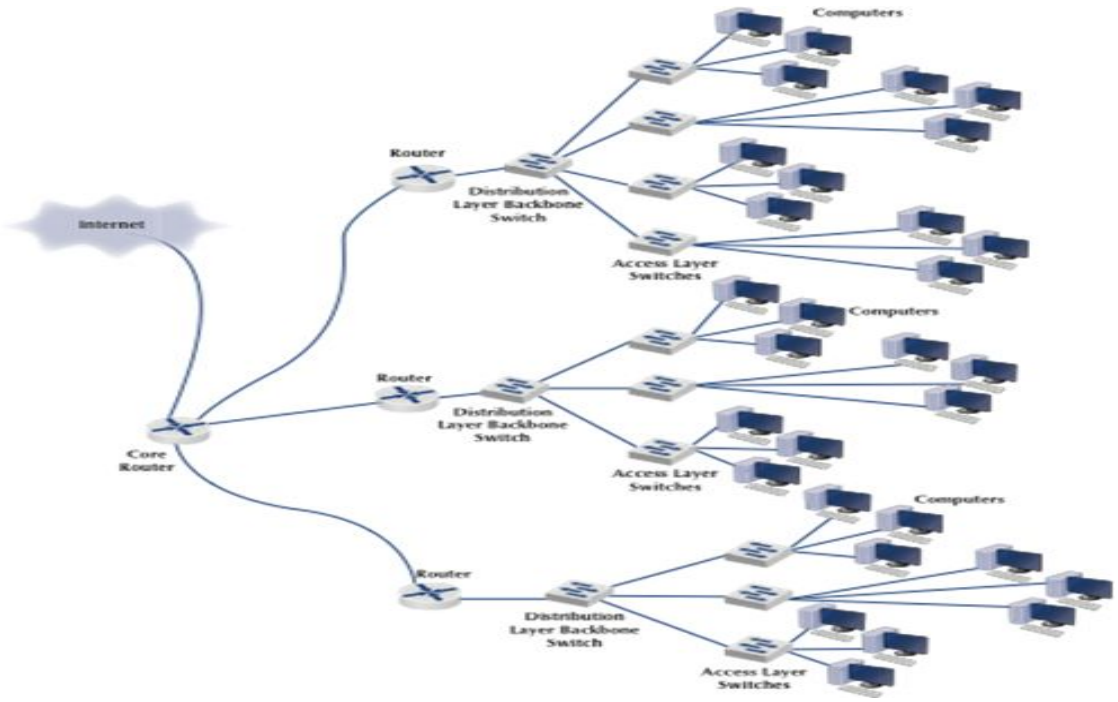
    - **Controlled Access**- Each device must get “permission” to transmit

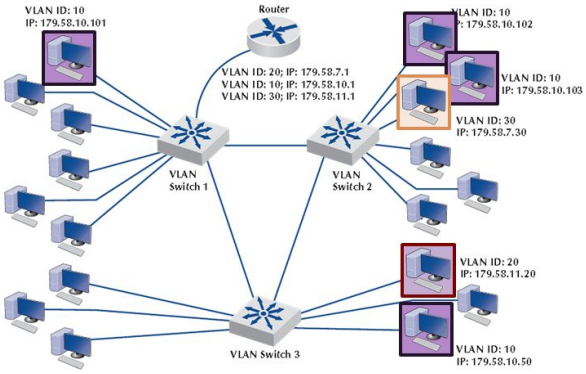
- **What polling means from a networking perspective**
    - **Polling:** is the process of sending a signal to a client that gives it permission to transmit or asks it to receive.
        - Roll-call polling
            - Central device (controller) determines which devices can transmit
            - Each client is checked periodically to see if it needs to transmit
        - Hub Polling (token passing)
            - One device begins the poll and then passes it to another device until it reaches them all
- **How an application layer address is translated to an IP address**
    - DNS Request Packet
- **The difference between the logical and physical design of a circuit**
    - The word circuit has two very different meanings in networking, and sometimes it is hard to understand which meaning is intended. Sometimes, we use the word circuit to refer to the physical circuit—the actual wire—used to connect two devices. In this case, we are referring to the physical media that carries the message we transmit, such as the twisted pair wire used to connect a computer to the LAN in an office. In other cases, we are referring to a logical circuit used to connect two devices, which refers to the transmission characteristics of the connection, such as when we say a company has a T1 connection into the Internet. In this case, T1 refers not to the physical media (i.e., what type of wire is used) but rather to how fast data can be sent through the connection.
- **The definition of a bottleneck**
    - In any network, there may be a bottleneck, a circuit that is filled almost to its capacity and thus is the critical point that determines whether users get good or bad response times. When users complain about a slow network, it is usually because there is a bottleneck circuit somewhere in the network.
- **How a star, ring, and mesh network work**

Architecture	Advantages	Disadvantages
Ring	• Robust to loss of any one circuit	• Long routes may increase communication latency
Star	• Simpler management • Messages require 1 or 2 hops • Circuit failure primarily affects a single site	• Susceptible to traffic problems • Failure of the central site will cause complete network failure
Mesh	• Generally short routes • Robust to the circuit loss or overloaded circuits	• Expensive

- **The difference between a hub, router, and switch**
  - Hub
    - Least expensive, least intelligence
    - If a message comes in for a specific computer, sends that message to all computers
    - Layer 1
  - Switch
    - Similar to hub, but learns, based upon experience, where a specific computer is located (sends message only to the destination)
    - Layer 2 (sometimes 3)
  - Router
    - Most expensive, most intelligence
    - Using protocols, know where every computer is located on a network

- **Different types of backbone networks and their logical and physical topologies**
  - **Switched**
  - 

- **Routed**
- 

- **Virtual**
- 

- · **Different backbone network options for a firm, the topologies of each, and the benefits and drawbacks**
  - **Switched -** good for distribution layer
    - Pros: inexpensive and fast
    - Cons: not as flexible
  - **Routed -** good for core layer
    - Pros : LAN segmentation
    - Cons: tend to be slower, more expensive, harder to manage
  - **Virtual -** good for very large networks
    - Pros: very flexible LAN segmentation
    - Cons: Very complex to manage

- **Different approaches to monitor connections on a network**
    -
- **The definition and purpose of network segmentation**
    - **Segmenting**: Breaking up large files into smaller segments (and putting them back together). Segments may be passed individually to the application layer or after reassembly. The size of the segment depends on the network and data link layer protocols.
- **The activities associated with each of the stages of network design**
    - Needs analysis
        - Understand current and future network needs (users and applications)
    - Technology design
        - Examine available technologies to determine which meet or exceed needs
        - If needs are difficult to estimate, build higher capacity
    - Cost assessment
        - Evaluate financial costs of technology
- **The definition and types of media access control**
    - Controls which device transmits and when
    - **Contention- –Transmit whenever circuit is available with no centralized control**
    - **Controlled- Each device must get "permission" to transmit, similar to raising a hand**
- **The different layers of the backbone architecture**
    - **Access layer-**how users access network
    - **Distribution layer-**connects access layer to core layer (within building)
    - **Core layer-**connects BN between buildings and to WAN/internet
- **The advantage of a VPN versus a private WAN connection**
    - **VPN** is more cost effective and flexible
    - **WAN** isn't affected by internet disruptions, more compatible
- **Options to improve backbone performance**
    - Upgrade server/routers/switches/hardware
    - Upgrade circuits
    - Reduce demand
- **The definition of visioning**
    - Emailed Dr Schwarz: "In this context, visioning is more of a broader idea of thinking about the vision for the network in a company."

- **Options to monitor and control a network**
    A. **Managed networks** consist of managed devices that enable a network manager to consistently monitor the performance of the network (may be more expensive for initial investment, but save more money in management)
    B. **Network management software**: allows managers to monitor performance and configuration of devices on network (system and management software) **(Exam Question) Network Management Software enables:**
        a. Load Balancing
            i. Spreading the traffic to different devices in server farm/cluster
        b. **Traffic Shaping**
            i. Movement of traffic within the network
        c. Configuration Management
            i. Configuration of devices on the network
        d. Performance management
            i. Monitor the performance of the network
    C. Simple network management protocol (SNMP):
        1) Most commonly used protocol for managing network devices
        2) The network management software uses SNMP to communicate with software agents on managed devices
        3) Data is stored in management information base (MIB)

Performance and Configuration

- **Be able to state the five layers of the OSI model in order; Be able to identify the functionality of each of the layers; Be able to match the protocols to the layers of the OSI model**

Layer	Purpose	Example Protocols/ Standards	PDU
5. Application	**User's access to network, software to perform work**	**HTTP, SMTP, DNS, FTP, DHCP, IMAP, POP, SSL**	**Packet (or Data)**
4. Transport	**End-to-End Management** **1. Link application layer to network** **2. Segmenting and tracking** **3. Flow Control**	**TCP, UDP**	**Segment**
3. Network	**Deciding where the message goes**	**IP, ICMP**	**Packet**

	1. **Addressing** 2. **Routing**		
2. Data Link	**Move a message from one device to the next** 1. **Controls hardware** 2. **Formats the message** 3. **Error checking**	**Ethernet**	**Frame**
1. Physical	**Transmits the message**	**100BASE-T, 802.11n**	

- **The three choices when outsourcing to the cloud and be able to match them to the grid**
  - IaaS
  - PaaS
  - Saas
  -

	Traditional Thin-Client Client-Server		Infrastructure as a Service (IaaS)		Platform as a Service (Paas)		Software as a Service (SaaS)	
	Internal	Outsourced	Internal	Outsourced	Internal	Outsourced	Internal	Outsourced
Application Logic	X		X		X			X
Data Storage	X		X		X			X
Data Access Logic	X		X			X		X
Operating System	X		X			X		X
Virtualization Software	X		X			X		X
Server Hardware	X			X		X		X
Storage Hardware	X			X		X		X
Network Hardware	X			X		X		X

- **The six components of a LAN and the two broad choices that are available when designing the LAN**
  - Client, server, NIC, wiring, ap/routers/switches, software
  - Two Broad Choices when designing the LAN
    - Wired ethernet
    - Wireless ethernet

<u>Applications</u>

- **Best practices for architecture and technology for LAN design**

The best practice for architecture and tech for LAN design is to install dedicated ethernet circuits for desktops along with a wireless network overlay for extra devices.

o Architecture
Switched has best cost to performance ratio at the distribution layer
Most organizations use routed at the core layer
VLANs are becoming more widely used, especially for organizations needing the flexibility
o Technologies
Gigabit Ethernet for distribution layer
Gigabit Ethernet or faster for core layer
Redundant devices and connections

- **Should companies build to network capacity? Why or why not?**

Typically, companies build just above capacity so there is room for growth. Scalable architectures are also a good solution so that companies can upgrade components later on bottleneck by bottleneck.

- **The advantage of layers, from an OSI model perspective (be able to identify 3)**
    - By separating networking functions into logical smaller pieces, network problems can more easily be solved through a divide-and-conquer methodology. OSI layers also allow extensibility. New protocols and other network services are generally easier to add to a layered architecture.Allows different types of network hardware and software to communicate.
- o Advantages of Layers

Networking functionality is modular and the software/hardware at any layer can be more easily substituted
E.g., substitute wired for wireless at the physical layer
Easier to troubleshoot or make changes to one layer at a time
Application developers only need to worry about the application layer in their programs