# Final Exam Prep

Applied Data Communications and Networks (York University)

# AP ITEC 3210 FINAL EXAM REVIEW

Network DESIGN

ABSTRACT

A Final Exam Review that encompasses content for final exam preparation

York University Winter 2021

AP ITEC 3210

# Table of Contents

- Standards and key characteristics:

| Standard | Frequency | Non-overlap. channels | Maximum data rate | Maximum range | Backward compatibility | Status |
|---|---|---|---|---|---|---|
| 802.11b | 2.4 GHz | 3 | 11 Mbps | 150 m | N.A | Obsolete |
| 802.11a | 5 GHz | 8 to 12 | 54 Mbps | 50 m | N.A | Obsolete |
| 802.11g | 2.4 GHz | 3 | 54 Mbps | 150 m | 802.11b | Obsolete |
| 802.11n | 2.4 GHz | 3 | 450 Mbps | 100 m | 802.11b / g | Still in use |
| 802.11ac | 5 GHz | 8 to 12 | Up to 6.9 Gbps | 100 m | 802.11 a | Best |

## *WEEK 8 LECTURE*

## CHAPTER 6 – NETWORK DESIGN (FITZ)

## KEY TERMS

### A. Local Area Network (Access Layer)

- **1st network architecture component and Local Area Network (LAN)**
- **Typical speed: 1 Gbps**
- **Provides wired and wireless access to network**
- Focuses on connecting client nodes, such as workstations to the network and ensures that packets are delivered to end user computer.
  - **Examples:**
    - **Network**
    - **Hubs**
    - **(Layer 2 & 3) Switches**
    - **Wireless Access Points**

### B. Baselines

- **Part of Needs Analysis**
- **Gain understanding of the current operations (application systems and message).**
- Provides a baseline against which future design requirements can be measured
- **Examples:**
    - **Operations**
    - **processing times**
    - **work volumes**
    - **current communication network).**

### C. Bottleneck

- **Place where performance of an entire system is limited by capacity at some point in a network.**
- Exist on physical circuits on a networking device
- Network managers are concern about them since fixing or upgrading these points with bottleneck improves network performance.

### I. TCP Fairness – Fairness Goal (KUROSS)

- **If K TCP sessions share same bottleneck link of bandwidth R, each should have the average rate of R/K.**

### D. Building Backbone Network (Distribution Layer)

- **2nd network architecture component and Distribution Layer.**
- Distributes network traffic to and from LANs.
- Uses same basic technology used in the LAN (LAN-based routers and Layer 3 switches).
- Ensures that packets are properly routed between subnets in enterprise.
- Buy faster switches since building backbone carries more traffic than a LAN.
- **Typical Speeds: 10 Gbps**

### E. Building-Block Network Design Process

- **Simpler approach to network design**
- **"Narrow and Deep Process":** Use few standard components to **simplify design and reduce costs.**
- **Assumes that network demand will grow**, therefore, makes no attempt to accurately understand current network demand.
- **Needs analysis** involves developing a logical network design that contains geographic scope of network, categorization of current and future network needs of the various network segments, users and applications as either typical or high traffic.
- **Technology design** produces a set of one or more physical network design. Network design and simulation tools contributes in selecting the technology that typical and high-volume users, application and network segments will use.
- **Cost Assessment** is the final step and usually done through RFP which specifies what equipment,

software, and services are desired and ask vendors to provide their best prices.

- **One of the keys to gaining acceptance by senior management** of the network design relies on their language **(cost, network growth and reliability).**

**Three major steps in current network design:**

I. Needs Analysis

- **Understand current and future network needs of users, departments and applications.**
- User access and the needs of applications drive the network design process from top into the centre of network.
- Needs classified as typical or high volume and specific tech needs are identified.
- **Create metrics of current operations to compare sign requirement against (refer to *baselines*).**
- **Outcome of the needs analysis** and set of network diagrams are also **logical** because they **answer the "what"** (Deliverable: Logical Network Design).

1. **Break down the network into architecture components (Layered Approach).**
   - Evaluate all 8 components
   - Easiest to start with Wide Area Network when top-down approach
   - Geographic Scope of Network
2. **Review the existing and expected applications that will use the network.**
   - Identify hardware and software requirements for these apps.
   - Identify protocols used by these apps.
3. **Identify and assess network users.**
   - Some users may have different needs and their needs can be classified as typical or high volume.
   - How many of each type of user?
4. **Categorize network requirement**
   - Mandatory
   - Desirable
   - Wish-list

II. Technology Design

- **Development of a physical network design (or set of possible design).**
- **Designer estimates about network needs** and of each category of user and circuit in current technology (1 Gbps Ethernet) and match needs to technology.
- **Predicting network demand is difficult** and **resolved by building more than expected capacity** and then monitor growth so they can expand the network ahead of growth pattern.
- Designing which hardware needs to be purchase and if possible, upgrade existing equipment.

1. **Designing clients and servers**
   - Specify of the devices needed in standard units.
   - "**Typical" users** are allocated **base-level clients.**
   - **"Advanced" users** are **allocated advanced clients.**
   - **Servers** are similarly allocated based on **application needs.**
   - Definitions of "typical" and "advanced" change as hardware costs fall, and capabilities increase.
2. **Designing circuits**

**Capacity Planning:**

- **Estimating the circuit size and type** of the standard and advanced network for each type of network (LAN, backbone, or WAN).
- **Typical circuit for Wired LANs:** 100 Mbps or 1Gbps.
- **Designing circuit capacity is more challenging** b/c backbones more traffic from many computers at one time and more choices in standard sizes.

### Circuit Loading:

- **Assessment of the amount of data transferred across a circuit or currently in the future.**
- 80% of circuit loading information is easy to collect.
- 20% needed for precise estimates is extremely difficult and expensive to find.

#### a) Estimating circuit traffic

- **Average traffic vs peak circuit traffic.**
  - *e.g., online banking network peaks at mid-morning and prior to closing.*

- **Designing for Peak traffic is ideal**
  - If possible, the max number of characters transmitted per 2-second interval if peaks must be met.

#### b) Estimating message volume

- **Average traffic vs peak circuit traffic.**

#### c) Precision may not be the major concern

- **Obtaining precise estimates is difficult and expensive.**
- Standard circuit speeds **"stair step"**
  - Instead of focusing on making prediction of future traffic needs, we **use standard network components and expect in future to reduce** management and design **costs.**
  - The reason **we stick on standard circuit "stair step"** instead of estimating traffic since it is time-consuming.
  - Traffic typically increases more than anticipated.

### Network Designers plan for Excess Capacity:

- Upgrading costs 50-80% more than designing higher capacity time.
- Very few complains about over capacity
- The **turnpike effect** occurs when traffic increases faster than forecast.
  - When networks are efficient and fast, users will use them more frequently.
  - Most networks designed with excess capacity end up using overcapacity within 3 years.

### Network Design Tools:

#### 1. Modeling

- **First step involves users creating diagrams of existing or proposed network.**
- Some modeling tools requires to create network diagram from scratch.
- User must place all network components (i.e., server, client computers and circuit on the diagram) manually.

#### 2. Discovery

- Some tools can **automatically create network diagrams by examining existing network.**

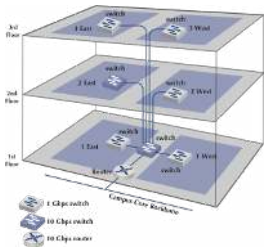
#### 3. Simulation

- **A mathematical technique used to model the behavior of a network under real conditions.**

- Simulates applications and users generating traffic and responding to messages.
- Tailored to users' needs by entering specific parameter values specific to network or average values provided by the network.
- User can examine the results to **see estimated response times** throughout one simulation is completed which may **highlight potential problems.**

**Deliverable (One or more physical network designs):**

- **Multiple designs may be created to highlight tradeoffs between performance and cost.**
- Critical part is design of circuits and networking devices
- Designs for new/upgraded clients and servers



- Representation of physical network design which answers the "how"
- It is 10 Gbps because it is design for LAN for conference room.
- There is a building backbone switch (10 Gbps switch) that organize local area network.

## III. Cost Assessment

- **Assess the cost of various physical network design alternatives.**
- **Main items are the costs of software, hardware and circuits.**
- Complex process that requires analysis of many factors which involves:
  1. **Circuit Costs** (Cabling and Installation provided by common carriers).
  2. **Internetworking Devices** (i.e., Switches and Routers)
  3. **Hardware Costs (**servers, printers, uninterruptible power supplies, backup tape drives).
  4. **Software Costs for** (OS, App software, Middleware)
  5. **Network management** (software and hardware) **costs,** training, monitoring and maintenance costs.
  6. **Tests and maintenance costs** (Operation costs to run the network)
  7. **WAN and Internet Circuits (**leased from common carriers).

### 1. Request for Proposal (RFP

- **Used for large network purchases**
- **Specifies what equipment, software and services desired from vendors to provide their best prices.**
- Items are categorized as mandatory, important, desirable or several scenarios are provided which lets the vendor proposes the best solution.
- Allows the organization to evaluate offerings from different providers

**Multi-vendor Proposals:**

- Difficult to manage
- Provide better performance
- Less expensive

**Selling the Proposal to Management:**

- Understand that **networks, data centers, and most information technology** is viewed as a **cost center.**
- Make a business case by focusing on organizational needs and strategy.
- The importance of network speed, reliability, and security are easy for non-technical users to understand
- Avoid focusing on technical details and jargon.

**Deliverables:**

1. **Finalized (FRP) For Request Proposal** goes to potential vendors.
2. **Revised physical network diagram** with technology design complete and product and costs are specified at this point.
3. **Business case** that provides support for **network design,** expressed in business objects.

### Request for Proposal (RFP) Key Parts:

#### 1. Background Information

- Organizational profile
- Overview of current network
- Overview of new network
- Goals of new network

#### 2. Network Requirements

- Choice sets of possible network designs (hardware, software, circuits)
- Mandatory, desirable, and wish list items
- Security and control requirements
- Response time requirements
- Guidelines for proposing new network designs

#### 3. Service Requirements

- Implementation time plan
- Training courses and materials
- Support services (e.g., spare parts on site)
- Reliability and performance guarantees

#### 4. Bidding Process

- Time schedule for the bidding process
- Ground rules
- Bid evaluation criteria
- Availability of additional information

#### 5. Information required from vendor

- Vendor corporate profile
- Experience with similar networks
- Hardware and software benchmarks
- Reference list

### F. Campus Backbone Network (Core Layer)

- **3rd Network Architecture Component and "Core Layer".**
- **Backbone of the network and includes the high-end (Layer 3) Switches and high-speed cable (Fiber).**
- Concerned with speed and ensures reliable delivery of packets since it carries more traffic than building backbone.
- **Typical Speed: 40 Gbps**

### G. Common Carrier

- **Private companies** such as AT&T, Bell Canada, Sprint, and Bell South that **provide communication services to public.**
- Profit-oriented and provides local telephone services (i.e., Bellsouth), which is a **local exchange carrier (LEC),** whereas long-distance services (i.e., AT&T) is called an **interexchange carrier (IXC).**

### H. Data Center

- **Contains the organization's servers (e.g., database and email servers) and typically spread around the world.**
- **LAN** but because of heavy ingoing and outgoing traffic, it is designed and managed very differently than the LANS for user access.
- **Located centrally in the enterprise campus** with a very high-speed connection into the campus backbone **(Core Layer).**

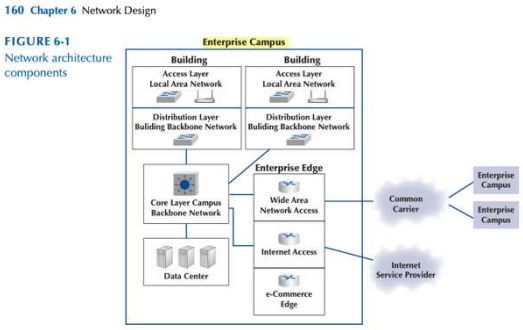
## I. Network Requirements Categorization

- **After network requirements are identified, they are organized into:**

1. Mandatory Requirements
2. Desirable Requirements
3. Wish-list Requirements

- This information enables the **development of a minimum level of mandatory requirements** and a **negotiable list of desirable requirements** that are **dependent on cost and availability.**
- **Example:**
  - Desktop video conferencing might be a wish-list but omitted if it increased network costs beyond budget.

## J. Enterprise Campus




- This organization has three **enterprise campuses** in different cities that are connected by WAN provided by common carrier such as AT & T.
- Each campus has several buildings that are connected by a backbone network.

## K. Geographic Scope

- Whether the network is a new network a network upgrade, the primary objective of this stage (finding baseline) is to define the **geographic scope of the network** and the applications that will use it.

## L. Internet Access

- **Enables the organization to connect to the Internet.**
- Large organizations use the same technologies to connect to the Internet as they use in WAN.
- Small companies and individuals use cable modem from cable company.

## M. Logical Network Design

- **The goal of the needs analysis step.**
- **Statement of the network elements** to meet the needs or the organization.
- Does not specify products or tech to be used.
- **Focuses on the fundamental functionality needed** (e.g., high speed access network) which in the tech design stage will be translated into specific tech (e.g., switched 100Base-T)

## N. Network Architecture Component

- **Enterprise edge** means dividing internal external access points that connects to specific enterprise and connected to internet and e-commerce edge (provided e-commerce services.
- **Common Carrier** defined the boundary between internal and external
- **Standard arrangement** of building backbone network is building 1 switch and 1 router.
- **Data Center** dedicated to data processing.

1. **Local Area Network (LAN or Access Layer)**
2. **Building Backbone (Distribution Layer)**
3. **Campus Backbone (Core Layer)**
4. **Data Centers**
5. **Wide Area Network (WAN) [Enterprise Edge]**
6. **Internet Access [Enterprise Edge]**
7. **E-Commerce Edge [Enterprise Edge]**

## O. Network Models

### I. OSI Model

1. **Application (Layer 7)**
2. **Presentation (Layer 6)**
3. **Session (Layer 5)**
4. **Transport (Layer 4)**
5. **Network (Layer 3)**
6. **Data Link (Layer 2)**
7. **Physical (Layer 1)**

### II. Internet Model

1. **Application (Layer 5)**
2. **Transport (Layer 4)**
3. **Network (Layer 3)**
4. **Data Link (Layer 2)**
5. **Physical (Layer 1)**

### III. Alternative Internet Model Model

1. **Application**
2. **Internetwork = Transport + Network**
3. **Hardware = Data Link + Physical**

## P. Physical Network Design

- **Starts with the client and server computers needed to support the users and applications.**
- **Developed after once needs have been defined in the logical network design.**
- If new network, then new computers need to be purchased.
- If existing, the servers need upgrade to newest technology.
- After designing, circuits and devices connecting them are designed.

## Q. Traditional Network Design Process (Structured Approach)

- Structured system analysis and design process.
- Network **analysis phase** includes meeting with users to determine needs and applications, along with estimating data traffic on each part.
- Not building a network that disallows traffic or has substantial network capacity which means there is a lot of waste.
- Follows analysis, design and implementation phase and can still be **iterative.**
- **Brainstorm and interact with stakeholders** to figure out the actual needs in terms of availability of network (needs-analysis or network analysis phase).
- During the network **design phase**, the logical and physical networks are designed, and circuits and hardware selected
- **Implementation phase** is the building and implementing of the network
- **Default built-in limitations to the growth and need to change network design** as the needs of the organization and technology itself changed.

### I. Pros:

1. **Useful** for **static** and **slowly evolving networks.**

### II. Cons:

1. Costly
2. Time consuming
3. Not adequate today due to:
    a. Rapid changes in technology
    b. Escalating network traffic demands
    c. Decrease in hardware cost
    d. Increase in staff costs

## R. Turnpike Effect

- **Occurs when the network is used to a greater extent than was expected because it is available, efficient and provide new services.**
- Growth factor for network use varies 5 – 50%.

- In some cases, exceed 100% for high growth organizations.
- Important in network design because types of messages may be different than those which the network was originally designed.

### S. Wide Area Network (WAN) Access

- **Private network that connects its different campus location and usually leased from common carrier.**
- Private use of the organization and only carries its network traffic from one campus to another.
- Circuits used In the WAN are traditionally different than the Ethernet

## KEY CONCEPTS

### A. Keys to Designing A Successful Data Communications Network

- Thorough needs analysis
- Developing one or more physical network designs.
- Designing to operate and maintain with minimal staff intervention.

### B. Traditional Approach Vs. Building Block-Approach

- **Traditional network design** uses structured approach for analysis and design which has a built-in restriction to growth and needs to change network design.
- **Building-Block Approach** uses a simpler approach to network design known as “Narrow and Deep Process” which uses few standard components to simplify design and reduce costs. It also assumes that network demand will grow, thus network designers plans for excess capacity.

### C. Why is it important to analyze needs in terms of both application systems and users?

- To ensure than network can support the bandwidth and other operational characteristics required by the user applications.

### D. On what should design plan be based?

- Geographic scope of the network
- The number of users and applications
- Current future network needs of the various network segments
- Costs of the network and maintenance.

### E. What are some major problems that can cause network designers to fail?

#### I. Technology Design Problems

- Buying wrong equipment/services
- Vendor misrepresentation or product/services did not work as intended.

#### II. Need Analysis Problems

- Inaccurate/Incomplete Requests
- Significant change in business requirements as the network was installed.

#### III. Overall Problems with the Design Process

- Lack of network design skills internally
- Did not use external consultants or system integrators who bungle the project

### F. What are the issues important to consider in explaining a network design to senior management?

- In management perspective, network is a cost center which is a significant expense but no visible impacts.
- To gain senior management acceptance, one must talk in terms of cost, network growth and reliability.
- Discuss the growth in network use.

### G. Is it important to have the fastest wireless LAN technology in House?

- No because the technology may be faster than Internet access to apartment. It is only good for connections between networking devices within the house since speed to internet is restricted by the ISP.

### H. What is the reason for slow adoption of Building-Block Approach?

- The **approach requires network managers to speak in terms of upper management** (cost, network growth, reliability) rather than the language of technology (Ethernet, ATM, and DSL).

### I. What types of networks are design tools most important?

- **Large complex networks require the use of network design tools.**
- The many devices on such systems and the variety of services requested by users requires that network managers organize and manage the process using system management software.

## PRACTICE QUESTIONS

### A. Is Network planning always necessary?

- **Network planning is not always necessary because:**
- Networks need to be upgrade/replaced more frequently than Information System
- Some network technology can change rapidly, and network grows rapidly

### B. Who is responsible for the network maintenance? What is the function of the network architect, network admin and what is the link between the two?

- **Network manager**: responsible for network maintenance
- **Network architecture:** building the blueprint for new network
- **Admin:** manages the day to day operations of the network
- **Architecture and Admin Link:** builds a network that is easy to administer

### C. What are the Components and Subcomponents of Building Block Approach?

1. **Need analysis: Analysis existing network components**
    a. Baseline
    b. Network components
    c. Application systems
    d. Network users
    e. Needs categorization
2. **Technology Design: Client and Servers Circuits**
    f. Clients and servers
    g. Circuits
3. **Cost Assessment**
    h. Off the shelf
    i. Request for approval

**Reaching the final design:**

- Complete initial cost assessment

- Refine the needs analysis if a budget issue raises
- Cycles through all three phases design
- Stop when a final design meets requirements and fits budget

### D. What information can you get from Network Management Tools?

- **Managed devices are more expensive** because they have CPU and software built on them.

- **Management Information Base (MIB):** raw data that includes about traffic network (table format, array format) (e.g., traffic level, serial numbers, etc.)

- **Network Management Tools:** used to build reports that analyze data from (MIB).
  - Keep track of traffic level
  - Problem and alerts the admin
  - Response Time
  - Availability of the network – deals with uptime and downtime of network
  - Capacity of Network – deals with data rate and how many devices you want to involve in the network
  - Performance

### E. What are the most important measures in baseline related to network traffic?

- Throughput (average and peak)
- Number of dropped frames due to error detection
- Number of dropped frames due to congestion
- Number of collisions

### F. Network Design Tools and Feature

- Represents resource capacity and bandwidth
- Identify bottle necks
- Identify applications and protocols causing congestion.
  - Measure, estimate and report utilization, availability, etc.

### G. Which of the following is NOT making traditional design approach less appropriate for today's network?

a. The underlying technology of networking devices is changing very rapidly
b. The underlying technology of client and server devices is changing very rapidly
c. The underlying technology of circuits is changing very rapidly
d. Growth in network traffic is very high
**e. The most expensive part of any network is the hardware**

## CHAPTER 7 – WIRED AND WIRELESS (LAN) LOCAL AREA NETWORKS (FITZ)

## KEY TERMS

### A. Access Point (AP)

- **Wireless Access Point is a radio transceiver that connect computers (wireless clients)** into **wired LANs** (using 100Base-T or 1000-Base T) instead of connecting using hubs/switches and **enable computers near it to communicate with each other.**

**If a frame first transmitted to the AP:**

- **AP** then **retransmits the frame** over the wireless/wired network (i.e., transmitted twice)
  - Server should be placed on a WLAN because client computers cannot reach it directly but communicate through AP.

**For multiple access points:**

- **Each APs uses a different channel** (different radio frequencies) to avoid interference.

### B. Active Directory Service (ADS)

- Most important function of a Network Operating Service.
- Provide **info about resources on the network that are available to the users,** such as shared printers, shared file servers, and application software.
- **Microsoft Active Directory Service** works in the same manner as TCP/IP DNS service.

### C. Association with an AP

- Searching for available AP lets NIC either engage in **active or passive scanning.**
- During **active scanning, the NIC transmits a special probe frame** on all frequencies in use.

**When an AP receives a frame:**

- includes all the **relevant information for a NIC to associate with it.**
- **Multiple probes** from the same AP are possible and the NIC has the final say on which association. The difference in time is significant.
- Once the **NIC associates with an AP, it begins exchanging packets over the wire with it.**
- **Refer to Beacon Frame**

### D. Beacon Frame

- Most important function of a Network Operating Service (NOS).
- **During passive scanning, the NIC listens on all channels** for a special frame called **beacon frame that is sent out by an access point.**
- Contains all the necessary information for a NIC to associate with it.

**Once a NIC detects a beacon frame:**

- It can decide **to associate with it and start communication** on the frequency channel set by the access point.

### E. Bottleneck

- **Network Admin locates bottleneck (the part of network restricting data flow) to improve performance.**
- Either lies in **network server** or **network circuit.**
- For **network server,** it lacks sufficient capacity to process all request t receives in timely manner.
- For **network circuit,** network server process all received client requests, but it lacks enough capacity to transmit all requests to server.
- Third location is client computers but extremely unlikely.

### F. Cable Plan

- **Plan for the network layout which includes info such as:**
    1. Cost of cabling
    2. Location of cabling
    3. Location and quantity of hubs
    4. Available ports
    5. Local city fire codes that must be followed
    6. Identification labels of the cable.

### G. Cabling

- **Critical to plan for the effective installation and use of LAN cabling.**

- **Cheapest time** to install network is during the **construction of the building.**
- **Adding cable to an existing building** can **cost significantly more** since the **costs to install cable** (i.e., paying those doing the installation and additional construction) are substantially more than the cost of the cable itself
- It is **expensive to re-install the cable if the cable plan does not meet the organization's needs.**

## H. Carrier Sense Multiple Access With Collision Detection (CSMA/CD)

- **Media access control in Wi-FI and two approaches.**
- **Contention-based technique** that wait until the bus is free (sense for carrier) and then transmit.
- **Fine if no computer attempts to transmit at same time ("collision").**
- Computers wait until no other devices are transmitting and then transmit the data.
- Before a computer can transmit in WLAN, it must first establish an **association** with a specific AP.

### Collision:

- Two computers located some distance from one another can both listen to the circuit, find it empty, and begin to simultaneously.
- **Two messages collide and destroy each other and this simultaneous transmission is called "collision".**

## I. Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA)

- **Media access control in Wi-Fi** is Carrier Sense Multiple Access with Collision Avoidance **(CSMA/CA),** which is similar to the contention-based CSMA/CD approach used by Ethernet.
- With CSMA/CA, **computers listen before they transmit**, and if no one else is transmitting, they proceed with transmission.
- CSMA/CA has **two media access control approaches:**

### 1. Distributed Coordinated Function (DCF)

- **Called "Physical Carrier Sense Method"** since it depends on the ability of computers to physically listen before they transmit.
- With DCF**, each frame in CSMA/CA** is **sent using stop-and-wait ARQ.**
- **DCF works well in traditional Ethernet** because every computer on the shared circuit receives **every transmission on the shared circuit** but in a wireless environment, this is not always true.

### After the sender transmits one frame:

- **it immediately stops and waits for an ACK from the receiver** before attempting to send another frame.

### When the receiver of a frame detects the end of the frame in a transmission:

- **Waits a fraction of a second** to make sure the sender has really stopped transmitting, and then **immediately transmits an ACK (or a NAK).**
- The **original sender** can then **send another frame, stop and wait for an ACK, and so on.**
- The **time interval between a frame and the matching ACK** is so **short** that no other computer has the opportunity to begin transmitting.

### Physical Carrier Sense Method:

- **Intended design is that the time the receiver waits** after the frame transmission ends before sending an ACK.

## 2. Point Coordinated Function (PCF)

- **Called "Virtual Carrier Sense Method"**
- A **computer at the extreme edge of the range limit from the AP on one side may not receive transmissions** from a computer on the extreme opposite edge of the AP's range limit.
- **Optional and always be used, never used or used for frames exceeding a certain size** set by WLAN manager.

### Hidden Node Problem:

- **Computers at the opposite edges of the WLAN are hidden from each other.**
- When the hidden node problem exists, the **AP is the only device guaranteed to be able to communicate with all computers** on the WLAN.
- Therefore, **the AP must manage the shared circuit using a controlled-access technique,** not the contention-based approach of traditional Ethernet.
- Refer to **Request to Send (RTS)**
- Refer to **Clear to Send (CTS)**

### Controlled-Access Methods:

- Provide **poorer performance in low-traffic networks** because computers must **wait for permission before transmitting** rather than just waiting for an unused time period.
- **Work better in high-traffic WLANs**, because **without controlled access, there are many collisions.**

### J. Channel

- When designing a WLAN, one must ensure that AP's don't interfere with each other (transmitted on same frequency).
- Therefore, each AP is set to transmit on different **channel** and each channel uses a different part of **2.4 or 5GHZ frequency range.**

### K. Clear To Send (CTS)

- **Access point (AP)** responds with a **CTS** by **specifying the amount of time for which the circuit is reserved** for the requesting computer.
- **All computers hear the CTS and remain silent** for the specified time period.

### L. Collision Detection (CD)

- **Solution to collision is to listen while transmitting.**
- **If the NIC detects any other signals** than its own, it presumes that collision has occurred and **sends a jamming signal.**
- **All computers stop transmitting and wait for the circuit to become free** trying to retransmit and the problem with this is it could retransmit at same time.
- The solution is for **each computer to wait a random amount of time** after the colliding message disappears before retransmitting.

### M. Collision Domain

- This **shared multipoint circuit requires computer to take turns using it** and it is called CD since if two computers ever did accidentally **transmit at the same time, there would be a collision.**
- When **one computer transmits, all the other computers must wait,** which is very inefficient.
- Security issue since any frame can be read by any computer

### N. Directional Antenna

- Used on **AP** and **projects a signal on only one direction.**
- Signal is **concentrated in a narrower, focused area,** the signal is stronger and therefore will

**carry farther than the signal from an AP** using an **omnidirectional antenna.**

- Directional antennas are most often **used on the inside of an exterior wall of a building, pointing to the inside of the building.**
- This **keeps the signal inside the building** (to reduce security issues) and has the benefit of **increasing the range of the AP.**

## O. Domain Controller

- **Active Directory servers can also act as DNS servers.**
- **Within each domain, there is a domain controller that resolves address information (**much like a DNS server resolves address information on the Internet).
- **The domain controller is also responsible for managing authorization information** (e.g., who is permitted to use each resource) **and** making sure that resources are available only to authorized users.
- **Resolves the textual name in the LDAP request to network address** and if authorized users, then it provides contact info for the resource.

## P. Ethernet

- Most common used LAN accounting for 70% of all LANS.
- **Data Layer or Layer 2 Protocol**

### I. Hub-Based Ethernet

- Uses **logical topology of bus with physical topology of star.**
- It uses a contention-based media access technique called **Carrier Sense Multiple Access with Collision Detection (CSMA/CD).**
- **Uses different network cabling:**
  - **10Base-2,**
  - **10Base-5,**
  - **10Base-T,**
  - **10Broad-36.**

**Frames:**

- All **frames** from any computer flow onto the central cable (or bus) through it to all computers on the LAN.
- **Every computer on the bus receives all frames sent on the bus,** even those intended for other computers.
- **Before processing incoming frames,** the Ethernet software on each **computer checks the data link layer** address and **processes** only those frames addressed to that computer.

### II. Switch-Based Ethernet

- **Logical topology of star with Physical topology of star**.
- **Operate on the destination MAC address of each packet** processed to determine which port to pass on each packet presented for transmission.
- **Each port on the switch is in a separate collision domain** and contain two devices: **Switch** and **End-user device.**
- **Learn and store in memory** in the **form of a forwarding table,** the specific port location of each MAC address for every device connected to any of its ports.

**Forwarding tables are initially:**

- **Empty** and do not know what Ethernet address is attached to what port.

**Before forwarding tables are complete:**

- **It acts like a hub (broadcast frames to correct destination)** and it takes a minute to learn most address in busy network.
- If computer is **not communicating for more than 300 seconds (>5min),** its entry is usually removed from forwarding table and active connections are placed on top.

### If a switch receives a frame:

- **It reads the frame's data link layer source address** and **compares this address to its forwarding table.**

### If the Ethernet Address is not in the forwarding table:

- The **switch adds it, along with the port on** which the frame was received.

### If a Switch receives a frame with destination address that is not in forwarding table:

- The switch must still **send the frame to the correct destination.**
- It must **retransmit the frame to all ports,** except the one on which the frame was received.
- **It will simply ignore all frames not addressed to them** and the one computer for whom the frame is addressed will recognize its address and will process the frame

### What happens to the computer with frames addressed?

- It includes **sending an acknowledgement (ACK) or a negative acknowledgement (NAK) back to the sender.**

### Switch:

- **Intelligent device with small computer** used to **manage set of separate point-to-point circuits**.
- **Link-layer devices and used to group devices**
- Learn forwarding table using flooding, learning and MAC addresses

## 1. Layer-2 Switch

- **Uses the Ethernet Address (MAC address)** to decide which port to use.

## III. Three Modes of Switches:

- **Most switches today use cut-through of fragment free switching.**
- Cut-Through Switching
- Store-and-Forward Switching
- Fragment-Free Switching

### 1. Cut-Through Switching

- **Frames retransmitted on outgoing circuit as soon as it reads destination address in the frame.**
- **Advantage:**
  - **low latency** (time it takes a device from receiving a frame to transmitting it) resulting in fast network**,** but some capacity wasted.
- **Used only when income data has the same data rate** for incoming/outgoing circuits.
- **Disadvantage:**
  - **begins transmitting before it has processed the frame check** sequence at the end which may contain an error.
- For an erroneous frame it won't be noticed by the switch until almost all have been transmitted (when the check sequence is read and processed).

### 2. Store-and-Forward Switching

- **Frames retransmitted** after **entire frame is received and error check is complete**
- **Advantage:**
  - **Providing higher latency** but slower network since it prevents invalid frame consuming network capacity.
- **Disadvantage:**

        - **Slower, but fewer errors** since if it detects error, then the switch discards the frame.

    - **Used regardless incoming/outgoing circuit has same data rate** since entire frame is stored in switch before forwarded.

3. **Fragment-Free Switching**
    - **Frames retransmitted** once the header **(First 64 bytes) is received and has no errors.**
    - Compromise between store and forward cut-through.
    - **Advantage:**
        - **providing higher latency**
        - **better error control** than **cut-through switch.**
    - **Disadvantage:**
        - **Providing lower latency** and **worse error control** than **store-and-forward switching.**

## Q. Fiber-Optic Cable

- Uses **high-speed streams of light pulses from lasers or LEDS** that carry info inside hair-thin strands of class called optical fibers.
- Earliest fiber-optic system was **multimode,** meaning that light could reflect the cable at many angles.

### Multimode:

- **Disadvantage**:
    - **Excessive signal (attenuation) weakening**
    - **dispersion** (spread of signal so that different parts of signal arrive at different times at the destination).
- **Early multimode was limited to 500 meters.**

### Graded-Index Multimode:

- Resolve the problem of early multimode by **changing the refractive properties of glass fiber.**
- Compensates for the longer distance it must travel with light in the center of fiber.
- Increases effectiveness at least under **1000 meters.**

### Single-Mode:

- **Transmit a single direct beam of** light through a cable that ensures the **light reflects in only one pattern**, in part because the **core diameter** has been **reduced from 50 microns** to about **5–10 microns.**
- This smaller-diameter core **allows the fiber to send a more concentrated light beam**, resulting in **faster data transmission speeds** and longer distances, often up to **100 kilometers**.

### Fibre-Optic Cable Features:

1. **Type of network:**
    - Used for virtually **any type of network.**
2. **Transmission distance:**
    - Fiber optics can transmit up to **75 miles**
    - New types can reach more than **600 miles.**
3. **Security and Cost:**
    - **Most secure and expensive**
4. **Error Rates**
    - **Lowest** error rates.
5. **Transmission Speed:**
    - Between **1Gbps and 40 Gbps**

## R. Forwarding Table

- **Lists** the **Ethernet address of the computer connected to each port on the switch.**
- For the **first few minutes** until the forwarding table is complete, **the switch acts like a hub**.
- As forwarding table becomes **more complete**, it begins to **act more like a switch.**

- Refer to **Switch-based Ethernet.**

### S. Hub

- **Treat as a junction box that permits new computers to be connected to the network** as easily as plugging a power cord into an electrical socket.
- Provide 4, 8, 16, 24 **(4 to 24) port sizes** into which network cables can be plugged.
- **LAN component that serves two purposes:**

1. **Provide an easy way to connect network cables**
   - Link cables from different devices with sometimes more than one type of cabling.
2. **Acts as repeaters by reconstructing and strengthening incoming signals**
   - Deals with attenuation

### T. IEEE 802.3

### U. IEEE 802.11

### V. Latency

### W. LAN (Local Area Network)

- Group of **microcomputers** or other **workstation devices** located within a **small area** and are **connected by a common cable.**
- **Part of a larger backbone network** connected to **other LANs, a host mainframe,** or **public networks.**

## IV. Wired and Wireless LAN Components

### 1. Client

- Request info from servers

### 2. Servers

- Deliver info to clients

**Best Practices to improve network performance on the servers:**

- Improving server performance can be approached in the context of hardware and software:
  - **Software methods:**
    - Changing the NOS
    - Fine-tuning the NOS.
  - **Hardware methods:**
    - Adding a second server
    - Upgrading the server's

### 3. Network Interface Card (NIC)

**Wired LANs connection:**

- **Physical layer connection** and known as **network cards** and **network adapters** which **operates at layer 1 (Physical) and Layer 2 (Data Link).**
- Used to connect the computer to network cable.

**Wireless LANs connection:**

- NIC is **the radio transmitter that sends or receives** messages on a specific radio frequency.
- **Wired or wireless NIC built** into motherboards.
- Ethernet NICs contain **unique MAC address.**

### 4. Circuits

**Wired LANs connection:**

- Connected through **network circuit or cables** such as:

a) **Unshielded Twisted-pair (UTP) Cable**
   - Useful due to low cost which leads to being commonly used.

b) **Shielded Twisted-Pair (STP) Cable**
   - Produced for area with low electrical interference.

c) **Fiber-Optic Cable**
   - Perfect for building backbone networks since it is thinner and lighter with higher capacity.
   - Refer to fiber-optic cable

| Name | Type | Maximum Data Rate | Used by |
|---|---|---|---|
| Category 3 | UTP | 10 Mbps | 10BASE-T |
| Category 5 | UTP/STP | 100 Mbps | 100BASE-T |
| Category 5e | UTP/STP | 1 Gbps | 1000BASE-T |
| Category 6/6a | UTP/STP | 10Gbps | 10GBASE-T |
| OM1 (62.5/125 µm) | Fiber | 1-10 Gbps | 1000BASE-SX |
| OM3 (50/125 µm) | Fiber | 10-100 Gbps | 10GBASE-SR |

## 5. Access Points (APs)

### Wireless LANs connection:

- Connects **computers (wireless clients into Wired LANs** instead of connecting using hub/s switches.
- Enables computers near it to communicate with each other.
- Refer to **Access Point**.

### Wired LANs connection:

- Refer to **Switches**
- Refer to **Hubs**

## 6. Network Operating System (Software)

- Software that controls the network and provides two sets of software:

1. **Runs on network server(s)**
    - Provides the software that performs the functions associated with the **data link, network, and application layers** and usually the **computer's own operating system.**
    - Enables server operations
    - Handle request sent from clients

2. **Runs on the network client(s).**
    - Provides the software that performs the functions associated with the **data link and the network layers** and must **interact with the application** software and **the computer's own operating system.**
    - Runs at client computers

- Provides **directory service**
- Provide **network profiles** which specifies resources that devices and users can access.
- Refer to **Domain Controller**
- Refer to **Active Directory Service**
- Refer to **Network Profile**

## X. Lightweight Directory Access Protocol (LDAP)

- When a **client computer wishes to view available resources or access them,** it **sends a message** using an industry standard directory protocol called **lightweight directory access protocol (LDAP)** to the **ADS domain controller.**
- Refer to **Domain Controller**

## Y. Load Balancer

- Also known as **"load balancing switch"** and acts as a **router at the front of server farm.**
- **it forwards it to one specific server** using its **IP address** and a **simple round-robin formula** is used (requests go to each server one after the other in turn).
- The **load balancer stops sending requests to it,** and the network continues to operate without the failed server.
- Load balancing makes it **simple to add servers (or remove servers) without affecting users.**

## Z. Logical Topology

- **Illustrates how the network operates with the various protocols that may be running.**
- Explains how the network works conceptually like logical data flow diagram (DFD) or Logical Entity Relationship Diagram (ERD) in systems analysis and design or database design.

- A single network can have multiple protocols.

### AA. MAC Address Filtering

- The AP permits the **owner to provide a list of MAC addresses (i.e., layer 2 addresses).**
- The AP **only processes frames** sent by computers **whose MAC address** is in the **address list.**
- **I**f a computer with a MAC address not in the list sends a frame, the AP ignores it.
- There is a software that changes MAC address on wireless NIC and hacker could **use packet sniffer to discover a valid MAC address and fake its legitimacy.**
- Filtering like WEP and **protects against only casual thief.**

### BB. Managed APs (Access Points)

- **Wired into a Wi-Fi Controller** (rather than a normal hub or switch).
- **Report what devices are attached** to them and **how busy they are** to the controller, which **balances traffic across the APs it manages.**
- If device connects to **busy AP, controller instructs AP to deny access** to that device and the device automatically connects to the next AP.

#### Best Practice in Networking:

- **Improves overall network performance** since the **number of devices connected** to each AP and the **traffic amount each receives is balanced** across the managed AP.

### CC. Network-Attached Storage (NAS)

- **General-purpose computer:** server that runs a server operating system (e.g., Windows and Linux).
- It has a **small processor and a large amount of disk storage** and is designed solely to **respond to requests for files and data.**
- NAS can also be attached to LANs, where they function as fast file servers.

### DD. Network Profile

- **Specifies what resources on each server are available** on the network for use by other computers and which devices or people are allowed what access to the network.
- Normally **configured when the network is established** and remains in place until someone makes a change.
- In a LAN, the server hard disk may have various resources that can or cannot be accessed by a specific network user (e.g., data files and printers).
- A **password may be required to grant network access** to the resources.

### EE. Network Segmentation

- **Divide the LAN into smaller segment** and break a network into smaller parts.

#### Wired LAN

- Adding one of more new switches and spreading the computers across these new switches.

#### Wireless LAN

- Adding more APs that operate on different channels.
- Important to check signal interference such as Bluetooth/cordless phones.

### FF. Network Server

- Refer to **Network Operating System**.

### GG. Omnidirectional Antenna

- Most WLANs are installed using APs that have omnidirectional antennas.
- **Antenna transmits in all directions simultaneously.**

- Some antennas are built into the AP itself, while others stick up above it.
- **Dipole antenna**

### HH. Overlay Network

- Build the **usual switched Ethernet networks** as the **primary LAN** but also **install Wi-Fi for laptops and mobile devices.**

**Best Practice LAN Design:**

- Use Wired Ethernet for the primary LAN with Wi-Fi as an overlay network.

### II. Performance Checklist

#### I. Increase Server Performance

- Software
- Fine-tune the network operating system settings
- Hardware
- Add more servers and spread the network applications across the servers to balance the load
- Upgrade to a faster computer
- Increase the server's memory
- Increase the number and speed of the server's hard disk(s)

#### II. Increase Circuit Capacity

- Upgrade to a faster circuit
- Increase the number of circuits

#### III. Increase Circuit Capacity

- Move files from the server to the client computers.
- Increase the use of disk caching on client computers.
- Change user behavior

### JJ. Physical Topology

- **Illustrates exactly where all the hardware and cabling are 'physically' located and connected.**
- How the network is physically installed like a physical DFD or ERD.

### KK. Port

- **Each connection point where a cable can be plugged**.
- Each port has a **unique number.**
- When **a cable is plugged into a port**, the **signal travels down the cable** like it was directly connected to the hub or switch.
- Refer to the **Hub.**

### LL. Power Over Ethernet (POE)

- Needs no external power and the **power is provided from a POE switch** over the unused wires in a category 5/5e cable.
- POE APs are **more expensive** but can be **located anywhere you can run Cat 5/5e cable,** even if there are no power outlets nearby.

### MM. Powerline Networking

- **Provides Ethernet over the existing electrical power wires** in your house at rates up to **1 Gbps.**
- Convert the traditional wired Ethernet signal that runs over **Cat 5e cables into a signal that can travel over the electrical power** wires.

### NN. Probe Frame

- Refer to **Association with an AP.**

### OO. Redundant Array Of Inexpensive Disks (RAID)

- **Used in applications requiring fast processing of large volumes of data** (e.g., multimedia).
- **Provide fault-tolerance**

- Storage technology made of many separate disk drives.
- When a file is written to a RAID device, it is written across several separate and redundant disks.

### PP. Request To Send (RTS)

- Any **computer wishing to transmit first sends an RTS to the AP,** which may or may not be heard by all computers.
- The RTS **requests permission to transmit and to reserve the circuit** for the sole use of the requesting computer for a specified time.

### QQ. Server Virtualization

- Opposite of server farms and load balancing.
- The **process of creating several logically separate servers** (e.g., a Web server, an email server, and a file server) **on the same physical computer.**
- Run on the same physical computer but appear separate to the network (and if one crashes, it does not affect the others running on the same computer).

**Advantage:**

- **Saves money by reducing physical servers one buys and operates**.
- Providing the benefits of having logically separate device and OS.

### RR. Site Survey

- **Determines the:**
    - Feasibility of the desired coverage,
    - The potential sources of interference,
    - The current locations of the wired network into which the WLAN will connect,
    - Estimate of the number of APs required to provide coverage

### SS. Small-Office, Home-Office (SOHO)

- **Switches** can be designed for SOHO environments and usually it offers five 10/100/1000 Mbps ports.
- Refer to the **Hub.**
- Refer to the **802.11ad**.

### TT. Storage Area Network (SAN)

- **LAN devoted solely to data storage** and the **devices** of SAN may **be large set of database servers** or a **set of network-attached disk rays.**
- When the amount of data to be stored exceeds the practical limits of servers, the SAN plays a critical role.
- When data are needed, clients send the request to a server on the LAN, which obtains the information from the devices on the SAN and then returns it to the client.

### UU. Symmetric Multi-Processing (SMP)

- **Enables one server to use up to 16 CPUs.**
- Provide excellent performance but cost more (often $5,000–$15,000).

### VV. Topology

- **Basic geometric layout of the network**
- The way in which computers on the network are interconnected.
- **Categorized into:**
    - **Physical Topology**
    - **Logical Topology**

### WW. Twisted-Pair Cable

- All LAN cables are rated for the maximum distance they can be used (typically **100 meters for twisted-pair cable**)

- Refer to **Circuits**.

## XX. Wardriving

- Special-purpose software tools available on the Internet that will **enable you to learn more about the WLANs you discover,** with the **intent of helping you to break into them.**
- Type of wireless reconnaissance.

## YY. Wireless Ethernet (Wi-Fi)

- **Commercial name for a set of standards** developed by the **IEEE 802.11 standards group.**
- A group of vendors selling 802.11 equipment **trademarked the name Wi-Fi to refer to 802.11** because they believe that consumers are more likely to buy equipment with a catchier name than 802.11.

## ZZ. Wi-Fi Controller

- Refer to **managed APs**.

## AAA. Wi-Fi Protected Access (WPA)

- **Every frame is encrypted using a key,** and the key can be **fixed in the AP** or can be **assigned dynamically as users login.**
- The difference is that the **WPA key is longer than the WEP key** and thus is harder to break.
- More importantly, the **key is changed for every frame that is transmitted to the client**.
- Each time a frame is transmitted, the key is changed.

## BBB. Wired Equivalent Privacy (WEP)

- The AP **requires the user to have a key** to **communicate** with it and **all ingoing and outgoing data in the AP are encrypted** by public and private key.
- If a computer does **not** have the **correct WEP key,** it **cannot understand** any messages transmitted by the AP, and the AP will not accept any data that are not encrypted with the correct key.
- The **WEP keys are produced dynamically**, much like the way in which a DHCP server is used to dynamically produce IP addresses.
- When an **AP first discovers a new client** computer, it **requires the user to log in** before it will communicate with the client computer.

## CCC. Types of Ethernet

| Name | Maximum Data Rate |
|---|---|
| 10Base-T | 10 Mbps |
| 100Base-T | 100 Mbps |
| 1000Base-T | 1 Gbps |
| 1000Base-F | 1 Gbps |
| 10 GbE | 10 Gbps |
| 40 GbE | 40 Gbps |
| 100 GbE | 100 Gbps |

- **100-Base T and 1000-BaseT** are the most common forms of Ethernet
- **1000-Base F, 1GbE, 40GbE, and 100 GbE** can use Ethernet's traditional half-duplex approach but most are configured full duplex.
- Most of them are designed to run over fiber-optic cables but some use traditional twisted-pair cables (e.g., Cat 5e)

### 10/100/1000 Mbps Ethernet

- The standard that can **autosense which speed it needs to run at between the speeds of 10Mbos or 100Mbps or 1 Gbps.**
- It **depends on to the type of NIC running** at the **individual node** and the type of switch port that the node connects into.

- It is commonplace to run 10/100/1000 Mbps switches in LAN operating environments where there are older NICs already operating and no real business case requirements for upgrading these nodes.

## DDD. Types of Wireless Ethernet (Wi-FI)

### I. 802.11a

- **Obsolete and legacy tech**

**Perfect conditions:**

- 8 channels of 54 Mbps
- Max range of 50 metres to 100 ft.
- Speed of 20 Mbps at 50-foot ranges are common due to interference of drywall and brick wall

### I. 802.11ac

- IEEE 802.11 ac is **latest version**
- **Runs in two different frequency spectrums simultaneously (2.4 and 5 GHz)** to provide high data speed rates.
- **RTS/CTS media access control is sent on a separate frequency** range to not interfere dta transmission.
- Default **modulation technique** is **256-QAM.**

**Perfect conditions:**

- 8 channels running at 433 Mbps
- Max range of 100 meters (300 ft).
- Actual throughput is it uses six symbols to send 5 bits.
- **Efficiency of data link protocol:** 300 Mbps
- Users see max speed within 20-30 metres of AP.
- **Max range data rates:** 90 Mbps per channel (60 Mbps throughput).

**Alternative version (Perfect Conditions)**

- Provide 1 channel of 6.9 Gbps (throughput of 4.9 Gbps)

### II. 802.11ad

- **WiGig** is a specialized version of wirless Internet
- **Max range** of 10 meters (30 feet).
- **Does not penetrate walls and used only in same room.**
- **Suited to SOHO environments** with digital entertainment needs.
- **Also expected to be used in high-density office areas** that have cubicles in same open space.

### III. 802.11b

- **Obsolete and legacy tech**

**Perfect conditions:**

- 3 channels of 11 Mbps
- Each with max range of 150 meters or 450 feet.

### IV. 802.11g

- **Obsolete and legacy tech**

**Perfect conditions:**

- 3 channels of 54 Mbps
- Each with max range of 150 meters or 450 feet.

### V. 802.11i (WPA2)

- **Newest and most secure type of WLAN security.**
- Uses the **Advance Encryption Standard (AES).**
- **User logins to login server to obtain master key** and the user's computer and **AP negotiate a new key that will be used for the session** until user leaves the WLAN.

**Advance Encryption Standard (AES).:**

- 3 channels of 54 Mbps
- Each with max range of 150 meters or 450 feet.

### VI. 802.11n

- Obsolete version but used still since its cheap.

- Possible to configure **dual-band AP** which **combines all the channels into one "dual-band" channel** that provides **600 Mbps.**

**Perfect conditions:**

- 3 channels (1, 6, 11) of 450 Mbps
- Max range of 100 meters or 300 feet
- Older versions provide maximum 300 Mbps.

## KEY CONCEPTS

### A. Types of Servers

#### I. File Servers

- Allow many users to share the same set of files on a common, shared disk drive.

#### II. Database Servers

- Perform database processing on those files associated with client-server computing.
- Benefit is reducing amount of data moved between server and client workstation.
- Minimize data loss and prevent widespread data inconsistencies.

#### III. Print Servers

- Handle print requests on the LAN.
- Help reduce the load on main LAN file or database server and increase network efficiency.

#### IV. Communication Servers

- Dedicated to performing communication processing

- **Fundamental Types of Communication Servers:**

1. **Fax Servers**
   - Manage a pool of fax-board that enable LAN users to send and receive faxes.
2. **Access Server**
   - Dialing into the LAN by telephone
3. **Modem Server**
   - Dialing out

### B. Compare and contrast category 5 UTP, Category 5e UTP, and category 5 STP.

### C. How to decide how many APs are needed

| Category | Type | Max. Data Rate (Mbps) | Often Used By | Cost ($/foot) |
|---|---|---|---|---|
| 5e | UTP | 100 | 1,000Base-T Ethernet | .10 |
| 5 | UTP | 100 | 100Base-T Ethernet | .07 |
| 5 | STP | 100 | 100Base-T Ethernet | .18 |

### and its location for best performance.

- **Network manager bases it in four data factors:**

1. Nominal data rates
2. Error rates
3. Efficiency of data link layers protocols used
4. Efficiency of media access control protocols

### D. Length of a message calculation

$$\frac{\text{length of bits}}{\text{speed of cable}} = \text{nanosecond}$$

$$(\text{time takes to transmit}) * \text{speed of light} = \text{length in feet}$$

**Example:**

a) Let's assume that the smallest possible message is 64 bytes. If we use 100Base-T, how long (in feet or meters) is a 64-byte message? Hint: you can assume that the electricity in the cable travels at approximately the speed of light (186,000 miles per second).

**Solution:**

$$\frac{64 \text{ bytes x } 8 \text{ bits/byte}}{100 \text{ million bits per second}} = 0.0000052 \text{ seconds}$$

$$0.0000052 \text{ seconds} * 186{,}000 \text{ miles per second} = .9672 \text{ miles or about } 5{,}100 \text{ feet}$$

*WEEK 9 LECTURE*

## CH.4 (FITZ) – Data Link Layer

## KEY TERMS

### A. Access Request

- **Each device must get permission to transmit, similar to raising a hand.**
- Client computers that want to transmit **send a request to transmit to** the device that is controlling the circuit (e.g., the **wireless access point**).
- The controlling device grants permission for one computer at a time to transmit.
- Refer to **Controlled Access**.

**When one computer has permission to transmit:**

- All other computers wait until that computer has finished.
- Then, if they have something to transmit, they use a contention technique to send an access request.

### B. Acknowledgment (Ack)

- Refer to **Synchronous Transmission**.

### C. Amplifiers

- Takes **the incoming signal, increases its strength,** and **retransmits** it on the next section of the circuit.
- **Used on analog circuits** such as the telephone company's voice circuits.

**Analog Circuits:**

- It is important to recognize that **the noise and distortion are also amplified,** along with the **signal.**
- Refer to **Error Prevention**.

### D. Asynchronous Transmission

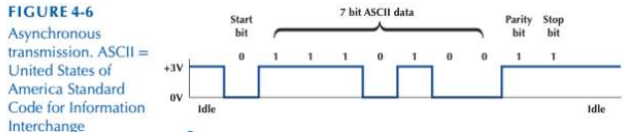



FIGURE 4-6 Asynchronous transmission. ASCII = United States of America Standard Code for Information Interchange

- **Each character is transmitted as a totally independent entity** with its own **start** and **stop bits** to inform the receiving computer that the character is beginning and ending.
- **Referred to as start-stop transmission** since the transmitting computer can transmit a character whenever it is convenient.
- **Typically used on point-to-point full-duplex circuits** (i.e., circuits that have only two computers on them), so media access control is not a concern.
- Some older protocols have **two stop bits instead** of the **traditional single stop bit.**
- **Defines the idle signal** (the signal that is sent down the circuit when no data are being transmitted) as the **same as the stop bit.**

### E. Continuous Automatic Repeat Request (Arq)

- Refer to **Continuous ARQ**

### F. Checksum

- **Typically, 1 byte is added to the end of the message** and **calculated by adding the decimal value of each character in the message**, **dividing the sum by 255,** and using the **remainder as the checksum.**
- The receiver calculates its own checksum in the same way and compares it with the transmitted checksum.
- If the two values are equal, the message is presumed to contain no errors.
- Use of checksum **detects close to 95% of the errors for multiple-bit burst errors.**

### G. Contention Access

- Opposite of controlled access.

- **Computers wait until the circuit is free** (i.e., no other computers are transmitting), and then transmit whenever they have data to send.
- **Used in Ethernet local area networks.**
- **Contention-based systems improved** to the **extent where they deliver throughput** and more **competitive** than controlled access due to **hardware cost** considerations.

## H. Continuous ARQ

- **The sender does not wait for an acknowledgment** (acK) after sending a message and it immediately sends the next one.
- While the messages are being transmitted, the sender examines the stream of returning acknowledgments.
- If it **receives an NAK, the sender retransmits the needed messages.**
- **Full-duplex transmission technique** since both sender and receiver is transmitting simultaneously.
    - **Sender:** sending messages
    - **Receiver:** sending ACKs and NACKs

## I. Controlled Access

- Common in Wireless LANs
- One device controls the circuit and chooses which client can transmit at what time.

- **Commonly Used Techniques:**
    - **Access Requests**
    - **Polling**

## J. Cyclical Redundancy Check (Crc)

- **Error-checking scheme** and adds 8, 16, 24 or 32 bits to the message.
- **Message** is treated as **one long binary number, P.**
- Before transmission, the data link layer (or hardware device) divides P by a fixed binary number, G, resulting in a whole number, Q, and a remainder, R/G.
- **So, P/G = Q + R/G.**

**Example:**

- If P = 58 and G = 8, then Q = 7 and R = 2.
- G is chosen so that the **remainder R will be either 8 bits, 16 bits, 24 bits, or 32 bits.**
- The remainder, **R, is appended to the message** as the error checking characters before transmission.
- The receiving hardware **divides the received message by the same G,** which **generates an R.**
- If R does not agree with locally generated CRC, the message is assumed to be in error.

## K. Efficiency

- Efficiency of data throughput **varies inversely** as the desired amount of error detection is increased.

## L. Error Detection

- **Send extra data with each message and added to each message by the data link layer of the sender** based on some mathematical calculations performed on the message.
- Some are built into hardware.

### Error Detection Methods:

1. **Parity Checking**
2. **Checksum**
3. **Cyclical Redundancy Checking (CRC)**

## M. Error Prevention

### 1. Shielding

- **Protecting wires by covering them with insulating coating** prevents impulse noise, cross-talk and intermodulation noise.

- More expensive cable leads to more installation difficulty.

### 2. Moving cables away from sources of noise

- **Impulse noise:** avoiding lights and heavy machinery or locating communication cables away from power cables.
- **Cross-Talk:** physical separation of cables from other cables.

### 3. Changing multiplexing techniques

- From Frequency Division Multiplexing to Dime Division Multiplexing.
- Changing the frequencies/size of guardbands in FDM

### 4. Avoid attenuation

- Use repeaters or amplifiers.

## N. Error Rates

- Inter-Exchange Carriers (IXCs) that provide data transmission circuits provide statistical measures specifying typical error rates and the pattern of errors that can be expected on the circuits they lease.
- **Example:**
  - **The error rate might be stated as 1 in 500,000, meaning there is 1 bit in error for every 500,000 bits transmitted.**

## O. Ethernet (IEE 802.3ac)

| Preamble | Start of Frame | Destination Address | Source Address | VLAN Tag | Length | DSAP | SSAP | Control | Data | Frame Check Sequence |
|---|---|---|---|---|---|---|---|---|---|---|
| 7 bytes | 1 byte | 6 bytes | 6 bytes | 4 bytes | 2 bytes | 1 byte | 1 byte | 1–2 bytes | 46–1,500 bytes | 4 bytes |

FIGURE 4-8a Ethernet 802.3ac frame layout

- Ethernet is a popular LAN protocol and further refined and developed into a formal standard called IEEE 802.3ac.
- Uses a contention media access protocol and several standard versions of Ethernet.

### Ethernet II

- Commonly used version of Ethernet and ike SDLC, it **uses a preamble to mark the start of the frame.**
- It has the **same source and destination address format as Ethernet 802.3ac.**
- The type field is used to specify an ACK frame or the type of network layer packet the frame contains (e.g., IP).
- The **data and frame check sequence fields are the same as Ethernet 802.3ac.**
- **Ethernet II has an unusual way of marking the end of a frame** since it uses bipolar signaling to send 1s (positive voltage) and 0s (negative voltage).
- **When the frame ends,** the sending computer **transmits no signal** for 96 bits (i.e., neither a 0 or a 1).

## P. Even Parity

- When the seven bits of an ASCII character have an even (2, 4, or 6) number of 1s, and therefore a 0 is placed in the eighth parity position.
- **Example:**
  - **Assume that we are using even parity with 8-bit ASCII.**
  - **The letter V in 8-bit ASCII is encoded as 01101010.**
  - **Because there are four 1s (an even number), parity is set to 0.**
  - **This would be transmitted as 011010100**
- Refer to **Parity Checking**.

## Q. Forward Error Correction

## R. Frame

## S. Go-Back-N Arq

## T. Hamming Code

## U. High-Level Data Link Control (HDLC)

- **Formal standard** developed by the International Organization for Standardization (150) and **essentially the same as SDLC.**
- The primary differences are that the **address and control fields can be longer than in the SDLC** frame.
- HDLC also has several additional benefits, such as a **larger sliding window for continuous ARQ.**
- It uses a **controlled access media access protocol.**

**Variant: Link Access Protocol-Balance (LAP-B)**

- Scaled-down version of HDLC.

**Variant: Cisco HDLC (cHDLC)**

- Include a network protocol field

### V. Information Bits

- Convey the user's meaning

### W. Logical Link Control (LLC) Sublayer

- **First sublayer and data link layer's connection to the network layer above it.**
- **At the sending computer,** it is **responsible for communicating with the network layer software** (e.g., Internet Protocol (IP)) and for taking the network layer Protocol Data Unit (PDU)—usually an IP packet—and surrounding it with a data link layer PDU—often an Ethernet frame.

### X. Major Sources of Errors

**First six is important:**

- Line outages
- White Noise
- Impulse Noise
- Cross-talk
- Echoes
- Attenuation
- Intermodulation Noise

**Common in Analog**:

- Jitter
- Harmonic Distortion
- Phase Hits

#### I. Line Outages

- **Catastrophic cause of errors and incomplete transmission.**
- Occasionally, a communication circuit fails for a brief period.
- Caused by faulty telephone end office equipment, storms, loss of the carrier signal, and any other failure that causes a short circuit.
- When designing redundancy, considering this error is called "farmer with a back hoe".

#### II. White Noise (Gaussian Noise)

- **Caused by the thermal agitation of electrons and it is inescapable.**
- There still would be some white noise despite perfect insulation.
- White noise usually is **not a problem unless it** becomes so strong that it **obliterates the transmission.**
    - To resolve this issue**, increase signal to noise ratio** where **electronical signal increases and overpowers white noise.**

#### III. Impulse Noise

- **Primary source of errors in data communications.**
- Sources include:
    - voltage changes in adjacent lines
    - lightning flashes during thunderstorms
    - fluorescent lights
    - poor connections in circuits.

#### IV. Cross-Talk

- Occurs when **one circuit picks up signals in another.**
- It **occurs between pairs of wires** that are:

    - carrying separate signals
    - multiplexed links carrying many discrete signals,
    - microwave links in which one antenna picks up a minute reflection from another antenna.
- **Between lines increases with:**
    - increased communication distance
    - increased proximity of the two wires
    - increased signal strength
    - higher frequency signals.

## V. Echoes

- **Caused by poor connections** that **leads the signal to reflect back** to the transmitting equipment.
- If the **strength of the echo is strong enough** to be detected, it causes **errors.**
- **Cross-talk and white noise**, have such **a low signal strength**.
- **Occur in fiber optic** cables when connections between **cables are not properly aligned.**

### Echo suppressors:

- Devices that reduce potential for echo errors.

## VI. Attenuation

- **Loss of power a signal suffers** as it **travels from the transmitting computer to** the **receiving computer.**
- Some power is absorbed by the medium or is lost before it reaches the receiver and this **power loss** is a **function of the transmission method and circuit medium.**
- **High frequencies lose power more rapidly** than low frequencies during transmission, so the received signal can thus be distorted by **unequal loss of its component frequencies.**

### Repeaters:

- Used digitally to **correct for attenuation** due distance.
- **Replicates incoming distorted digital signal and** sent it on deeper into the network as if it is new.
- **Fewer repeaters necessary to correct for attenuation and make it cost-effectiveness.**

### Amplifiers:

- Used to **boost diminishing or attenuating analog signals over longer distance.**
- Boost attenuating analog signal, but also boost the error noise in signal.

## VII. Intermodulation Noise

- **Special type of cross-talk** and **the signals from two circuits combine to form a new signal** that falls into a **frequency band reserved** for another signal.
- **Multiplexed signal** has many **different signals amplified together and slight variations** cause intermodulation noise.
- A maladjusted modem may transmit a strong frequency tone when not transmitting data, thus producing this type of noise.

## VIII. Jitter

- **Affect the accuracy of the data being transmitted** because minute variations in amplitude, phase, and frequency always occur.
- The signal may be **impaired by continuous and rapid gain and/or phase changes.**

## IX. Harmonic Distortion

- **Caused by an amplifier on a circuit** that does **not correctly represent its output** with what was delivered to it on the input side.

## X. Phase Hits

- Short-term shifts "out of phase," with the possibility of a shift back into phase.

## Y. Media Access Control

- **Handles when messages get sent and controls which and when device transmits**
- **Critical in local area networks** and to ensure that no two computers attempt to transmit data at same time and if they do, they must be able to recover the problem.

### Important on:

- **Multipoint (shared) circuits**
  - Several computers shared same circuits.
- **Half-duplex point-to-point circuits**
  - Require computers to take turns

### Unimportant on:

- **Full-duplex point-to-point circuits**
  - Two computers on the circuits
  - Permits either computer to transmit anytime and no media access control.

### Two Media Access Control (MAC) Approaches:

1. **Contention Access**
2. **Controlled Access**

## Z. Media Access Control (Mac) Sublayer

- **Controls the physical hardware and second sublayer.**

### At the receiving computer:

- **Takes the data link layer PDU from the LLC (Link Logical Control) Sublayer and converts it into a stream of bits.**
- It controls when the physical layer transmits the bits over circuit.
- Receives a stream of bits from physical layer and **translates it into a coherent PDU for error correction and detection.**

### Data Link Protocol Functions:

1. Controls when computers transmit (media access control)
2. Error Detection and Correction (Error Control)
3. Identifies start and end of a message by using PDY (message delineation)

## AA. Odd Parity

- When the seven bits of an ASCII character have an even (1, 3, 5 or 7) number of 1s, and therefore a 1 is placed in the eighth parity position.
- **Example:**
  - **Assume that we are using even parity with 8-bit ASCII.**
  - **The letter V in 8-bit ASCII is encoded as 01101010.**
  - **Because there are three 1s (an odd number), parity is set to 1.**
  - **This would be transmitted as 011010101.**

## BB. Overhead Bits

- Used for error checking and marking the start and end of characters and packets.
- A parity bit used for error checking is an **overhead bit** since it does not send the user's data.

## CC. Parity Bit

- Based on the number of 1s in each byte transmitted.
- Set to make total number of 1s in the byte an even number or an odd number.
- Refer to **Parity Checking**.

## DD. Parity Checking

- **Oldest and simplest error-detection method**
- One additional bit is added to each byte in the message
- Refer to Odd Parity
- Refer to **Even Parity**

## EE. Point-To-Point Protocol (PPP)

| Flag | Address | Control | Protocol | Data | Frame Check Sequence | Flag |
|---|---|---|---|---|---|---|
| 1 byte | 1 byte | 1 byte | 2 bytes | Variable Length | 2 or 4 bytes | 1 byte |

- **Designed to transfer data over a point-to-point circuit** but **provides an address so that it can be used on multipoint circuits.**
- The **frame starts with a flag and has a 1-byte** address (which is not used on point-to-point circuits and ends with a flag.
- The control field is typically not used.
- The protocol field indicates what type of data packet the frame contains (e.g., an IP packet).
- The data field is variable in length and may be up to 1,500 bytes.
- The frame check sequence is usually a CRC-16 but can be a CRC-32.

## FF. Polling

- **Logical topology of bus**
- Process of **sending a signal to a client computer that gives it permission to transmit.**
- **Client stores all messages that needs to transmit** and periodically, the controlling device (i.e., Wireless AP) polls the client to check if it has data to send.
- **(Kuross) Master node "invites" slave nodes** to transmit in turn and typically used with "dumb" slave devices since not all computers are created equal.
- **Contention-Based**

**Concerns:**

- polling overhead
- latency
- single point of failure (master)

### I. Roll-Call Polling

- **Central device (controller) determines which devices can transmit.**
- Each client is checked periodically to see if it needs to transmit, and it is possible to modify to **select clients in priority** so that **some get polled more often than others.**
- **The front end processor works consecutively through a list of clients,** first polling terminal 1, then terminal 2, and so on, until all are polled.
- Usually, a timer "times out" the client after waiting several seconds without getting a response.

**Example of Roll-Call Polling:**

- **One could increase the priority of client 1 by using a polling sequence such as 1, 2, 3, 1, 4, 5, 1, 6, 7, 1, 8, 9.**

### II. Hub Polling (Token Passing)

- **Used in LAN multipoint configurations (i.e., token ring)** that **do not have a central host computer.**
- One computer **starts the poll and passes it to the next computer on the multipoint circuit.**
- It sends its message and **passes** the poll to the next **until it reaches the first computer and restart the process**.
- **(Kuross) Control token passed from one node to next sequentially.**
- Token message
- Whoever has access to token, have access to link

**Concerns:**

- Token overhead
- Latency
- Single point of failure (token)

- If token fails to function properly, then the whole mechanism won't work properly

## GG. Synchronization

- The **recognition of the start and stop of each message** takes place for each individual character because the **start bit is a signal that tells the receiver** to **start sampling** the incoming bits of a character so the data bits can be interpreted into their proper character structure.
- A **stop bit** informs the receiver that the character has been received and resets it for recognition of the next start bit.

## HH. Synchronous Transmission

- **Whole blocks of data are transmitted as frames after the sender and the receiver has been synchronized**
- All the letters or data in one group of data are transmitted at one time as a block of data and it is called a **frame.**
- In this case, the **start and end of the entire frame must be marked,** not the start and end of each letter.
- Often used on both **point-to-point** and **multipoint circuits.**
- The **start and end of each frame** (synchronization) sometimes are **established by adding synchronization** characters (SYN) to the start of the frame.

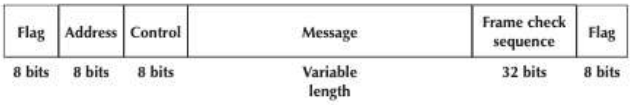
### For Multipoint Circuits, each packet must include:

- Destination address
- Source address
- Media access control is important.

### Synchronous Data Link Protocols:

### 1. Synchronous Data Link Control (SDLC)

- A **mainframe protocol** developed by IBM (1972).
- It uses a **controlled-access media access protocol** and using a **3270 protocol means one is using SDLC.**
- The **address field** identifies the **destination.**
- The **length of the address field** is **usually 8 bits** but can be set at **16 bits;** all computers on the same network must use the same length.
- **The control field identifie**s the kind of **frame that is being transmitted,** either information or supervisory.




#### I. Flag:

- Begins and ends with special bit pattern (01111110).

#### II. Address:

- Identifies destination and length of field can be 8 or 16 bits.
- All computers on same networks must use same length.

#### III. Control Field:

- Identifies type of frame being transmitted which is either information or supervisory.

#### Information Frame:

- Used for the transfer and reception of frames
- Frame numbering of contiguous frames and the like.

#### Supervisory Frame:

- Used to transmit **acknowledgement (ACKs and NAKs).**

IV. Message:

- Variable length and users' message

V. Frame Check Sequence Field

- 32 bit CRC code and older version is 16 bit

2. High-Level Data Link Control (HDLC)
3. Ethernet
4. Point-to-Point Protocol

### II. Throughput

- **Total number of information bits received per second** with consideration of overhead bits and the need to retransmit frames containing errors.
- **Small frames** provide **better throughput** for **circuits with more errors**
- **Larger frames** provide **better throughput in less-error-prone networks.**

### JJ. Transmission Efficiency

## CH.5 (KUROSS)

### A. Random Access Protocols

- When node has packet to send
  - Transmit at full channel data rate r.
  - No *a priori* coordination among nodes
- Two or more transmitting nodes → "collision",

**Random access mac protocol** specifies:

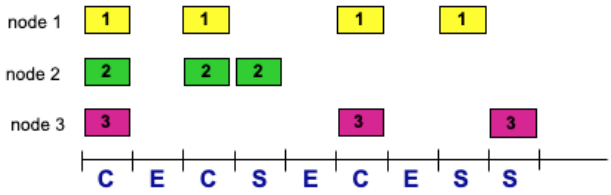
- How to detect collisions
- How to recover from collisions (e.g., via delayed retransmissions)

**Examples of Random access mac protocols:**

- Slotted aloha
- Aloha
- CSMA, CSMA/CD, CSMA/CA

### B. Slotted Aloha

- The random access **throughput can reach as**




**high as 37%**

- Nodes **start to transmit only slot beginning** and **synchronized in sense that** if we draw vertical line, it will not cross any frames.
- The **actual control is applied in overhead** and **reduced to minimum overhead.**
- There are already three nodes at the beginning, a **collision happens which is denoted by C.**

**Pros:**

- Single active node can continuously transmit at full rate of channel
- highly decentralized: only slots in nodes need to be in sync
- Simple

**Cons:**

- collisions, wasting slots
- idle slots
- nodes may be able to detect collision in less than time to transmit packet
- clock synchronization

### I. Throughput:

- The **throughput of efficiency of this link can be defined as** $G \times e^{-g}$.
  - E = np
  - G is attempt to transmission rate
- **Throughput first increases and then decreases** since the value of g decreases.
- When n value is large, the throughput will reach 0.

**If collision happens:**

- **Same nodes need to be retransmitted and increase the nodes.**

- The throughput or p success value would reach asymptotically 0.

### If the arriving rate is lambda:

- We will reach two crossing points.
- That means **the link will stay in stable condition** meaning **same nodes will arrive and depart (equilibrium point) where arriving rate = departing rate.**

### If the g increases slightly

- The throughput will increase slightly but arriving rate would be the same and more nodes will be departing, and n value would stay the same.

### If the transmission rate "G" is greater than throughput:

- **n value** would have to **increase since lambda would be more increasing** than the **throughput**

### If the n is from right side value:

- We would have more n values, then **the arriving rate is kept unchanged**, and **throughput would decrease** because more collisions will be happening and needs to be retransmitted.

- N is kept further greater and will move away through equilibrium will reach 0.

### If the n value decreases at the right equilibrium:

- It will need to nest collisions **as throughput would increase and be fixed at lambda arrival rate.**
- It means that n value would get smaller, and throughput would increase.
- Np = g - attempt to transmission rate.
- The **success would be 1/3 = 37% utilization of overall link capacity**

## II. Slotted Aloha Maximum Efficiency

$$N \times p \times (1-p)^{N-1}$$

N = number of nodes
P = probability

**Max efficiency = 1/e = .37**

1. **When there are N active nodes, the efficiency of slotted aloha is:**

$$Np(1-p)^{N-1}$$

**Find the value of p that maximizes this expression**

$$E(p) = Np(1-p)^{N-1}$$
$$E(p) = Np(1-p)^{N-1} - Np(N-1)(1-P)^{N-2}$$
$$= Np(1-p)^{N-2}((1-p) - p(N-1))$$

$$\boldsymbol{E'(p) = 0 \implies p* = \frac{1}{N}}$$

**Using the value of p found in (a), find the efficiency of slotted ALOHA by letting N approach infinity. Hint: $(1-1/N)^N$ approaches as $1/e$ as N approaches infinity**

$$E'(p*) = N\ \frac{1}{N}\left(1-\frac{1}{N}\right)^{N-1} = \frac{\left(1-\frac{1}{N}\right)^{N}}{\left(1-\frac{1}{N}\right)}$$

$$\lim_{N\to\infty}\left(1-\tfrac{1}{N}\right) = 1 \qquad \lim_{N\to\infty}\left(1-\tfrac{1}{N}\right)^{N} = \tfrac{1}{e}$$

**Thus:**

$$\lim_{N\to\infty} E(p*) = \frac{1}{e}$$

### Slotted Aloha Maximum Efficiency Example:

Assume that there are **2 active nodes**, each of which has an infinite supply of frames they want to transmit, and these frames have a **constant size of L bits**. If two or more frames collide, then all nodes will detect the collision.

There are two versions of the Aloha protocol: Slotted and Pure. In this problem we will be looking at the efficiency of these two variations. In the case of **Slotted Aloha, frames will be sent only at the beginning of a time slot, frames take an entire time slot to send, and the clocks of all nodes are synchronized.**

Please round all answers to 2 decimal places.

**Question 1:**
**Given a probability of transmission p = 0.24, what is the maximum efficiency?**

$$N \times p \times (1-p)^{N-1}$$
$$= 2 \times 0.24 \times (1-0.24)^{2-1}$$
$$= 0.48 \times (1-0.24)^{1}$$
$$= \mathbf{0.36\ or\ 36\%}$$

### C. Pure Unslotted Aloha

- Simpler and no synchronization
- When first frame arrives, it transmits immediately.
- Collision probability increases
  - Frame sent at $t_0$ collides with other frames sent in $[t_0-1, t_0+1]$

### Pure Aloha (Unslotted) Maximum Efficiency Example:

Assume that there are **3 active nodes,** each of which has an infinite supply of frames they want to transmit, and these frames have **a constant size of L bits.** If two or more frames collide, then all nodes will detect the collision.

**Question 1:**
**Given a probability of transmission p = 0.39, what is the maximum efficiency?**

$$p \times (1-p)^{2N-1}$$

$$= 0.39 \times (1-0.38)^{2(3-1)}$$

$$= 0.39 \times (0.62)^{2(2)}$$

$$= 0.39 \times (0.62)^{4}$$
$$= 0.05762771$$

$$= \mathbf{0.16}$$

## *WEEK 10 LECTURE*

## *WEEK 11 LECTURE*

## CHAPTER 11 – NETWORK SECURITY (FITZ)

## PRACTICE QUESTIONS

## *WEEK 12 LECTURE*

## *PASS SESSION*

## CHAPTER 8 – BACKBONE NETWORK

1. **What is the difference between a Routing Table and a Forwarding Table?**
   - Forwarding Table – MAC table
   - Router has **two control plane**
     - **1st: routing**
     - **2nd routing:** forwarding
   - Switches have **routing table**
   - **Routing Table (Layer 3 network layer)** is to **determine end-to-end path through network.**
   - **Forwarding table (layer 2 data link layer)** will **execute these best paths by mapping MAC address.**

2. **Which of the following Statements about switches are true?**
   a. **When a switch receives an Ethernet frame with a destination address that is not in its forwarding table, the switch will broadcast the frame out all of its other ports.**
   b. Cut-through switching has fewer errors than store and forward switching.
   c. Store and forward switching may only be used when the incoming and outgoing data circuits have the same data rate.
   d. A,B

e. A, B and C

**Answer: A**

**Store and forward switching:**

- it will wait until the entire frame prior to forwarding it

**Cut through switching:**

- it will begin the forwarding the frame as soon as the destination address Is identified.

**3. Which of the following is/are a major type of BBN architecture?**

a. switched BBN
b. Routed BBN
c. Multi switched
**d. A and B**
e. a,b and c

**Answer: D**

**4. Which of the following is true about CSMA/CD?**

a. The acronym refers to Carrier Sense Multiple Access with Collision Detection
b. It is a contention-based media access control technique
c. It is used in token ring protocol LANs (false since it is used in Ethernet)
**d. a and b**
e. a,b and c

**Answer: D**

**5. Switches:**

**a. learn addresses by reading the source and destination addresses**
b. operate at the physical layer only
c. connect two or more network segments that use different data link protocols (
d. connect two or more network segments that use different network protocols

have become more popular than layer 2 switches

Answer: A

- operates at physical layer, network layer, data link layer
- Switches uses the same protocols to be more efficient in time and cost.

**6. Which of the following is true about switched backbones?**

a. performance is improved over traditional (bridged or routed) backbone networks
b. each connection into the switch is a separate point-to-point circuit which supports simultaneous access by the LANs connected to the switch
c. there are many more networking devices in a switched backbone network
d. a and b
e. a,b,c

Answer: D

- For C, we only need a switch
- Switched backbone performs better than traditional
- Multipoint circuit: Wireless LAN, Wireless Access Point, HUb

**7. Device performance on a backbone network will not be improved by:**

a. using the same protocols in the backbone and the LANs
**b. translating packets from one protocol to another as they enter the BN**
c. ensuring that backbone devices have sufficient memory so that packets do not have to be retransmitted by the sender
d. a,b
e. a,b and c

**Answer: B**

- **Response time** – delays between sending and receiving a message
- **transfer time** – time it takes to receive message, processing time – time it takes to process
- **For A:** Use same protocol means you don't have transfer protocol each time will include response time.
- **B:** processing time would increase and response time would increase
- **C:** needs sufficient memory

**8. Which of the following is *not* a way that a router differs from a switch?**

a. **routers can connect two or more networks that use the same data link protocol**
b. routers only process messages that are specifically addressed to it
c. routers operate at the network layer
d. routers perform more processing on each message than switch
e. routers can choose the "best" route between networks for forwarding a packet

**Answer: A**

- Wireless LAN (WLAN) Not ethernet -based
  - contains receiving and destination mac address
  - if the protocol is ethernet-token ring, then the switches won't work.
- Switches only work with Ethernet Protocol
- B is false because switches can also process messages and sends
- C is false because C operates at data link layer
- D is true

**9. Circuit capacity on a backbone network will not be improved by:**

A. **going from 100Base-T Ethernet to 10Base-T Ethernet**
B. going from 100Base-T Ethernet to gigabit Ethernet
C. replacing a shared circuit backbone with a switched circuit backbone providing a faster circuit to the server
D. A,B
E. A,B AND C

**Answer: A since it decreases 90 mbps**

- B and C makes it faster

**10. Wireless LANs are never connected to a wire network. (True or False)**

False since **Overlay Network**

- **Wireless Lan over Wired Lan**
- Access points must be connected to Access Layer due to being best practice.

**11. Which of the following are true regarding switched BBNS?**

a) uses a star topology with one switch in the center
b) They are connected by a layer 2 switch
c) There is a switch serving each LAN that is connected to the backbone switch
d) A, B
**e) A,B,C**

**Solution: E**

**Layer 2 vs Layer 3 switch**

- **Layer 2 – refers to data link layer (used in access and distribution layer)**
  - Connected to each clients and servers and deals with only MAC address to transfer messages.
  - Only sends and receives data between clients internally.
  - Network (IP address is needed to transfer data in another building)
- **Layer 3 – refers to network layer (uses MAC and IP address) used in core layer**
- **Star topology:** means always there is one center switch and takes 2 hubs to transfer messages.

**12. What are managed and unmanaged Switches which one is better to use in a large and small network?**

- **Managed switches** - able to detect faulty transmissions from a failing network card, disable incoming circuit so that the card could not send any more messages and issue an alarm to the network manager.
- Sends reports to MIB and Network Administrator used software tools to change it.
- **Managed Switch** – send information to MIB (Management Information Base) (DB stores network information) and better for large enterprises.
- Hard to configure and more expensive since it's not plug and play and dedicate specific information in each port.
- **Unmanaged switches –** plug and play, less expensive and better for smaller clients (enterprises).

- **Switches (Layer 2)**: can't determine best port and only determine forwarding by forwarding table.

- **Layer 3 switch** combines forwarding and routing function

## CHAPTER 9 – WIDE AREA NETWORK

### 1. Switch-based Ethernet:

a. uses a hub to connect computers
b. has a physical topology of a ring
c. has a logical topology of a ring
d. has a logical topology of a bus
**e. usually enables all attached circuits to send or receive packets simultaneously**

**Solution: E**

1. **Shared ethernet – central device: hub**
Physical topology: star
Logical topology: bus
- Multipoint circuit – takes turns to use circuit (not efficient)

2. **Switched Ethernet – central device: switched ethernet**
Physical topology: star
Logical topology: star
- Point-to-point circuit: If server tells to send message to Computer A, then it only sends communication to Switch A

### 2. A__type of BN is a new type of LAN/BN architecture made possible by intelligent, high speed switches that assign computers to LAN segments via software, rather than by hardware.

a. Bridged backbone
**b. Virtual LAN**
c. Hubbed backbone
d. Collapsed backbone
e. Routed backbone

**Answer: B**

**Port-Based VLAN**
- 1 Switch with eight ports through the VLAN technology and based on software.
- Separate into multiple logical switches
- VLAN operates only in one switch
- Difference between VLAN and subnet is subnet is based on network layer with IP address, whereas VLAN segments based on data link layer.

### 3. How does layer 2 switch, layer 3 switch and VLAN switch functions?

- **Layer 2 switch** is a data link layer and uses ethernet address to decide which port to use.

- **Layer 3 switch** will be used in core layer and used for designing campus backbone and uses IP address and backbone

- **VLAN switches** uses special combination of layer 2 switches and routers and used to separate an existing physical network into multiple logical networks.

### 4. Which of the following would be part of an "ideal" backbone design for the future?

a. access layer composed of 10/100 layer 2 Ethernet switches
b. distribution layer composed of Ethernet Routers of 100 (or 1000) Base-F or Base-T
c. coax cabling throughout LANs and BN
**d. a,b**
e. a,b and c

**Solution: D**

- 1000 Base F – fibre speed
- 100 Base T – twisted pair
- Switch can support both 10 mbps and 100 mbps and switch depends on different devices
- Coax cable used by telephone and expensive.

### 5. The hardware devices for networks include switches, routers and VLAN switches, which of the following regarding these tables are correct?

a) Routers strip off the data link layer packet, process the network layer packet and forward packets based on the network layer address
b) VLAN switches are a combination of layer 2 switches and router
c. switches forward packets based on routing tables
d. Routers are layer 2 devices that acts as TCP/IP gateways
**e.)A,B**
f.) ALL of the above

**Answer: E**
- **Router works in the network layer** (IP address)

**6. In the structured design approach BBN refers to the**

a) Distribution layer that connects access layers
b) core layer that connects the distribution layers different of different adjacent buildings
c) distribution layer that connects layers of different buildings
d) core layer that connects the access layer
**e) a,b**
f) a,b and c

**Answer: E**

**7. Which of the following regarding VLANS are true?**

a) A VLAN is a flexible LAN/BBN architecture that assigns computers to LAN subnets by software.
b) VLAN switches: Special type of high-speed layer-3 switches.
c) Single-switch VLAN: One VLAN switch logically connects all computers and assigns them to the different VLANs
**d) a,b**
e) a,b and c

**Answer: D**

**8. These questions refer to routed BBN's. Which are true?**

a) Distribution layer switches are connected by switches
b) Within the LANs and distribution layers, traffic is based on physical layer addresses.
**c) Between distribution layers, message are sent to the core layer router, which forwards or routes the message based on its network layer address**
d) a,b
e) a,b and c

**Solution: C**

- You need router to connect switches.
- Within the LANs and distribution layers, traffic is based on MAC address.

**9. What are the best practice BNN design**

- **Access Layer:** Layer 2 Switch 100/1000 Base T (Twisted Pair) since traffic is between layers.
- Send message between access layer, traffic is based on MAC address
- **Distribution Layer:** Layer 2 Switch 1000 Base T Cat5e Cat6
- **Core Layer:** Router or Layer 3 Switch 1000 Base F
- **ACL:** Access Control List: blocks unauthorized traffic

**10. What are 3 Categories of MANs and WANs offered by common carriers?**

1. **Dedicated Circuit Network**
2. **Packet-Switched Network**
3. **VPN:** gives the equivalent of private packet-switched network over the public network

**11. What is a VPN**

- Point-to-point circuit that runs over internet

**How does it work?**

- **VPN Encapsulation:** VPN device or software + routers
- Encrypt the data and send it over the secured tunnel and decrypt it on the receiving end.
- **Tunnel: (SSL – Secure Socket Layer)** Envelope your data

**Advantages**

- Secured
- Low Encryption Cost

**Disadvantages**

- Unstable compatibility
- Affects technical goal: availability

**12. Which of the following is not a benefit of packet switched services?**

**a. The data transmission rates tend to be lower than dial-up or dedicated circuits.**
***Statement is true but not a benefit***

b. You don't have to set up dedicated circuits between each end point from which you wish to transmit and receive data and/or voice.

c. You have the flexibility to send data through a temporary circuit between two connections that will be disconnected as soon as the digital transmission is completed.

d. All circuits are less susceptible to a great deal of noise because they are digital.
All circuits are actually more susceptible

e. You don't have to specify all the interconnecting services you need for your WAN when

you buy the service.

Solution: A

- **Packet Switched** services provide common carrier.
- **Point of Prescence (POP)** – location at which the packet-switched network (or any common carrier network) connects into the local telephone exchange.
- **Dedicated circuits** dedicate to the use of two computers because it goes form one point to another.

### 13. What is CIR and MAR? terms used for packet-switched

- **Committed information Rate (CIR):** the data rate the Permanent Virtual circuits (PVC) guarantees to transmit (minimum data rate)
- **Maximum Allowable Rate (MAR):** Max data rate provided over CIR

### 14. What are some services commercially available for PSDN?

- **Frame Relay:** Low cost and data rates from 64 kbps to 45 Mbps
- **IP (MLPS, Multiprotocol Layer Switching):** 64 kbps to a 10 Gbps
- **Ethernet:** 1 Mbps to 40 Gbps

### 15. Which of the following is a way to reduce network demand?

a. shifting network usage from high cost times to lower cost times

b. using data compression techniques for all data in the network

c. moving data further from the applications and people who use them

**d. A,B**

e. A, B and C

**Solution: D**

### 16. When would you use T-line and when would you use SONET?

- Scalable
- Channels Fraction T-1, T1, T3
- FT01 has 64 kbps
- T1 64*24 = 1.544 Kbps

### 17. Which of the following is not a basic architecture for dedicated circuit networks?

a. ring
b. partial mesh
**c. bus**
d. star
e. full mesh

**Bus architecture is for Ethernet networks**

### 18. Which of the following is a benefit of packet switched services?

a. You don't have to set up dedicated circuits between each end point from and to which you wish to transmit data and/or voice.
b. You have the flexibility to send data through a temporary circuit between two connectionsthat will be disconnected as soon as the digital transmission is completed.
c. The data transmission rates tend to be lower than dial-up or dedicated circuits.
**d. a, b**
e. a, b, c

**Solution:** D

### 19. With a virtual private network, users create permanent virtual circuits through the Internet called:

a. bursts
b. cells
**c. tunnels**
d. rings
e. clouds

**Solution: C**

### 20. Which of the following is/are a way to reduce network demand?

a) shifting network usage from high cost times to lower cost times
b) using data compression techniques for all data in the network
c) requiring a network impact statement for all application software developed by the organization
d) moving data further from the applications and people who use them
**e) a,b,c**
f) a, b, c, d

**Solution: E**

## CHAPTER 11 – NETWORK SECURITY

### 1. Which of the following are Threats to business continuity?

a) Disruption
b) Destruction
c) Disasters
d) Invasion
**e) a,b,c**
f) All of the above

**Solution: E**

- Ensuring business continuity refers primarily to ensuring availability with some aspects of data integrity.
- **Disruption:** loss of or reduction in network service and may be minor or temporary

### 2. Controls are mechanisms that reduce/eliminate security threats and include

a) Preventive controls reveal unwanted events Ex: password
b) Detective controls reveal unwanted events Ex: auditing a software
c) Corrective controls rectify an unwanted event
d) A,B
**e) A,B and C**

**Solution: E**

- **Preventive controls:** mitigate or stop a person from acting or an event from occurring.
- **Detective controls:** reveal or discover unwanted events.
- **Corrective controls:** remedy and unwanted event or an intrusion

### 3. Controls must be periodically reviewed by external "experts" because-

a) They are operating effectively
b) They are updated/replaced when needed
c) To facilitate audit
**d) a and b**
e) a,b and c

**Solution: D**

- **Audit:** process of mapping network in terms of software and hardware, examine security documents such as user accounts, permissions, etc.)

### 4. Which of the following defines risk management?

**a) Key process in developing a secure network by analyzing and prioritizing security risks to IT assets**
b) Key process in developing a secure network by using network management software and managed devices
c) Key process in using preventive, detective and corrective mechanisms to mitigate risks
d) key process in forming a secure network by analyzing network management and creating control spreadsheets
e) None of the above

**Solution: A**

### 5. Which of the following define risk mitigation?

a) Take no actions for risks that have low impacts
**b) Use of control to remove or reduce impact of threat**
c) Transfer all or part of impact (e.g., insurance)
d) Take no action while collecting more information about threat and risk

**Solution: B**

- **Risk acceptance** – low impact
- **Risk mitigation** – uses control to counter the threat/minimize the impact
- **Risk transference**
- **Risk deferring** – do not take actions until more information is gathered

### 6. IT professionals and external auditors must:

a) Evaluate adequacy of the controls and degree of risk associated with each threat
b) Establish priorities for dealing with threats to network security
c) Create RFP's and control spreadsheets to aid network management
**d) a,b**
e) a, b and c

**Solution: D**

**RFP = Request for proposal (a bidding process)**

### 7. What does DoS and DDoS do?

**a) attacks prevent normal access to servers**
b) blue screen of death
c) data loss and system crashes
d) slow down computer networks by eating up bandwidth

**Solution: A**

- An attacker attempts to disrupt the target by flooding it with messages so that it cannot

processes messages from normal users.

- **DOS:** usually one and botnet which is automatic
- **DDOS:** many computers or laptops attack server by overloading server with HTTP requests

**8. Which of the following helps to protect against DoS and DDoS?**

a) traffic anomaly detector

b) traffic anomaly analyzer

c) encrypt data with two factor protection (more from client side)

**d) A,B**

e.) A,B and C

**Solution: D**

**9. Which of the following is not the best mechanism for device failure protection?**

a) Redundancy in the network
**b) Uninterruptible power supplies**
c) RAID storage technology
d) use of fault-tolerant servers

**Solution: B**

**Network redundancy:**

- process through which additional or alternate instances of network devices, equipment and communication mediums are installed within network infrastructure
- method for ensuring network availability in case of a network device or path failure and unavailability

**Uninterruptible power suppler or source (UPS):**

- electrical apparatus that provides emergency power to a load when the input power source or mains power fails

**Raid:**

- way of coordinating multiple disk drives to protect against loss of data availability if one of the drives fails

**Fault tolerance:**

- process of working a system in proper way in spite of occurrence of the failures in system.
- Hence, systems are design in such a way that in case of error availability and failure, system does the work properly and given correct result.

**10. Which of the following is required for physical security?**

**a) All servers and network equipment are in secured rooms and only authorized personnel can enter those rooms**

b) Disaster avoidance: i.e., storing critical data in multiple locations and avoiding locations prone to flood (basements) or natural disasters

c) Application-level firewalls: Filtering based on anomalous access to specific application

d) A,B

e) A,B and C

**Solution: A**

## CHAPTER 12 – NETWORK MANAGEMENT

**1. Which of the following is a basic function of a network manager?**

a. cost management
b. performance and fault management
c. Web surfing to shop on eBay
**d. a,b**
e. a,b and c

**What do Network Managers do?**

- Manage the day-to-day operations of the network.
- Provide support to network users.
- Ensure the network is operating reliably.
- Evaluate and acquire network hardware, software, and services.
- Manage the network technical staff.
- Manage the network budget, with emphasis on controlling costs.
- Develop a strategic (long-term) networking and voice communications plan to meet the organization's policies and goals.
- Keep abreast of the latest technological developments in computers, data communications devices, network software, and the Internet.

- Keep abreast of the latest technological developments in telephone technologies and network services.
- Assist senior management in understanding the business implications of network decisions and the role of the network in business operations.

**2. Which of the following is not considered a key management task for running a network?**

**a.) knowledge of frame relay**

b.) planning

c.) organizing activities

d.) directing activities

e.) controlling activities

**Solution: A**

**3. Which of the following refers to preventing, detecting, and correcting faults in thenetwork circuits, hardware, and software.**

**a. Fault management**

b. Fault tolerance

c. Firefighting

d. Performance management

e. Troubleshooting

**Solution: A**

- **Performance management:** ensuring the network is operating as efficiently as possible

**4. Desktop management:**

a. increases the cost of configuration management over the long term

b. requires managers to install software and application updates manually on client computers

**c. automatically produces documentation of software installed on each client computer**

d. a,b

e. a, b, and c.

**Solution: C**

**5. ___is a criterion that keeps track of the number of hours or days of continuous operation before a component fails.**

a. MTTDiagnose

b. MTTRespond

c. MTTRepair

d. MTTFix

**e. MTBF**

**Solution: E**

**6. Which of the following is an important step in reducing network costs?**

a. developing standards for computers on the network

b. automating as much of the network management process as possible

c. moving to fat client architectures (expensive)

**d. A,B**

e. A,B and C

**Solution: D**

**7. Documentation for network and application software:**

**a. is important for monitoring adherence to software license rules**

b. includes information about which data files each user can access

c. usually does not include information about any special purpose network software

d. a,b

e. a,b,c

**Solution: A**

**8. ___is a measure of how much it costs per year to keep one computer operating.**

a. Web gardening

b. Software installation cost

c. Hardware upgrade cost

d. **Total cost of ownership**
e. Support staff cost

**Solution: D**

**9. A costing method that examines only the direct costs of operating the computers, omitting softer indirect costs such as "wasted" time is referred to as:**

a.total cost of ownership

**b.network cost of ownership**

c.transactions costs

d.ownership privileges

e.total direct costs

**Solution: B**

**10. Which of the following are the main functions within end user support?**

a. resolving network faults

b. training

c. spin control

**d. a,b**

e. a,b,c

**Solution: D**

**Three main functions within end user support:**

- resolving network faults
- resolving user problems
- training

## FINAL EXAM REVIEW PASS

**1. Which of the following statement(s) about 802.11g is (are) true?**

a. 802.11g provides a maximum (equal) nominal data rate that is lower than that of802.11a
b. 802.11g provides more non-overlapping channels than 802.11b
c. 802.11g is compatible with Fast Ethernet
d. All of the above
**e. None of the above**

**Solution: E**

- Standards and key characteristics:

| Standard | Frequency | Non-overlap. channels | Maximum data rate | Maximum range | Backward compatibility | Status |
|---|---|---|---|---|---|---|
| 802.11b | 2.4 GHz | 3 | 11 Mbps | 150 m | N.A | Obsolete |
| 802.11a | 5 GHz | 8 to 12 | 54 Mbps | 50 m | N.A | Obsolete |
| 802.11g | 2.4 GHz | 3 | 54 Mbps | 150 m | 802.11b | Obsolete |
| 802.11n | 2.4 GHz | 3 | 450 Mbps | 100 m | 802.11b / g | Still in use |
| 802.11ac | 5 GHz | 8 to 12 | Up to 6.9 Gbps | 100 m | 802.11 a | Best |

**2. Which of the following statement(s) about wireless bridges is (are) true?**

a. They can connect two wire-based LANs
b. They can connect a wireless LAN to a wire-based LAN
c. They can connect two wireless LANs
d. a,b
**e. a,b and c**

**Solution: E**

**3. Which of the following is/are a step(s) under the traditional network design approach?**

a. An analyst develops cost estimates of the circuits needed to support the network.
b. An analyst meets with users to identify user needs.
c. An analyst takes the traffic on the current network and then multiplies that by a factor of 3.65 to come up with the estimate of the total traffic for the new network.
**d. a,b**
e. a,b and c

**Solution: D**

**4. Which of the following statements about LAN is/are true ? (Ch.7 )**

a. An access point plays the same role in a wireless network as a router does in a wired Ethernet network.
b. Many network hubs and switches incorporate repeaters to regenerate signals so that attenuation of the signal does not occur.

c. The NOS software for the server computer provides the physical, data link, and network layer functions.
d. A,B
e. A, B and C

**Solution: B**

- **Access point** is only used in access layer and equivalent to switch or hub in wired ethernet LAN (even if it is in wireless network).
- **Routers** are used in Core Layer/Network Layer/Gateway,
- If **routed backbone network layer,** then router can be used in distribution layer.

**5. Which of the following is used to model the behavior of the planned communication network once the proposed network map (Logical Design) is complete.**

a. Implementation
b. Post-implementation review
c. Documentation
**d. Simulation**
e. All of the above

**Solution: D**

**Simulation:** a mathematic technique in which the network comes to life and behaves as it would under real conditions, is used to model the behaviour of communication network.

**6. Which of the following is true about routed Backbone**

a. VLANs provide faster performance compared to switched, collapsed or routed backbone architectures.
b. The switches in the VLAN can send packets among themselves in a way that identifies the VLAN to which the frame belongs.
c. A VLAN requires the computer manager to reconfigure the physical cables to the switch if a computer is moved from one port to another port on a switch.
**d. a,b**
e. a,b and c

**Solution: D**

**VLAN (Virtual LAN)**

- New type of LAN-BN architecture made possible by intelligent high-speed switches.
- Layer 3 or Layer 2
- Networks in which computers are assigned to LAN segments by software rather than hardware
- Virtual LANs can be design so that they can act as though computers are connected via hubs.

**7. Which of the following are WLAN standards**

**a.802.11ac**
b.802.11a
c.802.3
d. a,b
e. a,b and c

**Solution: A**

**8. Which of the following is not a type of hardware device that can be used to interconnect networks?**

a. layer 3 switches
b. routers
**c. dumb terminals**
d. a,b
e. a,b and c

**Solution: C**

**9. A__geometric layout connects all computers in a closed loop, with each computer linked to the next usually with a series of point-to-point dedicated circuits.**

a. bus design
b. star design
c. full mesh design
**d. ring design**
e. partial mesh design

**Solution: D**

**10. Which of the following statements about Network management is true?**

a. Due to changing communication technologies,
b. One common configuration activity is updating the software on the client computers in the network.

c. In many organizations, configuration documentation takes the form of a large set of network diagrams, one for each LAN, BN, and WAN
d. a,b
**e. a, b and c**

**Solution: E**

11. **Which of the following would not be included as part of the physical network parameter statistics** monitored by a NMS (Network Management System)?

a. stats on multiplexers
b. stats on modems
c. stats on circuits in the network
**d. stats on user response times**
e. stats on malfunctioning devices

**Solution: d**

12. **Which of the following statements is true about Network Design**

a. The primary goal of the needs analysis step in network design is to develop a physical network design.
b. Network requirements can be divided into mandatory, desirable, and wish-list requirements.
c. Today, all network traffic is due to traffic from internal application systems.
**d. a,b**
e. a,b and c

**Solution: D**

13. **Which of the following statements are true**

a. A star topology is dependent upon the capacity of the central computer for its performance
b. In ring design WAN, failure in one circuit means that the network can most likely continue to function
c. A WAN with a ring topology can use full or half duplex circuits
d. A,B
e. A, B and C

**Solution: E**

14. **Which of the following statements are true?**

a. The cable to connect BNs is usually twisted pair.
b. **Routers connect two or more network segments that use the same or different data link protocols, but the same network protocol.**
c. Layer-3 switches switch messages based only on their data link layer address.
d. A,B
e. A, B and C

**Solution: B**

15. **Which of the Following statements is/are true?**

a. Ethernet is a layer 3 protocol, which operates at the network layer.
b. Wireless LANs use Carrier Sense Multiple Access with Collision Detection (CSMA/CD) for medic access control.
**c. A forwarding table tells a switch which port it should send out a packet to get to the destination computer.**
d. A,B
e. A,B and C

**Solution: C**

- Ethernet (Wired LAN) uses a contention-based media access control technique called Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- Ethernet is data link layer 2 protocol

- Wireless LAN uses Carrier Sense Multiple Access with Collision Avoidance

**16. Which of the following statements is/are true ?**

a. Today, all network traffic is due to traffic from internal application systems.
b. The traditional network design approach works well for rapidly growing network (slowly evolved network)
c. **The step of understanding current traffic on a network provides a baseline against which future network requirements can be compared.**
d. A,B
e. A,B and C

**Solution: C**

**17. What is following defines how Network address translation (NAT) works**

a) Filtering based on IP address and ACL rules
b) Filtering based on anomalous access to specific application
**c) Process by which a router converts one IP address to another, often from a publicly routable address to a private address and vice versa**
d) a,b
e.) A, B and C

**Solution: C**

**Network Address Translation:**

- Processing of converting between one set of public IP address that are viewable from the Internet and a second set of private IP addresses that are hidden from people outside the organization.

**18. Which of the following statement(s) about security measures is (are) true?**

a. **Honey pots prevent attacks by exposing hackers' methods and network's weaknesses**
b. DMZs prevent attacks by allocating a separate range of IP addresses to decoy services
c. Intrusion detection systems prevent attacks by filter traffic
d. A,b
e. A, B and C

**Solution: A**

**Honey pot**

- Consists of data that appears to be a legitimate part of the site and contain info or resources of value to attackers.
- Actually isolated, monitored, and capable of blocking or analyzing the attackers.

**Demilitarized zone (DMZ)**

- A physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted larger network such as internet
- Purpose is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of organization's network is firewalled.

**19. Which of the following is true about star topology:**

a. difficult to manage because the central computer receives and routes all messages in the network
b. **dependent upon the capacity of the central computer for its performance**
c. always slower than a ring network
d. less susceptible to traffic problems than other architectures

**Solution: B**

**20. In a ring design WAN,**

a. **messages can take a long time to travel from the sender to the receiver**
b. a message arrives at all computers on the network simultaneously
c. messages always arrive faster than in other types of layouts
d. messages are delivered directly from sender to receiver because there is a point-to-point connection directly between each sender and each receiver
e. messages always take one second to travel between sender and receiver

**Solution: A**

### Ring architecture

- connects all computers in a closed loop with each computer link to next
- Circuits are full-duplex or half-duplex circuits, meaning that messages flow in both directions around the ring.