SCHOOL OF INNOVATIVE TECHNOLOGIES & ENGINEERING

Module Information Pack

B.Sc (Hons.) Computer Science with Network Security

Version 6.0 (BCNS24AFT2)

Network Design & Management

BCNS3105C

Academic Year 2025-26 Semester 2

Blended Mode (Online and F2F)

Programme Director:	Dr. Sandhya Armoogum
Programme Coordinator	Prof. Vinaye Armoogum
Module Coordinator:	Mr. Rishi H. Heerasing
Module Convenor:	Mr. Rishi H. Heerasing
Office:	Room 2.14 Level 2 BLOCK G
Phone:	207 5250 ext. 124
E-mail:	rheerasing@utm.ac.mu
Academic Tutoring:	None
Classes Timing and Venue:	Mondays: 11:00 -14:00 at Lab G0.3
Credits & Level:	6 credits
Pre-requisites (If applicable):	BCNS1207C or equivalent
Co-requisites (If applicable):	None
Method of Delivery & frequency:	15x3 Hours blended classes + 45 Hours Self-Study
Method & Criteria of Assessment:	50% Coursework and 50% unseen Written Exams

Module Contents:

- Survey of the current technologies applicable to the development of corporate LAN, LAN to LAN connection, LAN interconnection via WAN and WLAN.
- Analysis, Design and Simulation of corporate networks through case-studies.
- Managing network performance and security.
- Fault and configuration management.

Learning Outcomes:

- Understand the fundamental requirements, concepts and issues involved in enterprise or backbone networks.
- Understand the need for proper network planning and how to implement same.
- Understand the necessary steps involved in efficient network design.
- Understand the different metrics and concepts in network performance.
- Understand how to effect fault and configuration management.
- Understand the value of network cost management.
- Understand the need for logical security and how these are implemented.
- Understand the various LAN and WAN technologies available.

Tentative Module Schedule *(F2F on ODD weeks and ONLINE on EVEN weeks)*

Wk	Dates	Topics Covered
1	27/04/26 Online	**Network Performance:** Latency, Throughput, Reliability, Availability, Bing Tool
2	04/05/26 Online	**Introduction:** Elements of enterprise networks: justifications, goals and benefits. Interoperability issues
3	11/05/26 F2F	**Network Design:** Traditional vs. Building Block Approach, Needs Analysis, Technology Design and Cost Assessment
4	18/05/26 ONLINE	**Network Management:** Configuration & Cost Management, End-user Support, Network Management Tools: Hardware & Software Requirements.
5	25/05/26 F2F	**Switching:** Transparent Bridging, Spanning Tree Protocol
6	01/06/26 ONLINE	**Redundancy:** Backup, UPS, RAID
7	08/06/26 F2F	**Network Management (cont.):** Simple Network Management Protocol (SNMPv1), ASN1.0, Basic Encoding Rules, OSI Identifier Tree
8	15/06/26 ONLINE	**Network Security:** Firewalling, DMZ, Subnetting, Application and Protocol Gateways. Network Monitoring Software, Computer malware
9	22/06/26 F2F	**LAN Technologies:** Ethernet, WLAN (IEEE 802.11x), Bluetooth
10	29/06/26 ONLINE	**WAN Technologies:** xDSL, Frame Relay, ATM, MPLS, WiMAX, 4G, 5G, VSAT
11	06/07/26 F2F	**Packet Tracer Labs**
12	13/07/26 ONLINE	**Packet Tracer Labs**
13	20/07/26 ONLINE	Buffer
14	***27/07/26 F2F***	***Open-Book Class Test (20%) + Submission of Network Design Assignment***
15	***03/08/26 F2F***	***Class Test Post Mortem***

Note: I shall be on special leave for an overseas training from the 22nd July to 2nd August.

Reading List

Recommended Textbooks (as per availability in the UTM Resource Centre)**:**

- **Panko R. (2005) *Business Data Networks & Telecommunications*, 5th Ed., (D4.6PAN)**
- Fitzgerald & Dennis (2012) *Business Data Communications & Networking*, 11th Ed.*
- Stallings W (2004) *Business Data Communications*, 4th Ed., Prentice-Hall Inc. (D4.6STA)
- Hallsall F. (2001) *Data Communications, Computer Networks, and OSI*, 4th Ed., Addison-Wesley. (D4.6HAL)

* E-book available at http://www.rishiheerasing.net/modules/bcns3105/readings.html

Other Reading Materials: Papers/Articles/Websites:

- Companion site for *Computer Networking: A Top-Down Approach featuring the Internet*, 2nd Ed. at http://wps.aw.com/aw_kurose_network_2
- Fitzgerald & Dennis (2012) *Business Data Communications & Networking*, 11th Ed., at https://www.safaribooksonline.com/library/view/business-data-communications/9781118086834/

Past Exam Papers

Available at the end of this MIP and from Post-Semester Site

Module Assets

Available on **Nefertum's Shrine** at www.rishiheerasing.net/modules/bcns3105/bcns3105.html

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

Software needed will be Wireshark and Cisco ® Packet Tracer and are available Tools section.

I would recommend that you download the latest version of these two software from their official websites. You need to register a free account on Cisco Networking Academy to download the latest version of Packet Tracer at https://www.netacad.com/resources/lab-downloads?courseLang=en-US

Introduction to Enterprise Networking

Definition: An enterprise network is one in which the network spans **multiple sites**, includes **multiple computing platforms**, and interconnects **multiple protocols**.

Two main goals of an enterprise network:

- Maximise the interoperability capabilities of an enterprise's network users.
- Minimise the expense of the network infrastructure.

An enterprise may be a hospital, a government agency or an international bank.

Motivations

1. **Multi-site:** Not so long ago, ***all*** networks were multi-site networks, more or less by definition. The idea of a Local Area Network (LAN) did not exist, except in a few laboratories or research environments. Organizations had few computers, and those were usually isolated in big "glasshouse" computer rooms with heat & air circulation requirements. There was no need to "network" three mainframe computers in the same room. One simply carried the data in the form of computer tapes from machine to machine. A network then implied what came to be called a WAN (Wide Area Network), to distinguish them from the newer ***single*** site networks of the 1980s: the LAN.

2. **Multi-platform:** Should be distinguished for multi-vendors. Multi-platform refers to the kind of computing device and not necessarily who manufactures and distributes it. For example many vendors (for example, DEC, HP, and others) manufacture mini-computers, PCs, and "in-between"-sized computers loosely known as "servers". IBM also manufactures these devices along with mainframes. An organization may have a mainframe, mini-computer, and several kind of "PCs" and still be considered single-vendor because these platforms have different operating systems, application packages, and internal data formats. In fact, even organizations with nothing more powerful than desktop clients and dedicated servers on LANs may have UNIX-based workstations, disk operating system (DOS)-based PCs, and System 7 Macintoshes, sometimes even on the same LAN.

3. **Multi-protocol**: There is a need to link together multiple network protocols into a coherent whole. Today, there are "open" (in other words, non-proprietary) network protocols that do a more or less adequate job of networking computing products from different vendors together. Some even do an outstanding job at a fraction of the proprietary protocol's cost. Even if an organization were to try to build a large multi-site, multi-platform network using only one, open, standard protocol, the organization will quickly realise that the effort would be futile. There is simply no current, mature, fully-defined protocol capable of running over both WAN and LAN with equal ease. TCP/IP and ATM do come close.

These **three** ingredients – **multi-site**, **multi-platform**, and **multi-protocol** - uniquely define the enterprise network. A common variation is "enterprise-wide network", but this merely indicates the same thing with more letters.

Reasons for Enterprise Networks

- Sharing information
- Sharing expensive resources
- Reducing network costs
- Reducing MIS costs
- Giving companies freedom of location
- Enabling networking between companies

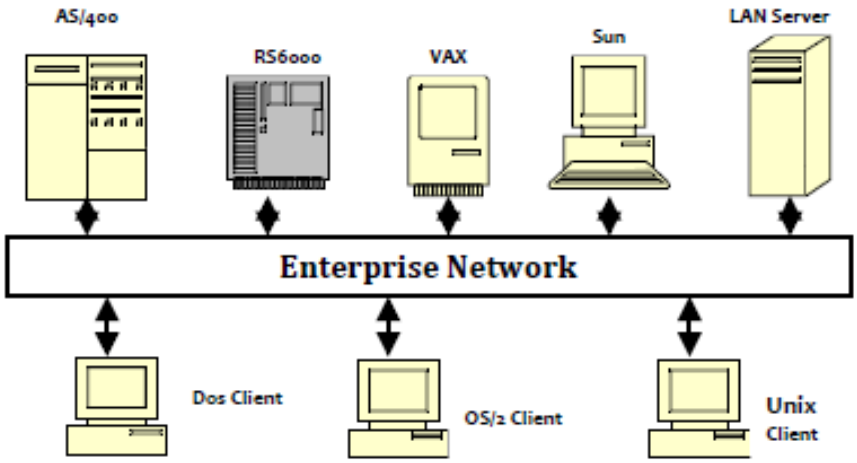
The Client/Server Model of computing and Enterprise Networking

The relationship of the C/S model of computing and Enterprise Network is easy to understand. The clients attach to servers over networks. Without an enterprise network, there would be different kind of networks – potentially one for each platform and protocol. The enterprise network is necessary to enable every client to access every server in the organization. The C/S concept is so important to enterprise networks that the key points are listed below:

- Clients are PCs with workers
- Servers are PCs with administrators
- Clients and servers are connected by networks
- Any client should be able to connect to any server
- Enterprise networks allow this to happen

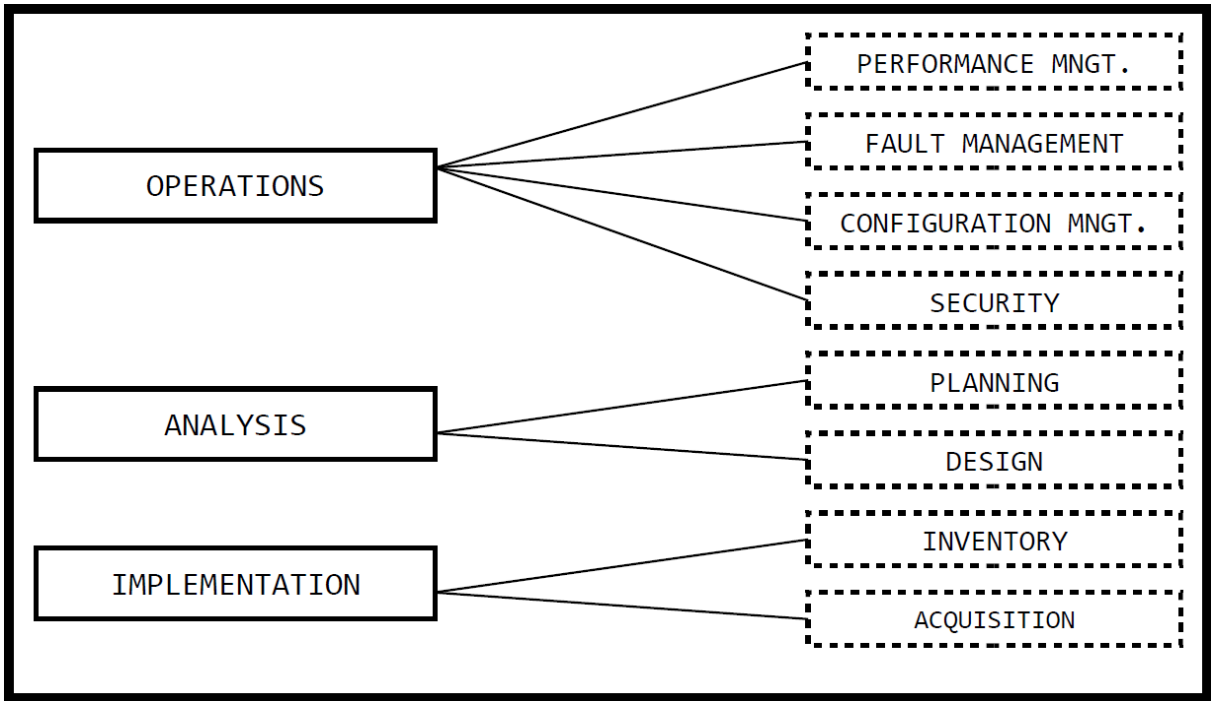
The Interoperability and Administration Problem

The idea of **interoperability** is an important one, not only in enterprise networks, but in all networks. **Interoperability** involves more than a concept of **internetworking**, as important as it is. **Internetworking** is the capability of separate networks to send data back and forth to each other. **Internetworking** has no conception of the utility of the data exchanged. That is the bits representing a data file may not be correctly interpreted on the destination computer after going through a WAN. This is the job of some task doing an interoperability function between the source and destination.



Network Administration

Basic groups and functions in Network Administration



The structure above shows one common way of dividing the Network Administration tasks in large organizations. Smaller organizations will have other structures. One common variation is to have an Implementation Group under the Planning Group umbrella. The most important point is that all the functions – from Performance Management to Acquisition – must be done by someone, somewhere, sometime, somehow, if the network is to be useful to its users.

The Benefits of Enterprise Networks

The benefits are closely related to the reasons for building enterprise networks mentioned earlier. The enormous benefits of allowing all employees to share critical information and expensive resources have a direct impact on an organization. Less replication of both the information and the resource is needed to allow these assets to be used more effectively.

The cost reductions involved with consolidating expensive network links used in building entirely separate networks is also a real benefit. The elimination of support for every possible platform and protocol in favour of a supported set of enterprise-wide platforms and protocols is a less direct benefit. The potential of allowing inter-enterprise communication between companies and customers can benefit an organization in terms of efficiency and customer satisfaction.

The strategic advantages of quicker market response, reduced inventories (due to a more timely Management Information), and the allowance of a large company to react and behave similar to a much smaller and agile, aggressive company, are just as real, but harder to quantify and measure.

Requirements Analysis

Requirement Analysis involves defining the problems on the existing networks in an organization – this, in turn automatically determines the goals of the enterprise network. The Requirement Analysis evaluates the business value of the technology. Defining the goals (hence the benefits) of the enterprise network helps to design the network. The Requirement Analysis should pinpoint and prioritize the business problems that need improvement. Focusing on the requirements will prevent a company from wasting resources on unnecessary features.
Once a clear set of goals have been defined, it is easier to outline the benefits and justify the cost of the enterprise network. The Requirement Analysis document should become the basis for the **RFP** (Request for Proposal) put out for competitive bid or used internally by the network designers to plan the enterprise network.
The Requirement Analysis phase has generally been skipped by organizations building departmental LANs. It is common to build LAN by buying shrink-wrapped NOS (Netware, Windows Server, etc…) The hardware, both clients and servers, is frequently purchased mail-order from a company catalogue. Sometimes, the administrator may hire a part-time consultant to implement the LAN. Either way, there is no time or energy spent in a Requirement Analysis. This approach usually works fine for departmental LANs. Even if the resulting network is not exactly what the users wanted, there is usually little impact on the organization's bottom line. The effects of a bad departmental LAN are localized. The whole corporation is not affected. The expense involved is relatively minor, compared to the corporation's total computing budget.

Requirement Analysis Benefits

- Defines the current network(s) problems
- Define the enterprise network goals
- Enables construction of a cost-effective network
- Allows establishment of priorities
- Justifies costs to upper management
- Allows writing of better contracts
- Defines criteria for project completion and success

Business Models

The enterprise network should be an asset to the organization, not a political football to be passed around as one group seeks to outdo another in the corporate environment. The network is there for business functions. The enterprise network must fit the business structure of the organization and vice-versa. For the enterprise network to solve business problem effectively, a business model should be constructed from which the technology and physical components of the enterprise network flow as a matter of course.

Another common name today for the business model is "**workflow analysis**". The business model need not mention computers or networks. Rather, the business model concentrates on exactly how work gets done in the organization. The business model is a written description of how business is performed. The goal is to gain a general understanding of a corporation's business practices. The business model should describe in detail how work flows through the departments, which personnel perform each task, and identify any dependencies between the various work groupings and departments. The steps that should be taken to perform the workflow analysis to construct the business model are well understood and commonly followed.

Business Model / Workflow Analysis

- Designate a team of managers, users, and network personnel
- Name a project leader
- Interview personnel in each department, including end-users
- Determine business flows between departments
- Determine the dependencies between departments
- Determine the bottlenecks of the present system

1. *Designate a project team of managers, users, and network personnel*
   The key is the inclusion of the users. Many corporations are reluctant to pull workers from their assigned tasks to have them participate in projects of this kind, but this is exactly the point. The users who know the work flow, and, more importantly, the business problems have many more insights than manager or other personnel Because the enterprise network must ultimately serve the users' and workers' needs, it is critical to ensure their participation.

2. *Name a project leader*
   Not all technically proficient personnel are adequate leaders. The leader should be a senior member of the organizations who is familiar with all aspects of the business and is respected by both subordinates and peers. It would be a further advantage for the leader to be popular, but many effective leaders are not, however, particularly well liked by their colleagues.

3. *Interview personnel in each department including end-users*
   The goal is to determine each employee's function and the effectiveness of any existing computer systems and networks. Here the inclusion of end-users on the project team is also essential. End-users typically become very close-mouth and reluctant to point out business problems to managers and supervisors. They are much more candid with peers, however, and will talk freely about their role in the department and any problems encountered.

4. *Determine business flows between departments.*
   Because the enterprise network must span the entire corporation, it is essential to determine exactly which departments interact most frequently with other departments and for what purposes. The flow of information also should be traced. Again, it is not necessary to record exact network capabilities employed – the emphasis is on the business needs not the technology.

5. *Determine the dependencies between the departments.*
   The workflow document must identify the critical path of work through the entire organization. Orders may need to be processed and filled in an exact order, with specific permissions, for instance.

6. *Determine the bottlenecks of the present system.*
   This should be the outcome of the business model. The preceding steps will identify some components of the business as slower as and less efficient than others. Some departments may need more timely information, more raw information or access to remote information to work more effectively. Many interoperability requirements are identified by this step.

Technology Models

The business model should identify many procedures to be streamlined or changed. The next step in the entire requirements analysis is to construct a technology model. The technology model should describe in very broad terms just how an enterprise network could be used to achieve the business model. However, before constructing the technology model, three steps are necessary. The first is to take an inventory of any existing end-user and networking equipment. Second, the actual network requirements must be determined. Finally, the present state of network technology and possible near-term changes in available technology should be factored into the plan.

A complete and accurate inventory of existing equipment must be made. In each location and department, a complete list of hardware, applications, and protocols used must be compiled.

After the inventory has been compiled, the network requirements must be determined. General network requirements issues are:

- Connectivity
- Existing hardware and software
- Volume of data to be transferred
- Response Time and Availability and Reliability
- Projected Growth

Once the network requirements have been set, the final step of building the network technology itself is ready to be taken. Traditionally, the network designers take the network requirements and build the technology model. This is the network designer main function and job.
Once it has been determined that the technology model and the network design is sound, a physical model of the network can be built. Usually, the language of the technology model is general ("a fast packet network") whilst that of the physical model is specific ("Frame Relay").
The output of the physical model phase is a document describing the exact network components needed, and their locations. This document forms the basis for a RFP (Request for Proposal) that will be given to interesting vendors and implementers.

All complete RFPs should usually include the following:

- Introduction
- Proposal Requirements and Specifications
- Installation, Maintenance and Support
- Training and Criteria

When the winning bidder has been notified that their response to the RFP has been accepted, the final step in the process of preparing to build an enterprise network is to issue a contract. The contract is normally known as the Statement of Work (SOW) for the network project. The easiest way to generate a SOW for the project is to take the RFP and turn the major sections into requirements. There are three sections that must be added to the contract, however.

- Payment Schedule.
- Indemnification.
- Changes and Modifications
- Completion criteria.

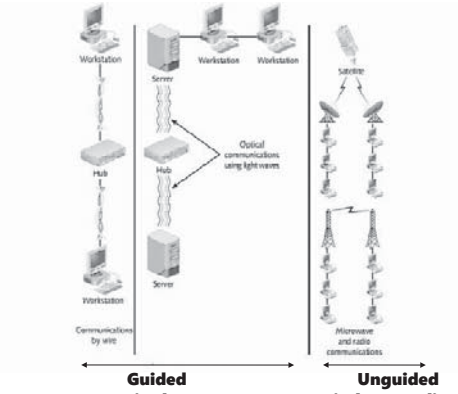
Introduction to Networks

Slide Set 1

Network: Definition

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

Types of Communication Links



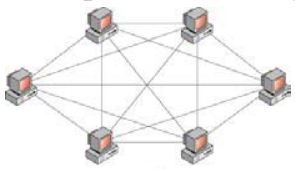
Physical Topology

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

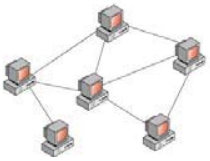
Mesh Topology

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

Full-Mesh:

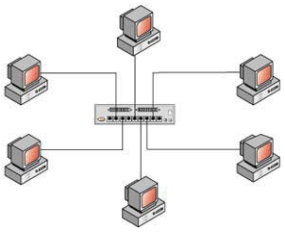


Partial-Mesh:



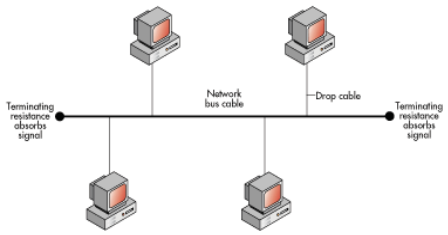
Star Topology

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



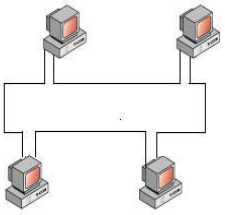
Bus Topology

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



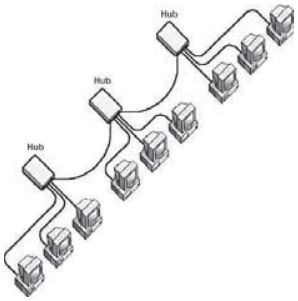
Ring Topology

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



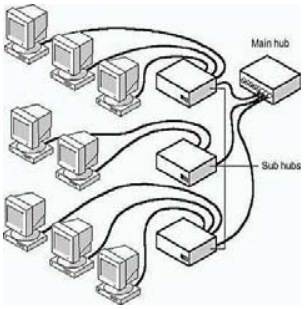
Hybrid: Star Bus Topology

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



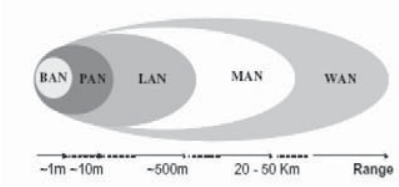
Hybrid: Star Ring Topology

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



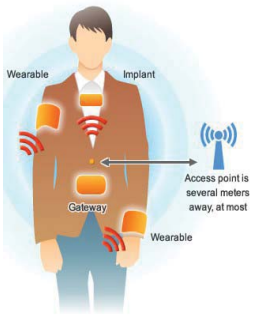
Network Types Defined

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



Body Area Network (BAN)

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

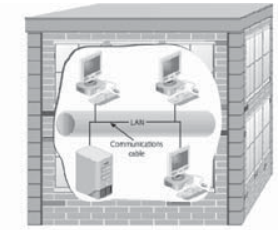


Personal Area Network (PAN)

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

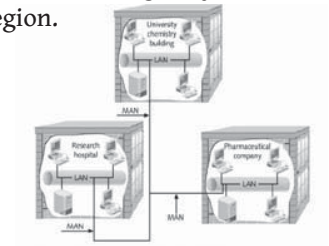
Local Area Network (LAN)

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



Metropolitan Area Network

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



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

Wide Area Network (WAN)

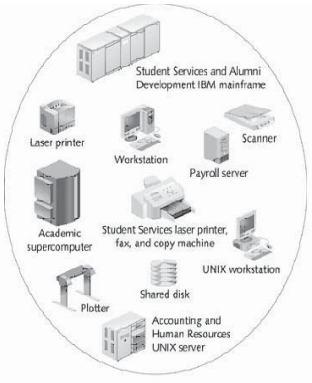
- Provides long-distance transmission of data, voice, image and video information over large geographic areas that may comprise a country, a continent, even the whole world.
- The best example of a WAN is the **Internet**.

Identifying a Network Type

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

Network Classification

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



Resources in an enterprise network

Events that Led up to LANs and WANs

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

LAN/WAN History: 1960s

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

LAN/WAN History: 1970s

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

LAN/WAN History: 1980s

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

LAN/WAN History: 1990s

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

LAN/WAN History: 2000s

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

LAN/WAN History: 2010s

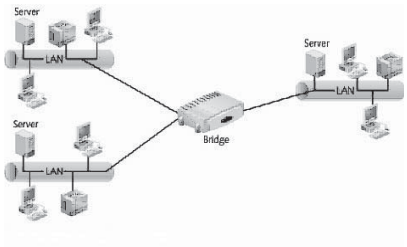
- Cloud Services commonplace
- Internet of Things (IoT)
- 10G, 25G, 40G and 100G Ethernet has been developed

LAN/WAN Integration

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

Bridges

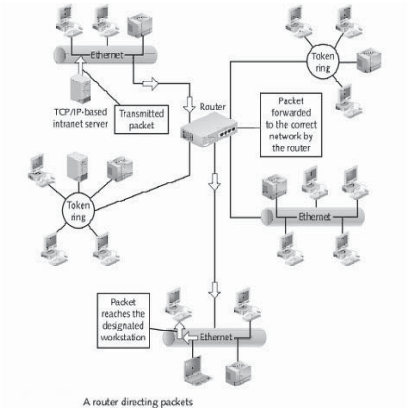
- Connect different LANs or LAN segments using the **same access** method



Routers

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

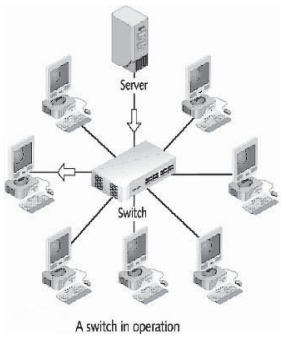
Routers



A router directing packets

Switches

- Link network segments
- Forward and filter frames between segments



A switch in operation

Network Planning & Design

Slide Set 2

Traditional Network Design

- The traditional network design approach follows a structured systems analysis and design process similar to that used to build application systems.
  - The network analyst meets with users to determine the needs and applications.
  - The analyst estimates data traffic on each part of the network.
  - The analyst designs circuits needed to support this traffic and obtains cost estimates.
  - Finally, a year or two later, the network is implemented.

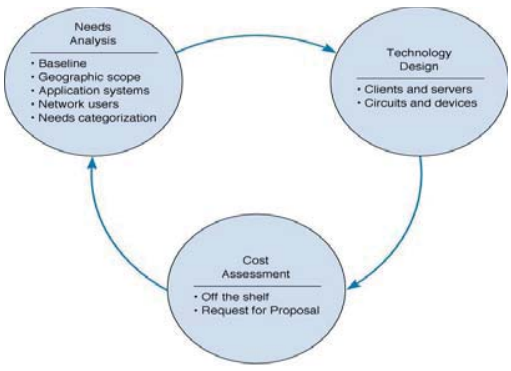
Traditional Network Design

- Three forces are making the traditional design approach less appropriate for many of today's networks:
  - 1. The underlying technology of computers, networking devices and the circuits themselves are rapidly changing.
  - 2. Network traffic is growing rapidly.
  - 3. The balance of costs has changed dramatically over the last 10 years.

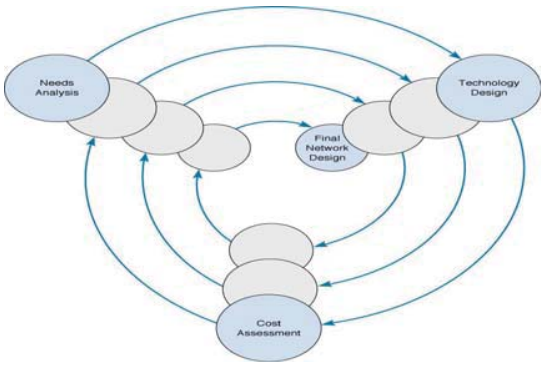
Building Block Network Design

- While some organizations still use the traditional approach, many others use a simpler approach to network design, the building block approach.
- This approach involves three phases: needs analysis, technology design, and cost assessment (Fig. 11-1).
- When the cost assessment is initially completed, the design process returns to the needs analysis phase and cycles through all three phases again, refining the outcome of each phase.
- The process of cycling through all three design phases is repeated until a final design is decided on (Fig. 11-2).

Building Block Network



Reaching a Final Network Design



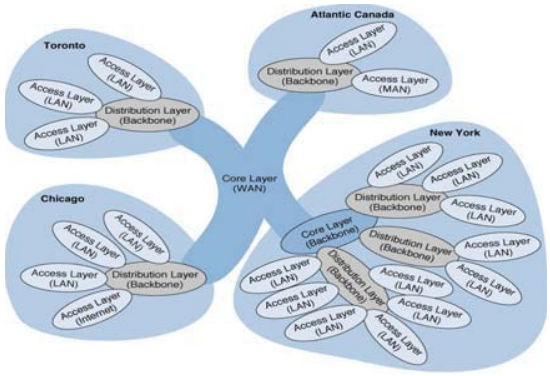
Needs Analysis

- The first step is to analyze the needs of network users along with the requirements of network applications.
- Most efforts today involve upgrades and not new network designs, so most needs may already be understood.
- LAN and BN design issues include improving performance, upgrading or replacing unreliable or ageing equipment, or standardizing network components to simplify network management.
- At the MAN/WAN level, circuits are leased and upgrades involve determining if capacity increases are needed.
- The object of needs analysis is to produce a logical network design, which describes what network elements will be needed to meet the organization's needs.

Geographic Scope

- Needs analysis begins by breaking the network into three parts based on their geographic and logical scope:
  - The access layer which lies closest to the user
  - The distribution layer which connects the access layer to the rest of the network
  - The core layer which connects the different parts of the distribution layer together.

Geographic Scope



Application Systems

- The designers must review the applications currently used on the network and identify their location so they can be connected to the planned network (*baselining*).
- Next, applications expected to be added to the network are included.
- It is also helpful to identify the hardware and software requirements and protocol type for each application.

Network Users

- In the past, application systems accounted for the majority of network traffic. Today, much network traffic comes from Internet use (i.e. e-mail and WWW).
- The number and type of users that will generate network traffic may thus need to be reassessed.
- Future network upgrades will require understanding how the use of new applications, such as video, will effect network traffic.

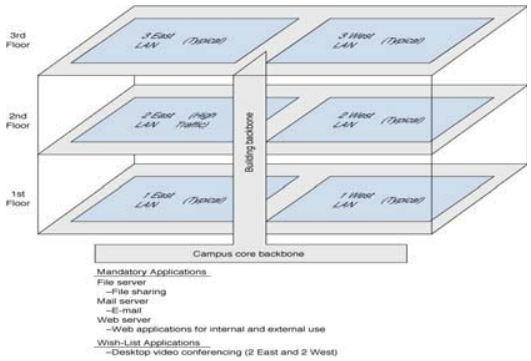
Categorizing Network Needs

- The next step is to assess the traffic generated in each segment, based on an estimate of the relative magnitude of network needs (i.e. *typical* vs. *high volume*). This can be problematic, but the goal is a relative understanding of network needs.
- Once identified, network requirements should be organized into *mandatory requirements*, *desirable requirements*, and *wish-list requirements*.

Deliverables

- The key deliverable for the needs assessment stage is a set of network maps, showing the applications and the circuits, clients, and severs in the proposed network, categorized as “typical” or “high volume”.

Logical Network Design



Technology Design

- After needs assessment has been completed, the next design phase is to develop a technology design (or set of possible designs) for the network.

Designing Clients and Servers

- For the technology design, the idea behind the building block approach is to specify the computers needed in terms of standard units.
- “Typical” users are allocated “base level” client computers, as are servers supporting “typical” applications.
- “High volume” users and servers are assigned “advanced” computers.
- The definition for a standard unit, however, keeps changing as hardware costs continue to fall.

Designing Circuits and Devices

- Two interrelated decisions in designing network circuits and devices are: 1) deciding on the fundamental technology and protocols and 2) choosing the capacity each circuit will operate at.
- Capacity planning means estimating the size and type of the “standard” and “advanced” network circuits for each type of network.
- This requires some assessment of the current and future circuit loading in terms of average vs. peak circuit traffic.

Estimating Circuit Traffic

- The designer often starts with the total characters transmitted per day per circuit, or if possible, the maximum number of characters transmitted per two second interval if peak demand must be met.
- While no organization wants to overbuild its network and pay for unneeded capacity, going back and upgrading a network often significantly increases costs.

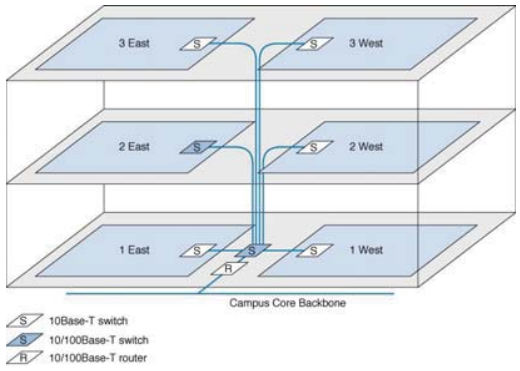
Network Design Tools

- Network modeling and design tools can perform a number of functions to help in the technology design process.
- Some modeling tools require the user to create the network map from scratch. Other tools can "discover" the existing network.
- Once the map is complete, the next step is to add information about the expected network traffic and see if the network can support the level of traffic that is expected. This may be accomplished through simulation models.
- Once simulation is complete, the user can examine the results to see the estimated response times and throughput.

Deliverables

- The key deliverables at this point are a revised set of network maps that include general specifications for the hardware and software required.
- In most cases the crucial issue is the design of the network circuits.

Physical Network Design



Cost Assessment

- Cost assessment's goal is to assess the costs of various network alternatives produced as part of technology design. Costs to consider include:
  - Circuit costs for both leased circuits and cabling.
  - Internetworking devices such as switches and routers.
  - Hardware costs including servers, memory, NICs & UPSs.
  - Software costs for operating systems, application software and middleware.
  - Network management costs including special hardware, software, and training.
  - Test and maintenance costs for monitoring equipment and supporting onsite repairs.
  - Operations costs to run the network.

Request for Proposal

- Background Information
  - Organizational profile; Overview of current network; Overview of new network; Goals of the new network
- 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
- Service Requirements
  - Implementation time plan; Training courses and materials; Support services (e.g., spare parts on site); Reliability and performance guarantees
- Bidding Process
  - Time schedule for the bidding process; Ground rules; Bid evaluation criteria; Availability of additional information
- Information Required from Vendor
  - Vendor corporate profile; Experience with similar networks; Hardware and software benchmarks; Reference list

Deliverables

- There are three key deliverables for this step:
  - 1. An RFP issued to potential vendors.
  - 2. After the vendor has been selected, the revised set of network maps including the final technology design, complete with selected components.
  - 3. The business case written to support the network design, expressed in terms of business objectives.

Network Management

Slide Set 3

Learning Objectives

- Understand what is required to manage the day-to-day operation of networks
- Be familiar with the network management organization
- Understand configuration management
- Understand performance and fault management
- Be familiar with end users support
- Be familiar with cost management
- Understand the role and functions of network management software
- Be familiar with several types of network management hardware tools

Outline

- ***Introduction***
- ***Organizing the Management Function***
  - *The Shift to LANs and the Internet*
  - *Integrating LANs, WANs and the Internet*
  - *Integrating Voice and Data Communications*
- ***Configuration Management***
  - *Configuring the Network and Client Computers*
  - *Documenting the Configuration*
- ***Performance and Fault Management***
  - *Network Monitoring, Failure Control Function, Performance and Failure Statistics, Improving Performance*
- ***End User Support***
  - *Resolving Problems, Providing End User Training*
- ***Cost Management***
  - *Sources of Costs, Reducing Costs*
- ***Network Management Tools***
  - *Network Management Software*
  - *Network Management Hardware*

Introduction

- Network management means monitoring and controlling the network so that it is working properly and providing value to its users.
- A lack of planning and organization can mean that network managers spend most of their time **firefighting** - dealing with breakdowns and immediate problems.
- The main areas of network management are:
  - Configuration Management
  - Performance and Fault Management
  - End-user support
  - Cost Management
  - Security

The Shift to LANs and the Internet

- Since the 1980's networks have moved from using mainframes and terminals to PCs, LANs and the Internet.
- Mainframes are still important, but network management now focuses more on LANs, BNs and Internet resources.
- Currently, a critical issue is the integration of organizational networks and applications. There are two main problems.
- One integration problem is the technical compatibility of technologies and protocols.
- A second one is in the cultural differences in personalities and management styles of network managers. WAN & mainframe managers prefer more highly structured and controlled environments than do LAN and Web managers.

Integrating Voice & Data Communications

- Traditionally, voice and data networks were separate, i.e., the telephone system and the organizational LAN, respectively.
- Separate networks mean higher network costs as well as additional staffing requirements.
- Integrating voice and data simplifies the network, and can lower network costs.
- Most organizations will likely integrate voice and data within the next 5 years.

Configuring Network and Client Computers

- **Configuration management** means configuring the network's hardware and software and documenting that configuration.
- Two common configuration activities are
  - adding and deleting user accounts.
  - updating the software on the client computers attached to the network.
- Electronic software delivery (ESD) can be used to manage costs by eliminating the need to manually update each and every client computer.

Documenting Hardware and Software

- Configuration documentation includes information on network hardware, software, and user and application profiles.
- Net hardware documentation uses a set of maps.
- This must be supplemented with lists of hardware details on each component such as serial number, vendor, date of purchase, warranty information, repair history, phone number for repairs, etc.
- Documenting network software is similar, but includes other information such as the network OS, software release date and site license details.

Documenting User and Application Profiles

- The third documentation type is the user and application profiles, which must be automatically provided by the network Operating System or outside software agreements.
- Other network documentation that must be routinely developed and updated include software, standards and operations manuals, vendor contracts, and licenses.
- Documentation should include details about performance and fault management, maintenance guidelines, DRP, end-user support and cost management.

Performance and Fault Management

- **Performance management**: ensuring the network is operating as efficiently as possible.
- **Fault management**: preventing, detecting, and correcting faults in the network circuits, hardware, and software.
- The two are interrelated. Both require **network monitoring**, i.e., tracking the operation of network circuits and devices to determine how heavily they are being used and ensure they are operating properly.

Network Monitoring

- Most organizations use network management software to monitor and control their networks.
- The parameters monitored by a network management system fall into two distinct categories: **physical network statistics** and **logical network information**.

Network Monitoring Parameters

- **Physical network statistics** come from monitoring the operation of modems, multiplexers, and circuits linking hardware devices.
- **Logical network parameters** include performance measurement systems that track user response times, traffic volume on a specific circuit, the destinations of network packets, and other indices showing the network's service level.
- **Performance tracking** is important since it enables network managers to be proactive and respond to problems before users complain, otherwise network management can revert to firefighting.

Failure Control Function

- Failure control requires problem reporting, often handled by the Help Desk.
- A central troubleshooting group should also be responsible for contacting hardware, software vendors or common carriers.
- To aid in network monitoring, **managed devices** are now being installed that record data on the messages they process and send this information back to a central management database. (see SNMP later)
- Numerous software packages are available for recording fault information. These produce reports called **trouble tickets**.

Handling Network Problems

- Managers use trouble tickets to do **problem tracking**, enabling them to systematically address problems, tracking who is responsible for problem correction and how it's being resolved.
- This also allows **problem prioritization** ensuring critical problems get higher priority.
- Finally, maintaining a **trouble log** is helpful for reviewing problem patterns on the network and can be used to identify which network components are the most problematic.

Performance and Failure Statistics

- The main performance statistics are the number of packets moved on a circuit and the **response time**.
- Another factor is **availability**; the percent of time the network is available. **Downtime** is the percent of time the network is not available.
- Failure statistics include:
  - **Mean time between failures (MTBF)** indicates the reliability of a network component.
  - **Mean time to repair (MTTR)** equal to the mean time to diagnose plus the mean time to respond plus the mean time to fix a problem.

MTTRepair = **MTTDiagnose** + **MTTRespond** + **MTTFix**

Availability and Reliability

$$\text{Availability} = \frac{uptime}{uptime + downtime} = \frac{MTBF}{MTBF + MTTR}$$

Availability	Lost Time (hours)	Lost Time (minutes)	Lost Time (seconds)
60.00%	3504		
65.00%	3066		
70.00%	2628		
75.00%	2190		
80.00%	1314		
85.00%	876		
90.00%	438		
95.00%	219.4		
96.00%	175.2		
97.00%	131.4		
98.00%	87.6		
99.00%	43.8		
99.50%	21.9		
99.90%	8.76	525.6	
99.99%	0.876	52.6	3153.6
99.999%	0.0876	5.3	315.36
99.9999%	0.00876	0.5	31.536
99.99999%	0.000876	0.1	3.1536

1 yr mission = 365 days/yr * 24 hrs/day = 8760 hrs/yr

Just as a remind

$$\text{Reliability} = e^{-T/\Phi}$$

$$\text{Reliability} = e^{-\Lambda T}$$

$$\text{Reliability} = e^{-N}$$

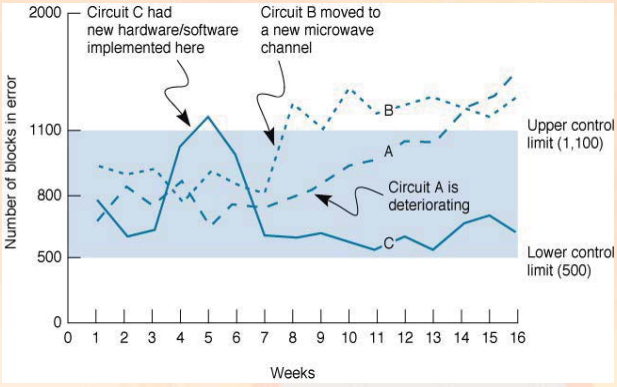
Reliability	Failures per year	Failures per 10 years	Failures per 100 years
10.00%	2.30		
20.00%	1.61		
30.00%	1.20		
40.00%	0.92		
50.00%	0.69		
60.00%	0.51		
70.00%	0.36		
80.00%	0.22	2.23	
90.00%	0.11	1.05	
95.00%	0.05	0.51	
99.00%	0.01	0.10	1.01
99.50%	0.005	0.05	0.50
99.90%	0.001	0.01	0.10
99.99%	0.0001	0.001	0.01
99.999%	0.00001	0.0001	0.001
99.9999%	0.0000010	0.00001	0.0001
99.99999%	0.0000010	0.000001	0.00001

1 yr mission = 365 days/yr * 24 hrs/day = 8760 hrs/yr

Where $\Phi = MTBF$, $\Lambda = Failure\ Rate$

N = *number of failures*, T = *mission time*

Quality Control Chart used to track network performance



Improving Performance

- There are three general activities related to performance management, whether on a LAN, BN or MAN/WAN:
  - Policy-based management
  - Server load balancing
  - Service-level agreements

Policy-based Management

- In policy-based management the network manager uses special software to set priority policies for network traffic.
- These take effect when the network becomes busy.
- For example, video-conferencing might be given a high priority since delays will have the highest impact on the performance of that application.

Server Load Balancing

- Load balancing means sharing the processing load between servers.
- A separate load balancing server is usually needed to allocate the work between processors.
- The load-balancing server then allocates tasks to the other processors, using an algorithm such as a round robin formula.

Service Level Agreements

More organizations are beginning to establish service level agreements with their common carriers and service providers, which specifies the type of performance and fault conditions that the organization will accept.

End User Support

- Supporting end users means solving the problems users have using the network.
- End-user support can be grouped into three areas:
  - Resolving network problems
  - Resolving software problems
  - Training

Resolving Problems

- Problems stem from three major sources:
  - **Hardware device failures**
  - **A lack of user knowledge on proper operation**
  - **Problems with software, software settings or software compatibility**
- Problem resolution in large organizations is organized at three levels:
  - **The Help Desk handles basic queries**
  - **If this is not enough, staff members with specialized skills specific to the problem at hand are brought in**
  - **If the second level specialists are still not enough, technical specialists with a higher level of training are contacted to look into the problem**

Providing End-User Training

- End-user training needs to be an ongoing part of network management.
- Training programs are also important since employees often change jobs within an organization and so the organization can benefit from cross-training.
- Training is usually conducted using in-class or one-on-one instruction or with online training materials provided.

Cost Management

- Because of its large and rapidly growing budget, network management must carefully monitor network costs and will likely be called upon to justify cost increases.
- This requires measuring the cost of supporting users, allocating networking department budgets between hardware, software, personnel and other costs and understanding how these costs are changing.

Total Cost of Ownership

- The **total cost of ownership** (TCO) is a measure of how much it costs per year to keep one computer operating.
- TCO studies indicate it can cost up to five times the value of the computer to keep it operational.
- The TCO for a typical Windows computer is about $8-12,000 per computer per year !!!
- Although TCO has been widely accepted, many organizations disagree with the practice of including user "waste" time in the measure and prefer to focus on costing methods that examine only the direct costs of operating the computer.

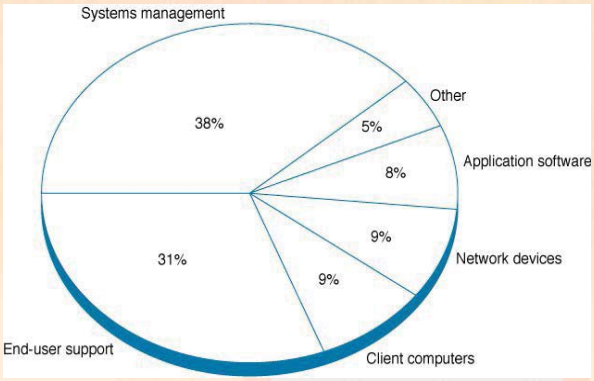
Net Cost of Ownership

- **Net Cost of Ownership (NCO)** is an alternative to TCO that measures only direct costs, leaving out so-called "wasted" time.
- NCO costs per computer are between $1500-$3500, so management for a 100-user network require an annual budget of between $150,000-$350,000.
- Using NCO, the largest network budget items are:
  - **Personnel cost, accounting for 50-70% of costs**
  - **WAN circuits**
  - **Hardware upgrades and replacement parts**

Network Personnel Costs

- Since the largest item in any network budget today is **personnel time**, cost management needs to focus on ways to reduce personnel time, not hardware costs.
- The largest use of personnel time is in **System management**.
- The second largest source is **User Support**.

Network management personnel costs



Reducing Network Costs

Five Steps to Reducing Network Costs:

1. Develop standard hardware and software configurations for client computers and servers.
2. Automate as much of the network management function as possible by deploying a solid set of network management tools.
3. Reduce the costs of installing new hardware and software by working with vendors.
4. Centralize Help Desks.
5. Move to thin-client architectures.

Network Management Software

- Network management software is designed to provide automated support for some or all of the network management functions.
- There are three fundamentally different types of network management software:
  - Device management software
  - System management software
  - Application management software

Network management software (Source: HP OpenView)

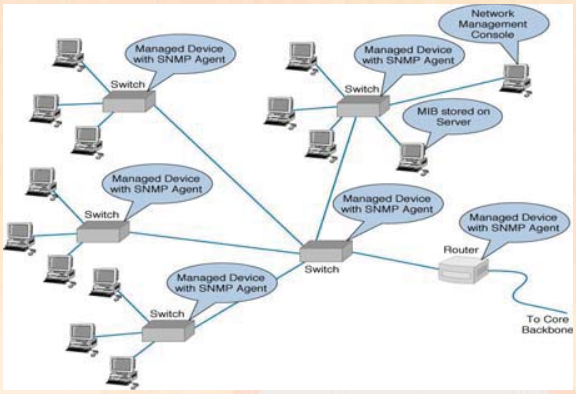
Network Management Software

- One major problem is ensuring that hardware devices from different vendors can understand and respond to the messages sent by the network management software of other vendors.
- The two most commonly used network management protocols are:
  - Simple Network Management Protocol (SNMP, part of the TCP/IP protocol suite)
  - Common Management Interface Protocol (CMIP, developed by ISO)

Simple Network Management Protocol

- **SNMP**: TCP/IP suite protocol for network management that allows agents to communicate with each other and other network devices
- **Agents**: programs residing on network devices that gather and share network status information
- **Management Information Bases (MIBs)**: databases of network status statistics such as traffic levels, error rates & data rates
- **Network Management Console**: when requested, data from the MIBs is sent to a Network Management Console.

Network Management with SNMP (More Later)



Network Management Hardware

- Most network management hardware is used to test circuits. Circuit testing can be divided into three areas:
- **Analogue testing** involves troubleshooting the communications circuits on the analog side of the modem supplied by common carriers.
- **Digital testing** involves testing digital communication circuits.
- **Protocol testing** involves testing the sign-on/sign-off procedures, checking the contents of packets, and examining message transmission times.

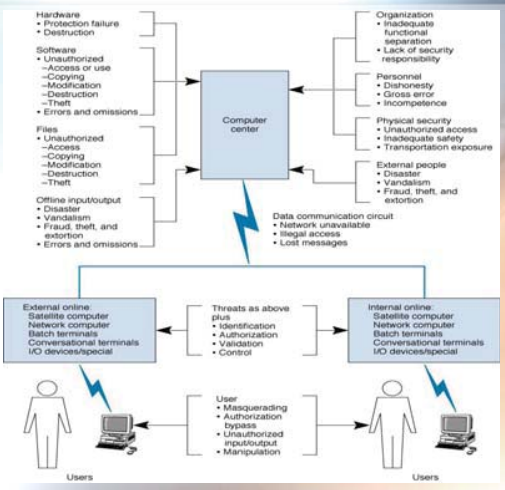
Slide Set 4

Network Security

Introduction

- Security is a major networking concern. 52% of the respondents to the 2006 Computer Security Institute/FBI Computer Crime and Security Survey reported unauthorized use of computer systems in the last 12 months.
- Gartner estimates losses from cyber attacks worldwide at $16.7 billion for year 2007.
- It means more than preventing a hacker from breaking into your computer, it also includes being able to recover from temporary service problems, or from natural disasters.

Common Threats to Network Security



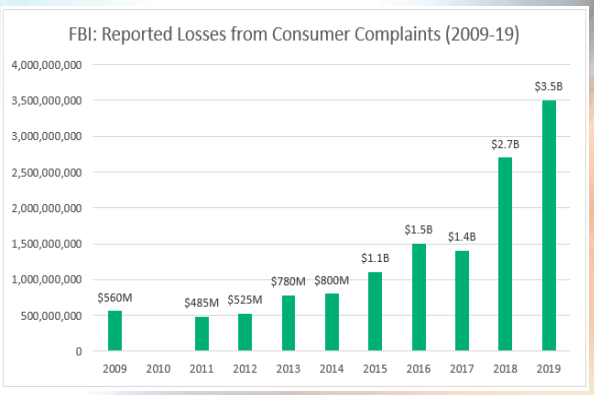
Types of Security Threats

- Disruptions are the loss or reduction in network service.
- Some disruptions may also be caused by or result in the destruction of data.
- Natural (or man-made) disasters may occur that destroy host computers or large sections of the network.
- Unauthorised access is often viewed as hackers gaining access to organizational data files and resources. However, most unauthorized access incidents involve employees.

Security Problems Are Growing

- The Computer Emergency Response Team (CERT) at Carnegie Mellon University was established with US DoD support in 1988 after a computer virus shut down 10% of the computers on the Internet
- In 1989, CERT responded to 137 incidents.
- In 2000, CERT responded to 21,756 incidents.
- By this count, security incidents are growing at a rate of 100% per year.
- In Mauritius, Computer Misuse and Cybercrime Act 2003, Data Protection Act 2017,

Number of Incidents and Losses reported in the USA



Network Controls

- Developing a secure network means developing mechanisms that reduce or eliminate the threats to network security, called controls.
- There are three types of controls:
  - Preventative controls - mitigate or stop a person from acting or an event from occurring (e.g. passwords).
  - Detective controls - reveal or discover unwanted events (e.g. auditing software, Intrusion Detection System IDS).
  - Corrective controls - rectify an unwanted event or a trespass (e.g. reinitiating a network circuit).

Network Controls

- It is not enough to just establish a series of controls; personnel need to be designated as responsible for network control and security.
- This includes developing controls, ensuring that they are operating effectively, and updating or replacing controls.
- Controls must also be periodically reviewed to:
  - ensure that the control is still present (verification)
  - determine if the control is working as specified (testing)

Security Threats

- A network security threat is any potentially adverse occurrence that can harm or interrupt the systems using the network, or cause a monetary loss to an organization.
- Once the threats are identified they are then ranked according to their occurrence.
- The next slide summarizes the most common cyber threats worldwide.

Top 15 Cyber Threats Worldwide

Evaluate the Network's Security

- The last step in designing a control spreadsheet is evaluating the adequacy of the controls and the degree of risk associated with each threat.
- Based on this, priorities can be decided on for dealing with threats to network security.
- The assessment can be done by the network manager, but it is better done by a team of experts chosen for their in-depth knowledge about the network and environment being reviewed.

Preventing Disruption, Destruction and Disaster

- Preventing disruptions, destructions and disasters mean addressing a variety of threats including:
  - Creating redundancy
  - Preventing natural disasters impact
  - Preventing theft
  - Preventing computer malware attacks
  - Preventing denial-of-service attacks

Network Redundancy

- The key to in preventing or reducing disruption, destruction and disaster - is **redundancy**
- Examples of components that provide redundancy include:
  - Uninterruptible Power Supplies (UPS)
  - Disk redundancy (RAID & Backup)
  - Network link redundancy (Spanning Tree Protocol)
  - Network topology (Mesh or Hybrid)
- Redundancy can be built into other network components as well.

Preventing Impact of Natural Disasters

- Disasters are different from disruptions since the entire site can be destroyed.
- The best solution is to have a completely redundant network that duplicates every network component, but in a different location.
- Generally speaking, preventing disasters is difficult. The most fundamental principle is to decentralize the network resources.
- Other steps depend on the type of disaster to be prevented.

Preventing Theft

- Equipment theft can also be a problem if precautions against it are not taken.
- Industry sources indicate that about $1 billion is lost each year to theft of computers and related equipment (USA statistic).
- For this reason, security plans should include an evaluation of ways to prevent equipment theft.

Preventing Computer Malware

- Special attention must be paid to preventing viruses that attach themselves to other programs and spread when the programs are executed.
- Macroviruses attach themselves to documents and become active when the files are opened are also common. Anti-malware software packages are available to check disks and files to ensure that they are virus-free.
- Incoming e-mail messages are the most common source of viruses. Attachments to incoming e-mail should be routinely checked for viruses.
- The use of filtering programs that 'clean' incoming e-mail is also becoming common.

Detecting Disruption, Destruction & Disaster

- One function of network monitoring software is to alert network managers to problems so that these can be corrected.
- Detecting minor disruptions can be more difficult.
- The network should also routinely log fault information to enable network managers to recognize minor service problems.
- In addition, there should be a clear procedure by which network users can report problems.

Disaster Recovery Plans (DRP)

- The goal of the disaster recovery plan (DRP) is to plan responses to possible disasters, providing for partial or complete recovery of all data, application software, network components, and physical facilities.
- Critical to the DRP are backup and recovery controls that enable an organization to recover its data and restart its application software should some part of the network fail.
- The DRP should also address what to do in a variety of situations, such as, if the main database is destroyed or if the data center is destroyed.

Preventing Intruder Access

- Four types of intruders attempt to gain unauthorized access to computer networks.
  1. Casual hackers who only have limited knowledge of computer security.
  2. Security experts whose motivation is the thrill of the hunt.
  3. Professional hackers who break into corporate or government computers for specific purposes.
  4. Organization employees who have legitimate access to the network but who gain access to information they are not authorized to use or view.

Preventing Unauthorized Access

- A proactive approach that includes routinely testing your security systems is key to preventing unauthorized access.
- Access related security issues include:
  - Security policies
  - User profiles
  - Physical security
  - Firewalls
  - Network address translation
  - Encryption

Developing a Security Policy

- The security policy should clearly define the important network components to be safeguarded along with controls needed to do that.
- The most common way for a hacker to break into a system is through "social engineering" (breaking security simply by asking how).

Elements of a Security Policy

- Names of responsible individuals.
- Incident reporting system and response team.
- Risk assessment with priorities.
- Controls on access points to prevent or deter unauthorized external access.
- Controls within the network to ensure internal users cannot exceed their authorized access.
- An acceptable use policy.
- User training plan on security.
- Testing and updating plans.

User Profiles and Forms of Access

- The limits of what users have access to on a network are determined by user profiles assigned to each user account by the network manager.
- The profile specifies access details such as which data and network resources a user can access and the type of access (e.g., read, write, create, delete).
- Most access is still password based, that is, users gain access based on something they know.
- Many systems require users to enter a password in conjunction with something they have, such as a smart card. ATM cards work in this way.
- In high-security applications, users may be required to present something they are, such as a finger, hand or the retina of their eye for scanning by a biometric system.

User Profiles: Managing User Access

- User profiles can limit the allowable log-in days, time of day, physical locations, and the allowable number of incorrect log-in attempts.
- Creating accounts and profiles is simple, as they are created when new personnel arrive.
- One security problem is often created because network managers forget to remove user accounts when someone leaves an organization.

Managing Users

- It is important to screen and classify both users and data (need to know).
- The effect of any security software packages that restrict or control access to files, records, or data items should also be reviewed.
- Adequate user training on network security should be provided through self-teaching manuals, newsletters, policy statements, and short courses.
- A well publicized security campaign can also help deter potential intruders.

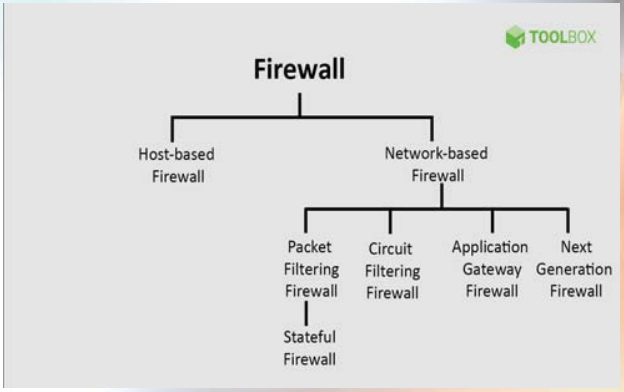
Physical Security

- Physical security means implementing access controls so only authorized personnel have access to areas where network equipment is located.
- Each network component should have its own level of physical security.
- Two important areas of concern are network cabling and network devices.
- Network cables should be secured behind walls.
- Network devices such as hubs and switches should be secured in locked wiring closets.

Network Firewalls

- Firewalls are used to prevent intruders on the Internet from making unauthorized access and denial of service attacks to your network.
- A firewall is a router/gateway, or special purpose computer that examines packets flowing into and out of the organization's network (usually via the Internet or corporate Intranet), restricting access to that network.
- The two main types of network firewalls are packet-level firewalls and application-level firewalls.

Firewall Classification



Packet-Level Firewalls

A packet-level firewall (or packet filter) examines the source and destination address of packets that pass through it, only allowing packets that have acceptable addresses to pass.

Packet filtering firewall advantages

- A single device can filter traffic for the entire network
- Extremely fast and efficient in scanning traffic
- Inexpensive
- Minimal effect on resources, network performance and end-user experience

Packet filtering firewall disadvantages

- Because traffic filtering is based entirely on IP address, packet filtering lacks broader context that informs other types of firewalls
- Doesn't check the payload and can be spoofed (unless it performs SPI as well)
- Not an ideal option for every network
- Access control lists can be difficult to set up and manage

Circuit-Level Firewalls

A packet-level firewall (or packet filter) examines the source and destination address of packets that pass through it, only allowing packets that have acceptable addresses to pass.

Packet filtering firewall advantages

- A single device can filter traffic for the entire network
- Extremely fast and efficient in scanning traffic
- Inexpensive
- Minimal effect on resources, network performance and end-user experience

Packet filtering firewall disadvantages

- Because traffic filtering is based entirely on IP address, packet filtering lacks broader context that informs other types of firewalls
- Doesn't check the payload and can be spoofed (unless it performs SPI as well)
- Not an ideal option for every network
- Access control lists can be difficult to set up and manage

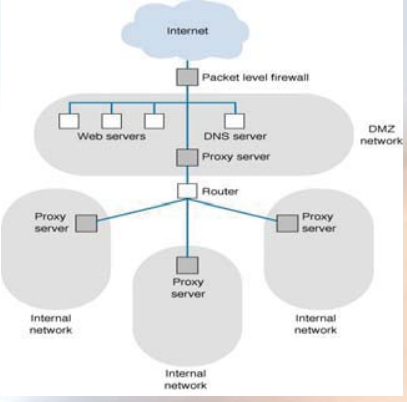
Application-Level Firewalls

- An application-level firewall or application gateway acts as an intermediate host computer, separating a private network from the rest of the Internet, but it works on specific applications, such as Web site access.
- The application gateway acts as an intermediary between the outside client making the request and the destination server responding to that request, hiding individual computers on the network behind the firewall.
- Because of the increased complexity of what they do, application level firewalls require more processing power than packet filters which can impact network performance.

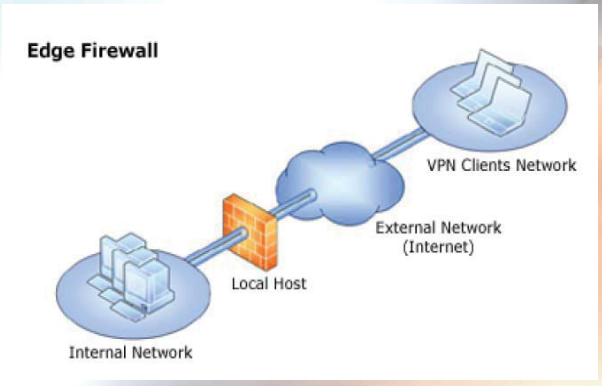
Network Address Translation

- Network address translation (NAT) is used to shield a private network from outside interference.
- An NAT uses an address table, translating network addresses inside the organization into aliases for use on the Internet. So, internal IP addresses remain hidden.
- Many organizations combine NAT servers, packet filters and application gateways, maintaining their online resources in a "DMZ network" between the two.

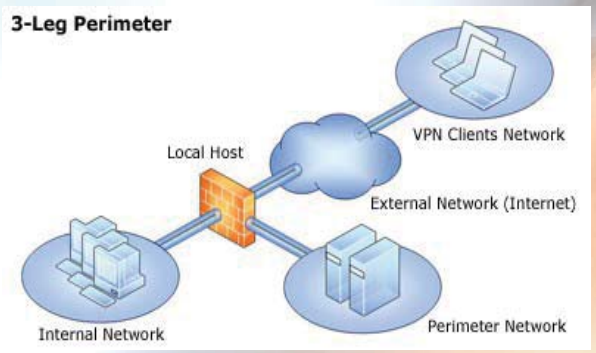
Typical network layout



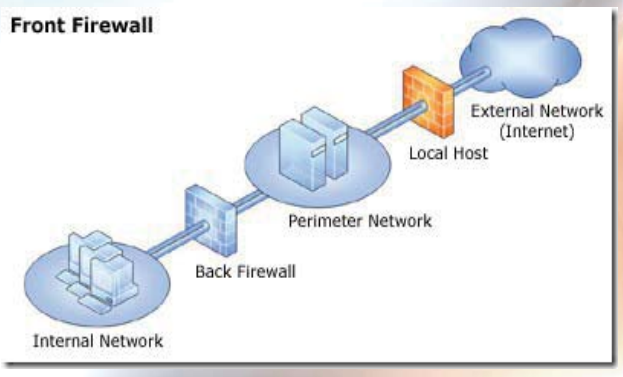
Network Template 1



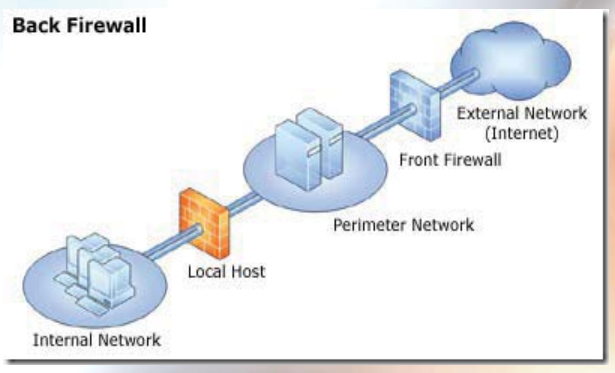
Network Template 2



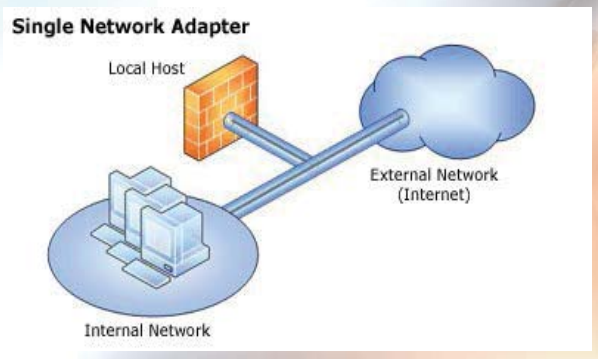
Network Template 3



Network Template 4



Network Template 5

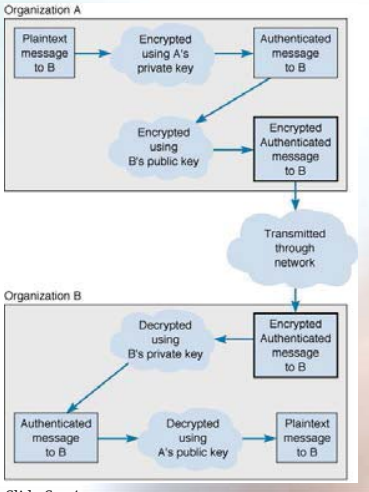


Security Holes

- Security holes are made by flaws in network software that permit unintended access to the network. Operating systems often contain security holes, the details of which can be highly technical.
- Once discovered, knowledge about the security hole may be quickly circulated on the Internet.
- A race can then begin between hackers attempting to break into networks through the security hole and security teams working to produce a patch to eliminate the security hole.

Digital Signatures

- PKE also permits authentication (digital signatures), which essentially uses PKE in reverse. The digital signature, is a small part of the message, and includes the name of the sender and other key contents.
- The digital signature in the outgoing message is encrypted using the sender's private key
- The digital signature is then decrypted using the sender's public key thus providing evidence that the message originated from the sender.
- Digital signatures and public key encryption combine to provide secure and authenticated message transmission



Digital Signatures

Certificate Authorities (CA)

- One problem with digital signatures involves verifying that the person sending the message is really who he or she says they are.
- A **certificate authority (CA)** is a trusted organization that can vouch for the authenticity of the person of organization using authentication.
- The CA sends out a digital certificate verifying the identity of a digital signature's source.
- For higher level security certification, the CA requires that a unique "fingerprint" (key) be issued by the CA for every message sent by the user.

Redundancy

Slide Set 5

Fault Tolerance and Redundancy

- Fault Tolerance – the ability to withstand a partial failure and to continue to operate even though it may impact upon performance
- Redundancy – used to provide an exact duplicate of the primary system in hardware and software. In a Windows NT or 2003 environment the BDC (Backup Domain Controller) provide the redundancy for the PDC (Primary Domain Controller)
- Support for the network infrastructure comes from:
  - Backup
  - Uninterruptible Power Supply
  - Redundancy

Backing Up Data

- The process of copying data stored on a computer, and making an exact duplicate of that data on another usually removable storage media.
- This may be achieved by simply copying the data to a floppy disk, a Tape backup device, an external hard disk drive, transferring to a remote system via a network, an optical media such as a DVD, etc..
- Speed is a critical factor, and since the process of backup can take several hours it is usually scheduled for off-peak hours, or when the system is not in use.

Backup and Archiving Software

In business environment, where data are usually held within servers, the backup process is performed via specialised software. The advantages are:

1. Backup process is automated and the data type, frequency, type of backup, etc. can be configured.
2. Compression can be used while backing up data. This uses smaller storage space on the target medium and also save time if data are being backup on network drive or cloud storage.
3. Encryption can be used while backing up data. This ensure confidentiality.
4. Data Integrity checks can be performed on the backup data for added security.

Chronology of Storage Technology

- Obsolete: LS-120 floppy drive (max 120 MB), Iomega Zip (max 200 MB), Jaz (max 2 GB) drives, 1.44 MB floppy drive.
- Nearing obsolescence: Digital Data Storage (DDS: max 160 GB) from HP superseded by LTO, DVD±R/W (max 8.4 GB), Advanced Intelligent Tape (AIT: max 400 GB), Digital Linear Tape (DLT: max 800 GB).
- Popular: Linear Tape Open (LTO: 800 GB), Super Advanced Intelligent Tape (SAIT: max 2 TB), T10000 from StorageTek with max 1 TB, USB Flash drive (max 2 TB), SSD HDD (max 100 TB), Cloud Storage (as required).

Most common types of Backup

- **Full Backup** – backs up all the data on the system, does not take in to account if the data has changed since the last backup, used for the first backup of a system. Data compression and confidentiality are also used.
- **Differential** – Uses the 'archive bit' to determine if the file has changed since the last **full** backup, takes longer than an incremental backup, but is quicker to restore.
- **Incremental** – uses the 'archive bit' to determine if a file has changed since the last **full**, **differential** or **incremental** backup, takes less time than differential backup, takes more time to restore as restoration requires the last full backup plus use of all incremental tapes

Backup Strategy

How far back do tapes need to be kept ?

- With little data a full backup each night is conceivable using a single tape (risky!!!)
- A different tape each day is more reliable, but not as practical
- A normal backup each evening is time consuming, the majority of data does not change from day to day, therefore duplicate data is being repetitively stored
- A rotation of tapes is the most common approach, four tapes being used Monday to Thursday (for either incremental or differential), a separate tape is used each Friday for a full backup
- On the last Friday of the month the tape is kept as an archive

Tape Backups

Incremental or Differential Backup

Normal Backup

MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	
1	2	3	4	5	WEEK 1
1	2	3	4	6	WEEK 2
1	2	3	4	7	WEEK 3
1	2	3	4	Monthly	WEEK 4

Uninterrupted Power

- UPS are categorized by their ability to cater for 9 common power problems (see next slide):
  - Level 3 UPS usually called Back-up or Stand-by UPS (1-3)
  - Level 5 UPS usually called Line-Interactive, Smart UPS (1-5)
  - Level 9 UPS usually called On-Line, Smart UPS (1-9)
- Which devices need to stay up and running? Usually only the server has UPS. Do workstations also need UPS?
- If you require the server to be running for more than 30 minutes, consider a high capacity UPS or a generator.
- Consider using software to perform a clean shutdown of systems if the power cut is at a time when the system is unattended, e.g. PowerChute

9 common Power problems

1 – Power Failure: A total Loss of Utility Power
2 – Power Sags: Short term low voltage
3 – Power Surge: Short term high voltage (spike)
4 – Undervoltage: Long term low voltage (brownouts)
5 – Overvoltage: Long term high voltage
6 – Electrical Line Noise: caused by RFI or EMI (e.g. lightning)
7 – Frequency Variation: A change in frequency stability
8 – Switching Transients: very brief (nanos) undervoltage (notch)
9 – Harmonic Distortion: distortion caused by non-linear loads

Fault-Tolerant Servers

For high availability, fault-tolerance servers provide redundancy across major system components such as:

- Redundant power-supplies, fans, etc.
- Redundant processors, memory, hard disk drives, network interface cards, etc...

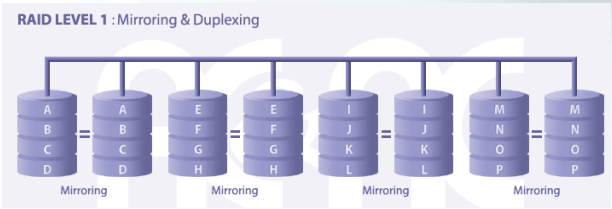
Note that the above cater primarily for hardware failures not software failures.

Clustering as well as virtualization is another approach for minimizing software failures and thus increase uptime.

RAID 0 – Disk Striping

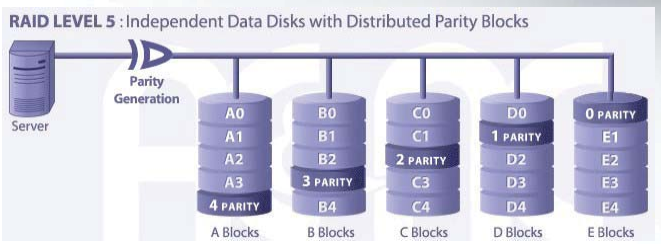
RAID Level 0 requires a minimum of 2 drives to implement

RAID 1 – Disk Mirroring



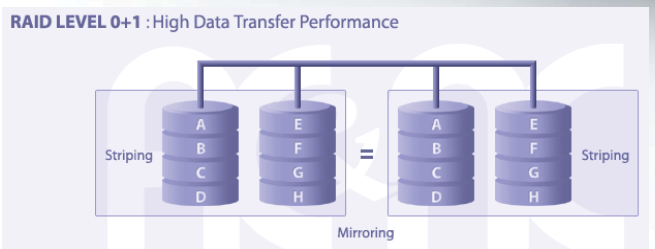
RAID Level 1 requires a minimum of 2 drives to implement

RAID 5 – Disk striping with Parity



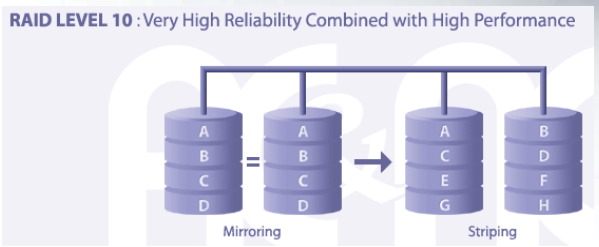
RAID Level 5 requires a minimum of 3 drives to implement

RAID 0+1 – Mirroring of Disk Stripes



RAID Level 0+1 requires a minimum of 4 drives to implement

RAID 10 – Disk mirroring with striping



RAID Level 10 requires a minimum of 4 drives to implement

MANs & WANs

Slide Set 6

MAN & WAN

- MAN & WAN Purposes
  - Link sites (usually) within the same corporation
  - Remote access for individuals who are off-site
  - Internet access for individuals or firms

MAN & WAN

- Technologies for Individual Internet Access
  - Telephone modems
  - DSL lines / Cable modems
  - Wireless Internet access
- Site-to-Site Transmission within a Firm
  - Private line networks
  - Public switched data networks (PSDNs)
  - Virtual Private Networks (VPNs)
    - Propagation over the Internet with added security
    - Low cost per bit transmitted

MAN & WAN

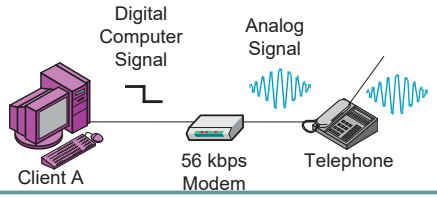
- High Costs and Low Speeds
  - High cost per bit transmitted compared to LANs
  - Lower speeds (most commonly 56 kbps to a few megabits per second)

Typical WAN speeds:
56 kbps to a few megabits per second.

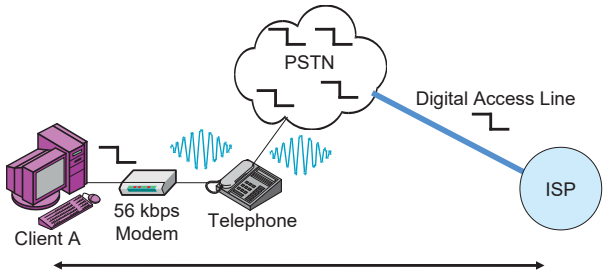
Individual Internet Access: Telephone Modems

Telephone Modem Communication

- Computers are digital sources
- Telephone transmission lines are analog
- A modem converts between the two



Telephone Modem Communication



For 56 kbps Download Speed
ISP Must Have a Digital Connection, Not a Modem

Digital Subscriber Lines (DSLs)

DSLs provide data over the existing 1-pair voice-grade access line that already goes to residences and small businesses.

Nowadays, for higher connection speed, copper lines have been replace by optic fiber.

Digital Subscriber Lines (DSLs)

- DSLs provide digital data transmission over the single-pair voice-grade local loop that already runs to residential customer premises.
  - These lines are already installed, so no cost to run new access lines (as there is with private lines).
  - Single-pair voice-grade UTP was not meant to carry data. Sometimes it works. Other times, it does not. Depends primarily on whether distance to the nearest end office is too far.

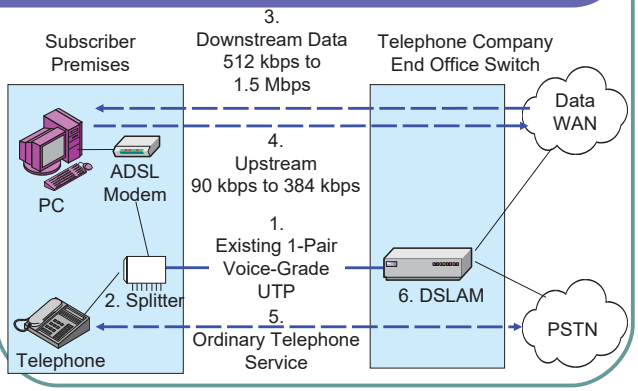
Digital Subscriber Lines (DSLs)

- Asymmetric DSL (ADSL)
  - Asymmetrical throughput
    - Downstream speed up to 1 Gbps
    - Upstream speed up to 60 Mbps
    - Excellent for Web access with large downloads and streaming content.
    - Convenient for e-mail
  - Aimed at residential customers
    - Throughput is NOT guaranteed
    - DSLAM often oversubscribed, slowing access

Digital Subscriber Lines (DSLs)

- Symmetric DSL Services
  - Speed is symmetric
    - Same upstream and downstream
  - Aimed at business customers
    - Throughput IS guaranteed
  - Several Types of Symmetric DSL
    - HDSL (768 kbps): Half of a T1 private line (later)
    - HDSL2 (1.544 kbps): Full T1 private line speed
    - SHDSL: Flexible (384 kbps to 2.3 Mbps)

Asymmetric Digital Subscriber Line (ADSL)

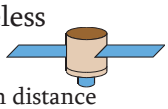


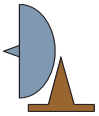
Wireless Access Systems

- Wireless Access to the Internet
- Fixed Versus Mobile
  - Fixed
    - For homes and offices (fixed locations)
    - Use dish antennas
    - Higher speeds
  - Mobile
    - People travelling within a city or farther
    - Need omnidirectional antennas
    - Lower speeds

Wireless Access Systems, Continued

- Satellite Versus Terrestrial Wireless
  - Satellite
    - Expensive because of transmission distance
    - Expensive because satellites are expensive to launch and maintain
    - Can cover large areas
  - Terrestrial
    - Earth-based radio stations
    - Service within a city





Wireless Access Systems, Continued

802.16 WiMAX

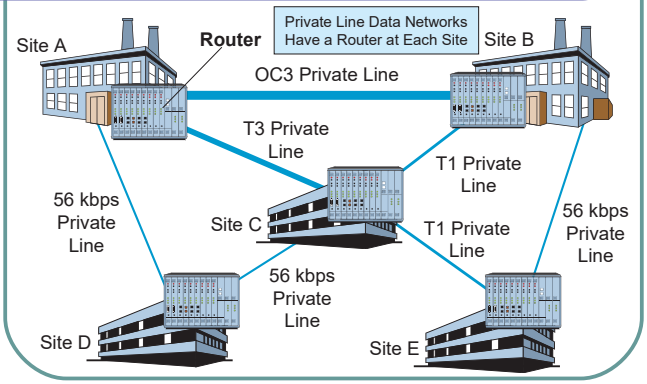
- One of several terrestrial wireless access standards under development
- Fixed version being standardized first
  - 20 Mbps up to 50 km (30 miles)
- Mobile version under development (802.16e)
  - 3 Mbps to 16 Mbps for mobile users

Site-to-Site Networking: Private Line Networks

Private Line Networks for Voice and Data

- Connect sites via private lines
- Perspective
  - User firm must do all the planning and installation
  - User firm must operate and maintain the network
  - Labour-intensive site-to-site networking

Private Line Networks for Data



Private Line Speeds

Trunk Line	Speed	Medium
North American Digital Hierarchy		
56 kbps (DS0 Signaling)	56 kbps (sometimes 64 kbps)	2-pair DG* UTP
T1 (DS1 Signaling)	1.544 Mbps	2-pair DG* UTP
Fractional T1	128 kbps, 256 kbps, 384 kbps, 512 kbps, and 768 kbps	2-pair DG* UTP
Bonded T1s (multiple T1s acting like a single line)	Varies (usually up to 6 Mbps)	2-pair DG* UTP
T3 (DS3 Signaling)	44.7 Mbps	Optical Fiber

*DG = Data Grade

Private Line Speeds, Continued

Trunk Line	Speed
CEPT Multiplexing Hierarchy (Europe)	
64 kbps	64 kbps
E1	2.048 Mbps
E3	34.4 Mbps
Japanese Multiplexing Hierarchy	
64 kbps	64 kbps
J1	1.544 Mbps (same as U.S. T1)
J3	32.1 Mbps

Private Line Speeds, Continued

Trunk Line	Speed
*SONET/SDH**	
OC3/STM1	156 Mbps
OC12/STM4	622 Mbps
OC48/STM16	2.5 Gbps
OC192/STM64	10 Gbps
OC768/STM256	40 Gbps

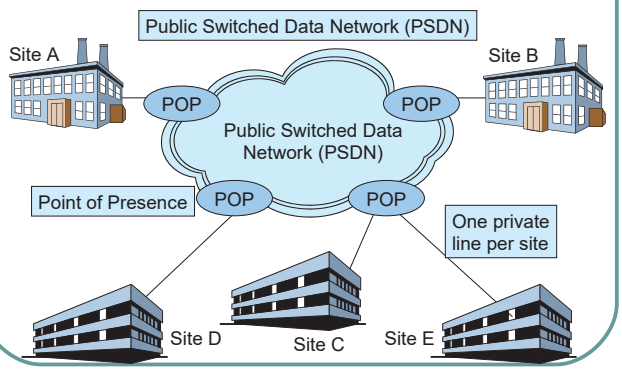
Notes: SONET and SDH speeds are multiples of 51.84 Mbps.
(Figures listed are rounded off for readability)
OCx is the SONET designation.
STMx is the SDH designation.

Private Line Speeds, Continued

- Perspective
  - Most the range of greatest demand for site-to-site transmission is 56 kbps to a few megabits per second
  - So the largest market for private lines consists of T1 and fractional T1 lines or the equivalent in various countries

Site-to-Site Networking: Public Switched Data Networks

Private Line versus Public Switched Data Networks

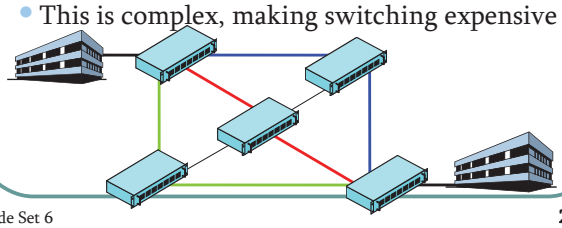


Private Line versus Public Switched Data Networks

- Private Line Network
  - Company must plan, buy switching equipment, and operate the network. Requires much labor.
- Public Switched Data Network
  - PSDN carrier provides planning, switching, and operation of the network. This greatly reduces corporate management labor.
  - PSDN drawn as a cloud to indicate that users do not need to understand it because the PSDN handles all of the details.

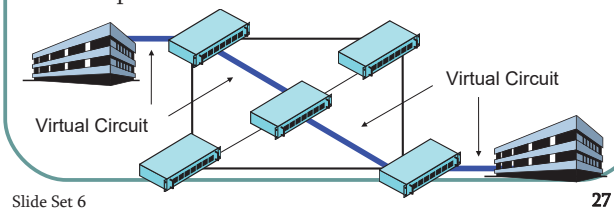
Virtual Circuit

- PSDN Switches Are Arranged in Meshes
  - Loops so multiple alternative paths between stations
  - Switches must consider alternative paths
  - This is complex, making switching expensive



Virtual Circuit, Continued

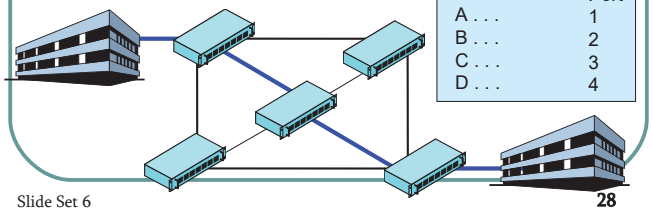
- PSDNs Create Virtual Circuits
  - Virtual circuit is a single path (data link) between two stations
  - Set up before transmission begins
  - Only a single possible path, so switching is fast and inexpensive



Virtual Circuit, Continued

- PSDNs Create Virtual Circuits
  - Switching table has virtual circuit instead of data link layer addresses
  - Frame header has a virtual circuit number, NOT a destination address

Virtual Circuit	Port
A . . .	1
B . . .	2
C . . .	3
D . . .	4



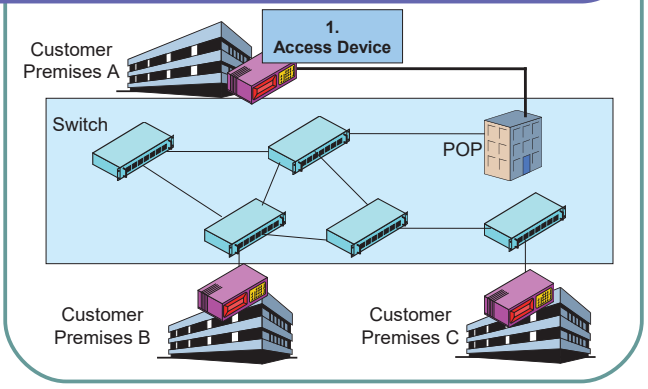
Site-to-Site Networking: Frame Relay (FR)

The most popular PSDN

Frame Relay (FR)

- The most popular PSDN Today
  - Speed range is 56 kbps to up to 40 Mbps
  - Matches main speed range of corporate WAN demand (56 kbps to a few megabits per second)
- FR Switching is Designed to Minimize Cost
  - Switching is somewhat unreliable to reduce cost per frame
  - Switching uses virtual circuits to reduce cost
  - Cost minimization is important in WAN communication

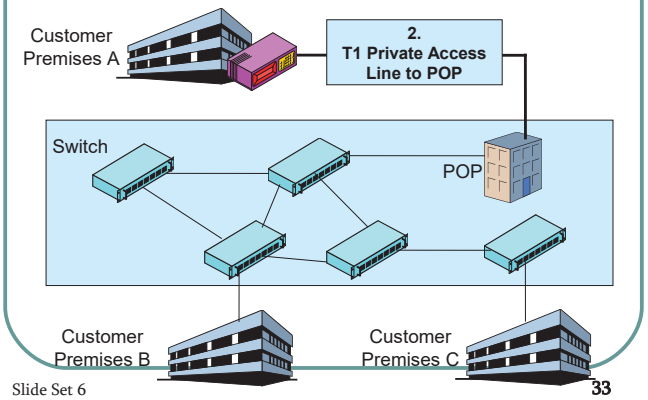
Frame Relay Network



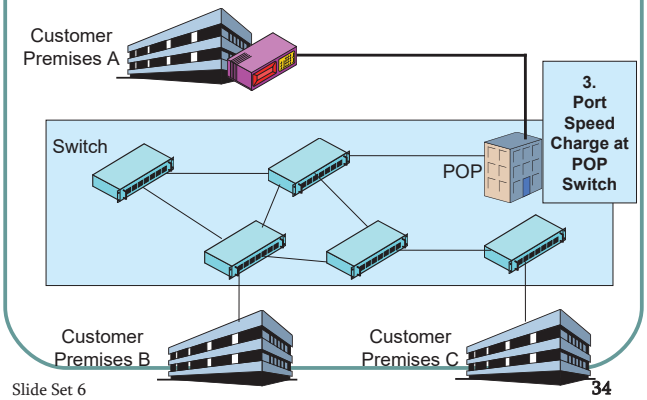
Frame Relay Network, Continued

- CSU/DSU
  - Channel service unit (CSU) protects the access line from unapproved voltage levels, etc. coming from the firm
  - Data service unit (DSU) converts between internal digital format and digital format of access link to Frame Relay network.
    - May have different baud rate, number of states, voltage levels, etc.

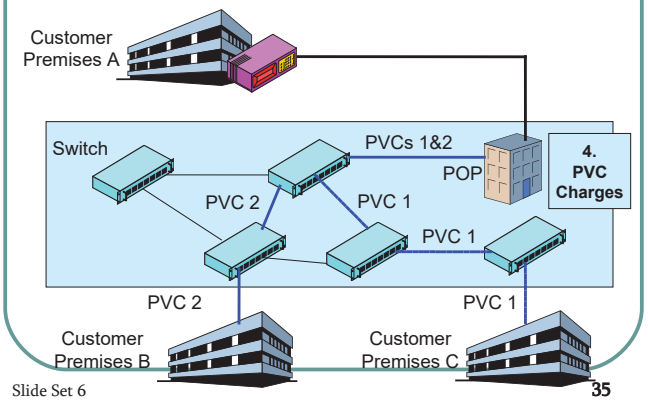
Frame Relay Network, Continued



Frame Relay Network, Continued



Frame Relay Network, Continued



Frame Relay Network, Continued

- Permanent Virtual Circuits (PVCs)
  - Set up once, kept in place for months or years
  - Between a firm's sites (which rarely change)
  - The most common form of virtual circuit today
- Switched Virtual Circuits (SVCs)
  - Set up at beginning of a communication session
  - Taken down at the end of the session
  - More expensive than PVCs, less common

Frame Relay Network, Continued

- Frame Relay Pricing Recap
  - Frame relay access device at site (or router)
  - Private line from site to POP
  - Port on the POP
    - Pay by port speed
    - **Usually the largest price component**
  - Permanent virtual circuits (PVCs) among communicating sites
    - **Usually the second-largest component of prices**
  - Other charges

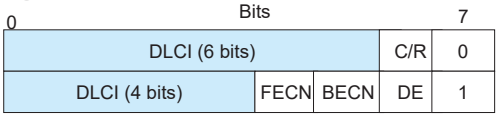
Frame Relay Frame

- Variable Length Frames
  - *Start flag* (01111110) to signal start of frame
  - *Address field* has variable length (2-4 octets)
  - *Information field* to carry data (variable)
  - *CRC (Cyclical Redundancy Check) field* to detect errors (2 octets)
    - If find errors, switch discards the frame
  - *Stop flag* (01111110) to signal end of frame

01111110	Address	Information	CRC	01111110

Frame Relay Frame, Continued

- Address Field of Frame Relay Frame
  - Variable Length: 2-4 octets
  - Usually 2 octets (as shown below)
  - Data link control indicator (DLCI, pronounced dull'-see) is the virtual circuit number (10 bits long in 2-octet form)



Site-to-Site Networking: Asynchronous Transfer Mode: ATM

Asynchronous Transfer Mode: ATM

- ATM is a faster PSDN than Frame Relay
  - Frame Relay: 56 kbps up to about 45 Mbps
  - ATM: 1.5 Mbps up to 155 Mbps
- Not Competitors. Most PSDN Vendors Offer Both to Customers
  - FR for low-speed customer needs
  - ATM for higher speeds (at higher prices)
- As corporate demand grows, ATM may increase its market share

ATM Cell

- Fixed length (53 octets) frame allows simpler and therefore faster processing at switches
  - For instance, switch does not have to do calculations to figure out how much buffer space it will need for a cell, as is the case with Frame Relay's variable-size frame.
  - 53 Octets
    - 5 octets of header
    - 48 octets of payload (data)
  - Fixed length frames are called ***cells.***

ATM Cell, Continued

- Short Cell Length Limits Latency at Each Switch
  - Switches may have to wait until the entire frame arrives before processing it and sending it back out.
    - With shorter frames, there is less latency at each switch along the path
  - Important in continent-wide WANs that require cells to pass through many switches
  - Especially important for voice, which is highly latency-intolerant (ATM was created for digitized voice)

Site-to-Site Networking: Multi protocol Label Switching: MPLS

MPLS-Multi Protocol Label Switching

MPLS is a data-carrying mechanism for both circuit-based and packet-switched clients. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, Frame Relay, and Ethernet frames.

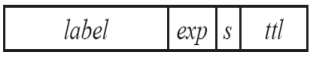
Router has two main elements

– Forwarding and routing

- Label switching is an alternative to IP forwarding
- MPLS (multi protocol label switching) combines benefits of virtual circuit with flexibility and robustness of datagram forwarding
- An MPLS-capable router uses traditional IP routing, but replaces IP forwarding with label switching.

Label Encoding

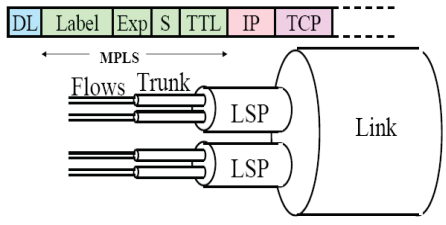
- MPLS uses 32 bits for label encoding
  - 20 bits for actual label
  - 2 power 20 (2^20) labels possible



Label: Label Value, 20 bits (0-16 reserved)
Exp.: Experimental, 3 bits (earlier Class of Service)
S: Bottom of Stack, 1 bit (1 = last entry in label stack)
TTL: 8 bit Time to Live

Flows, Trunks, LSPs, and Links

- Label Switched Path (LSP): All packets with the same label
- Trunk: Same Label+Exp
- Flow: Same MPLS+IP+TCP headers



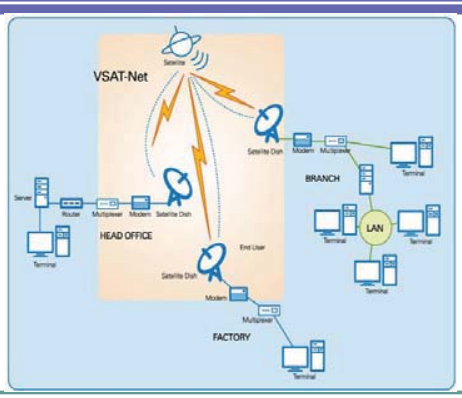
Site-to-Site Networking: Very Small Aperture Terminal: VSAT

is a two-way satellite, ground station with a dish antenna that is smaller than 3 meters

VSAT

VSAT can be used for data, voice, video or internet applications. It is used to communicate with or to link together locations using satellite connectivity. VSAT data rates typically range from narrowband up to 4 Mbps. A VSAT consists of two parts, a transceiver that is placed in direct line of sight to the satellite and a device that interfaces with the transceiver such as a PC. The transceiver receives or sends a signal to a satellite transponder in the sky. The satellite sends and receives signals from a ground station computer acting as a hub for the system. Each end user is interconnected with the hub station via the satellite, forming a star topology. The hub controls the entire operation of the network. For a user to communicate with another, each transmission has to first go to the hub station which then retransmits it via the satellite to the user's VSAT.

VSAT Illustration



Site-to-Site Networking: Metropolitan Area Ethernet

Ethernet is moving into metropolitan area networks

Metropolitan Area Ethernet

- Ethernet is moving beyond the LAN
  - Moving into the metropolitan area network (within a single urban area)
- New 802.3 standards (10 Gbps and 40 Gbps) being developed primarily for long distances of 10 km or more
- E-Line service: to connect LANs at two sites
- E-LAN service: to connect LANs at multiple sites
- Cheaper than ATM for high speeds
- Familiar technology so easy to manage
- Still lacks standards for carrier-class service
- New but growing rapidly compared to Frame Relay and ATM

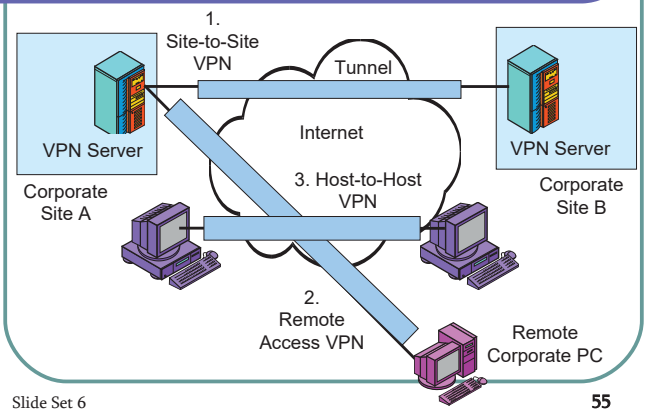
Site-to-Site Networking: Virtual Private Networks: VPNs

VPNs: Transmission over the Internet with added security

Virtual Private Network Issues

- Virtual Private Network (VPN)
  - Transmission over the Internet with added security
  - Some analysts include transmission over a PSDN with added security
- Why VPNs?
  - Lower transmission cost per bit transmitted than PSDNs
  - Adequate security

Virtual Private Network (VPN)



VPN Technologies

- SSL/TLS
  - Limited to remote access VPNs
  - SSL (Secure Sockets Layer) was its original name
    - IETF changed it to Transport Layer Security
  - Created to protect HTTP traffic in E-commerce
  - Built into every browser and web server, so easy to implement
  - Good if all traffic over the VPN will be HTTP
    - Beginning to handle other protocols
  - Moderate security

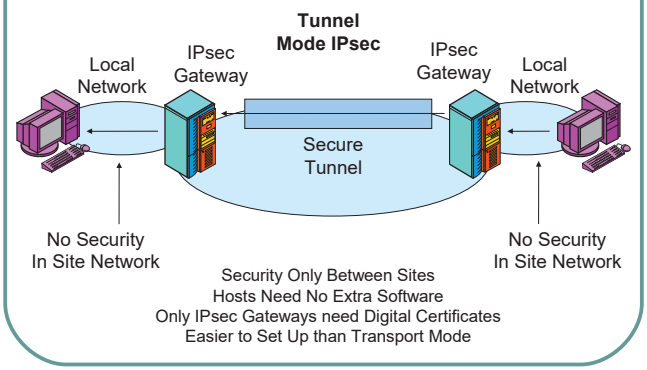
VPN Technologies, Continued

- Point-to-Point Tunneling Protocol (PPTP)
  - For remote access VPNs
  - Operates at the data link layer
  - Transparently provides security to all messages at higher layers
  - Software exists on all client PCs, but individual PCs must be configured to work with PPTP, and this is somewhat expensive
  - Good for remote access when not all traffic is HTTP
  - SSL/TLS has pushed PPTP almost entirely aside in the marketplace.

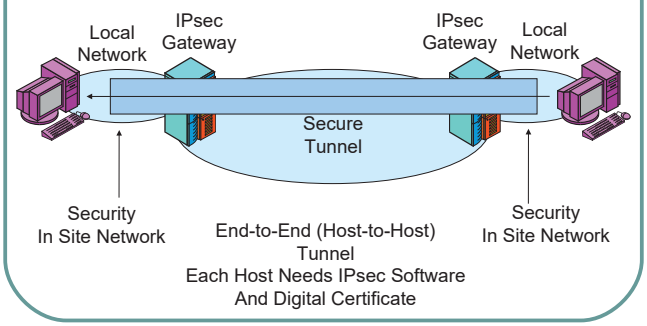
VPN Technologies, Continued

- IPSec
  - For all types of VPN (remote access, site-to-site, host-to-host)
  - Operates at the Internet layer
    - Transparently protects traffic at all higher layers
  - Very strong security
  - Requires digital certificates for all computers
    - Creating an infrastructure for certificates is expensive
    - Installation and setup on individual client PCs is expensive

IPsec in Tunnel Mode



IPSec in Transport Mode



Wireless LANs

Slide Set 7

Wireless LANs

- The Big Thing in local area networking today
- Gives mobility to users within the corporate premises
- Not a competitor yet for wired Ethernet LAN but wireless speed increasing everyday; mostly used to extend the wired LAN's resources

Wireless vs Wired: Pros and Cons

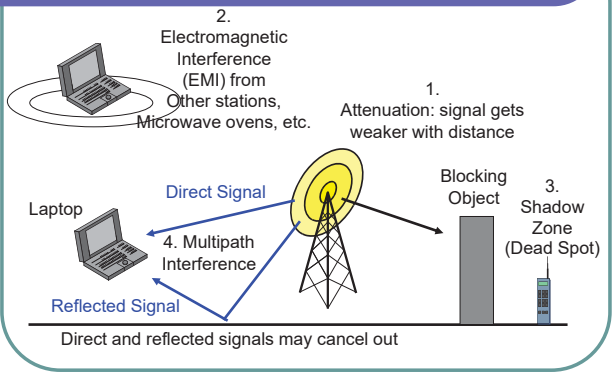
Parameter	Wireless	Wired
Security	Less Secure	More Secure
Data Rate	Slower (300 Mbps)	Faster (10 Gbps)
Setup and Deployment Cost	Cheaper	More Expensive
Connection Reliability	Less Reliable	More Reliable
Mobility	Higher	Much Lower
Deployment Speed	Faster	Slower
Range and Coverage	Smaller*	Larger
Robustness	Better	Weaker
Flexibility to change	Higher	Lower

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

Some Terminologies

- An Access Point (AP) or wireless Access Point is usually a device that only allows wireless clients (stations) to connect to it. Examples of wireless clients (smartphone, laptops, PDAs, tablets, Smart TVs, etc...)
- A wireless router is an AP which also contains a number wired ethernet ports that allows wired clients to connect to it. Basically, it is an AP+network switch.
- A wireless gateway is usually a wireless router which integrates a modem to provide Internet access as well. Basically, it is an AP+Switch+Modem (This is the one most of us have at home (Residential Gateway).
- A Hotspot is usually the same thing as a wireless gateway.

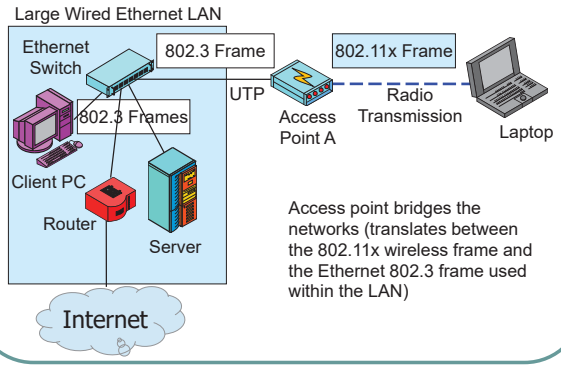
Wireless Propagation Problems



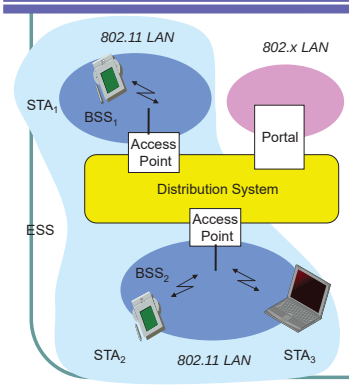
Wireless Propagation Problems

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

Typical 802.11 Wireless LAN Operation with Access Points



Architecture of an wireless network



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

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

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

Portal
- bridge to other (wired) networks

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

Typical AP modes of Operation

1. Infrastructure (Local/Managed) Mode
2. Client (Relay/Repeater) Mode ***
3. Sniffer (Monitor) Mode ***
4. Rogue Detector Mode ***
5. Bridge (Mesh) Mode ***

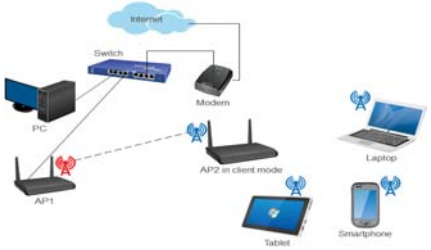
***(not available on all AP models)

1. Infrastructure (Local/Managed) Mode

The tablet, smartphone and laptop all connect wirelessly to the AP.

2. Client (Relay/Repeater) Mode

In this scenario, AP1 has internet connection, but the three stations are not in range to connect to it. AP2 is configured as client mode and connects to AP1 to allow the stations connected to the former to get internet access.

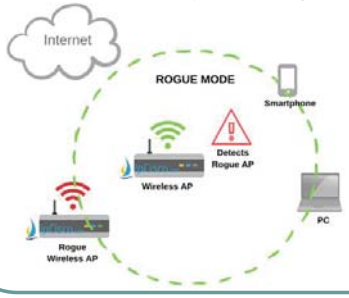


3. Sniffer (Monitor) Mode

In sniffer or monitor mode, the AP does not broadcast any SSID hence no wireless clients can connect to it but it can still receive wireless frames from stations. A laptop can connect remotely to the AP and perform sniffing with the appropriate software e.g. Wireshark

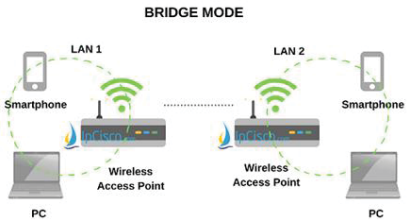
4. Rogue Detector Mode

In this mode, the AP is used to detect rogue devices. This detection is perform by inspecting the MAC address.



5. Bridge (Mesh) Mode

In Bridge mode, the two APs effectively establishes a point-to-point connection between themselves bridging 2 wireless LAN segments. If more than 2 APs are present, they can then establish point-to-multipoint connections effectively creating a mesh.



Ad-Hoc or P2P Mode

In this mode, the stations connect to each other without the need of an access point (AP)

802.11 Wireless LAN Standards

802.11 Standard	Date	Frequency	Channel Bandwidth	Non-Overlapping Channels	Max Data Transfer	Antenna Configuration	Range
802.11b	1999	2.4GHz	20MHz	1, 6, and 11	11Mbps	1x1 SISO	~300ft
802.11a	1999	5.0GHz	20MHz	See Notes	54Mbps	1x1 SISO	~150ft
802.11g	2003	2.4GHz	20MHz	1, 6, and 11	54Mbps	1x1 SISO	~300ft
802.11n	2009	2.4GHz and 5.0 GHz	20MHz and 40MHz	See Notes	100-600Mbps	Up to 4x4 MIMO	~300ft
802.11ac	2013	5.0GHz	20, 60, 80, and 160 MHz	See Notes	1Gbps	Up to 3x3 MU-MIMO	~300ft

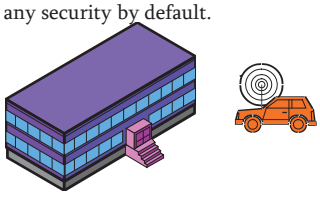
24 NOC in 20 MHz channels

24 NOC in 20 MHz channels
12 NOC in 40 MHz channels

24 NOC in 20 MHz channels
12 NOC in 40 MHz channels
6 NOC in 80 MHz channels
2 NOC in 160 MHz channels

802.11x Security

- Automated Drive-By Hacking (War Driving)
  - Can read traffic from outside the corporate walls
  - Can also send malicious traffic into the network
  - This was possible as the first generation of APs did not have any security by default.



802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Initial flawed security method developed by the 802.11 Working Group for 802.11 devices in 1997.
  - All stations share the same encryption key with the access point. This key cannot be changed as it was a static key
  - Shared static keys means that a large volume of traffic is encrypted with the same key
  - With so much traffic generated with one unchanging key, cryptanalysts (code-breakers) can crack the key by collecting data for a few days
  - Once the key is cracked, the attacker can read all messages and send attack messages into the network without going through a firewall filter

802.11 Security, Continued

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

802.11 Security, Continued

- Because of the security issues around WEP, the Wi-Fi Alliance developed Wi-Fi Protected Access (WPA) in 2003. Shortly afterward in 2004, they released WPA2 and in 2018 they released WPA3.

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

802.11 Security, Continued

- Wireless Protected Access (WPA)
  - Stopgap security method introduced before full 802.11i security could be developed
  - It was often possible to upgrade older WEP products to WPA because the underlying hardware was the same as WEP.
  - It uses Temporal Key Integrity Protocol (TKIP). It addressed the two flaws present in WEP by using MIC instead of CRC-32 and increasing the IV of RC4 from 40 bits to 48 bits.

802.11 Security, Continued

- Wireless Protected Access 2 and 3
  - In WPA2, encryption and integrity check are performed within single logical block – CCM and both are based on AES.
  - In WPA3, both encryption and data integrity are enhanced even further from WPA2. The only downside is that more processing power is required. Not many wireless devices support WPA3 yet.

802.11 Security, Continued

- Ways to strengthen your Wireless LAN
  - **Do not use WEP**. Use WPA, WPA2 or WPA3 instead.
  - Enforce MAC address Association (i.e only allowed wireless adapters can join your wireless network)
  - Disable SSID broadcast once all permitted stations have been allowed to join the wireless network.
  - Enable Access Point firewall features to mitigate potential attacks.

Simple Network Management Protocol

Slide Set 8

Network Management Framework

- Internet network management framework
  - MIB: management information base
  - SMI: data definition language
  - SNMP: protocol for network management
  - security and administration
- presentation services: ASN.1

Network Management standards

OSI CMIP

- Common Management Information Protocol
- designed 1980's: *the* unifying net management standard
- too slowly standardized

SNMP: Simple Network Management Protocol

- Internet roots (SGMP)
- started simple
- deployed, adopted rapidly
- growth: size, complexity
- currently: SNMP V3
- *de facto* network management standard

SNMP overview: 4 key parts

- Management information base (MIB):
  - distributed information store of network management data
- Structure of Management Information (SMI):
  - data definition language for MIB objects
- SNMP protocol
  - convey manager <-> managed object info, commands
- security, administration capabilities
  - major addition in SNMPv3

SMI: data definition language

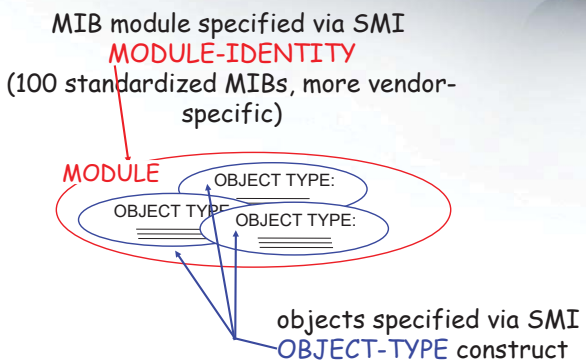
PURPOSE: syntax, semantics of management data well-defined, unambiguous

- BASIC DATA TYPES:
  - straightforward
- OBJECT-TYPE
  - data type, status, semantics of managed object
- MODULE-IDENTITY
  - groups related objects into MIB module

BASIC DATA TYPES

Integer
Integer32
Unsigned32
Octet String
Object Identifier
IPaddress
Counter32
Counter64
Gauge32
Time Ticks
Opaque

SNMP MIB



SMI: Object, Module examples

OBJECT-TYPE: **ipInDelivers**

```
ipInDelivers OBJECT TYPE
  SYNTAX      Counter32
  MAX-ACCESS  read-only
  STATUS      current
  DESCRIPTION
    "The total number of input
     datagrams successfully
     delivered to IP user-
     protocols (including ICMP)"
::= { ip   9}
```

MODULE-IDENTITY: **ipMIB**

```
ipMIB MODULE-IDENTITY
  LAST-UPDATED "941101000Z"
  ORGANZATION "IETF SNPv2
               Working Group"
  CONTACT-INFO
    " Keith McCloghrie
     ....."
  DESCRIPTION
    "The MIB module for managing IP
     and ICMP implementations, but
     excluding their management of
     IP routes."
  REVISION "019331000Z"
  .........
::= {mib-2 48}
```


MIB example: UDP module

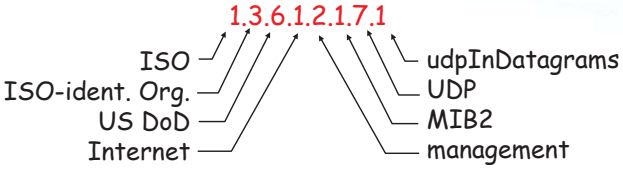
Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# underliverable datagrams no app at port
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	# datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port in use by app, gives port # and IP address

SNMP Naming

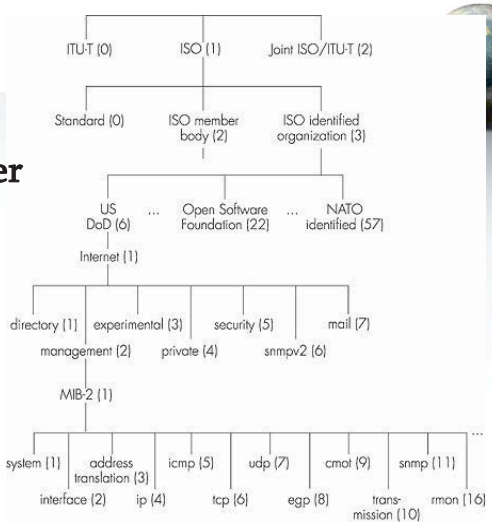
question: how to name every possible standard object (protocol, data, more..) in every possible network standard.

answer: *ISO Object Identifier tree:*

- hierarchical naming of all objects
- each branchpoint has name, number

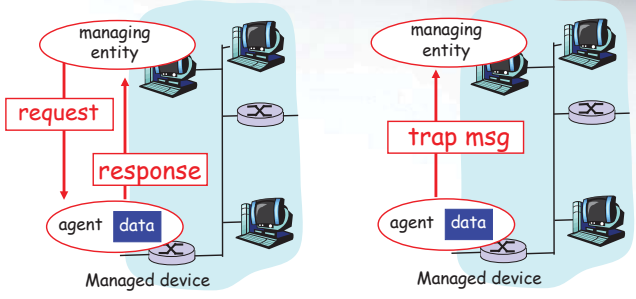


OSI Object Identifier Tree



SNMP protocol

Two ways to convey MIB info, commands:



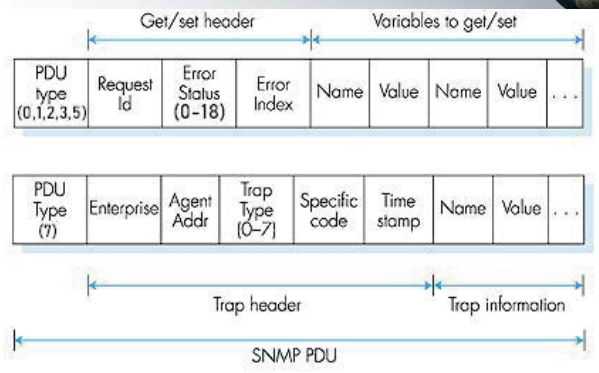
request/response mode

trap mode

SNMP protocol: message types

Message type	Function
GetRequest GetNextRequest GetBulkRequest	Mgr-to-agent: "get me data" (instance,next in list, block)
InformRequest	Mgr-to-Mgr: here's MIB value
SetRequest	Mgr-to-agent: set MIB value
Response	Agent-to-mgr: value, response to Request
Trap	Agent-to-mgr: inform manager of exceptional event

SNMP v2/3 protocol messages format



SNMP v2/3 PDU Type Values

PDU Type: An integer value that indicates the PDU type:

PDU Type Value	PDU Type
0	*GetRequest-PDU*
1	*GetNextRequest-PDU*
2	*Response-PDU*
3	*SetRequest-PDU*
4	Obsolete, not used (this was the old *Trap-PDU* in SNMPv1)
5	*GetBulkRequest-PDU* (has its own format, see below)
6	*InformRequest-PDU*
7	*Trapv2-PDU*
8	*Report-PDU*

SNMP v2/3 Error Status field Values

Error Status Value	Error Code	Description
0	noError	No error occurred. This code is also used in all request PDUs, since they have no error status to report.
1	tooBig	The size of the *Response-PDU* would be too large to transport.
2	noSuchName	The name of a requested object was not found.
3	badValue	A value in the request didn't match the structure that the recipient of the request had for the object. For example, an object in the request was specified with an incorrect length or type.
4	readOnly	An attempt was made to set a variable that has an Access value indicating that it is read-only.
5	genErr	An error occurred other than one indicated by a more specific error code in this table.
6	noAccess	Access was denied to the object for security reasons.
7	wrongType	The object type in a variable binding is incorrect for the object.
8	wrongLength	A variable binding specifies a length incorrect for the object.
9	wrongEncoding	A variable binding specifies an encoding incorrect for the object.
10	wrongValue	The value given in a variable binding is not possible for the object.
11	noCreation	A specified variable does not exist and cannot be created.
12	inconsistentValue	A variable binding specifies a value that could be held by the variable but cannot be assigned to it at this time.
13	resourceUnavailable	An attempt to set a variable required a resource that is not available.
14	commitFailed	An attempt to set a particular variable failed.
15	undoFailed	An attempt to set a particular variable as part of a group of variables failed, and the attempt to then undo the setting of other variables was not successful.
16	authorizationError	A problem occurred in authorization.
17	notWritable	The variable cannot be written or created.
18	inconsistentName	The name in a variable binding specifies a variable that does not exist.

SNMP security and Administration

- encryption: DES-encrypt SNMP message
- authentication: compute, send MIC(m,k): compute hash (MIC) over message (m), secret shared key (k)
- protection against playback: use nonce
- view-based access control
  - SNMP entity maintains database of access rights, policies for various users
  - database itself accessible as managed object!

Outline

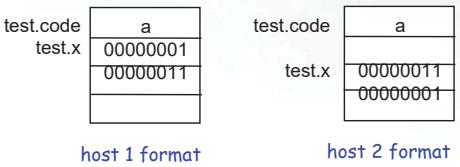
- What is network management?
- Internet-standard management framework
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - SNMP Protocol Operations and Transport Mappings
  - Security and Administration
- The presentation problem: ASN.1

The presentation problem

Q: does perfect memory-to-memory copy solve "the communication problem"?

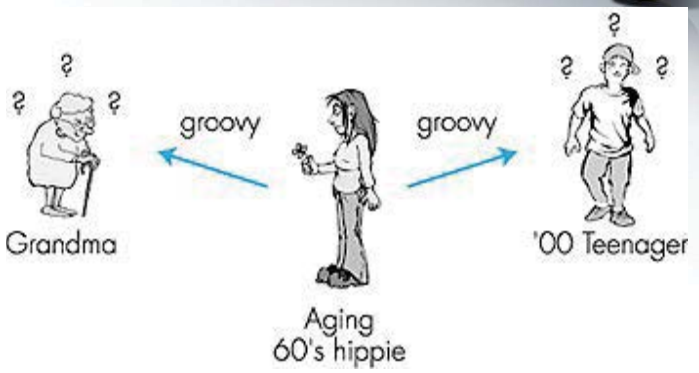
A: not always!

```
struct {
   char code;
    int x;
   } test;
test.x = 256;
test.code='a'
```



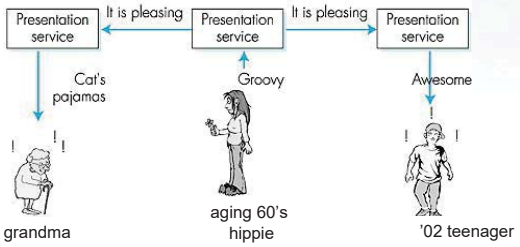
problem: different data format, storage conventions

A real-life presentation problem



Solving the presentation problem

1. Translate local-host format to host-independent format
2. Transmit data in host-independent format
3. Translate host-independent format to remote-host format



ASN.1 Abstract Syntax Notation 1

- ISO standard X.680
  - used extensively in Internet
  - like eating vegetables, knowing this "good for you"!
- defined data types, object constructors
  - like SMI
- BER: Basic Encoding Rules
  - specify how ASN.1-defined data objects to be transmitted
  - each transmitted object has Type, Length, Value (TLV) encoding

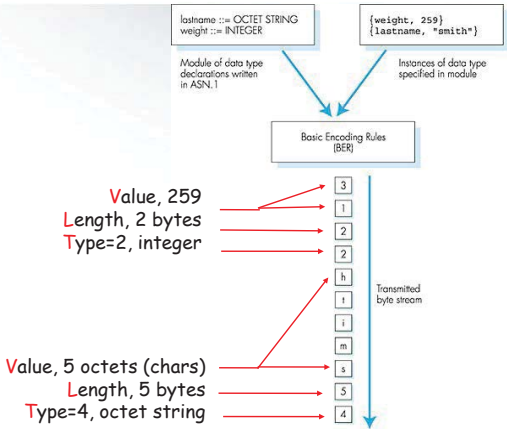
TLV Encoding

Idea: transmitted data is self-identifying

- T: data type, one of ASN.1-defined types
- L: length of data in bytes
- V: value of data, encoded according to ASN.1 standard

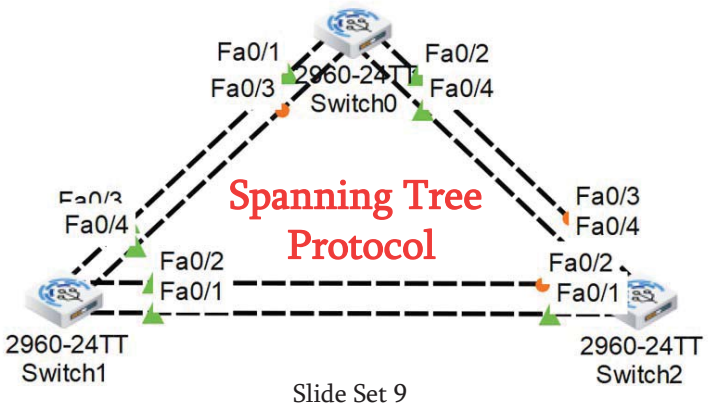
Tag Value	Type
1	Boolean
2	Integer
3	Bitstring
4	Octet string
5	Null
6	Object Identifier
9	Real

TLV encoding example



Network Management: summary

- network management
  - extremely important: 80% of network "cost"
  - ASN.1 for data description
  - SNMP protocol as a tool for conveying information
- Network management: more art than science
  - what to measure/monitor
  - how to respond to failures?
  - alarm correlation/filtering?



Slide Set 9

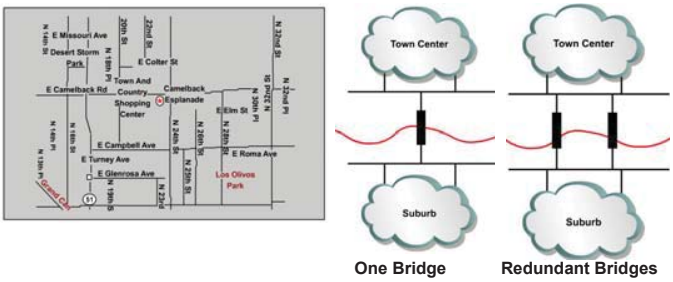
Overview

- Define redundancy and its importance in networking
- Describe the key elements of a redundant networking topology
- Define broadcast storms and describe their impact on switched networks
- Define multiple frame transmissions and describe their impact on switched networks
- Identify the benefits and risks of a redundant topology
- Describe the role of spanning tree in a redundant-path switched network
- Identify the key elements of spanning tree operation
- Describe the process for root bridge, root ports, designated ports election

Redundancy

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

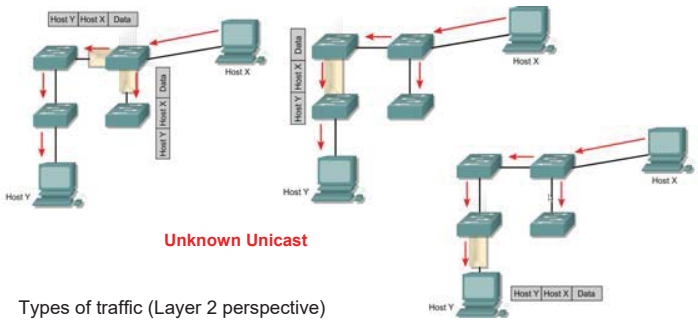
Redundant topologies



One Bridge Redundant Bridges

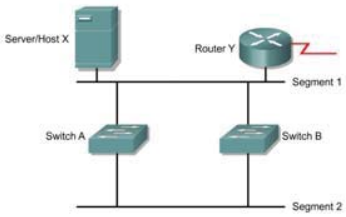
- A network of roads is a global example of a redundant topology.
- If one road is closed for repair there is likely an alternate route to the destination

Types of Traffic



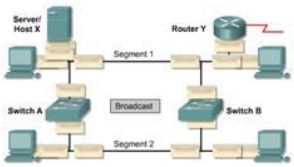
Types of traffic (Layer 2 perspective)
Known Unicast: Destination addresses are in Switch Tables
Unknown Unicast: Destination addresses are not in Switch Tables
Multicast: Traffic sent to a group of addresses
Broadcast: Traffic forwarded out all interfaces except incoming interface.

Redundant switched topologies



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

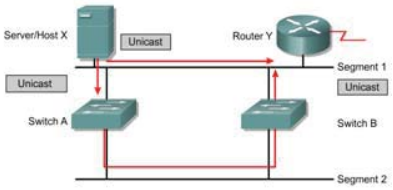
Broadcast Storm



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

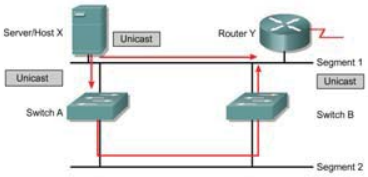
- Broadcasts and multicasts can cause problems in a switched network.
- If Host X sends a broadcast, like an ARP request for the Layer 2 address of the router, then Switch A will forward the broadcast out all ports.
- Switch B, being on the same segment, also forwards all broadcasts.
- Switch B sees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

Multiple frame transmissions



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

Multiple frame transmissions



(Some changes to curriculum)

The router receives the frame because it is on the same segment as Host X.

Switch A does not have the MAC address of the Router Y and will therefore flood the frame out its ports. (Segment 2)

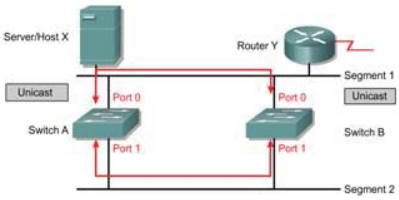
Switch B also does not know which port Router Y is on.

Note: Switch B will forward the the unicast onto Segment 2, creating multiple frames on that segment.

After Switch B receives the frame from Switch A , it then floods the frame it received causing Router Y to receive multiple copies of the same frame.

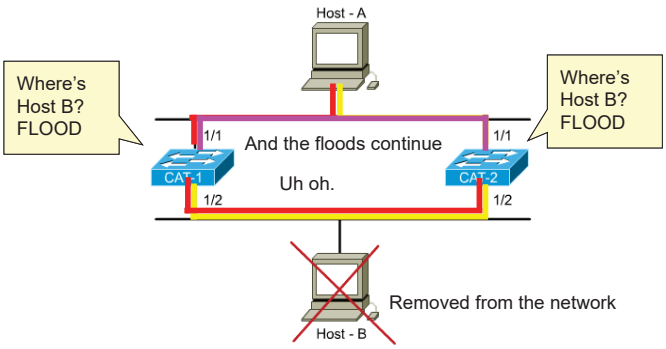
This is a causes of unnecessary processing in all devices.

Media access control database instability

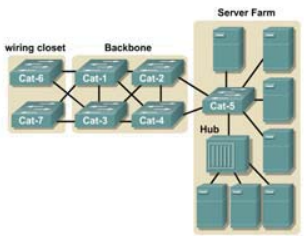


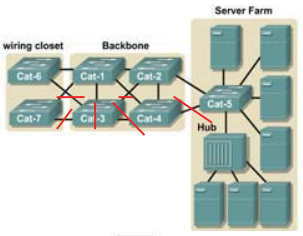
- In a redundant switched network it is possible for switches to learn the wrong information.
- A switch can incorrectly learn that a MAC address is on one port, when it is actually on a different port.
- Host X sends a frame directed to Router Y.
- Switches A and B learn the MAC address of Host X on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

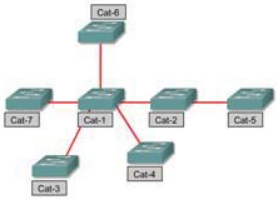
Layer 2 Loops - Flooded unicast frames



Redundant topology and spanning tree

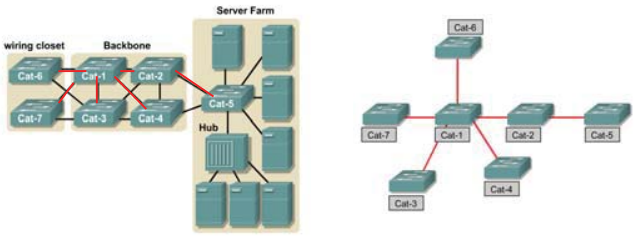






- Unlike IP, in the Layer 2 header there is no Time To Live (TTL).
- The solution is to allow physical loops, but create a loop free logical topology.
- The loop free logical topology created is called a tree.
- This topology is a star or extended star logical topology, the spanning tree of the network.

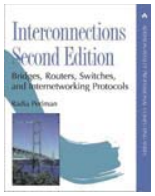
Redundant topology and spanning tree

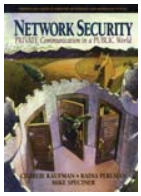


- It is a spanning tree because all devices in the network are reachable or spanned.
- The algorithm used to create this loop free logical topology is the **spanning-tree algorithm**.
- This algorithm can take a relatively long time to converge.

Spanning-Tree Protocol (STP)

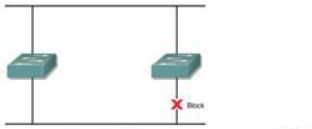
Radia Perlman, networking hero!



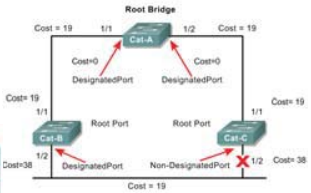


- Ethernet bridges and switches can implement the **IEEE 802.1D Spanning-Tree Protocol** and use the spanning-tree algorithm to **construct a loop free shortest path network**.
- Radia Perlman "is the inventor of the spanning tree algorithm used by bridges (switches), and the mechanisms that make link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

Spanning-Tree Protocol (STP)



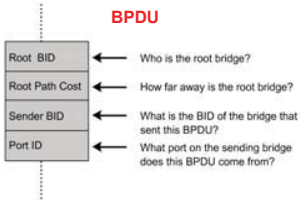
Link Speed	Cost(Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

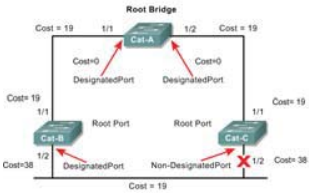


We will see how this works in a moment.

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

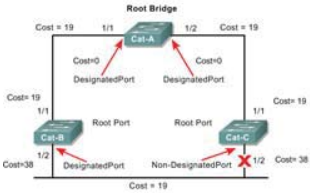
Spanning-Tree Protocol (STP)





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

Spanning-Tree Protocol (STP)



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

Select a **single switch that will act as the root** of the spanning tree

Calculate the **shortest path from itself to the root switch**

Designate one of the switches as the closest one to the root, for each LAN segment. This bridge is called the "**designated switch**".

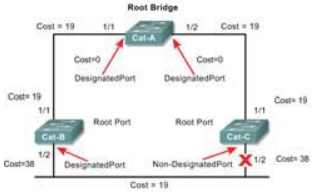
The designated switch handles all communication from that LAN towards the root bridge.

Choose one of its ports as its root port, for each non-root switch.

This is the interface that gives the best path to the root switch.

Select ports that are part of the spanning tree, the designated ports. Non-designated ports are blocked.

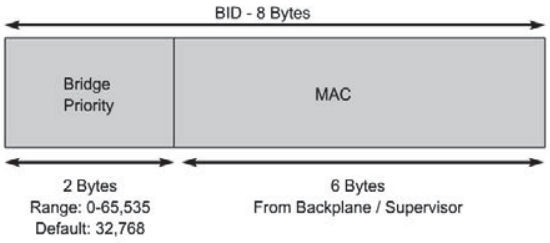
Two Key Concepts: BID and Path Cost



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

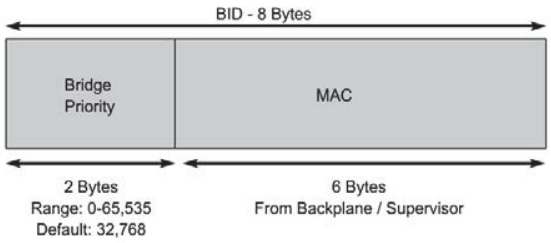
Rick Graziani graziani@cabrillo.edu

Bridge ID (BID)



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

Bridge ID (BID)



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

Path Cost

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

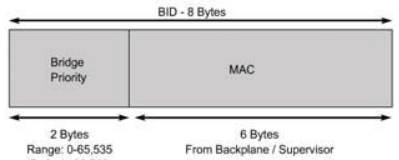
- Bridges use the concept of cost to evaluate how close they are to other bridges.
- This will be used in the STP development of a loop-free topology .
- **Originally, 802.1d** defined cost as 1000/bandwidth of the link in Mbps.
  - Cost of 10Mbps link = 100 or 1000/10
  - Cost of 100Mbps link = 10 or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

Path Cost

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

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

Path Cost



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

- You can modify the path cost by modifying the cost of a port.
  - Exercise caution when you do this!
- BID and Path Cost are used to develop a loop-free topology .
- But first the **3 STP Decision Sequence**

Three-Step STP Decision Sequence

- When creating a loop-free topology, STP always uses the same three-step decision sequence whenever it has to assign **Root Ports (RP) or Designated Ports (DP)** :

  Three-Step decision Sequence

  Step 1 - Lowest Path Cost to Root Bridge

  Step 2 - Lowest Sender BID

  Step 3 - Lowest Sender Port ID

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

Three-Step STP Decision Sequence

BPDU key concepts:

Bridges save a copy of only the best BPDU seen on every port.

When making this evaluation, it considers all of the BPDUs received on the port, as well as the BPDU that would be sent on that port.

As every BPDU arrives, it is checked against this three-step sequence to see if it is more attractive (lower in value) than the existing BPDU saved for that port.

Only the lowest value BPDU is saved.

Bridges send configuration BPDUs until a more attractive BPDU is received.

Okay, lets see how this is used...

Three Steps of Initial STP Convergence

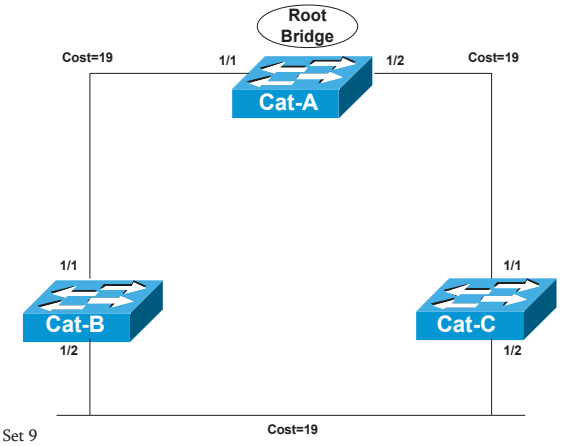
- The STP algorithm uses three simple steps to converge on a loop-free topology.
- Switches go through three steps for their initial convergence:

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

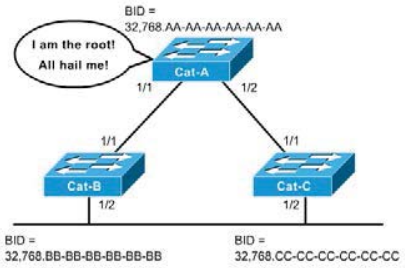
- All STP decisions are based on a the following predetermined sequence:

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

Step 1 Elect one Root Bridge



Step 1 Elect one Root Bridge



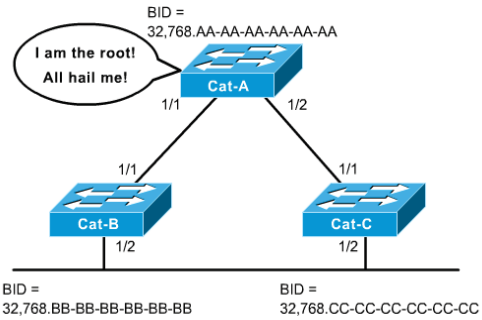
- When the network first starts, all bridges are announcing a chaotic mix of BPDUs.
- All bridges immediately begin applying the four-step sequence decision process.
- Switches need to elect a single Root Bridge.
- Switch with the **lowest BID** wins!

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

- This is known as the “Root War.”

Step 1 Elect one Root Bridge

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



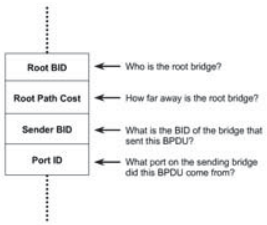
All 3 switches have the same default Bridge Priority value of 32,768

Step 1 Elect one Root Bridge

BPDU

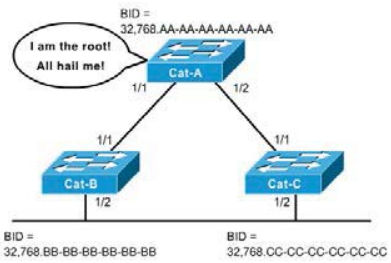
```
802.3 Header
  Destination:    01:80:C2:00:00:00  Mcast 802.1d Bridge group
  Source:         00:D0:C0:F5:18:D1
  LLC Length:     38
802.2 Logical Link Control (LLC) Header
  Dest. SAP:      0x42  802.1 Bridge Spanning Tree
  Source SAP:     0x42  802.1 Bridge Spanning Tree
  Command:        0x03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

Its all done with BPDUs!



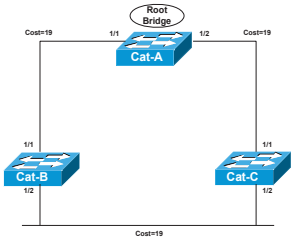
Configuration BPDUs are sent every 2 seconds by default.

Step 1 Elect one Root Bridge

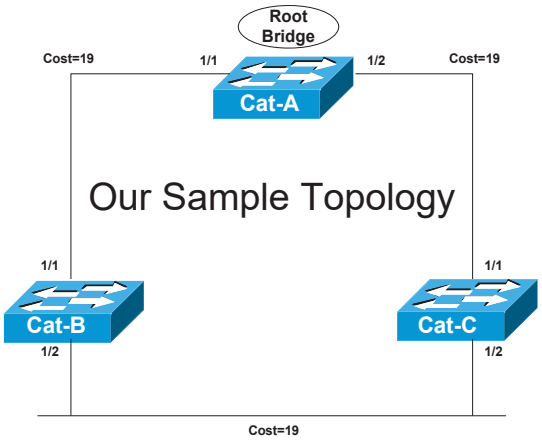


- At the beginning, all bridges assume they are the center of the universe and declare themselves as the Root Bridge, by placing its own BID in the Root BID field of the BPDU.
- Once all of the switches see that Cat-A has the lowest BID, they are all in agreement that Cat-A is the Root Bridge.

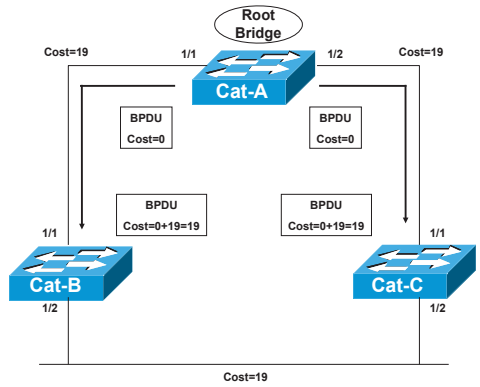
Step 2 Elect Root Ports



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



Step 2 Elect Root Ports



Step 1

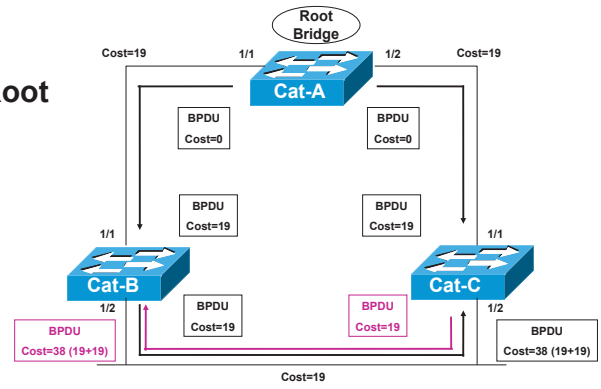
Cat-A sends out BPDUs, containing a Root Path Cost of 0.

Cat-B receives these BPDUs and adds the Path Cost of Port 1/1 to the Root Path Cost contained in the BPDU.

Step 2

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

Step 2 Elect Root Ports



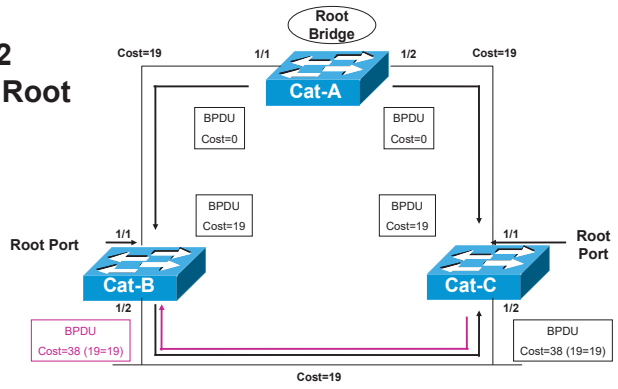
Step 3

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

Step 4

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

Step 2 Elect Root Ports



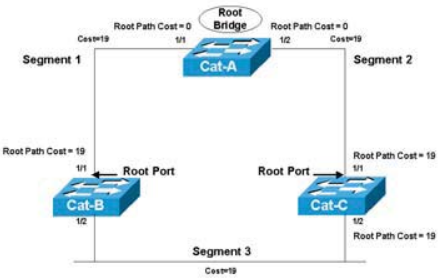
Step 5

Cat-B calculates that it can reach the Root Bridge at a cost of 19 via Port 1/1 as opposed to a cost of 38 via Port 1/2.

Port 1/1 becomes the Root Port for Cat-B, the port closest to the Root Bridge.

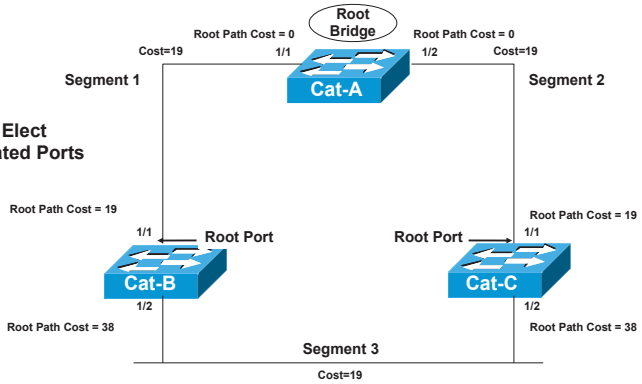
Cat-C goes through a similar calculation. Note: Both Cat-B:1/2 and Cat-C:1/2 save the best BPDU of 19 (its own).

Step 3 Elect Designated Ports

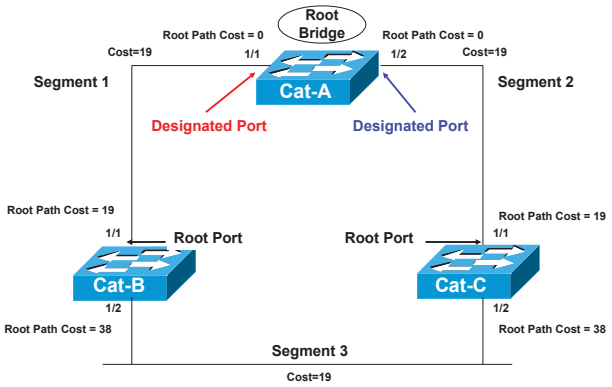


- The loop prevention part of STP becomes evident during this step, electing designated ports.
- A **Designated Port** functions as ***the single bridge port that both sends and receives traffic to and from that segment and the Root Bridge.***
- **Each segment in a bridged network has one Designated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

Step 3 Elect Designated Ports



- **Segment 1**: Cat-A:1/1 has a Root Path Cost = 0 (after all it has the Root Bridge) and Cat-B:1/1 has a Root Path Cost = 19.
- **Segment 2**: Cat-A:1/2 has a Root Path Cost = 0 (after all it has the Root Bridge) and Cat-C:1/1 has a Root Path Cost = 19.
- **Segment 3**: **Cat-B:1/2** has a **Root Path Cost = 38** and **Cat-C:1/2** has a **Root Path Cost = 38**. ***It's a tie!***

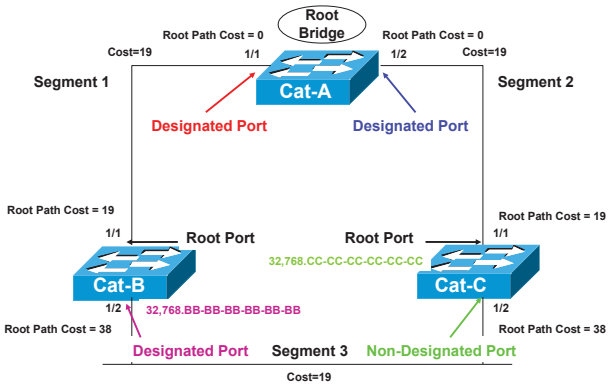


Segment 3

Both Cat-B and Cat-C have a **Root Path Cost of 38**, a tie!

When faced with a tie (or any other determination) STP always uses the three-step decision process:

1. Lowest Path Cost to Root Bridge; 2. Lowest Sender BID; 3. Lowest Sender Port ID



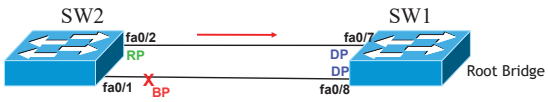
Segment 3 (continued)

1) Root Path Cost for both is 39, so a tie.

3) The sender's BID is lower on Cat-B than Cat-C, so Cat-B:1/2 becomes the **Designated Port for Segment 3**.

Cat-C:1/2 therefore becomes the **non-Designated (Blocking) Port for Segment 3.**

Sender Port ID tie breaker



Assume that SW1 is the Root Bridge. The path cost are the same on both links (say 19). So it's a tie!. Next, both ports on SW2 share the same BridgeID, so that is also a tie!

So, which Port on SW2 will be the Root Port? We might be tempted to say port fa0/1 as it has the lower portID. **WRONG !!!**

In fact we should look at the **Sender** Port ID as last tie-breaker!

The sender is the **Root Bridge** as he is the one **sending BPDUs** !!!

Therefore **fa0/2 on SW2** will be the **Root Port** as it is connected to PortID fa0/7 on the Root bridge which has a lower PortID than fa0/8.

STP Recap

- All switches go through three steps for their initial convergence:

STP Convergence

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

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

Three-Step decision Sequence

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

- **All ports of Root Bridge** are by **default Designated Ports**.
- **If one end of a link is a Root Port** then the other end **must be a Designated Port.**
- **If a link is unlabeled,** then one end **must be a Designated Port** and the other end **must be a non-Designated (Blocking) Port.**

Network Performance

Slide Set 10

Key Terms

- Bandwidth / Capacity of the network
- Throughput – Actual Rate of data passing a certain point in the network
- Latency (Delay) - delay incurred by a data from start to finish
  - Transmission Delay
  - Propagation Delay
  - Queuing/Buffer Delay
  - Processing Delay, etc…

Bandwidth/Capacity

Bandwidth can have two contexts in networking:

The first, Bandwidth measured in Hertz, refers to the range of frequency that a channel or link can have i.e. highest frequency – lowest frequency.

The second, bandwidth measured in bits per second, refers to the maximum rate of data that can be carried by a channel or link. This is often referred to as the Capacity to avoid confusion.

Bandwidth/Capacity

The Capacity of a channel or link is directly proportional to the Bandwidth available.

The higher the Bandwidth, the higher the capacity

This is shown by either the Nyquist and Shannon-Hartley Theorems below:

Nyquist: $C = 2B\log_2 M$ where M = no. of signal levels

Shannon-Harteley: $C = B \log_2 (1 + S/N)$ where S/N is the Signal power to Noise power ratio.

Throughput

Throughput is the actual rate of data passing a particular point in the network. It is measured in bits per second just like Capacity.

The throughput is always less or equal to the capacity of a channel or link.

The throughput can never exceed the capacity of a channel.

For example, in wireless LAN 802.11g, the capacity is 54 Mbps, but the throughput at a certain distance from the transmitter will always be less than 54 Mbps.

Latency

Latencies are the delays present in a communication system.

Some of these latencies are negligible but some are not.

The one-way latency is the sum of all the delays added up from source to destination.

The two-way latency is also referred as to the Round-Trip-Time (RTT) or response time.

Transmission Delay

Transmission Delay or Transmit time is the time needed to inject the data on the network for ongoing transmission. It is directly proportional to the size of data and inversely proportional to the bandwidth of the channel or link.

$$\text{Transmit Time} = \frac{\text{Size of data (in bits)}}{\text{Bandwidth (in bits per second)}}$$

Propagation Delay

Propagation Delay or Travel time is the time taken for the data signal to travel from source to destination. It is directly proportional to the distance between source and destination and inversely proportional to the speed of the signal.

$$\text{Propagation Delay} = \frac{\text{Distance (in meters)}}{\text{Speed (in m/s)}}$$

Queuing/Buffer Delay

Queuing Delay or Buffer Delay is the time taken to 'absorb' the data at the receiver It is usually assumed to be equal to the transmit time if the same amount of data is received and bandwidth is unchanged.

$$\text{Buffer Time} = \frac{\text{Size of data (in bits)}}{\text{Bandwidth (in bits per second)}}$$

Processing Delays

Processing Delay is the time taken to process some information in order to take a decision.

Processing delays such as: Switching delay, Error detection delay, when intermediate devices such as hubs, bridges, switches and routers are present.

These delays depend of the speed of the processing unit, the type and amount of memory, as well as, the switching technology used within those devices.

Switching Delay

Switching Delay = Time taken to move data from incoming port to appropriate outgoing port.

In a switch, this is the time taken to decide which appropriate outgoing port to forward a frame after inspecting the forwarding table.

In a router, this is the time taken to decide which appropriate outgoing port to route a packet after inspecting the routing table.

Error Detection Delay

Error Detection Delay = Time taken to check for errors withing a frame or packet header.

Error detection delay **only** takes place in a switch operating in **Store-N-Forward** mode **because it buffers the frame completely**.

Note: No error detection in switches operating in cut-through mode.

In a router, error detection occurs for both the frame content and the packet header as well.

Switch Buffer time in Cut-through mode

In cut-through mode, the switch does not buffer the entire frame before it starts switching and retransmitting the frame via the appropriate output port.

The buffer time is therefore less than that of a switch operating in Store-N-Forward mode.

Buffer time at switch in cut-through mode =

$$\frac{\text{Minimum Buffer bits}}{\text{Bandwidth in bps}}$$

Performance Statistics

- The main network performance parameter is the **response time** as seen previously.
- Another parameter is **availability**; the percent of time the network is available. **Downtime** is the percent of time the network is not available.
- Failure statistics include:
  - **Mean time between failures (MTBF)** indicates the reliability of a network component.
  - **Mean time to repair (MTTR)** equal to the mean time to diagnose plus the mean time to respond plus the mean time to fix a problem.

  MTTRepair = MTTDiagnose + MTTRespond + MTTFix

Availability

$$\text{Availability} = \frac{uptime}{uptime + downtime} = \frac{MTBF}{MTBF + MTTR}$$

Availability	Lost Time (hours)	Lost Time (minutes)	Lost Time (seconds)
60.00%	3504		
65.00%	3066		
70.00%	2628		
75.00%	2190		
85.00%	1314		
90.00%	876		
95.00%	438		
96.00%	350.4		
97.00%	262.8		
98.00%	175.2		
99.00%	87.6		
99.50%	43.8		
99.90%	8.76	525.6	
99.99%	0.876	52.6	3153.6
99.999%	0.0876	5.3	315.36
99.9999%	0.00876	0.5	31.536
99.99999%	0.000876	0.1	3.1536

1 year = 365 days/yr * 24 hrs/day = 8760 hrs/yr

Just as a remind

Reliability

$$\text{Reliability} = e^{-T/\Phi}$$

$$\text{Reliability} = e^{-\Lambda T}$$

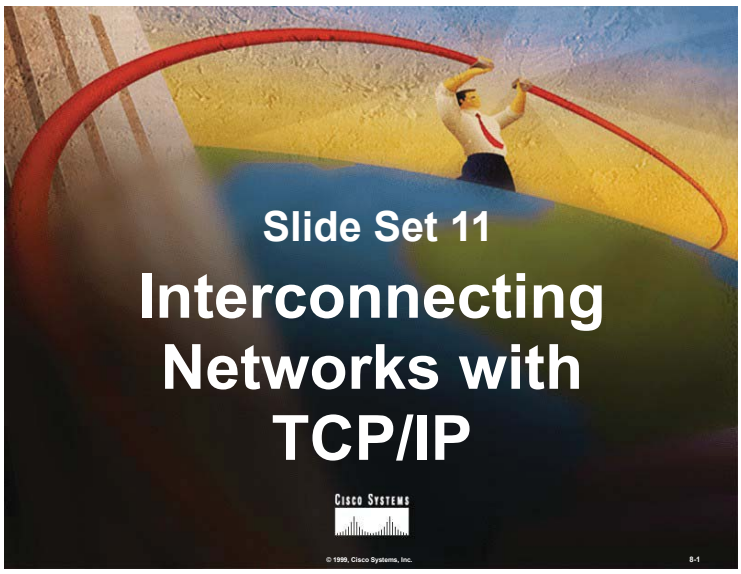
$$\text{Reliability} = e^{-N}$$

Reliability	Failures per year	Failures per 10 years	Failures per 100 years
10.00%	2.30		
20.00%	1.61		
30.00%	1.20		
40.00%	0.92		
50.00%	0.69		
60.00%	0.51		
70.00%	0.36		
80.00%	0.22	2.23	
90.00%	0.11	1.05	
95.00%	0.05	0.51	
99.00%	0.01	0.10	1.01
99.50%	0.005	0.05	0.50
99.90%	0.001	0.01	0.10
99.99%	0.0001	0.001	0.01
99.999%	0.00001	0.0001	0.001
99.99999%	0.0000010	0.00001	0.0001
99.99999%	0.00000010	0.000001	0.00001

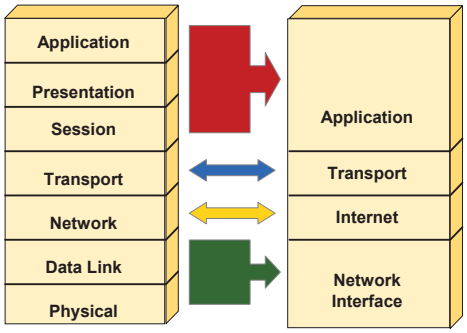
1 yr mission = 365 days/yr * 24 hrs/day = 8760 hrs/yr

Where $\Phi = MTBF$, $\Lambda = Failure\ Rate$

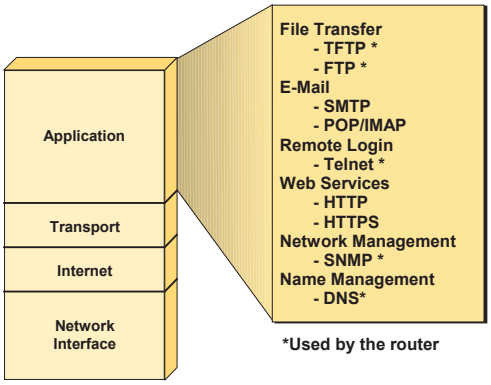
N = number of failures, T = mission time



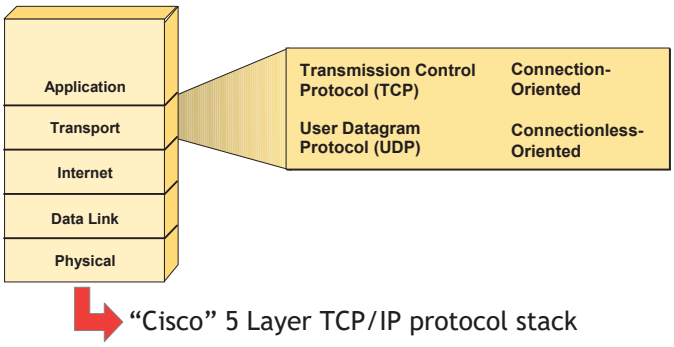
ISO OSI Reference Model vs. TCP/IP Protocol Stack



Application Layer Overview

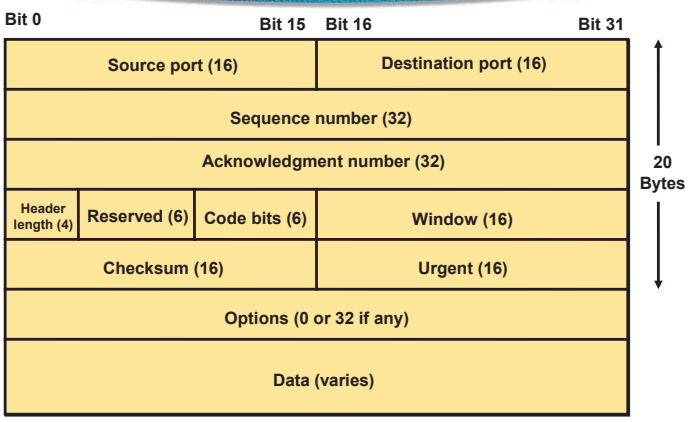


Transport Layer Overview

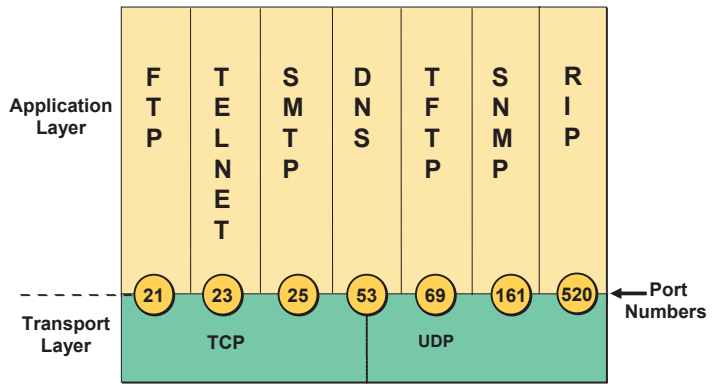


"Cisco" 5 Layer TCP/IP protocol stack

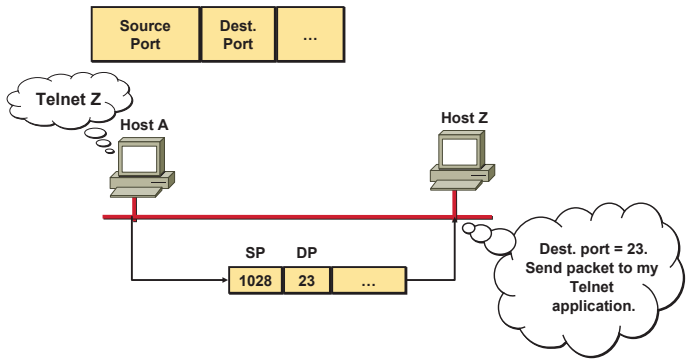
TCP Segment Structure Transport Layer PDU



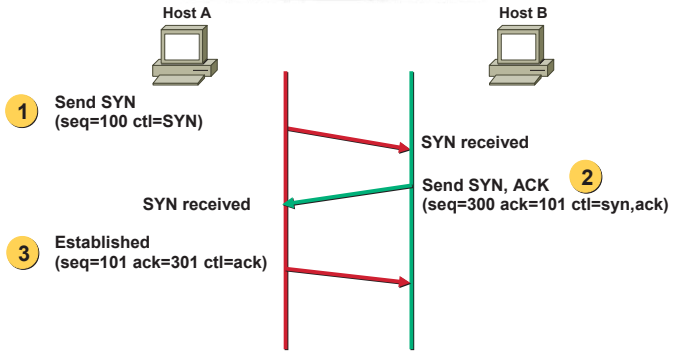
Port Numbers



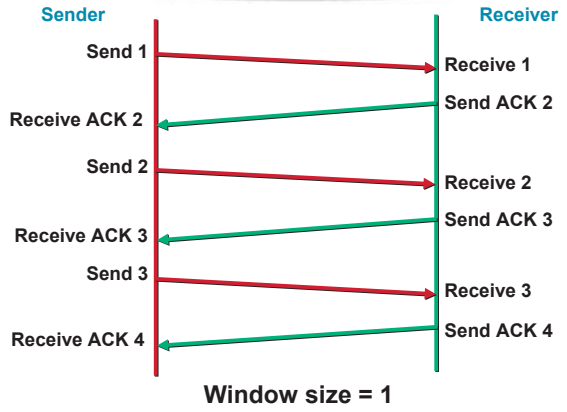
TCP Port Numbers



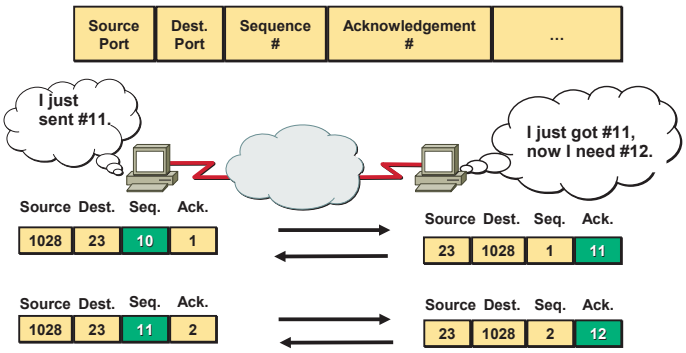
TCP Three Way Handshake/Open Connection



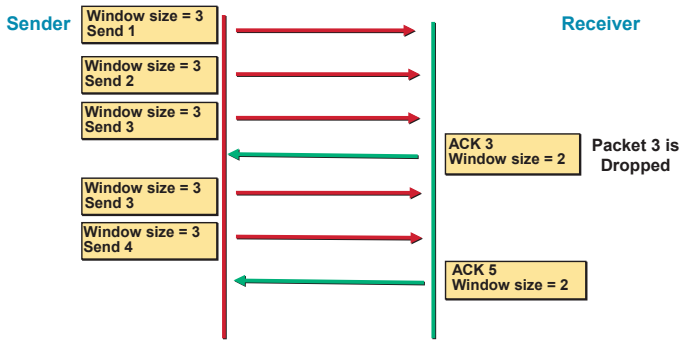
TCP Simple Acknowledgment



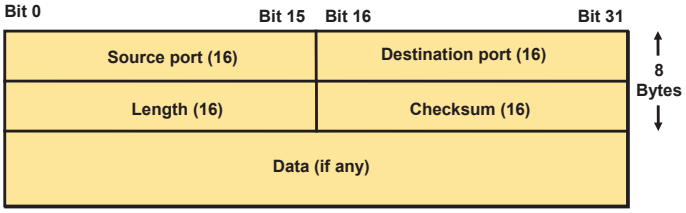
TCP Sequence and Acknowledgment Numbers



TCP Windowing

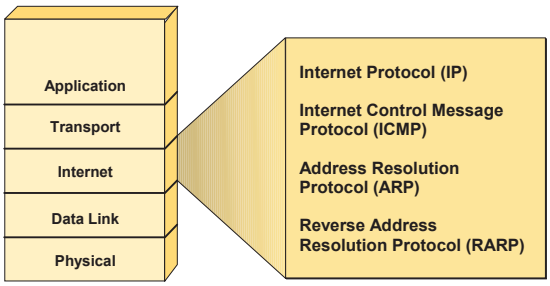


UDP Segment Structure Transport Layer PDU



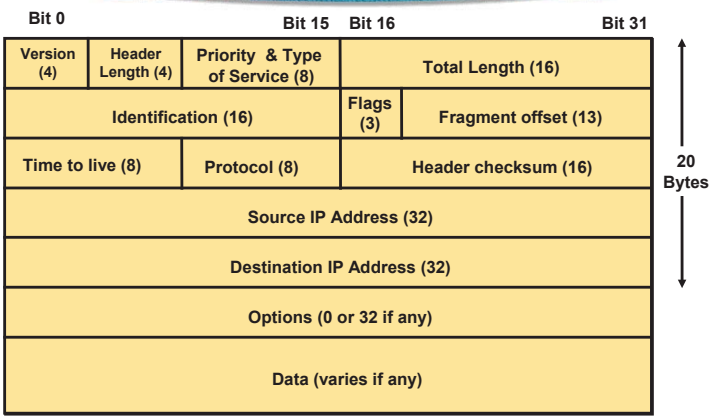
No sequence or acknowledgment fields

Internet Layer Overview

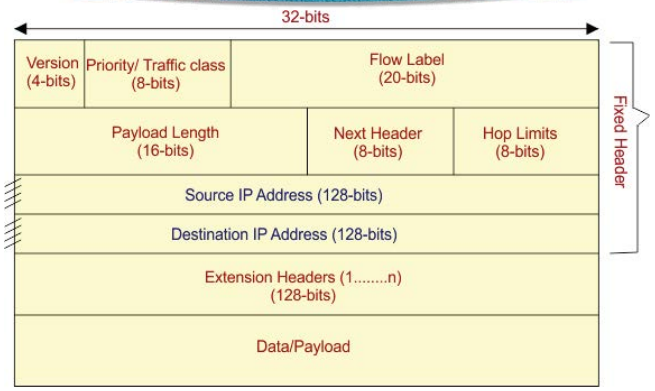


OSI network layer corresponds to the TCP/IP internet layer

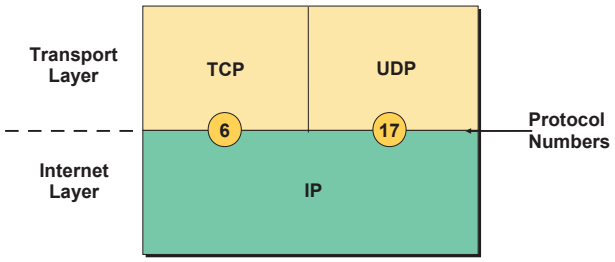
IPv4 Datagram Structure Internet Layer PDU



IPv6 Datagram Structure Internet Layer PDU

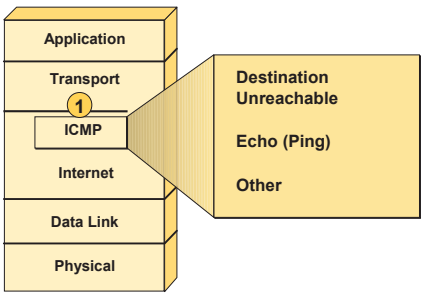


Protocol Field

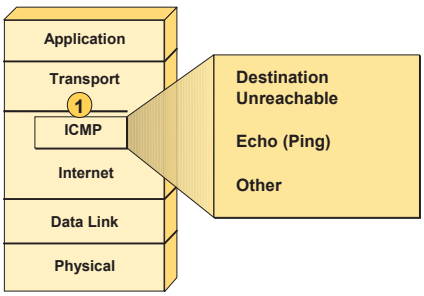


Determines destination upper-layer protocol

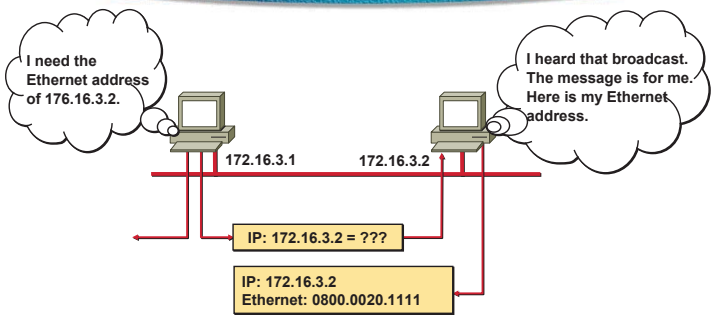
Internet Control Message Protocol



Ethernet Frame Structure Data Link Layer PDU



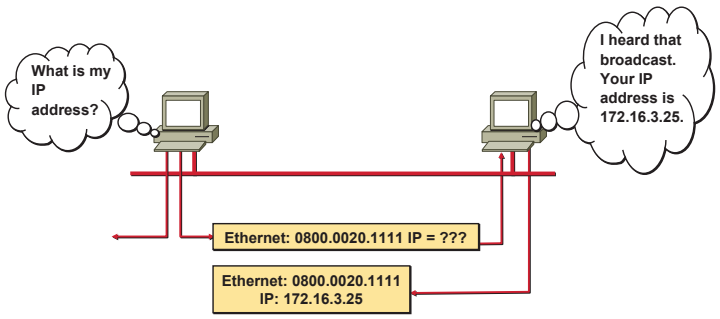
Address Resolution Protocol



Map IP → Ethernet

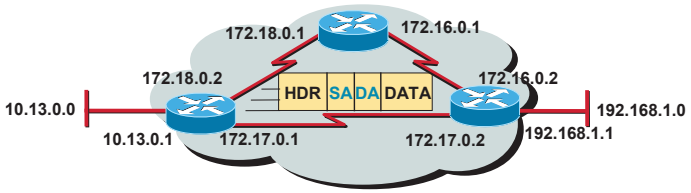
Local ARP

Reverse ARP



Map Ethernet → IP

Introduction to TCP/IP Addresses



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

IP Addressing

32 bits

Dotted Decimal	Network		Host	
Maximum	255	255	255	255
Binary	11111111	11111111	11111111	11111111
Example Decimal	172	16	122	204
Example Binary	10101100	00010000	01111010	11001100

Binary bit positions: 1–8, 9–16, 17–24, 25–32 (128 64 32 16 8 4 2 1)

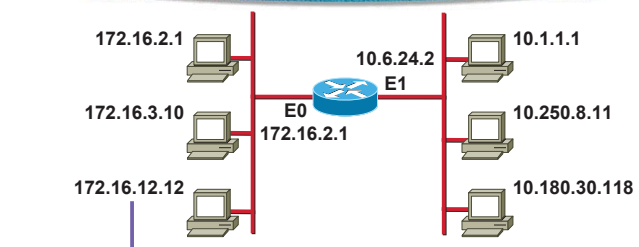
IP Address Classes

	8 bits	8 bits	8 bits	8 bits
Class A:	Network	Host	Host	Host
Class B:	Network	Network	Host	Host
Class C:	Network	Network	Network	Host
Class D:	Multicast			
Class E:	Research			

IP Address Classes

	Bits: 1–8	9–16	17–24	25–32
Class A:	0NNNNNNN	Host	Host	Host
	Range (1-126)			
Class B:	10NNNNNN	Network	Host	Host
	Range (128-191)			
Class C:	110NNNNN	Network	Network	Host
	Range (192-223)			
Class D:	1110MMMM	Multicast Group	Multicast Group	Multicast Group
	Range (224-239)			

Host Addresses



172.16 . 12 . 12
Network Host

Routing Table Network	Interface
172.16.0.0	E0
10.0.0.0	E1

 www.cisco.com ICND—8-25

Determining Available Host Addresses

Network		Host	
172	16	0	0
10101100	00010000	00000000	00000000
		00000000	00000001
		00000000	00000010
		⋮	⋮
		11111111	11111101
		11111111	11111110
		11111111	11111111

N
1
2
3
⋮
65534
65535
65536
- 2
65534

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

 www.cisco.com ICND—8-26

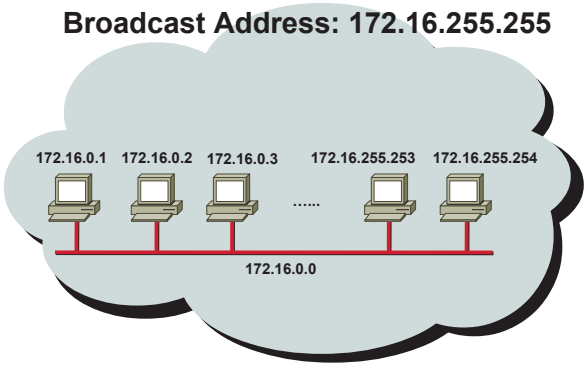
IP Address Classes Exercise

Address	Class	Network	Host
10.2.1.1			
128.63.2.100			
201.222.5.64			
192.6.141.2			
130.113.64.16			
141.201.257.10			

 www.cisco.com ICND—8-27

Addressing without Subnets

Broadcast Address: 172.16.255.255

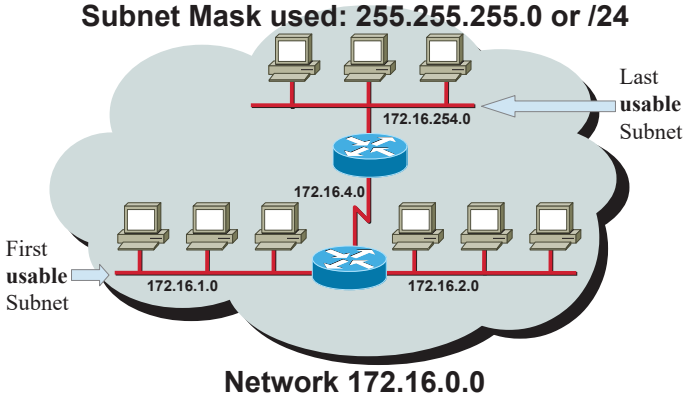


Network Address: 172.16.0.0

 www.cisco.com ICND—8-28

Addressing with Subnets

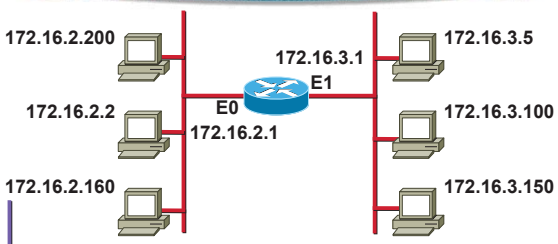
Subnet Mask used: 255.255.255.0 or /24



Network 172.16.0.0

 www.cisco.com ICND—8-29

Subnet Addressing if using SM = 255.255.255.0



172.16 . 2 . 160
Network Subnet Host

New Routing Table Network	Interface
172.16.2.0	E0
172.16.3.0	E1

 www.cisco.com ICND—8-30

Subnet Mask

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

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

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

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

Decimal Equivalents of Bit Patterns

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

Subnet Mask without Subnets

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

Subnets not in use—the default

Subnet Mask with Subnets

	Network		Subnet	Host
172.16.2.160	10101100	00010000	0 0 0 0 0 0 1 0	10100000
255.255.255.0	11111111	11111111	1 1 1 1 1 1 1 1	00000000
	10101100	00010000	0 0 0 0 0 0 1 0	00000000
Network Number	172	16	2	0

128 192 224 240 248 252 254 255

Network number extended by eight bits

Subnet Mask with Subnets (cont.)

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

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

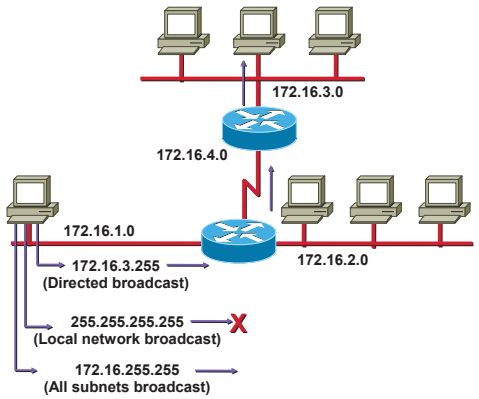
Network number extended by ten bits

Subnet Mask Exercise Answers

Address	Subnet Mask	Class	Subnet
172.16.2.10			
10.6.24.20			
10.30.36.12			

```
10.6.24.20          00001010.00000110.00011000.00010100
255.255.240.0       11111111.11111111.11110000.00000000
Subnet id           00001010.00000110.00010000.00000000
```


Broadcast Addresses



Addressing Summary Example

172	16	2	160

How many usable subnets = 2^10 – 2 = 1022 subnets

	172.16.2.160	10101100	00010000	00000010	10000000	Host 1
	255.255.255.192	11111111	11111111	11111111	11000000	Mask 2
8	172.16.2.128	10101100	00010000	00000010	10000000	Subnet 4
9	172.16.2.191	10101100	00010000	00000010	10111111	Broadcast 5
	172.16.2.129	10101100	00010000	00000010	10000001	First 6
	172.16.2.190	10101100	00010000	00000010	10111110	Last 7

3

How many hosts per subnet = 2^6 – 2 = 62 hosts per subnet

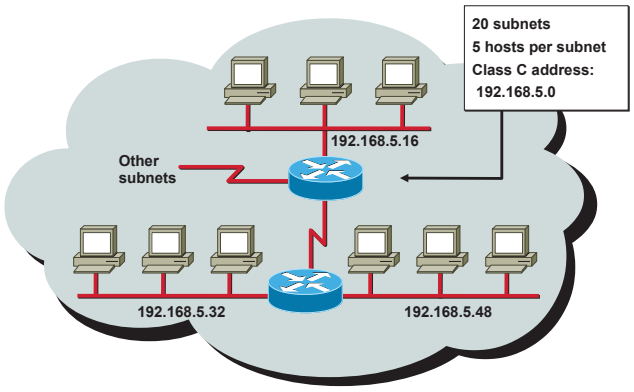
Class B Subnet Example

IP Host Address: 172.16.2.121
Subnet Mask: 255.255.255.0

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

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

Subnet Planning



Class C Subnet Planning Example

IP Host Address: 192.168.5.121
Subnet Mask: 255.255.255.248

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

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

Broadcast Addresses Exercise

IP Address	Subnet Mask	Class	Subnet Add	Broadcast Add
201.222.10.60	255.255.255.248			
15.16.193.6	255.255.248.0			
128.16.32.13	255.255.255.252			
153.50.6.27	255.255.255.128			

LAB EXERCISES

- **2 Wireshark Labs** (Duration: 2 Weeks)
- **3 Packet Tracer Labs** (Duration: 2 Weeks)

  (Note: You are advised to download and install the latest version of Packet Tracer from Cisco Academy website. You need to register and I will advise that you follow the tutorial to familiarize yourself with the software. Registration is free.

Wireshark Lab 0

Getting Started

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

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

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

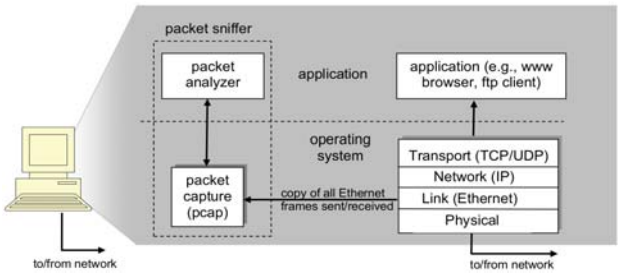


Figure 1

In Figure 1, the assumed physical media is an Ethernet, and so all upper layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you all messages sent/received from/by all protocols and applications executing in your computer.

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

We will use the Wireshark packet sniffer (www.wireshark.org) for these labs, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack. Wireshark is a free network protocol analyzer that runs on Windows, Linux, and Mac computers. It's an ideal packet analyzer for these labs – it is stable, has a large user base and good support with a user guide (www.wireshark.org/docs/wsug_html).

Getting Wireshark

Download Wireshark (Windows/64-bit) off my website from here or else visit the Wireshark home page and download the most compatible version for your computer.
Note: Ensure that you install the WinPcap 4.0 packet capture library if it is not already present on your machine. Please start WinPcap NPF as a service as well.

Starting Wireshark

After installation is complete, start the Wireshark program. You will be greeted by a initial capture screen as shown in Figure 2.

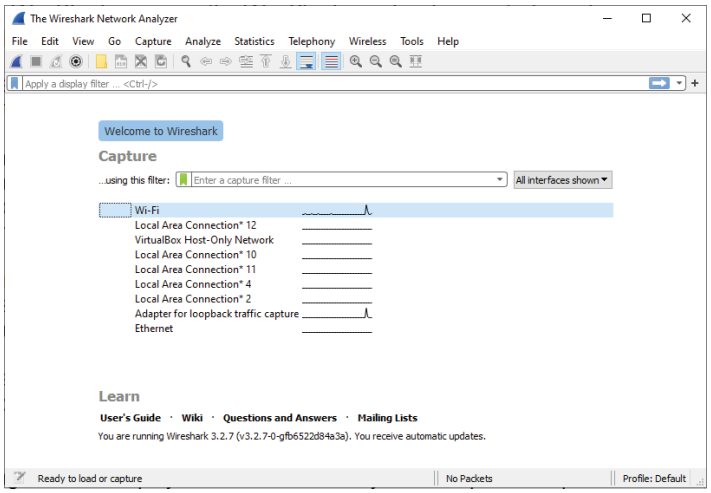


Figure 2

The different interfaces available on your system will be displayed here. It will be obviously be slightly different from the listing in Figure 2.

You will have to click and select the interface through which you are connected to your network. If it is a Laptop PC, it will most probably be by Wi-Fi and if it is a Desktop PC, it will be through one of the Local Area Connections. The little line graph to the right of the interface list will show you which interface is currently active. By default, my Wi-Fi is active and has been selected.

Performing a Capture on Wireshark

After having selected the correct interface, we now have to start a capture. The first four icons on the main toolbar controls the c  tions.

The blue shark fin icon is for starting a live capture. The second square icon is for stopping the current capture. (icon lights up as red when a capture is underway). The third icon is for aborting the current capture and restarting a capture (icon lights up as a green shark fin when a capture is underway. It will prompt you if you want to save the current capture or continue with a new capture without saving) and finally the fourth cogwheel icon is for setting capture options.

Now follow the three steps below to perform your first live capture.

1. Open your favorite browser (if you have not done so already), I would recommend you use Firefox or Chrome because these allow you to clear the browser cache easily. Also, it is recommended to keep network traffic to a minimum so ensure that you are using only one tab in your browser.

2. Enter this URL in your browser (**Do not press ENTER just yet**): **http://pages.intnet.mu/rhh**

3. Start a live capture in Wireshark by clicking on the blue shark fin icon. A new screen will appear in Wireshark. Now go to your browser and press ENTER. The above URL is from my old website hosted at Mauritius Telecom public web server. When the web page has fully loaded, only then, stop the Wireshark capture by clicking on the red square icon.

Analysing a Capture using Wireshark

You will notice that a new interface has appeared when you previously started the live capture which looks like the Figure 3 below:

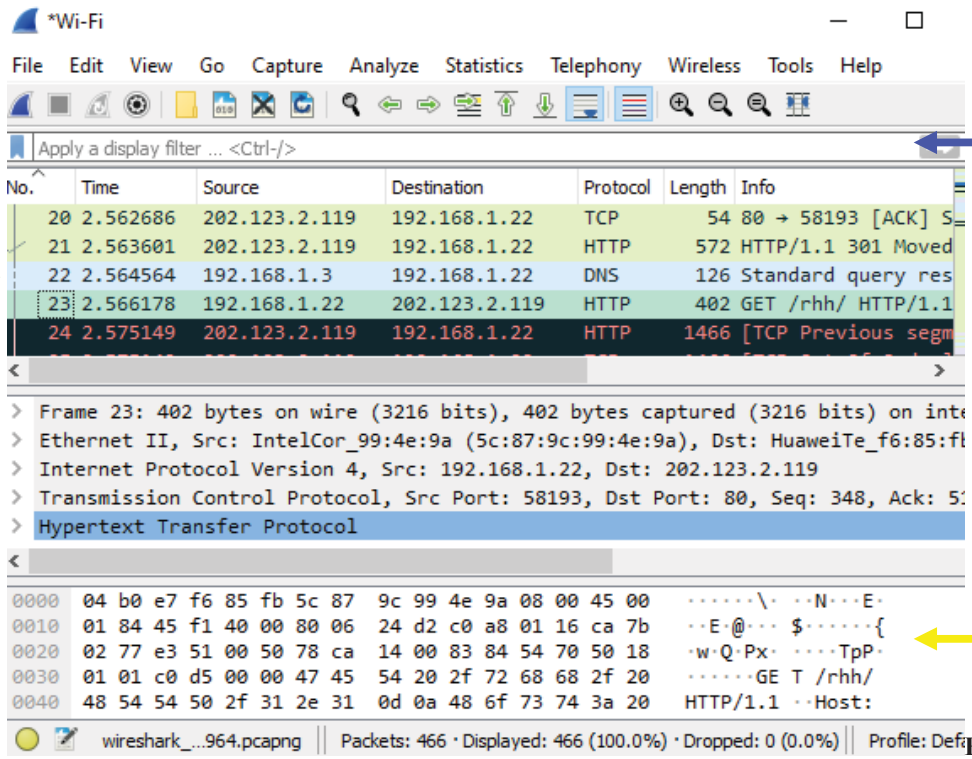


Figure 3

This is the main Wireshark interface. It consists of **four** major components:

The **packet-listing window** displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest level protocol that sent or received this packet.

The **packet-header details window** provides details about the packet selected (highlighted) in the packet listing window. (To select a packet in the packet listing window, place the cursor over the packet's one line summary in the packet listing window and click with the left mouse button.). These details include information about the Ethernet frame and its corresponding encapsulated PDUs. The amount of details displayed can be expanded or minimized by clicking on the arrows to the left of each PDU line in the packet details window. If the packet has been carried over TCP or UDP, these can also be expanded or minimized. Finally, details of the highest level protocol that sent or received data can also be obtained.

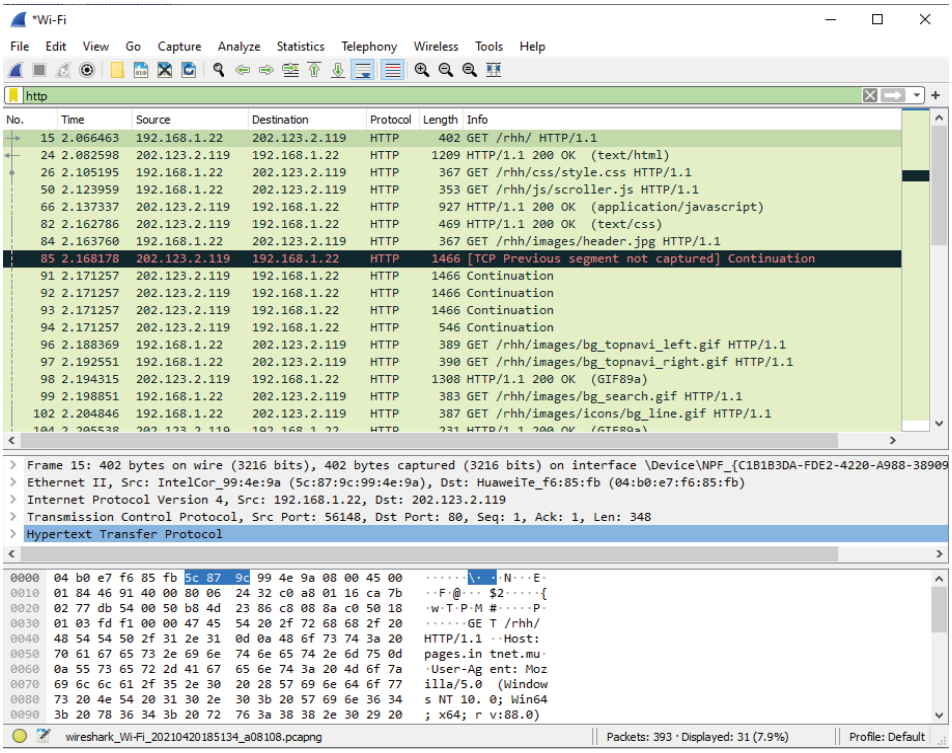
• The **packet-contents window** displays the contents of the captured frame in ASCII & Hexadecimal

• The **packet display filter field,** into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have Wireshark display only packets corresponding to HTTP messages.

Performing a filter using the Packet Display Filter field

You will notice that the packet-listing window consists of at many packets using numerous protocols. This can be overwhelming as sometimes you may wish to analyse only one specific kind of protocol. In this example, we will see how we can only filter HTTP messages.

1. Inside the packet display filter field, enter "http" and press Enter.
2. You should now only see HTTP messages in the packet-listing windows. It should look like below:



Answer the following questions based on your capture:

1. How long did it take from when the first HTTP GET message was sent until the respective HTTP response was received? (By default, the value of the Time column in the packet-listing window is in seconds)
2. What is the Internet address of the MT public pages webserver?
3. What is the Internet address of your computer?
4. Why were more GET messages needed to my old website?
5. What did your browser do before the first HTTP GET message was sent to the web server? *Hint: You will get the answer if you clear the filter by clicking on the cross button and examining the packets captured before the first HTTP GET messages.*

WireShark Lab 1 – HTTP

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

1. The Basic HTTP GET response interaction

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

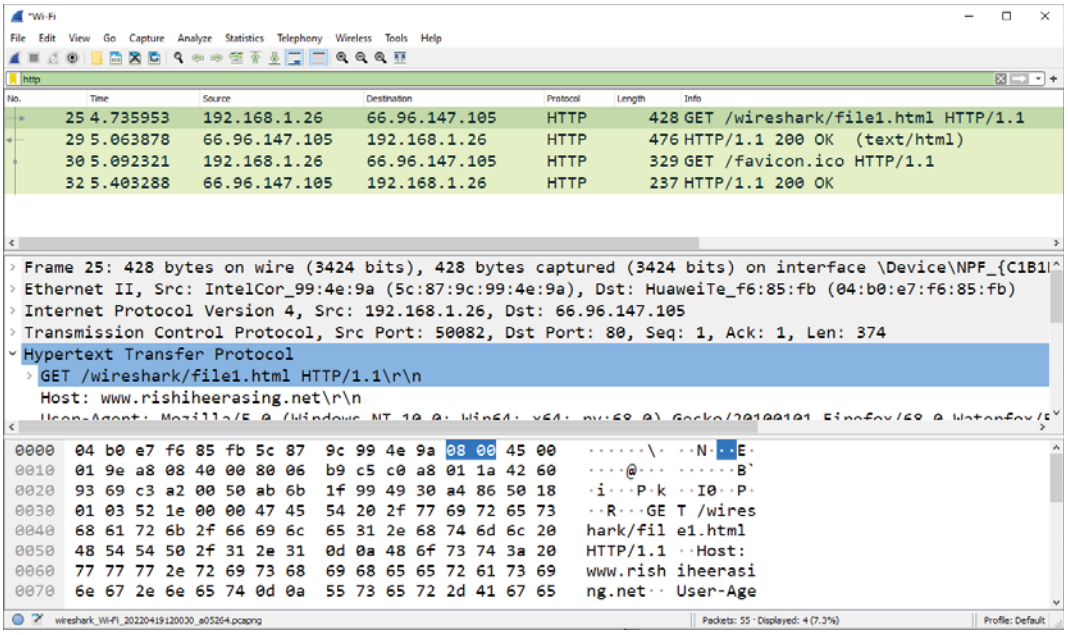


Fig. 1

The example in Fig. 1 shows in the packet-listing window that four HTTP messages were captured: the GET message (from your browser to the **www.rishiheerasing.net** web server) and the response message from the server to your browser. There are also two additional messages that are captured but this is dependent on your browser you used. The packet-contents window shows details of the selected message (in this case the HTTP GET message, which is highlighted in the packet-listing window). Recall that since the HTTP message was carried inside a TCP segment, which was carried inside an IP datagram, which was carried within an Ethernet frame, WireShark displays the Frame, Ethernet, IP, and TCP packet information as well. We want to minimize the amount of non-HTTP data displayed (we are interested in HTTP here, and will be investigating the other protocols is later labs), so make sure the boxes at the far left of the Frame, Ethernet, IP and TCP information have an greater than sign (>) (meaning there is hidden, not displayed information), and the HTTP line has a down arrow (v) (all information about the HTTP message is displayed).

By looking at the information in the HTTP request/response messages, **answer the following questions**. When answering the following questions, you should print out the request/response messages (see the WireShark Lab 0 for an explanation of how to do this) and indicate where in the message you've found the information. **(The questions below pertains to the first two messages captured only)**

1. Is your browser running HTTP version 1.0 or 1.1?
2. Which version of HTTP is the server running?
3. What languages (if any) does your browser indicate that it can accept to the server?
4. What is the IP address of your computer? Of the www.rishiheerasing.net server?
5. What is the status code returned from the server to your browser?
6. When was the HTML file you just retrieved last modified on the server?
7. How many bytes of content are being returned to your browser?

2. The HTTP CONDITIONAL GET/response interaction

Recall that most web browsers perform object caching and thus perform a conditional GET when retrieving an HTTP object. Before performing the steps below, make sure your browser's cache is empty. (For Google Chrome, enter the following in the address bar and press Enter: chrome://settings/privacy; then click Clear Browsing Data and ensure Cached Images and Files is ticked and click Clear Data. Now do the following:

A. Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
B. Start up the WireShark packet sniffer like before.
C. Enter the following URL into your browser: http://www.rishiheerasing.net/wireshark/file2.html
Press Enter. Your browser should display a very simple one line HTML page.
D. Once the page has loaded, reload the same page by clicking the Refresh icon on your browser or press F5.
E. Stop WireShark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

Answer the following questions:

8. Inspect the **first** HTTP GET request contents from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET message?
9. Inspect the **first** server response. Did the server explicitly return the contents of the file? How can you tell?
10. Now inspect the **second** HTTP GET request contents. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET message? If so, what information follows the "IF-MODIFIED-SINCE:" header?
11. What is the HTTP status code and phrase returned from the server in response to this **second** HTTP GET? Did the server explicitly return the contents of the file? Explain.

3. Retrieving Long Documents

In our examples thus far, the documents retrieved have been simple and short HTML files. Let's next see what happens when we download a long HTML file. Do the following:
A. Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
B. Start up the WireShark packet sniffer
C. Enter the following URL into your browser: http://www.rishiheerasing.net/wireshark/file3.html
Press Enter. Your browser should display the rather lengthy UTM Act 2002.
D. Stop WireShark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.
In the packet-listing window, you should see your HTTP GET message, followed by a multiple-packet response to your HTTP GET request. This multiple-packet response deserves a bit of explanation. Recall that the HTTP response

message consists of a status line, followed by header lines, followed by a blank line, followed by the payload. In the case of our HTTP response, the payload is the *entire* requested HTML file. The HTML content is rather large at 45,652 bytes. This is too large to fit in one single TCP packet. The single HTTP response message is thus broken into several pieces by TCP, with each piece being contained within a separate TCP segment. Each TCP segment is recorded as a separate packet by WireShark, and the fact that the single HTTP response was fragmented across multiple TCP packets is indicated by the "Continuation" phrase displayed by WireShark.

Answer the following questions:

12. How many HTTP GET request messages were sent by your browser?
13. How many data-containing TCP segments were needed to carry the single HTTP response?
14. What is the status code and phrase associated with the response to the HTTP GET request?
15. Are there any HTTP status lines in the data associated with a TCP induced "Continuation"?

4 HTTP Authentication

Finally, let's try visiting a web page that is password-protected and examine the sequence of HTTP message exchanged for such a site. The password protected page is actually the Post-Semester Site on my webpage.
The password is "**cndm**" (without the quotes). So let us access this "secure" password-protected page.

Do the following:
A. Start up your browser
B. Go to the following page in your browser: **http://www.rishiheerasing.net/protectedpost/login.php**
C. Once the page has fully loaded, start WireShark packet capture
D. Now enter the password given above in the text box and click on **Validate**. button (Note: Don't press Enter).
You will be then be brought to the CNDM Post-Semester page if you typed the password correctly.
E. Stop WireShark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

Now let's examine the WireShark output.

Answer the following questions:

16. Inspect the POST message contents, especially HTML Form URL encoded part. Do you see the password submitted in clear in the capture?
17. What should be done to ensure that the password and any other form data is encrypted?

The password 'cndm' that you entered can be found in the HTTP POST message sent to the server. If you scroll down in the contents window at the bottom, you should find the password in CLEAR !!!

Wireshark Lab 2 – Ethernet ARP

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

1. Capturing and analyzing Ethernet frames

Let's begin by capturing a set of Ethernet frames to study. Do the following:
A. First, make sure your browser's cache is empty. (*refer to previous labs.)*
B. Start up the Wireshark packet sniffer
C. Enter the following URL into your browser **http://www.rishiheerasing.net/wireshark/file3.html**
D. Stop Wireshark packet capture. First, note down the packet numbers (the leftmost column in the upper Wireshark window) of the HTTP GET message that was sent from your computer to **www.rishiheerasing.net**, as well as the first of the HTTP response message sent back to you. You should see a screen like Fig. 1 (where packet 175 in ***my screenshot*** contains the HTTP GET message).

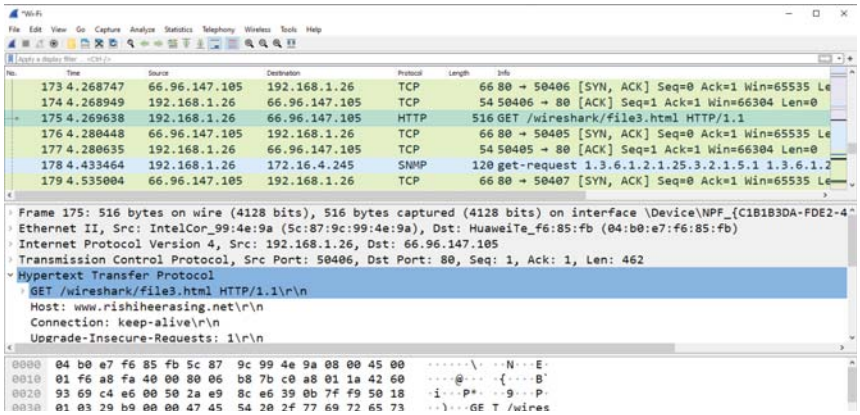


Fig. 1

Since this lab is about Ethernet and ARP, we're not interested in IP or higher layer protocols. So let's change Wireshark's "listing of captured packets" window so that it shows information only about protocols below IP. To have Wireshark do this, select *Analyze->Enabled Protocols*. Then uncheck the IPv4 box and select *OK*. You should now see a Wireshark window that looks like this:

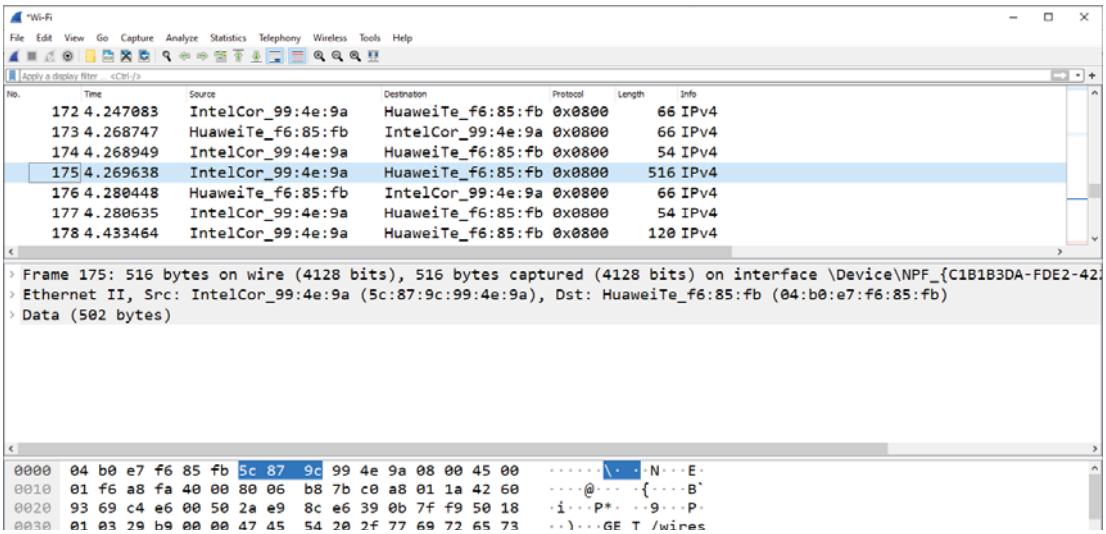


Fig. 2

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

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

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

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

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

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

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

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message (***Note****:You should have noted that down earlier*).

5. What is the value of the Ethernet source address? Is this the address of your computer, or of *www.rishiheerasing.net* webserver? (Hint: the answer is *No*). Which device has this as its Ethernet address?

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

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

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

2. The Address Resolution Protocol

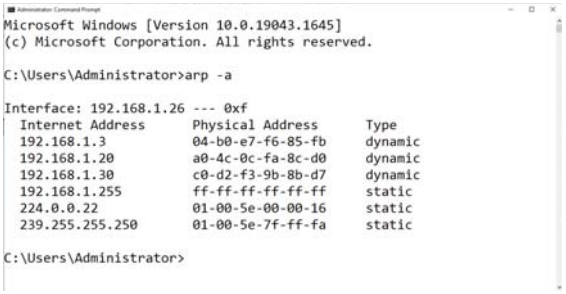
In this section, we'll observe the ARP protocol in action. I strongly recommend that you refresh yourself on this topic before proceeding.

ARP Caching

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

Let's take a look at the contents of the ARP cache on your computer:

• **MS-DOS.** Open a Command Prompt Window by typing *File->Run* and enter *cmd* then at the prompt enter *arp –a* and press Enter. *(Make sure you run as Administrator)*
The *arp –a* command will display the contents of the ARP cache on your computer. The screenshot below is the output on my computer:



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

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

• **MS-DOS.** The MS-DOS *arp –d ** command will clear your ARP cache. The *–d* flag indicates a deletion operation, and the * is the wildcard that says to delete all table entries. ***Note:*** *In Windows 7 and higher, the wildcard option does not work, so you will have to remove each entry individually using the command: arp -d [ip-address]*
E.g. arp -d 192.168.1.3 [You then repeat for the other entries and you check if it has cleared using arp -a]

Observing ARP in action

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

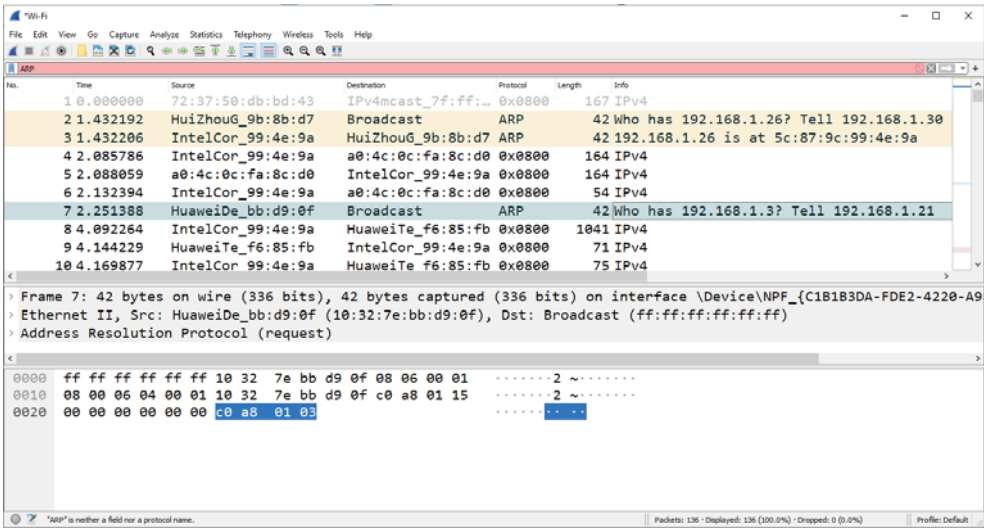


Fig. 3

In the example above, captured frames 2, 3 and 7 contain ARP messages.

Answer the following questions:

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

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

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

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

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

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

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

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

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

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

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

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

Extra Credit

EX-1. The *arp* command:

arp -s InetAddr EtherAddr

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

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

<>

UNIVERSITY of TECHNOLOGY, MAURITIUS

BSc (Hons) Computer Science with Network Security

Cohort: BCNS/16B/FT

Examinations for 2018 – 2019 / Semester 1

MODULE: COMMUNICATION & NETWORKING – DESIGN & MANAGEMENT

MODULE CODE: CAN 3102C

Duration: 2½ Hours

Instructions to Candidates:

1. **Attempt ALL FOUR questions.**
2. Start your answer to each question on a fresh page.
3. Each questions carry 25 marks.
4. Maximum marks achievable: 100
5. Silent calculators are allowed in the Examination Room.
6. Appendix is provided.

This question paper contains 4 questions and 6 pages.

QUESTION 1: (25 Marks)

a) "*One of the key attributes of an enterprise network is that it must be **multi-platform**.*"
Explain what you understand by this statement.

(2 marks)

b) Explain briefly why the building-block approach is now favoured instead of traditional network design. State the two main steps involved the technology design stage.

(3+3 marks)

c) Describe the following in relation to redundancy:
   i. RAID Level 10
   ii. Differential backup
   iii. Level 5 UPS

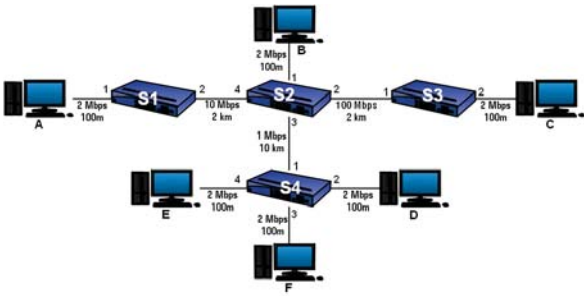
(4+2+2 marks)

d) In terms of performance, assuming a network with an *MTBF* of 6000 Hours and *MTTR* of 50 Hours:
   i. Calculate the percentage availability of the network.
   ii. Calculate the percentage reliability of such a network over a one-year period.
   iii. Estimate the average bandwidth between two hosts given that the RTT for a 64 bytes ICMP request-reply is 10 milliseconds and that for a 512 bytes ICMP request-reply is 200 milliseconds.

(2+3+4 marks)

QUESTION 2: (25 Marks)

a) The diagram below shows a network layout consisting of six hosts A, B, C, D, E and F with four switches S1, S2, S3 and S4 connecting them. The bandwidth and length of the links are also provided:



i. Calculate the ***one-way latency*** if Host A has to send 1200 bytes of data to Host D via switch S1, S2 and S4 which are all operating in ***Store-N-Forward*** mode and has a switching time of 1 millisecond per 100 bytes of data and assuming that the average speed of the signal in the links is $2x10^8$ m/s.

ii. Give the forwarding tables for each of the **four** switches after the 4 consecutive transmissions below:
   Host A to Host F,
   Host E to Host A,
   Host F to Host C,
   and Host C to Host A.

(5+8 marks)

[Please Turn Over]

b) The ASN.1 specification language is an integral part of the OSI Reference Model architecture, and is used in some protocols on the Internet. ASN.1 data objects are encoded for transmission using the Basic Encoding Rules (BER). Encode the following transmitted byte-stream in hexadecimal by using the following data type declarations and their corresponding instances:

```
name ::= OCTET STRING
value ::= INTEGER
true ::= BOOLEAN
{name, "RxBuffer"}
{value, 255}
{true, 1}
```

(4 marks)

c) In relation to network management, describe the following terms:
   i. SNMPv1 Trap message
   ii. Management Information Base.

(2+2 marks)

d) In respect to wireless network,
   i. Give one advantage of using IEEE 802.11a over the other flavours.
   ii. Give one advantage of using IEEE 802.11g over the other flavours.
   iii. Assume that you have a wireless access point that is using WEP, describe two ways in which you could make your wireless network more secure.

(1+1+2 marks)

QUESTION 3: (25 Marks)

a) Below is a network capture from a popular protocol analyzer utility. Give the **IPv4 destination** address in quad dotted decimal, the **total length** in bytes, the **upper layer protocol** for this datagram as well as the **destination port number** and deduce the **application layer protocol** used and determine whether this is a **request** or **response** message capture.

```
d0d0 4b4c ac37 84ef 187c 1460 0800 4500
0034 1084 4000 8006 5b9e c0a8 0107 ca7b
0277 c068 0017 ad01 bb22 0000 0000 8002
2000 95ca 0000 0204 05b4 0103 0308 0101
```

(2+2+2+2+2+2 marks)

b) Describe the essential features of a proxy server?

(5 marks)

c) What do you understand by data integrity? Give any one mechanism to enforce data integrity.

(2 marks)

d) What is a firewall? Describe the two main types of firewalls.

(2+4 marks)

QUESTION 4: (25 Marks)

A company occupies three floors of a building plus the basement. Each floor is occupied by one department and includes the office of one senior manager responsible for each department. Around 30 PCs having internet access are expected to be deployed on each floor. The basement accommodates several server machines. A high proportion of traffic remains within a single department. Much of the rest is access to the servers, though there is some inter-departmental traffic. For security reasons the senior managers should be accessible via a firewall router. The private internal network used: 192.168.17.0 /24. The company has Internet connectivity via an ADSL link from an ISP with a single, static, public Internet address: 202.123.21.124.

Draw a full network diagram for the company and make sure you identify any **network devices, transmission technology** and **media**. You must give the **IP**, **subnet mask** and **gateway** addresses for **all** devices and servers that you find pertinent to your design. You should show how a single public IP address can be shared among the whole staff and provide any special server configurations to. Give the network configuration for **1 staff PC** and **1 senior manager PC** from each department.

******END OF EXAM PAPER******

UNIVERSITY of TECHNOLOGY, MAURITIUS

BSc (Hons) Computer Science with Network Security
BEng (Hons) Telecommunication Engineering
BSc (Hons) Computing & Information Systems (Top-Up)

Cohorts: BCNS/17A/FT - BTEL/15B/FT – BCIS/19A/PT

Examinations for 2018 – 2019 / Semester 2

Examinations for 2019 / Semester 1

MODULE: COMMUNICATION & NETWORKING – DESIGN & MANAGEMENT

MODULE CODE: CAN 2103C

Duration: 2½ Hours

Instructions to Candidates:

1. **Attempt ALL FOUR questions.**
2. Start your answer to each question on a fresh page.
3. Each questions carry 25 marks.
4. Maximum marks achievable: 100
5. Silent calculators are allowed in the Examination Room.
6. Appendix is provided.

This question paper contains 4 questions and 6 pages.

QUESTION 1: (25 Marks)

a) How is internetworking different from interoperability?

(2 marks)

b) A logical network diagram is the deliverable at the end of the Needs Analysis stage in network planning. Briefly explain the different phases in this stage.

(6 marks)

c) Describe the following in relation to redundancy:

i. RAID Level 0+1
ii. Incremental backup
iii. Level 5 UPS

(4+2+2 marks)

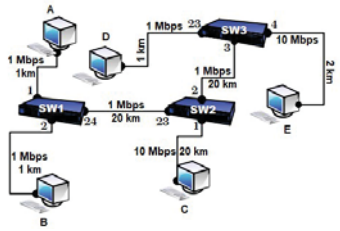
d) In terms of performance, assuming a network with an *MTBF* of 4800 Hours and *MTTR* of 120 Hours:

i. Calculate the percentage availability of the network.
ii. Calculate the percentage reliability of such a network over a one-year period.
iii. Estimate the average bandwidth between two hosts given that the RTT for a 32 bytes ICMP request-reply is 8 milliseconds and that for a 256 bytes ICMP request-reply is 16 milliseconds.

(2+3+4 marks)

QUESTION 2: (25 Marks)

a) The diagram below shows a network layout consisting of five hosts A to E with three switches SW1, SW2 and SW3 connecting them. The bandwidth and length of the links are as shown below:



(i) Calculate the ***one-way latency*** if **Host A** has to send 1500 bytes of data to **Host E** with all the switches operating in ***Store-N-Forward*** mode and has a switching time of 1 millisecond per 100 bytes of data and assuming that the average speed of the signal in the links is $2x10^8$ m/s.

(5 marks)

(ii) Assume that the forwarding table of the above switches are empty initially: Give the forwarding tables for each of the three switches after the four consecutive transmissions below:

1. Host A to Host E
2. Host D to Host A
3. Host E to Host C
4. Host C to Host D

(12X0.5 marks)

[Please Turn Over]

b) The ASN.1 specification language is an integral part of the OSI Reference Model architecture, and is used in some protocols on the Internet. ASN.1 data objects are encoded for transmission using the Basic Encoding Rules (BER). Given the following transmitted byte-stream in hexadecimal, identify the correct module identity and give the value in decimal of the module object it refers to:

06 08 31 33 36 31 32 31 34 33 02 02 07 5c

Direction of transmitted byte-stream

(4 marks)

c) In relation to network management, describe the following terms:

i. SNMPv1 Trap message
ii. Management Information Base.

(4+2 marks)

d) In respect to wireless network,

i. Give one advantage of using IEEE 802.11a over the other flavours.
ii. Give one advantage of using IEEE 802.11g over the other flavours.
iii. Assume that you have a wireless access point that is using WEP, describe two ways in which you could make your wireless network more secure.

(1+1+2 marks)

QUESTION 3: (25 Marks)

a) Please find below a capture from a popular protocol analyzer utility. Give the **destination** address in quad dotted decimal, the **total length** in bytes, the **upper layer protocol** for this datagram as well as the **source port number** and deduce the **application layer protocol** used and whether this is a **request** or **response** message capture.

```
d0d0 4b4c ac37 84ef 187c 1460 0800 4500
0039 1f37 4000 4006 8420 c0a8 0108 4260
9357 ff0f 0015 13ce 94ef 656a c69c 5018
433a 5160 0000 5354 4f52
```

(2+2+2+2+2+2 marks)

b) What do you understand by authentication?
Give one example of a mechanism to enforce authentication.

(4+1 marks)

c) What is a firewall? Describe the two main types of firewalls.

(2+6 marks)

QUESTION 4: (25 Marks)

A company occupies three floors of a building plus the basement. Each floor is occupied by one department and includes the office of one senior manager responsible for each department. Around 30 staff PCs having internet access are expected to be deployed on each floor. The basement accommodates several server machines. A high proportion of traffic remains within a single department. Much of the rest is access to the servers, though there is some inter-departmental traffic. For security reasons the senior managers should be accessible via a firewall router. The private internal network used: 172.16.0.0 / 16. The company has Internet connectivity via an ADSL link from an ISP with a single, static, public Internet address: 202.123.21.124.

Draw a full network diagram for the company and make sure you identify any **network devices, transmission technology** and **media**. You must give the **IP**, **subnet mask** and **gateway** addresses for **all** devices and servers that you find pertinent to your design. You should show how a single public IP address can be shared among the whole staff and provide any special server configurations to. Give the network configuration for **1 staff PC** and **1 senior manager PC** from each department.

******END OF EXAM PAPER******

UNIVERSITY of TECHNOLOGY, MAURITIUS

B.Sc. (Hons.) Computer Science with Network Security

Cohorts: BCNS/17B/FT

Examinations for 2019 – 2020 / Semester 1

MODULE: COMMUNICATION & NETWORKING DESIGN & MANAGEMENT
MODULE CODE: CAN3102C
Duration: 2½ Hours

Instructions to Candidates:

1. Attempt ALL **FOUR questions**.
2. Start your answer to each question on a fresh page.
3. Questions carry **equal** marks.
4. Maximum Marks = **100**
5. Silent calculators are allowed in the Examination Room.
6. Appendix provided

This question paper contains 4 questions and 7 pages.

ATTEMPT ALL 4 QUESTIONS

QUESTION 1: (25 Marks)

a) A Physical Network Diagram is the deliverable at the end of the Technology Design stage in the Building Block Approach to Network Design. Briefly describe the two different steps in this stage.

(6 marks)

b) Describe the following in relation to redundancy:

i. RAID Level 5
ii. Differential backup
iii. Level 5 UPS.

(4+2+3 marks)

c) In terms of performance, assuming a network with an *MTBF* of 2000 Hours and *MTTR* of 150 minutes:

i. Calculate the percentage availability of the network.
ii. Calculate the percentage reliability of such a network over a one-year period.
iii. Estimate the bandwidth between two hosts if an ICMP request-reply takes 99 ms for 100 bytes of data and 119 ms for 900 bytes of data.

(2+3+5 marks)

QUESTION 2: (25 Marks)

a) Below are two possible network topologies for a firm:

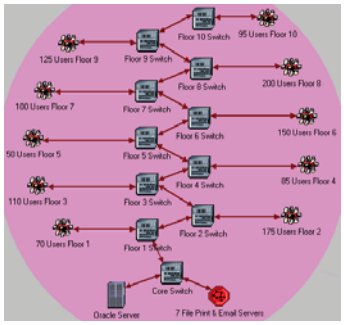


Figure 2.1

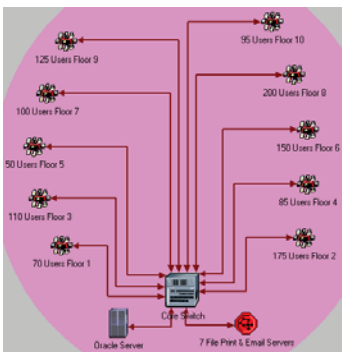


Figure 2.2

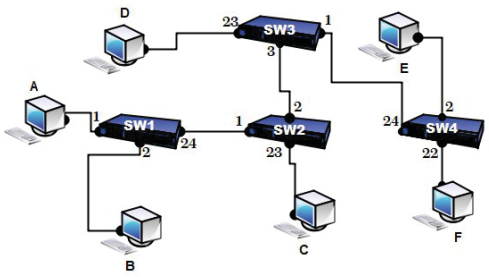
(P.T.O)

i. Identify the network topology in both Figure 2.1 and 2.2 above.
ii. In terms of latency, which topology is faster in accessing the Oracle Server?
iii. Calculate the total latency in transmitting a **1000 byte** frame from a user on the 10th floor till it is fully buffered by the Oracle server in Figure 1 assuming:
   1. Total cable run from a 10th floor user to the Oracle Server is **900** meters.
   2. Workgroup switches are "Store-N-forward". The core switch is "cut-through". Switching delay is **10** ms per 1000 bytes for all switches. The core switch starts retransmitting as soon as it has buffered 6 bytes.
   3. The network is 100-Base T/TX with signal propagation speed of 2 x10^8 m/s.

(2+1+5 marks)

b) Consider the arrangement of *self-learning* switches shown in the figure below. Assuming all forwarding tables are initially empty, give the forwarding tables for each of the 4 switches after the following consecutive transmissions:

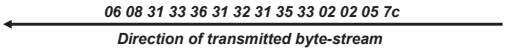
i. Host A to Host F
ii. Host F to Host D
iii. Host E to Host A
iv. Host D to Host E



(4 marks)

(P.T.O)

c) The ASN.1 specification language is an integral part of the OSI Reference Model architecture, and is used in some protocols on the Internet. ASN.1 data objects are encoded for transmission using the Basic Encoding Rules (BER). Given the following transmitted byte-stream in hexadecimal, identify the correct module identity and give the value in decimal of the module object it refers to:



(4 marks)

d) In relation to network management, describe the following terms:

v. SNMPv1 Trap message
vi. Management Information Base.

(2+1 marks)

e) With respect to the three WLAN standards, namely IEEE 802.11 a, b and g:

i. Give one distinct advantage of using IEEE 802.11a over the other flavours.
ii. Give one distinct advantage of using IEEE 802.11g over the other flavours.
iii. Sketch two common deployment modes for wireless LANs.
iv. Assuming you have a wireless access point already using WPA2, describe two ways in which you could make your wireless network even more secure.

(1+1+2+2 marks)

QUESTION 3: (25 Marks)

a) Find below a packet capture. Extract the **source MAC address**, the **destination IP address** in quad dotted decimal, the **source port number** and the **window size** for the segment. Deduce the **application layer protocol** used and decode the **application header content** as well.

```
565f 01ef 5cd2 dada 4b4c ac37 84ef 187c 1460 0800 4500
0040 b3d4 4000 4006 ef77 c0a8 010c 4260 9357 cdce 0015
7a3e b548 aeb5 5018 faa2 af8f 0000 5553 4552 2072 6973
6869 6865 6572 6173 696e 676e 6574 0d0a
```

(2+2+2+2+2+2 marks)

b) What do you understand by authentication? Give **two** mechanisms used to enforce authentication.

(2+2 marks)

c) Describe **two** different types of firewall.

(2+2 marks)

d) Give **five** features of a proxy server.

(5 marks)

QUESTION 4: (25 Marks)

A company occupies three floors of a building plus the basement. Each floor is occupied by one department and includes the office of one senior manager responsible for each department. About 30 PCs having internet access are expected to be deployed on each floor. The basement accommodates several server machines. A high proportion of traffic remains within a single department. Much of the rest is access to the servers, though there is some inter-departmental traffic. For security reasons the senior managers should be accessible via a firewall router. The private internal network used: 192.168.1.0. /24. The company has Internet connectivity via an ADSL link from an ISP with a single, static, public Internet address: 202.123.21.144.

Draw a full network diagram for the company and make sure you identify any **network devices, transmission technology** and **media**. You must give the **IP**, **subnet mask** and **gateway** addresses for **all** devices and servers that you find pertinent to your design. You should show how a single public IP address can be shared among the whole staff and provide any special server configurations to. Give the network configuration for **1 staff PC** and **1 senior manager PC** from each department.

*****END OF EXAM PAPER*****

UNIVERSITY of TECHNOLOGY, MAURITIUS

BSc (Hons) Computer Science with Network Security

BCNS/22A/FT

Examinations for 2024 / Semester 1

MODULE: NETWORKING – DESIGN & MANAGEMENT
MODULE CODE: BCNS 3105C
Duration: 2½ Hours

Instructions to Candidates:

1. **ATTEMPT ALL FOUR questions.**
2. Start your answer to each question on a fresh page.
3. Each question carries 25 marks.
4. Maximum marks achievable: 100
5. Silent calculators are allowed in the Examination Room.
6. 3-Page Appendix is provided.

This question paper contains 4 questions and 6 pages.

QUESTION 1: (25 MARKS)

a) Sketch a typical **hybrid star-ring** topology paying attention to how the clients and switching hubs are connected.

(3 marks)

b) With respect to an **Enterprise Network**,
   i. Describe briefly the **three** characteristics of such a network.
   ii. What are the **two** main goals of such a network?
   iii. Give **three** reasons for building such a network.

(3+2+3 marks)

c) The **Building Block Network Design** involves three phases; the needs analysis, the technology design and the cost assessment. Describe the steps involved in the **Technology Design** phase.

(6 marks)

d) In terms of **performance**, assuming a network with an **MTBF** of 12,000 Hours and **MTTR** of 30 days:
   i. Calculate the percentage **availability** of the network.
   ii. Calculate the percentage **reliability** of such a network over a **two-year** period.

(2+2 marks)

e) Given **four** disks, sketch the possible array configurations that you can implement in **RAID 5** showing how stripes A, B, C, D and E are written to each array configuration.
Give the effective size of each configuration if each disk has a size of 500 GB.

(4 marks)

QUESTION 2: (25 MARKS)

a)
   i. List the features of the three most common types of backup, giving an advantage and a disadvantage of each.
   ii. Give three advantages of using a dedicated backup software.

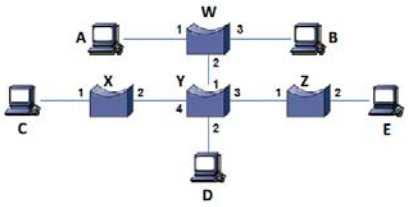
(6+3 marks)

b) Name the **three** categories of **UPS**, describing the power problems that are most appropriate to each category.

(3+3 marks)

c) Consider the arrangement of **self-learning bridges** shown in the figure below. Assuming all are initially empty, give the **forwarding tables** for each of the bridges W, X, Y and Z after the following successive transmissions:

- Host A sends to Host C,
- Host D sends to Host B,
- Host C sends to Host A,
- Host E sends to Host D,
- Host B sends to Host C.



(10 marks)

QUESTION 3: (25 Marks)

a) Consider a 100 Mbps Ethernet with a single **Store-N-Forward** switch mid-way in the path between two nodes A and B. Assume that there are no other nodes on the network and the distance between the two nodes is 5 kilometres. The propagation speed of the signal in the medium is 2 x10^8 m/s. Error detection at the switch introduces an average delay of 10 microseconds per 100 bytes of frame data. *(Assume all other delays to be negligible.)*

   i. What is the total transfer time (from the first bit sent by A to the last bit received by B) for a **1,000-byte** frame?
   ii. Same as (i) but the switch now operates **"cut-through"** mode and can retransmit the frame as soon as the first **400 bits** have been buffered.

(5+4 marks)

b) The **ASN.1** specification language is an integral part of the OSI Reference Model architecture, and is used in some protocols on the Internet. ASN.1 data object are encoded for transmission using the **Basic Encoding Rules** (BER). Give an example of a transmitted byte-stream in hexadecimal by using the following module of data type declarations and its corresponding instances:

```
Player: = OCTET STRING, Year: = INTEGER, Active: = BOOLEAN
{Player, "Leo"}, {year, 1987}, {Active, 1}
```

(6 marks)

c)
   i. Give the structures of typical SNMPv1 **get** and **trap messages**.
   ii. Which **MODULE IDENTITY** does this OBJECT ID belong to:

```
1.3.6.1.2.1.7.1
```

(8+2 marks)

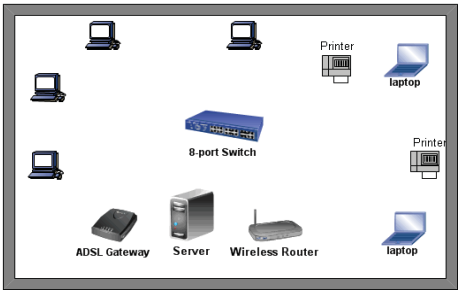
QUESTION 4: (25 Marks)

a) From the capture below: Give the datagram **source IP** address, **upper layer protocol**, **total length** in *decimal* and **header checksum** in *hexadecimal*; the segment **source port number** in *decimal* and hence deduce the **application layer protocol** used and whether the capture relates to a **request** or to a **response** message:

```
00 22 fa 05 78 7c 04 b0 e7 f6 85 fb 08 00 45 40
01 68 20 fa 40 00 35 06 a1 11 6d ec 52 94 c0 a8
01 1c 00 15 c9 69 37 f0 38 46 be 0b 22 f1 50 18
```

(1+1+2+1+1+2+2 marks)

b) A UTM graduate has been told to configure a small branch office to provide internal and external network connectivity. The office consists of 6 clients (4 wired and 2 wireless laptops), 1 server with two Ethernet network adapters, 2 network printers, 1 wireless router, one 8-port Ethernet switch and 1 basic ADSL gateway. All the clients will be on dynamic IP addressing and there is need for content filtering on the Internet. Staff are not allowed to access certain external sites e.g. Facebook or download some specific content such as mp3 files.
The layout of the office is given below:



[P.T.O]

Sketch a suitable physical network diagram for the office bearing in mind sound design principles. Your diagram should show how you would interconnect the devices present. You should mention specific system software, as well as the topology, the network class you will be using. You should describe how you would configure specific services, for example, Firewall and DHCP on the server. Additionally, you should give the sample network configuration, for the IP addressing scheme you have chosen, of one network printer; of the wireless router, of both network interfaces on the server and of the ADSL gateway.

(15 marks)

******END OF EXAM PAPER******

UNIVERSITY of TECHNOLOGY, MAURITIUS

B.Sc. (Hons.) Computer Science with Network Security

Cohort: BCNS/21A/FT

Examinations for 2023 / Semester 1

MODULE: Communication & Networking Design & Management
MODULE CODE: CAN 2103C
Duration: 2½ Hours

Instructions to Candidates:

1. Attempt **ALL FOUR QUESTIONS**.
2. Questions carry **equal** marks.
3. Maximum marks achievable = **100**
4. Silent calculators are allowed in the Examination Room.
5. Appendix is provided.

This question paper contains 4 questions and 5 pages.

ATTEMPT ALL FOUR QUESTIONS

QUESTION 1 (25 Marks)

a) Describe **four (4)** issues that are usually addressed in the **Needs Analysis** phase in the building-block approach to network design.

(4 marks)

b) Sketch a typical **hybrid star-bus** topology paying attention how the clients and switching hubs are connected.

(3 marks)

c)

i) What do you understand by MTTR?
ii) Calculate the annual downtime to the **nearest hour** if the availability of a network is **70%**.
iii) Calculate the percentage reliability of a system which suffers on average **4 failures per year** over **90 days**.

(3+2+3 marks)

d) Differentiate between each of the following:

i) **Packet-level** and **Application-level** firewalls
ii) **Incremental** and **Differential** backup modes

(2+2 marks)

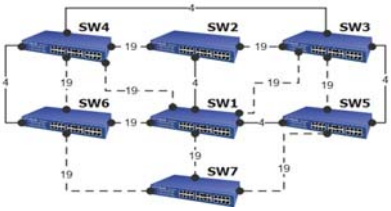
e) Using **all of eight** hard disks, sketch the array configuration that will provide **maximum redundancy** under **each** of **RAID 0+1** and **RAID 10** mode and show how stripes A, B, C, D, and E are written to each array. Give the total effective size of each array configuration if each hard disk has a size of **40 GB.**

(6 marks)

QUESTION 2 (25 Marks)

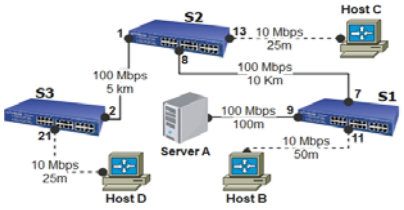
a) Consider the network layout below consisting of seven switches. SW1 has the lowest BridgeID and is the Root Bridge, while SW7 has the highest BridgeID in that order. All the switches use STP. Full links and dotted links have a path cost 4 and 19 as shown. Redraw the network diagram in your exam booklet and clearly:

i) Label all the root ports (RP), designated ports (DP) and blocking ports (BP)
ii) Give the final loop free topology with the blocked links removed.



(7.5 + 0.5 marks)

b) Consider the network topology below, consisting of three switches all operating in Store-N-Forward mode, and signal propagation speed is assumed to be **2x10^8** m/s. The switching delay is 1 ms per 100 bytes of data for all switches.



i) Calculate the one-way latency if 1500 byte is sent from Server A to Host D.
ii) Give the **forwarding tables** for each switch after the following **four** successive transmissions: Server A sends to Host D; Host D sends to Host B; Host C sends to Host D and Host C sends to Server A.

(8+9 marks)

QUESTION 3 (25 Marks)

a) In respect to wireless LANs,
   i) Give one (1) advantage of using IEEE 802.11a over the other flavours.
   ii) Give one (1) advantage of using IEEE 802.11g over the other flavours.
   iii) Sketch two (2) common deployment modes for wireless LANs.
   iv) Assume that you have a wireless access point that is using WEP; describe three (3) ways in which you could make your wireless network more secure.

(2+2+4+3 marks)

b) The **ASN.1** specification language is an integral part of the OSI Reference Model architecture, and is used in some protocols on the Internet. ASN.1 data objects are encoded for transmission using the **Basic Encoding Rules** (BER). Give an example of a transmitted byte-stream by using the following module of data type declarations and its corresponding instances:

title ::= OCTET STRING, year ::= INTEGER, hit ::= BOOLEAN
{title, "Avatar"}, {year, 2009}, {hit, "1"}

(6 marks)

c) Give the format of a typical **get message** and a **trap message** under SNMPv1.

(8 marks)

QUESTION 4: (25 Marks)

a) Below is a capture of an **Ethernet II** frame which contains an **IPv4** packet and a segment. Give the **source MAC address** in *hexadecimal*; the **source IP** address, the **upper layer protocol**, the **TTL** and the **header checksum** in *decimal*; the **source port number** in *decimal* and deduce the **application layer protocol** used:

```
5c87 9c99 4e9a 04b0 e7f6 85fb 0800 4550
0044 add6 4000 ef06 460b 4260 9357 c0a8
0122 0015 da1f 0822 422a
```

(7 marks)

b) A company occupies three floors of a building plus the basement. Each floor is occupied by one department and includes the office of one senior manager responsible for each department. About 30 PCs having internet access are expected to be deployed on each floor. The basement accommodates several server machines. A high proportion of traffic remains within a single department. Much of the rest is access to the servers, though there is some inter-departmental traffic. For security reasons the senior managers should be accessible via a firewall router. The private internal network used: 192.168.10.0 /24. The company has Internet connectivity via an ADSL link from an ISP with a single, static, public Internet address: 202.123.21.123.

Draw a full network diagram for the company and make sure you identify any **network devices, transmission technology** and **media**. You must give the **IP**, **subnet mask** and **gateway** addresses for **all** devices and servers that you find pertinent to your design. You should show how a single public IP address can be shared among the whole staff and provide any special server configurations to. Give the network configuration for **1 staff PC** and **1 senior manager PC** from each department.

(18 marks)

******END OF EXAMINATION PAPER******

UNIVERSITY of TECHNOLOGY, MAURITIUS

BSc (Hons) Computer Science with Network Security

BCNS/22B/FT

Examinations for 2024-25 / Semester 1

MODULE: NETWORKING – DESIGN & MANAGEMENT
MODULE CODE: BCNS 3105C
Duration: 2½ Hours

Instructions to Candidates:

1. **ATTEMPT ALL FOUR questions.**
2. Start your answer to each question on a fresh page.
3. Each question carries 25 marks.
4. Maximum marks achievable: 100
5. Silent calculators are allowed in the Examination Room.
6. 3-Page Appendix is provided.

This question paper contains 4 questions and 6 pages.

QUESTION 1: (25 MARKS)

a) Sketch a typical **hybrid star-ring** topology paying attention to how the clients and switching hubs are connected.

(3 marks)

b) With respect to an **Enterprise Network**,
   i. Describe briefly the **two** characteristics of such a network.
   ii. What are the **two** main goals of such a network?

(2+1 marks)

c) The **Building Block Network Design** involves three phases; the needs analysis, the technology design and the cost assessment. Describe the steps involved in the **Technology Design** phase.

(6 marks)

d) In terms of **performance**, assuming a network with an **MTBF** of 20,000 Hours and **MTTR** of 30 days:
   i. Calculate the percentage **availability** of the network
   ii. Calculate the **annual** percentage **reliability** of such a network
   iii. Estimate the bandwidth between two hosts if the average ICMP request-reply response time is **12 ms** for a **128-byte** ICMP packet and **22 ms** for a **1128**-byte ICMP packet.

(2+2+3 marks)

e)
   i. List the features of the three most common types of backup modes, giving an advantage and a disadvantage of each.
   ii. Give three advantages of using a dedicated backup software.

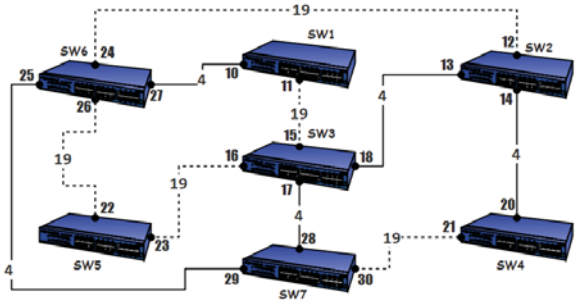
(6 marks)

QUESTION 2: (25 MARKS)

a) Consider the network layout below consisting of seven switches (SW1 to SW7). You can assume that SW1 has the lowest BridgeID whilst SW7 has the highest BridgeID in the same order. All switches support STP. Cost for links and Port IDs are as shown below.

Redraw the network diagram in your exam booklet and clearly:

i. Label the root bridge (RB), root (RP), designated (DP) & blocking (BP) ports.
ii. Redraw the final loop-free topology with the blocked ports and links removed.



(10+1 marks)

b) Assuming that Host A to Host G are connected to SW1 to SW7 at Port 1 to Port 7 **respectively** from the topology obtained in a(ii) above, give the **forwarding tables** for **each of the seven** switches after the following **four** successive transmissions:

i. Host E sends to Host B;
ii. Host G sends to Host E;
iii. Host D sends to Host B;
iv. Host B sends to Host D.

(14 marks)

QUESTION 3: (25 MARKS)

a) Consider a 1 Gbps Ethernet with a single **Store-N-Forward** switch mid-way in the path between two nodes A and B. Assume that there are no other nodes on the network and the distance between the two nodes is 2 kilometres. The propagation speed of the signal in the medium is 2 $x10^8$ m/s. Error detection at the switch introduces an average delay of 1 microsecond per 100 bytes of frame data. *(Assume all other delays to be negligible.)*

i. What is the total transfer time (from the first bit sent by A to the last bit received by B) for a **1,200-byte** frame?
ii. Same as (i) but the switch now operates **"cut-through"** mode and can retransmit the frame as soon as the first **960 bits** have been buffered.

(5+4 marks)

b) The **ASN.1** specification language is an integral part of the OSI Reference Model architecture, and is used in some protocols on the Internet. ASN.1 data object are encoded for transmission using the **Basic Encoding Rules** (BER). Give an example of a transmitted byte-stream in hexadecimal by using the following module of data type declarations and its corresponding instances:

```
ProductID: = OCTET STRING, Year: = INTEGER, Status: = BOOLEAN
{Player, "HP1102w"}, {year, 2023}, {Status, 1}
```

(6 marks)

c)

i. Give the structures of typical SNMPv1 **get** and **trap messages**.
ii. Which **MODULE IDENTITY** does this OBJECT ID belong to:

```
1.3.6.1.2.1.7.11
```

(8+2 marks)

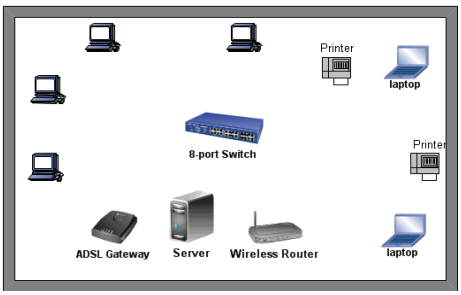
QUESTION 4: (25 Marks)

a) From the capture below: Give the datagram **Destination IP** address, **upper layer protocol** in *decimal* and **header checksum** in *hexadecimal*; the segment **source port number** in *decimal* and hence deduce the **application layer protocol** used; state whether this capture relates to a **request** or **response** message and finally decode the **application message**:

```
2c 7b a0 6f 84 bb 04 b0 e7 f6 85 fb 08 00 45 54
00 3a 83 38 40 00 38 06 3c e9 6d ec 52 94 c0 a8
01 20 00 15 e3 f0 85 62 2d 9b c6 8f d3 9a 50 18
00 e5 1a 3f 00 00 32 33 34 20 41 55 54 48 20 54
4c 53 20 4f 4b 2e 0d 0a
```

(1+1+1+1+1+1+4 marks)

b) A UTM graduate has been told to configure a small branch office to provide internal and external network connectivity. The office consists of 6 clients (4 wired and 2 wireless laptops), 1 server with two Ethernet network adapters, 2 network printers, 1 wireless router, one 8-port Ethernet switch and 1 basic ADSL gateway. All the clients are on dynamic IP addressing and there is need for Internet content filtering. Staff are not allowed to access certain external sites e.g. Facebook or download some specific content such as mp3 files. The layout of the office is given below:



[P.T.O]

Sketch a suitable physical network diagram for the office bearing in mind sound design principles. Your diagram should show how you would interconnect the devices present. You should mention specific system software, as well as the topology, the network class you will be using. You should describe how you would configure specific services, for example, Firewall and DHCP on the server. Additionally, you should give the sample network configuration, for the IP addressing scheme you have chosen, of one network printer; of the wireless router, of both network interfaces on the server and of the ADSL gateway.

(15 marks)

******END OF EXAM PAPER******

UNIVERSITY of TECHNOLOGY, MAURITIUS

BSc (Hons) Computer Science with Network Security

BCNS/23A/FT1 - BCNS/23A/FT2 - BCNS/21B/PT

Examinations for 2024-25 / Sem 2 - 2025 / Sem 1

MODULE: NETWORKING – DESIGN & MANAGEMENT
MODULE CODE: BCNS 3105C / BCNS 3205C
Duration: 2½ Hours

Instructions to Candidates:

1. **ATTEMPT ALL FOUR questions.**
2. Start your answer to each question on a fresh page.
3. Questions **DO NOT** carry equal marks.
4. Maximum marks achievable: 100
5. Silent calculators are allowed in the Examination Room.
6. 3-Page Appendix is provided.

This question paper contains 4 questions and 6 pages.

QUESTION 1: (22 MARKS)

a) Sketch a typical **hybrid star-bus** topology paying attention to how the clients and switching hubs are connected.

(3 marks)

b) The **Building Block Approach Model** involves three phases; Needs Analysis, Technology design and Cost Assessment. Describe the steps involved in the **Technology Design** phase.

(6 marks)

c) In terms of **performance**, assume a network with an **MTBF** of 50,000 Hours and an **MTTR** of 7 days:
   i. Calculate the percentage **availability** of the network
   ii. Calculate the **annual** percentage **reliability** of such a network
   iii. Estimate the bandwidth between two hosts if the average ICMP request-reply response time is **8 ms** for a **256-byte** ICMP packet and **24 ms** for a **1024-byte** ICMP packet.

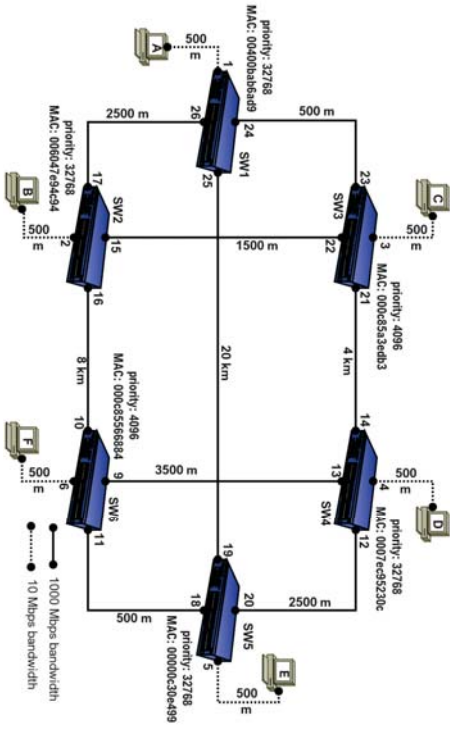
(2+3+2 marks)

d) Using **eight** hard disk drives of capacity of **100GB** each and showing how **five** stripes A to E are to be written, sketch the layout which will provide **maximum redundancy** and give the **effective size** under each of the array configuration:
   i. RAID 10;
   ii. RAID 0+1.

(6 marks)

QUESTION 2: (32 MARKS)

a) Consider the network layout below consisting of six STP switches (SW1 to SW6).



Please Turn Over

Redraw the network diagram, ignoring hosts A to F, and clearly:

   i. Label the root bridge (RB), root (RP), designated (DP) & blocking (BP) ports.
   ii. Redraw the final loop-free topology with the blocked links removed.

(10+1 marks)

b) Hosts A to F are connected to SW1 to SW6 at Port 1 to Port 6 **respectively** from the topology obtained in a(ii) above, give the **forwarding tables** for **each of the six** switches after the following **four** successive transmissions:

   i. Host E sends a frame to Host B;
   ii. Host F sends a frame to Host E;
   iii. Host D sends a frame to Host B;
   iv. Host B sends a frame to Host D.

(12 marks)

c) Assume that all the switches operate in **Store-N-Forward** mode. The propagation speed of the signal in the medium is $2x10^8$ m/s. Error detection at each switch introduces an average delay of **1 microsecond per 500 bytes** of frame data. *(Assume all other delays to be negligible.)*

   i. What is the total latency from the first bit sent by **Host A** to the last bit received by **Host C** for a **1,500-byte** frame?
   ii. Same as c(i) above but assume that **SW4**, **SW5** and **SW6** operate in **"cut-through"** mode and can retransmit the frame as soon as the first **600 bits** have been buffered. What is the new total latency for the same transfer?

(6+3 marks)

QUESTION 3: (16 MARKS)

a) The **ASN.1** specification language is an integral part of the OSI Reference Model architecture, and is used in some protocols on the Internet. ASN.1 data object are encoded for transmission using the **Basic Encoding Rules** (BER). Give the hexadecimal encoded byte-stream by using the following data type declarations and its corresponding instances:

```
Device: = OCTET STRING, Year: = INTEGER, OID: = OBJECT IDENTIFIER
{Device, "Switch"}, {year, 2025}, {OID, 1.3.6.1.2.1.1.3}
```

(6 marks)

b)

i. Give the structures of typical SNMPv1 **get** and **trap messages**.

ii. Which **MODULE IDENTITY** does this OBJECT ID belong to:

1.3.6.1.2.1.1.3

(8+2 marks)

QUESTION 4: (30 Marks)

a) From the capture below: extract the **source MAC** address; the **destination IP** address, the datagram **upper layer protocol** and **total length** in *decimal*; the segment **destination port** number and **length** in *decimal* and hence deduce the **application layer protocol** used; state whether this capture relates to a **request** or **response** message:

```
2c 7b a0 6f 84 bb 9e 55 eb 96 e8 f0 08 00 45 00
00 45 de fc 40 00 40 11 d8 20 c0 a8 01 1f c0 a8
01 1b 9e 38 00 a1 00 31 3d 46 30 27 02 01 01 04
06 70 75 62 6c 69 63 a1 1a 02 04 7d 75 bd 46 02
01 00 02 01 00 30 0c 30 0a 06 06 2b 06 01 02 01
```

(1+1+1+1+1+2+2+1 marks)

Please Turn Over

b) A company has recently subscribed for a 100 Mbps SDSL connection from its ISP and has been allocated a single public IP **202.123.21.121.**

- You are required to design and configure a network for the company which shall consists of **6 internal subnets** (each with Internet connectivity).
- 5 of the 6 subnets are assumed to have **25 wired PC, one file server, one internal web server** and **one network printer.**
- One of the 6 subnets shall have an Access Point with **28 laptops** connected to it.
- You are expected to use a Class C internal network: **192.168.31.0**
- Finally, **all 6 subnets** should make use of **dynamic IP addressing**.

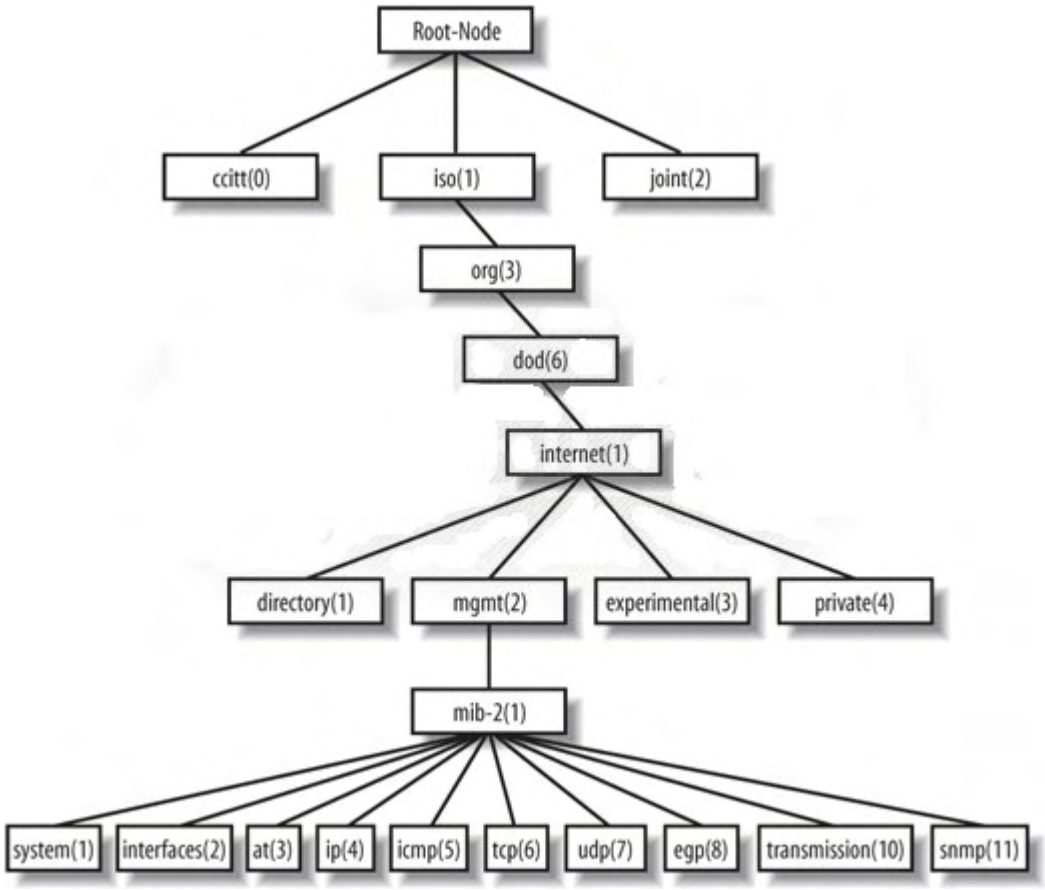
Draw the network layout and giving network configuration about:

- *Any pertinent additional devices or servers that may be required.*
- *Give the IP address, Subnet mask and Gateway address of one host and one printer from each of the 5 wired subnets and one host from the wireless subnet.*
- *You have to mention the internal subnet mask used to achieve the network requirements above.*
- *For minimum security, you are expected to make use of a Proxy Server or Firewall in the network.*

(20 marks)

******END OF EXAM PAPER******

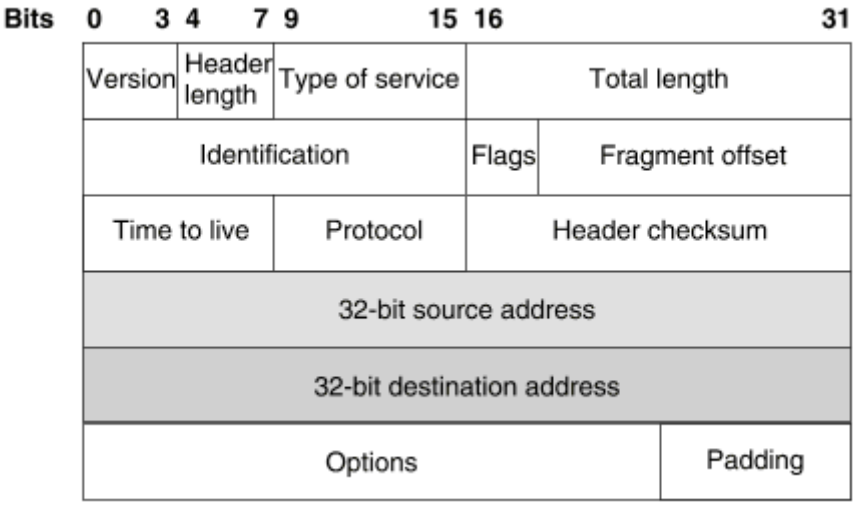
Object Identifier Tree



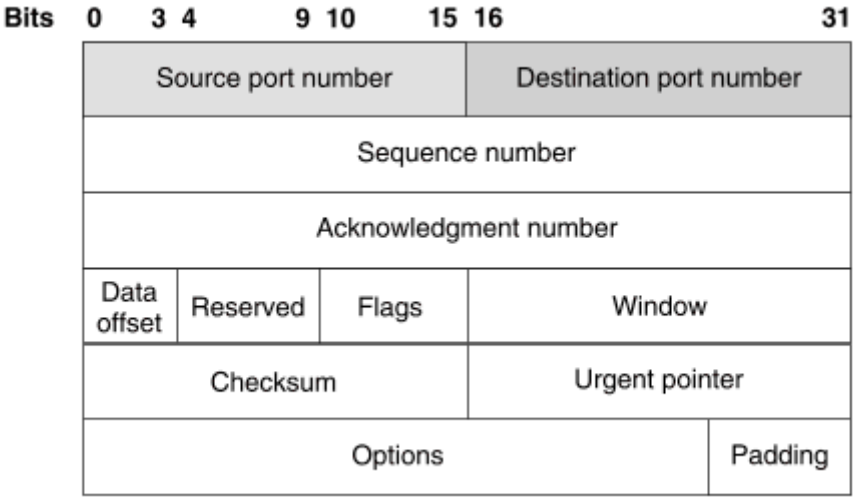
ASN.1 Universal Tag Type

Tag Value	Type
1	Boolean
2	Integer
3	Bit String
4	Octet String
5	Null
6	Object Identifier
9	Real

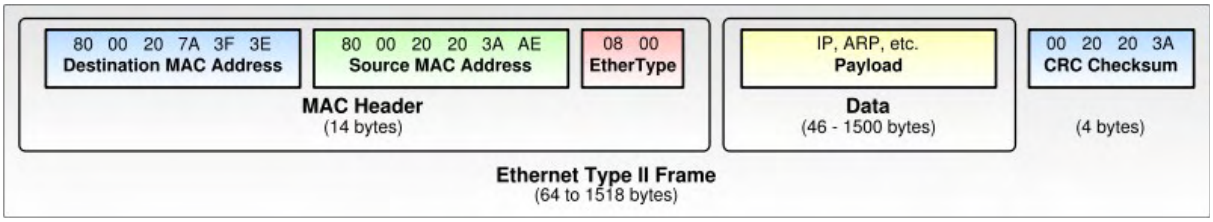
IPv4 (RFC 791) Datagram format



TCP (RFC 793) Segment format



Ethernet II frame format



ASCII Character Set

Low Order Bits		*High Order Bits* 0000 **0**	0001 **1**	0010 **2**	0011 **3**	0100 **4**	0101 **5**	0110 **6**	0111 **7**
0000	**0**	NUL	DLE	Space	0	@	P	`	p
0001	**1**	SOH	DC1	!	1	A	Q	a	q
0010	**2**	STX	DC2	“	2	B	R	b	r
0011	**3**	ETX	DC3	#	3	C	S	c	s
0100	**4**	EOT	DC4	$	4	D	T	d	t
0101	**5**	ENQ	NAK	%	5	E	U	e	u
0110	**6**	ACK	SYN	&	6	F	V	f	v
0111	**7**	BEL	ETB	‘	7	G	W	g	w
1000	**8**	BS	CAN	(	8	H	X	h	x
1001	**9**	HT	EM	)	9	I	Y	i	y
1010	**A**	LF	SUB	*	:	J	Z	j	z
1011	**B**	VT	ESC	+	;	K	[	k	{
1100	**C**	FF	FS	,	<	L	\	l	|
1101	**D**	CR	GS	-	=	M	]	m	}
1110	**E**	SO	RS	.	>	N	^	n	~
1111	**F**	SI	US	/	?	O	_	o	DEL