Chapter 3:
Security Part I: Auditing Operating Systems and Networks

IT Auditing, Hall, 4e

Learning Objectives

- Be able to identify the principal threats to the operating system and the control techniques used to minimize the possibility of actual exposures.
- Be familiar with the principal risks associated with commerce conducted over intranets and the Internet and understand the control techniques used to reduce these risks.
- Be familiar with the risks associated with personal computing systems.
- Recognize the unique exposures that arise in connection with electronic data interchange (EDI) and understand how these exposures can be reduced.

Operating System Control Objectives

- Protect itself against tampering by users.
- Protect users from accessing, destroying, or corrupting another user’s programs or data.
- Safeguard users’ application modules from destroying or corrupting other modules.
- Safeguard its own modules from destroying or corrupting other modules.
- Protect itself from its environment including power failures and other disasters.

Operating Systems Security

- **Log-On Procedure**:
  - First line of defense against unauthorized access consisting of user IDs and passwords.
- **Access Token:**
  - Contains key information about the user which is used to approve actions attempted during the session.
- **Access Control List:**
  - Assigned to each IT resource and used to control access to the resource.
- **Discretionary Access Privileges:**
  - Allows user to grant access to another user.

Threats to Operating System Integrity

- Accidental threats include hardware failures and errors in user applications.
- Intentional threats are often attempts to illegally access data or violate privacy for financial gain.
- Growing threat is destructive programs with no apparent gain, which come from three sources:
  - Privileged personnel who abuse their authority.
  - Individuals who browse the operating system to identify and exploit security flaws.
  - Individuals who insert viruses or other destructive programs into the operating system, either intentionally or unintentionally.

Operating Systems Controls

- **Access Privileges** - Audit Objectives:
  - Verify that access privileges are consistent with separation of incompatible functions and organization policies.
- **Access Privileges** - Audit Procedures:
  - Review policies for separating incompatible functions.
  - Review a sample of user privileges, especially access to data and programs.
  - Review security clearance checks of privileged employees.
  - Determine if users have formally acknowledged their responsibility to maintain data confidentiality.
  - Review users' permitted log-on times.

Password Controls

- A **password** is a secret code user enters to gain access to system or data.
- Common contra-security behaviors:
  - Forgetting passwords or failing to regularly change them.
  - Post-it-syndrome which puts passwords on display.
  - Simplistic passwords that are easy for criminals to anticipate.
- Most commonly passwords are **reusable**.
  - Management should require changes and disallow weak ones.
- **One-time passwords** are automatically generated constantly by the system when user enters a PIN.

Operating Systems Controls

- **Password Control** - Audit objectives:
  - Ensure adequacy and effectiveness of password policies for controlling access to the operating system.
- **Password Control** - Audit procedures:
  - Verify passwords are required for all users and that new users are instructed in their use and importance.
  - Ensure controls requiring passwords to be changed regularly.
  - Review password file for weak passwords.
  - Verify encryption of the password file.
  - Assess the adequacy of password standards.
  - Review account lockout policies and procedures.

Controlling Against Malicious & Destructive Programs

- Organizations can reduce threats:
  - Purchase software from reputable vendors in original packages.
  - Policy pertaining to unauthorized or illegal software.
  - Examine upgrades and public-domain software for viruses before implementation and use.
  - Implement procedures for changing programs.
  - Educate users regarding threats.
  - Test all applications before implementation.
  - Make frequent backups and limit users to read and execute rights only whenever possible.
  - Require protocols to bypass Trojan horses and use antiviral software.

Operating System Controls

- **Viruses & Destructive Programs** - Audit objectives:
  - Verify effectiveness of procedures to protect against programs such as viruses, worms, back doors, logic bombs, and Trojan horses.
- **Viruses & Destructive Programs** - Audit procedures:
  - Interviews to determine that operations personnel have been properly educated and are aware of risks.
  - Verify new software is tested on standalone workstations before being implemented.
  - Verify that antiviral software is current and that upgrades are frequency downloaded.

System Audit Trail Controls

- **System audit trails** are logs that record activity at the system, application and use level.
- Two types of audit logs:
  - **Keystroke monitoring** involves recording user's keystrokes and the system's response.
  - **Event monitoring** summarizes key activities related to system resources.
- Audit trails can be used to: detect unauthorized access, reconstruct events and promote personal accountability.
- Benefits must be balanced against costs.

Operating System Controls

- **System Audit Trails-** Audit objectives:
  - Ensure established system audit trail is adequate for preventing and detecting abuses, reconstructing key events and planning resource allocation.
- **System Audit Trails-** Audit procedures:
  - Verify audit trail has been activated per company policy.
  - Use data extraction tools to search for defined conditions such as: unauthorized users; periods of inactivity; periods of activity including log-on and log-off times; failed log-on attempts; and specific access.
  - Sample security violation cases and evaluate their disposition to assess security group effectiveness.

Intranet Risks

- Intercepting network messages:
  - Sniffing: Interception of user IDs, passwords, confidential e-mails, and financial data files.
- Accessing corporate databases:
  - Connections to central databases increase risk data will be accessible to employees.
- Privileged employees:
  - Overrides may allow unauthorized access critical data.
  - Organizations reluctance to prosecute.
  - Negligent hiring liability requires employers to check employee backgrounds. Courts holding employers responsible for employee criminal acts that could have been prevented with background check.

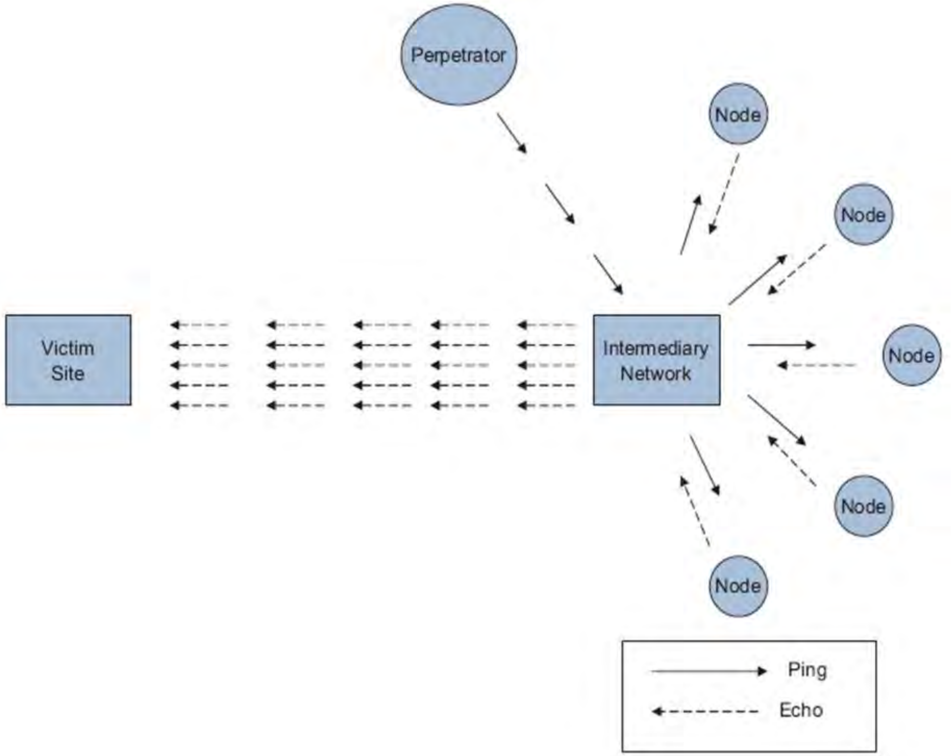
Internet Risks

- **IP spoofing** is masquerading to gain access to a Web server and/or to perpetrate an unlawful act without revealing one's identity.
- **Denial of service (DOS) attack** is an assault on a Web server to prevent it from servicing users.
  - Particularly devastating to business entities that cannot receive and process business transactions.
  - Motivation may be to punish an organization for a grievance or may be done for financial gain.
- Network topologies are subject to risks from equipment failure which can cause corruption or loss.

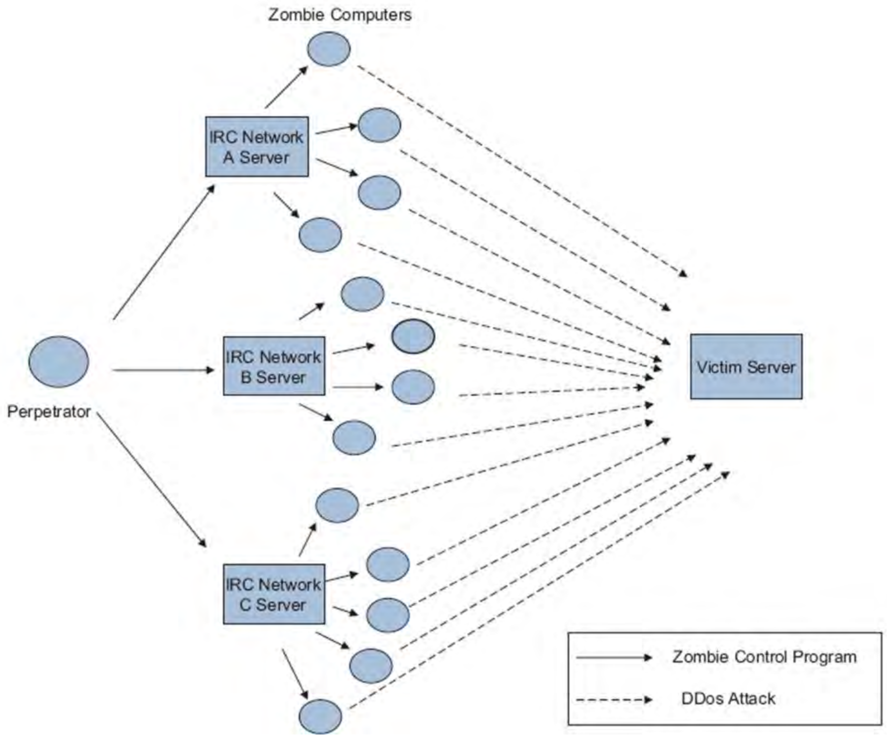
Three Common Types of DOS Attacks

- **SYN Flood**: When the three-way handshake needed to establish an Internet connection occurs, the final acknowledgement is not sent by the DOS attacker, thereby tying-up the receiving server while it waits.
- **Smurf**: DOS attacker uses numerous intermediary computers to flood the target computer with test messages, “pings” causing network congestion.
- **Distributed Denial of Service**:– May take the form of Smurf or SYN attacks, but distinguished by the vast number of **zombie** computers hijacked to launch the attacks.

SMURF Attack



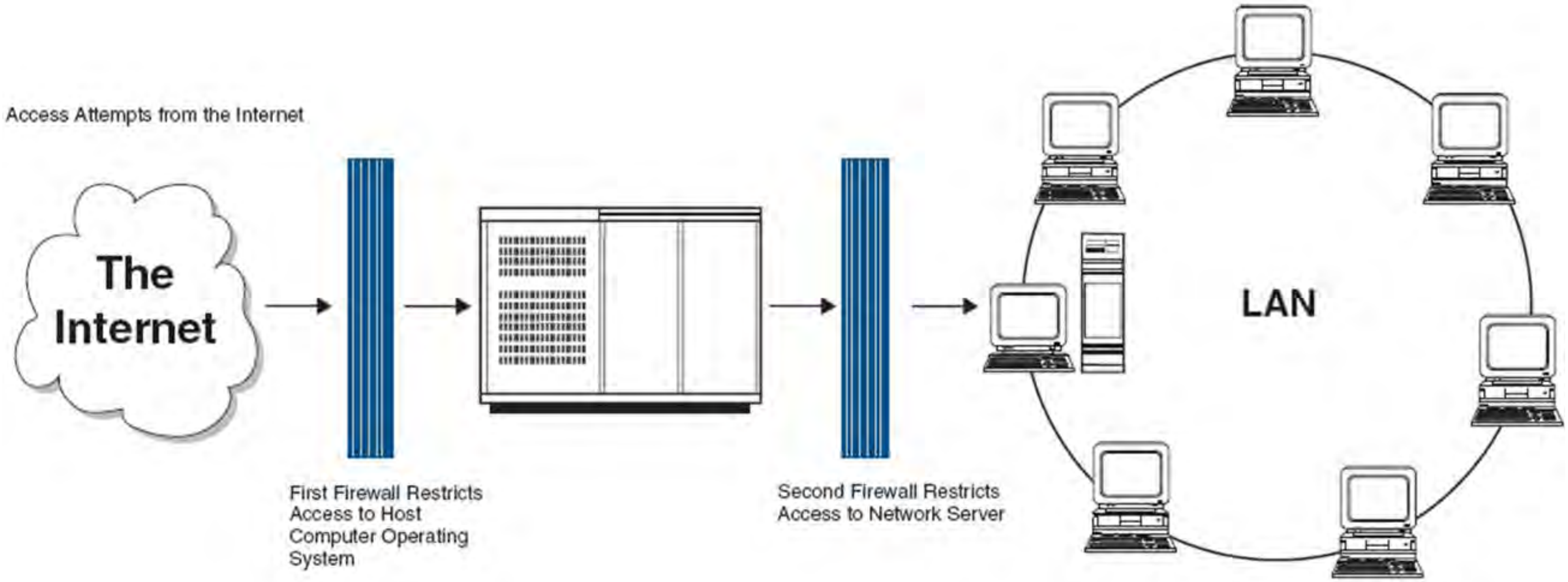
Distributed Denial of Service Attack



Controlling Risks from Subversive Threats

- **Firewalls** prevent unauthorized access to or from a private network. To accomplish this:
  - All traffic between the outside network and organization’s intranet must pass through the firewall.
  - Only authorized traffic is allowed to pass through the firewall which must be immune to all penetration.
- **Network-level firewalls** provide efficient, low security control.
  - **Screening router** examines source and destination addresses attached to incoming message packets but does not explicitly authenticate outside users.
- **Application-level firewalls** provide higher, customizable network security, but add overhead cost.
- Trade-off between convenience and security.

Dual-Homed Firewall


Access Attempts from the Internet
The Internet
First Firewall Restricts Access to Host Computer Operating System
Second Firewall Restricts Access to Network Server
LAN

Controlling DOS Attacks

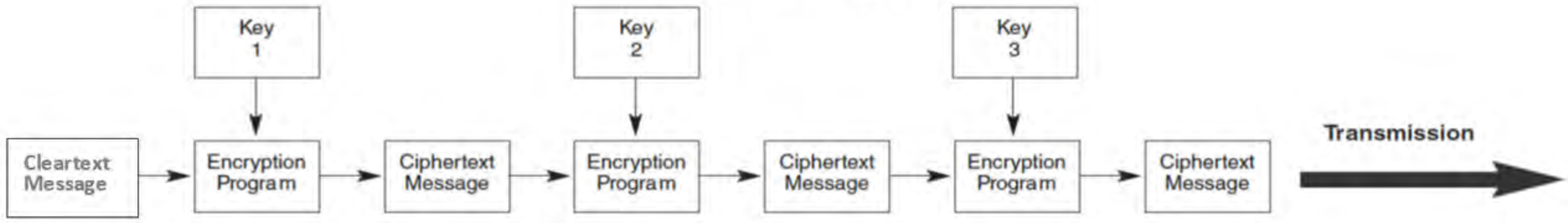
- **Smurf attacks**: Organizations can program firewalls to ignore identified attacking site.
- **SYN flood attacks** have two tactics:
  - Get Internet hosts to use firewalls that block invalid IP addresses.
  - Use security software to scan for half-open connections.
- To counteract DDos attacks organizations use **intrusion prevention systems (IPS)** that employ **deep packet inspection (DPI)**.
  - Works as a filter that removes malicious packets from the flow before they can affect servers and networks.

Encryption

- Conversion of data into a secret code for storage and transmission.
  - Sender uses an encryption algorithm to convert the original cleartext message into a coded ciphertext which is decoded at receiving end.
- Earliest is the **Caesar cipher** method.
- Two fundamental components:
  - **Key** is a mathematical value sender selects.
  - **Algorithm** is procedure of shifting letters in cleartext message number of positions key value indicates.
- **Private key** and **public key encryption** are two commonly used methods.

EE3 and ED3 Encryption

EEE3 Technique



Key 1

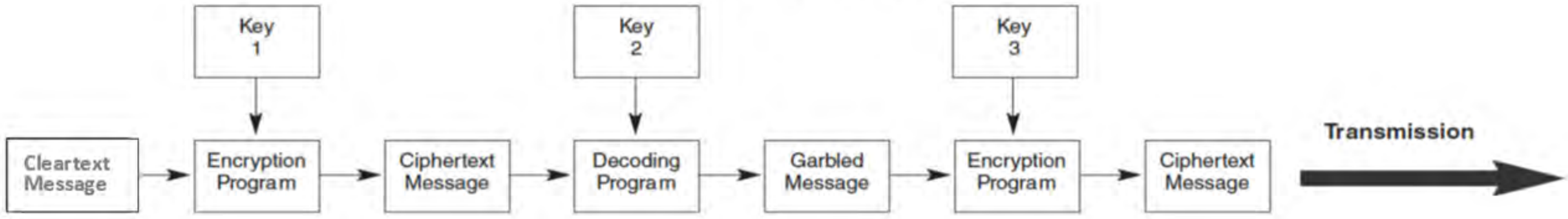
Key 2

Key 3

Cleartext Message → Encryption Program → Ciphertext Message → Encryption Program → Ciphertext Message → Encryption Program → Ciphertext Message

Transmission

EDE3 Technique



Key 1

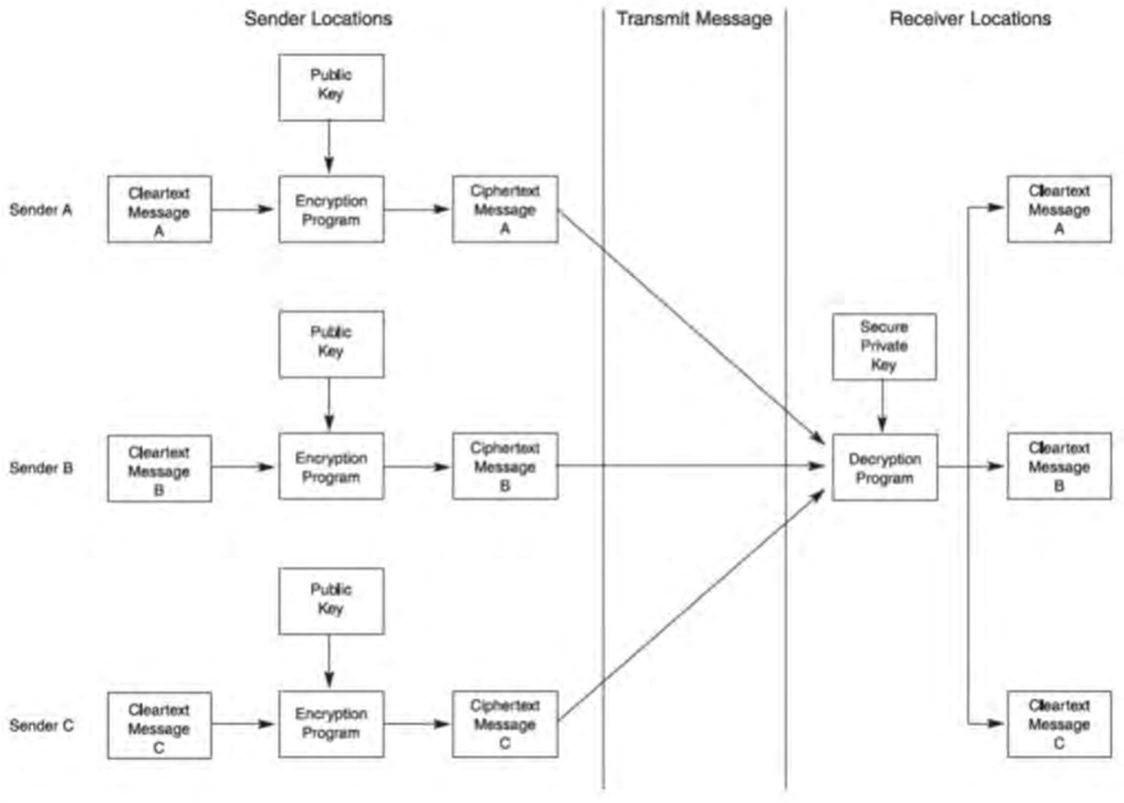
Key 2

Key 3

Cleartext Message → Encryption Program → Ciphertext Message → Decoding Program → Garbled Message → Encryption Program → Ciphertext Message

Transmission

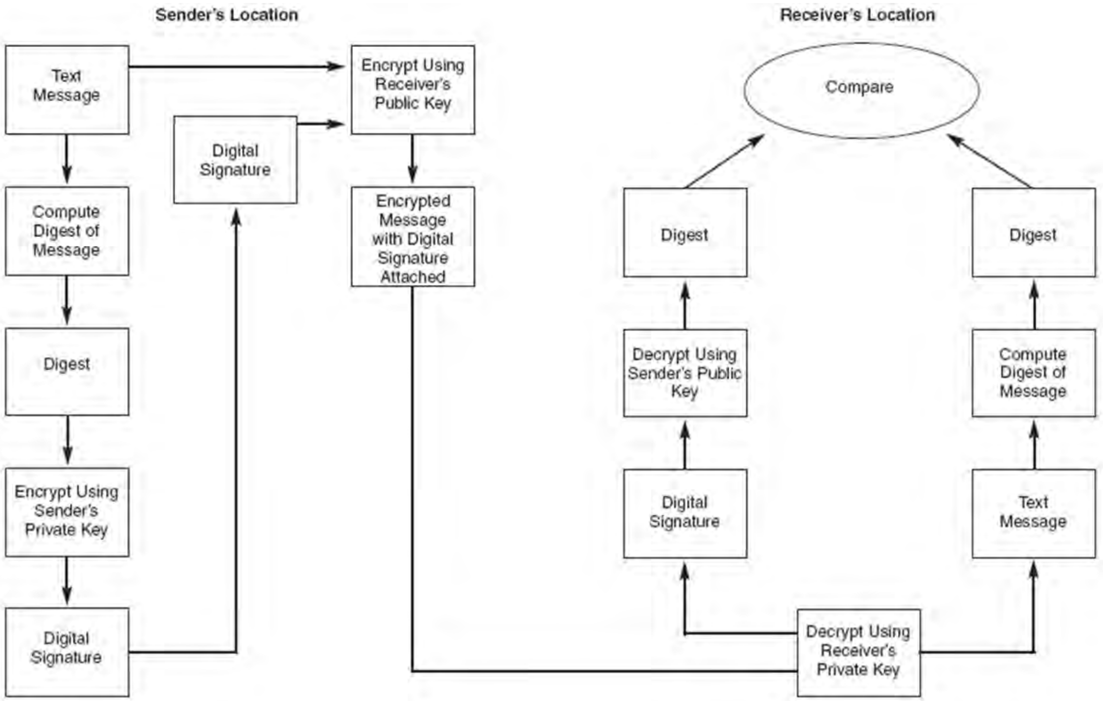
Public Key Encryption



Digital Signatures & Certificate

- **Digital signature** is electronic authentication that cannot be forged.
  - Sender uses a one-way hashing algorithm to calculate a **digest** of the text message which is encrypted to produce the digital signature.
- Verifying the sender's identity requires a **digital certificate** which is issued by a trusted third party called a **certification authority (CA).**
  - Public key encryption is central to digital authentication making public key management an important internal control issue.
  - **Public key infrastructure (PKI)** constitutes policies and procedures for administering this activity.

Digital Signature


Sender's Location
Receiver's Location
Text Message
Encrypt Using Receiver's Public Key
Compare
Digital Signature
Compute Digest of Message
Encrypted Message with Digital Signature Attached
Digest
Digest
Digest
Decrypt Using Sender's Public Key
Compute Digest of Message
Encrypt Using Sender's Private Key
Digital Signature
Text Message
Digital Signature
Decrypt Using Receiver's Private Key

Other Subversive Threat Controls

- **Message sequence numbering** inserts a sequence number in each message to prevent attempts to delete, change or duplicate a message.
- **Message transaction log** records all attempted accesses with user ID, time of access and location.
- **Request-response technique** sends control messages and responses randomly making it difficult for an intruder to circumvent.
- **Call-back device** requires a dial-in user to enter and password and be identified.

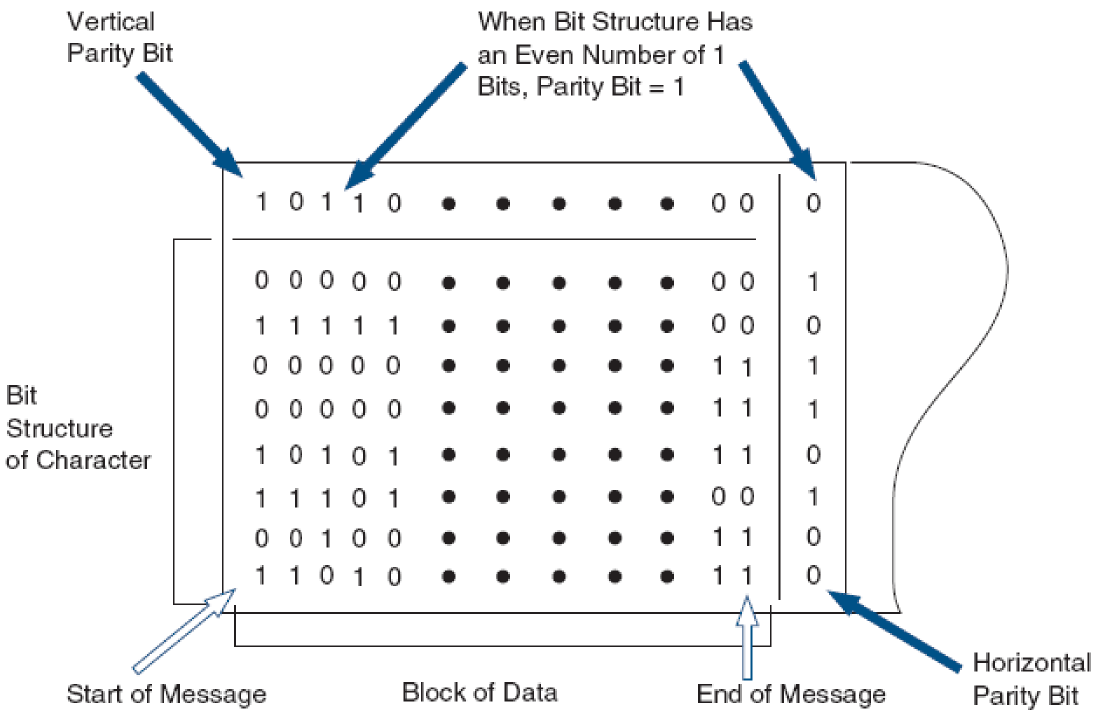
Operating Systems Controls

- **Subversive Threats-** Audit objectives:
  - Verify security and integrity of financial transactions.
  - Determine network controls (1) can prevent and detect illegal access; (2) will render captured data useless; and (3) are sufficient to preserve integrity and security of data.
- **Subversive Threats** - Audit procedures:
  - Review adequacy of firewall: flexibility, proxy services, filtering, segregation of systems; audit tools; weaknesses.
  - Verify IPS with DPI for organizations vulnerable to DDoS.
  - Review security procedures and message transaction logs.
  - Verify encryption process and test operation of the call-back feature.

Controlling Risks from Equipment Failure

- **Line errors** are losses from communications noise.
- Techniques to detect and correct data errors:
  - **Echo check** - receiver returns the message to the sender.
  - **Parity check** - extra bit is added onto each byte of data similar to check digits.
- Audit objective is to verify integrity of transactions by determining controls are in place to detect and correct message loss.
- Audit procedures include examining a sample of messages for garbled content and verifying all corrupted messages were retransmitted.

Vertical Parity Bit

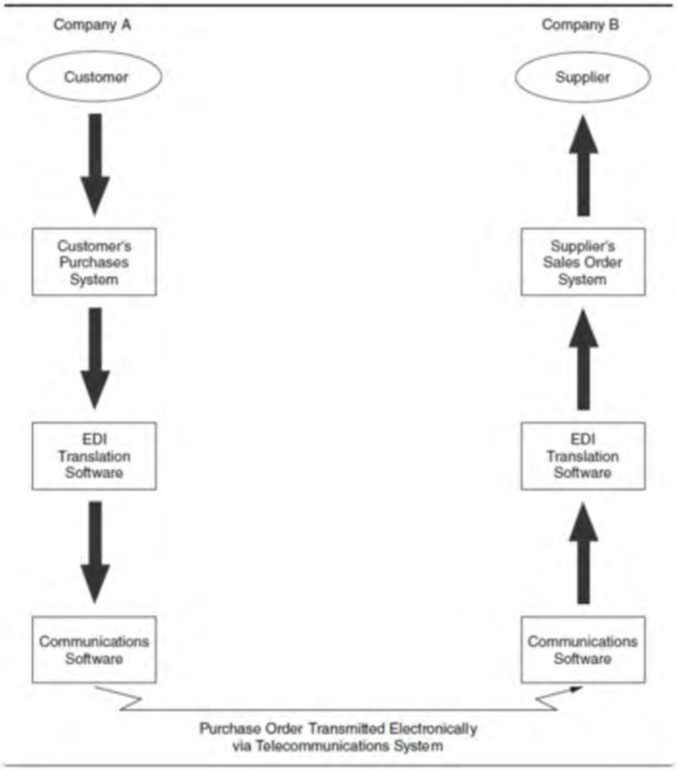

Vertical Parity Bit
When Bit Structure Has an Even Number of 1 Bits, Parity Bit = 1
Bit Structure of Character
Start of Message
Block of Data
End of Message
Horizontal Parity Bit

1	0	1	1	0	●	●	●	●	●	0	0	0
0	0	0	0	0	●	●	●	●	●	0	0	1
1	1	1	1	1	●	●	●	●	●	0	0	0
0	0	0	0	0	●	●	●	●	●	1	1	1
0	0	0	0	0	●	●	●	●	●	1	1	1
1	0	1	0	1	●	●	●	●	●	1	1	0
1	1	1	0	1	●	●	●	●	●	0	0	1
0	0	1	0	0	●	●	●	●	●	1	1	0
1	1	0	1	0	●	●	●	●	●	1	1	0

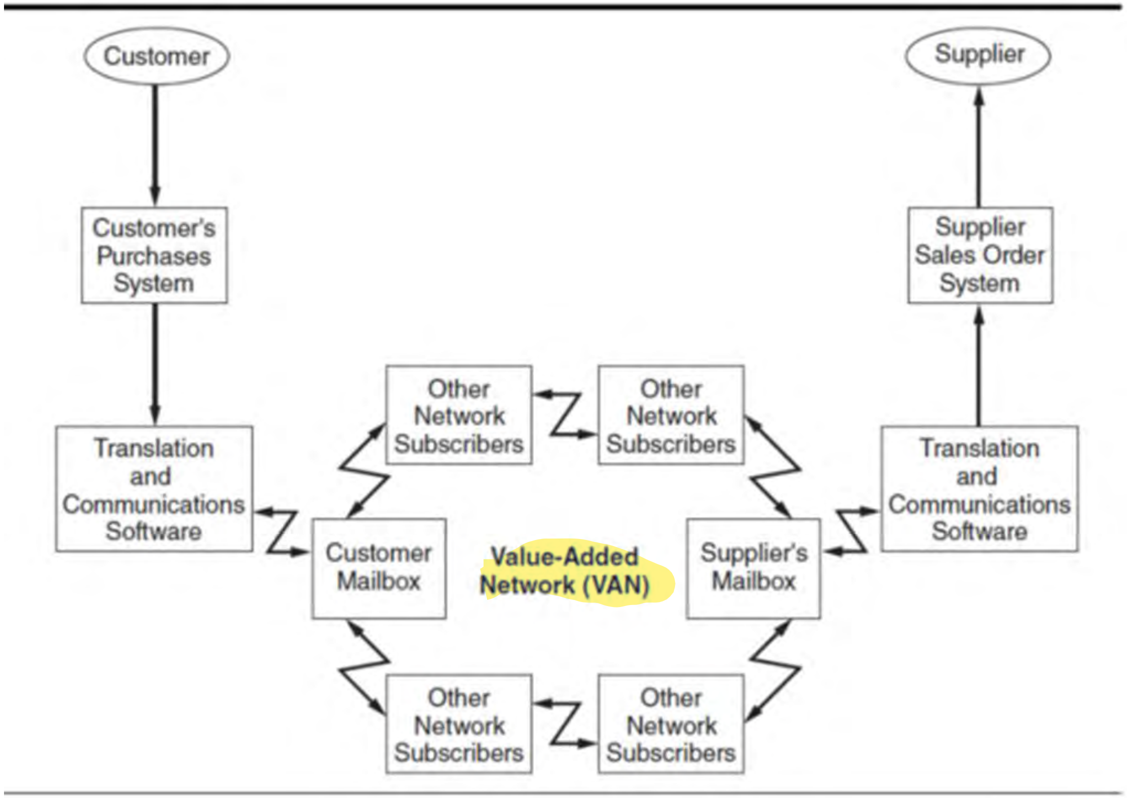
Auditing Electronic Data Interchange (EDI)

- EDI is the intercompany exchange of computer-processible business information in standard format.
- Key to success is use of standard format for messaging between dissimilar systems.
- Benefit of EDI:
  - Reduces or eliminates need for data entry.
  - Reduction of errors and paper forms.
  - Mailed documents replaced with cheaper transmissions.
  - Automated manual procedures and inventory reduction.

Overview of EDI



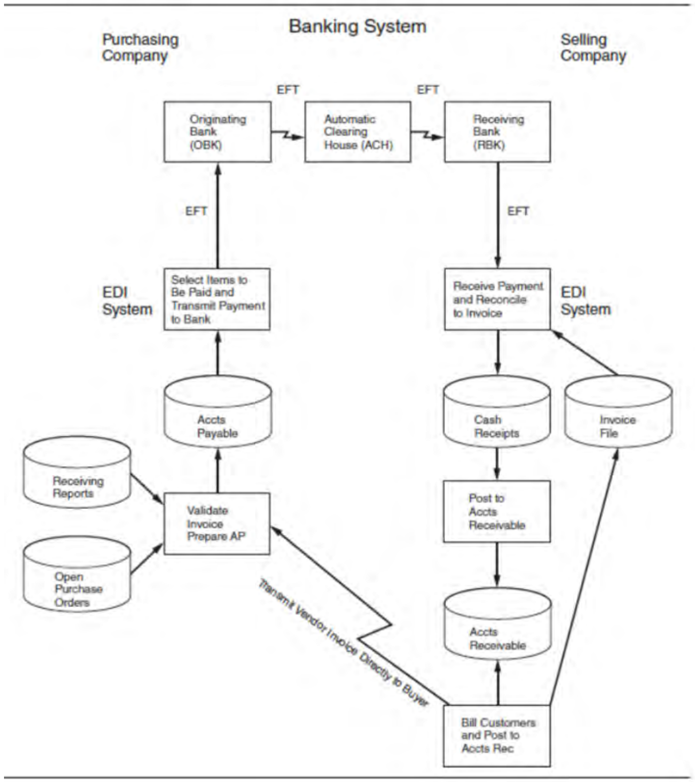
Value-added Network and EDI


Customer
Customer's Purchases System
Translation and Communications Software
Customer Mailbox
Other Network Subscribers
Other Network Subscribers
Value-Added Network (VAN)
Other Network Subscribers
Other Network Subscribers
Supplier's Mailbox
Translation and Communications Software
Supplier Sales Order System
Supplier

Auditing Electronic Data Interchange (EDI)

- Electronic funds transfer (EFT) processing more complicated than EDI for purchasing and selling.
  - Converting remittance information to electronic form can result in very large records.
- Both customer and supplier must establish EDI transactions are valid and authorized.
  - Some VANs have the capability of validating passwords and user ID codes for the vendor.
  - Before conversion, translation software can validate trading partner’s IDs and passwords.
  - Before processing, trading partner’s application software reference valid files to validate transaction.

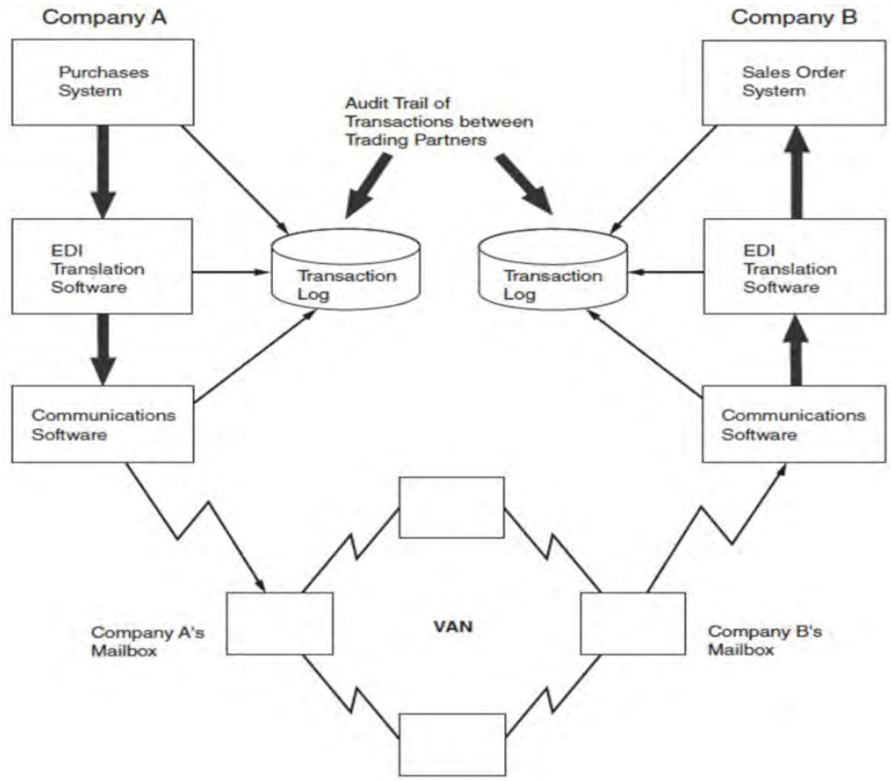
EFT Transactions Between Trading Partners



Auditing Electronic Data Interchange (EDI)

- Absence of source documents in EDI eliminates traditional audit trail and restricts audit tests.
- Audit objectives relating to EDI are to determine:
  - Transactions are authorized, validated, and in compliance with the trading partner agreement.
  - No unauthorized organizations can gain access to database.
  - Authorized trading partners have access only to approved data.
  - Adequate controls are in place to ensure a complete audit trail.

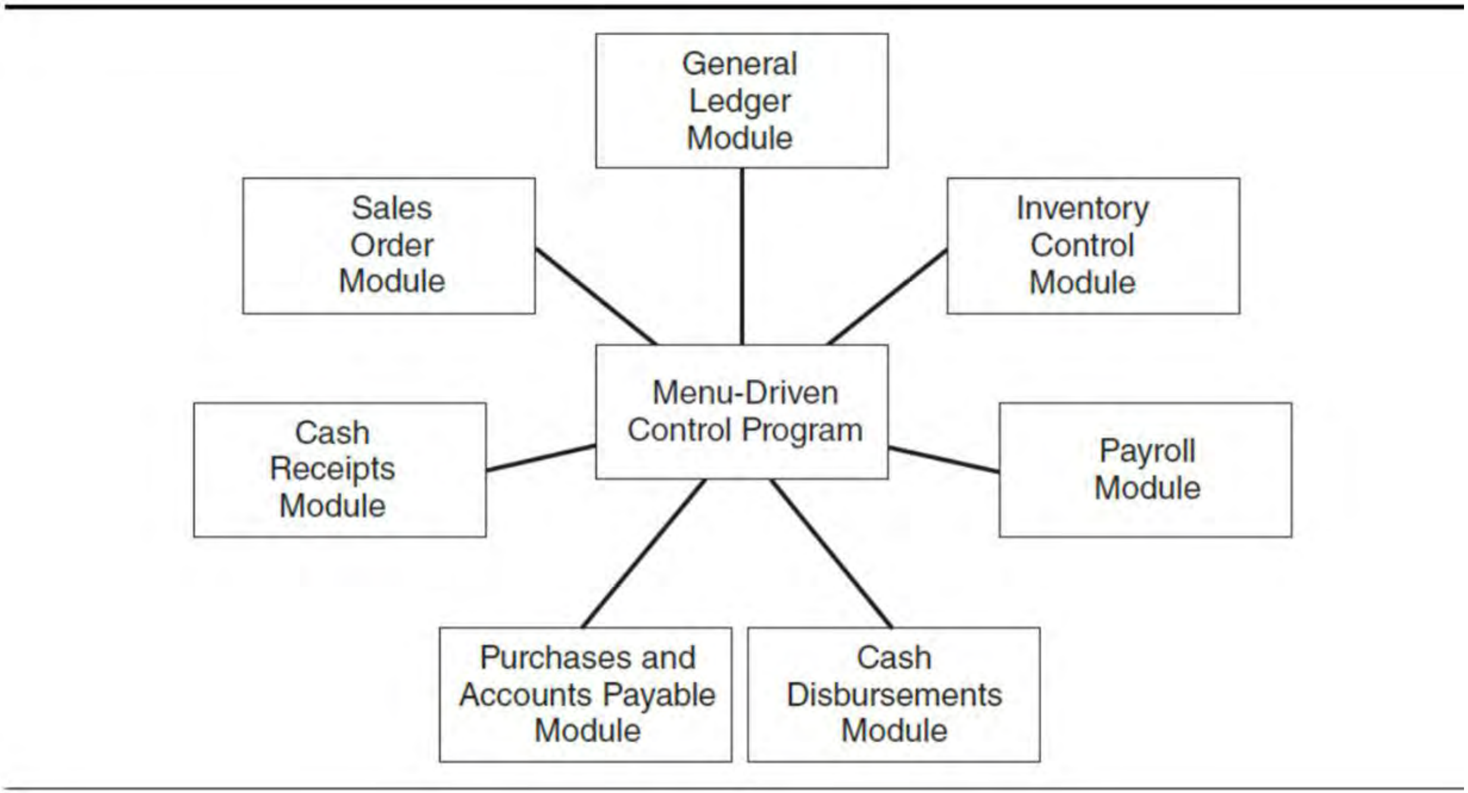
EFT System Using Transaction Control Log for Audi Trail



Auditing Procedures for EDI

- Tests of Authorization and Validation Controls:
  - Review agreements with VAN to validate transactions.
  - Review trading partner files for accuracy and completeness.
- Tests of Access Controls:
  - Verify limited access to vendor and customer files.
  - Verify limited access of vendors to database.
  - Test EDI controls by attempting to violate access privileges.
- Tests of Audit Trail Controls:
  - Verify existence of transaction logs.
  - Review a sample of transactions to verify key data values were recorded correctly.

PC Accounting System Modules



PC Systems Risks and Controls

- Operating System Weaknesses:
  - PCs provide only minimal security for data files and programs.
  - Once computer criminal gains access to user's PC, little to prevent stealing or manipulation of the data.
- Weak access control.
- Inadequate segregation of duties.
- Multilevel password control used to restrict employees sharing computers.
- Risk of theft and virus infection.
- Weak backup procedures.

Audit Objectives Associated with PC Security

- Auditor should verify:
  - Controls in place to protect data, programs, and computers from unauthorized access, manipulation, destruction, and theft.
  - Adequate supervision and operating procedures exist to compensate for lack of segregation between the duties of users, programmers, and operators.
  - Backup procedures are in place to prevent data and program loss due to system failures, errors and so on.
  - Systems selection and acquisition procedures produce applications that are high quality, and protected from unauthorized changes.
  - System virus free and adequately protected to minimize the risk of becoming infected with a virus or similar object.

Audit Procedures Associated with PC Security

- Observe PCs are physically anchored.
- Verify segregation of duties and/or adequate supervision.
- Confirm reports are prepared, distributed, and reconciled by appropriate management at regular and timely intervals.
- Determine multilevel password control as needed.
- Verify drives are removed and stored appropriately.
- Verify backup procedures are appropriate.
- Verify software purchases and selection and acquisition procedures.
- Review policy for using antiviral software.

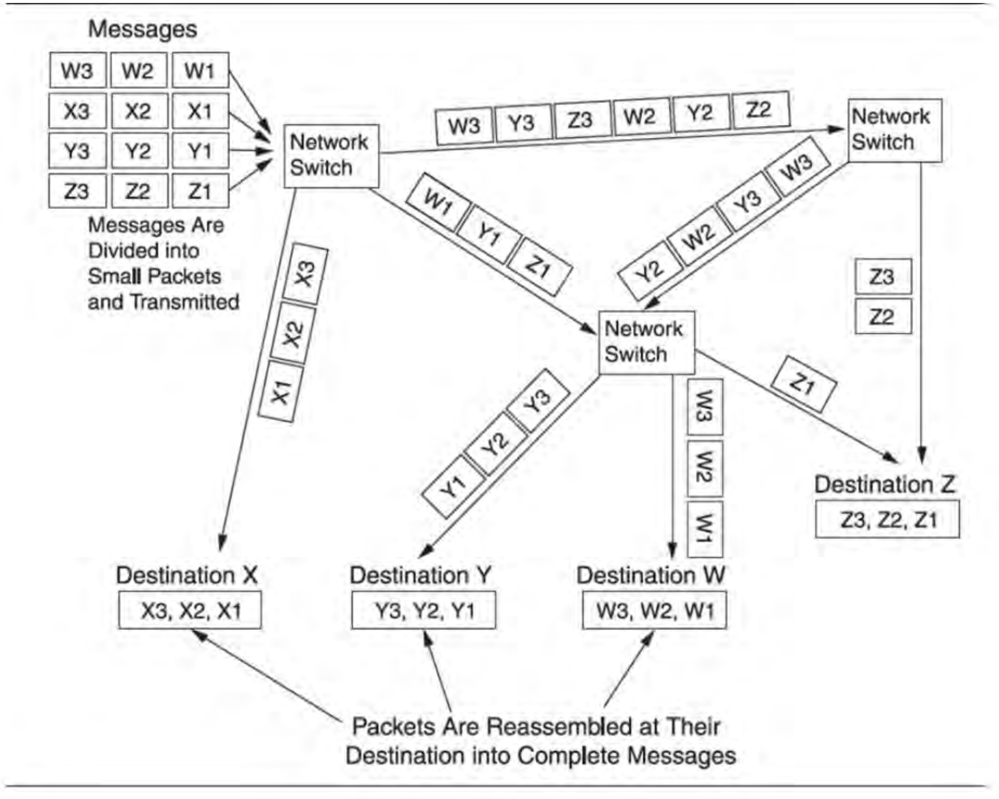
Internet & Intranet Technologies and Malicious & Destructive Programs

APPENDIX

Internet Technologies

- Packet switching:
  - Messages divided into small packets where each packet of the message may take a different routes.
- Virtual private network (VPN) is a private network within a public network.
- Extranet is a password controlled network for private users.
- World Wide Web (WWW) is an Internet facility that links users locally and globally.
  - Web pages are maintained at Web sites which are computer servers that support HTTP.

Message Packet Switching



Internet Addresses

- E-mail addresses:
  - Format is USERNAME@DOMAIN NAME
- URL address:
  - Defines the path to a facility or file on the Web.
  - Subdirectories can be several levels deep.
- IP address:
  - Every computer node and host attached to the Internet must have a unique Internet protocol (IP) address.

Protocols

- Rules and standards governing design of hardware and software that permit network users to communicate and share data.
- Functions include:
  - Facilitate physical connection between the network devices.
  - Synchronize transfer of data between physical devices.
  - Provide basis for error checking and measuring network performance.
  - Promote compatibility among network devices.
  - Promote network designs that are flexible, expandable, and cost-effective.

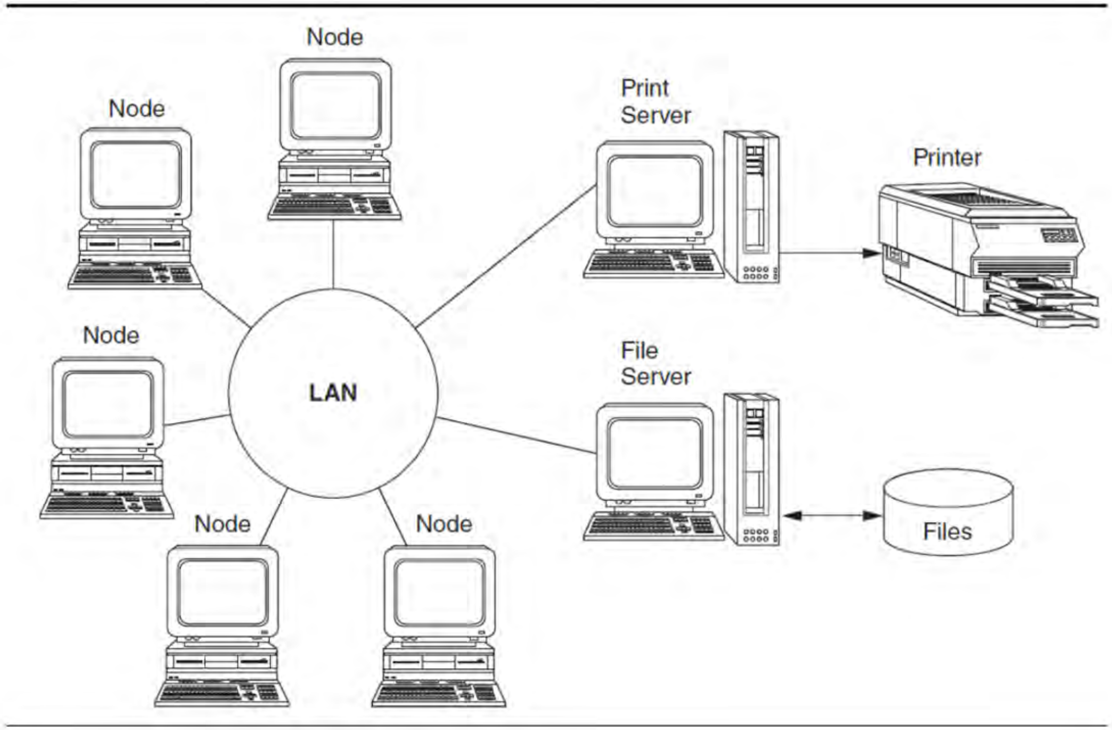
Internet Protocols

- Transfer Control Protocol/Internet Protocol (TCP/IP) permits communication between Internet sites.
- File Transfer Protocol (FTP) used to transfer files across the Internet.
- Simple Network Mail Protocol (SNMP) transmits e-mail messages.
- Secure Sockets Layer (SSL) and Secure Electronic Transmission (SET) are encryption schemes.
- Network News Transfer Protocol used to connect to Usenet groups on the Internet.
- HTTP and HTTP-NG control Web browsers.
- HTML is the document format used to produce Web pages.

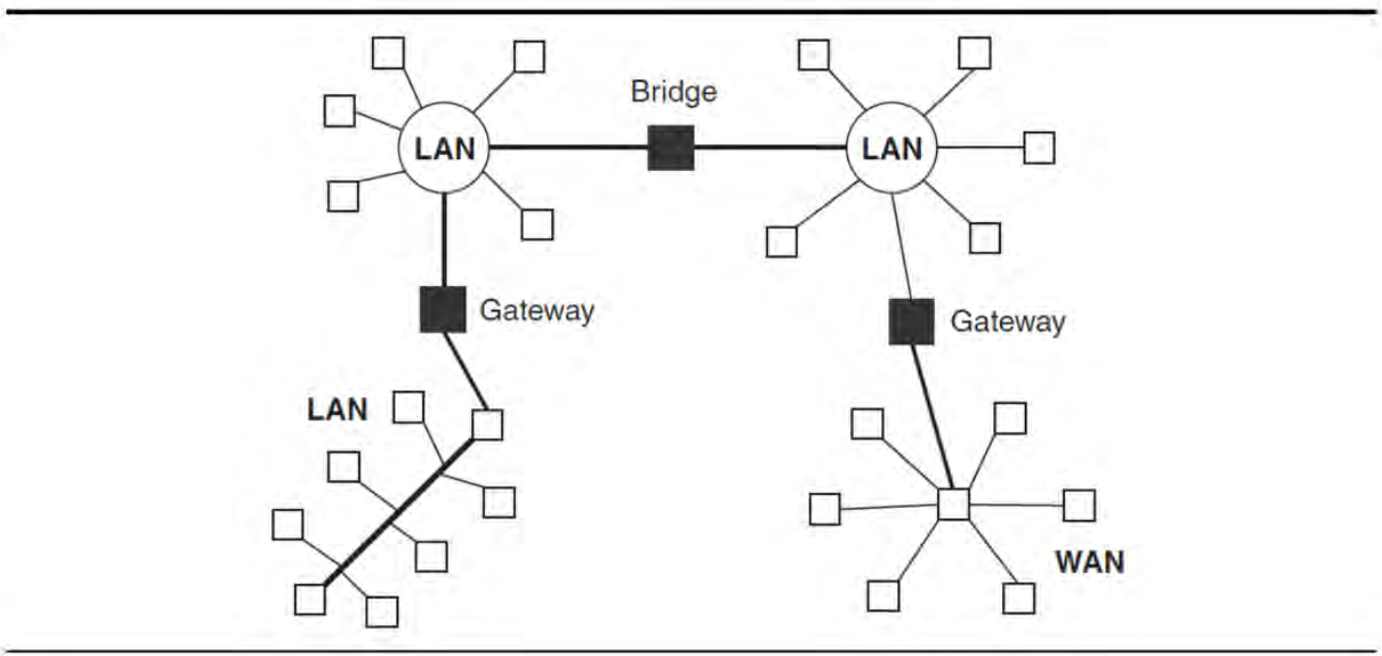
Intranet Technologies

- A network topology is the physical arrangement of network components.
- Networks are classified as LANs or WANs:
  - Local area networks (LANs) can cover several miles and connect hundreds of users.
  - Networks that exceed geographic limitations of LANs are wide area networks (WANs).
- The physical connection of workstations to the LAN is achieved through a network interface card (NIC).
- A server is used to store the network operating system, application programs, and data to be shared.

LAN with File and Print Servers



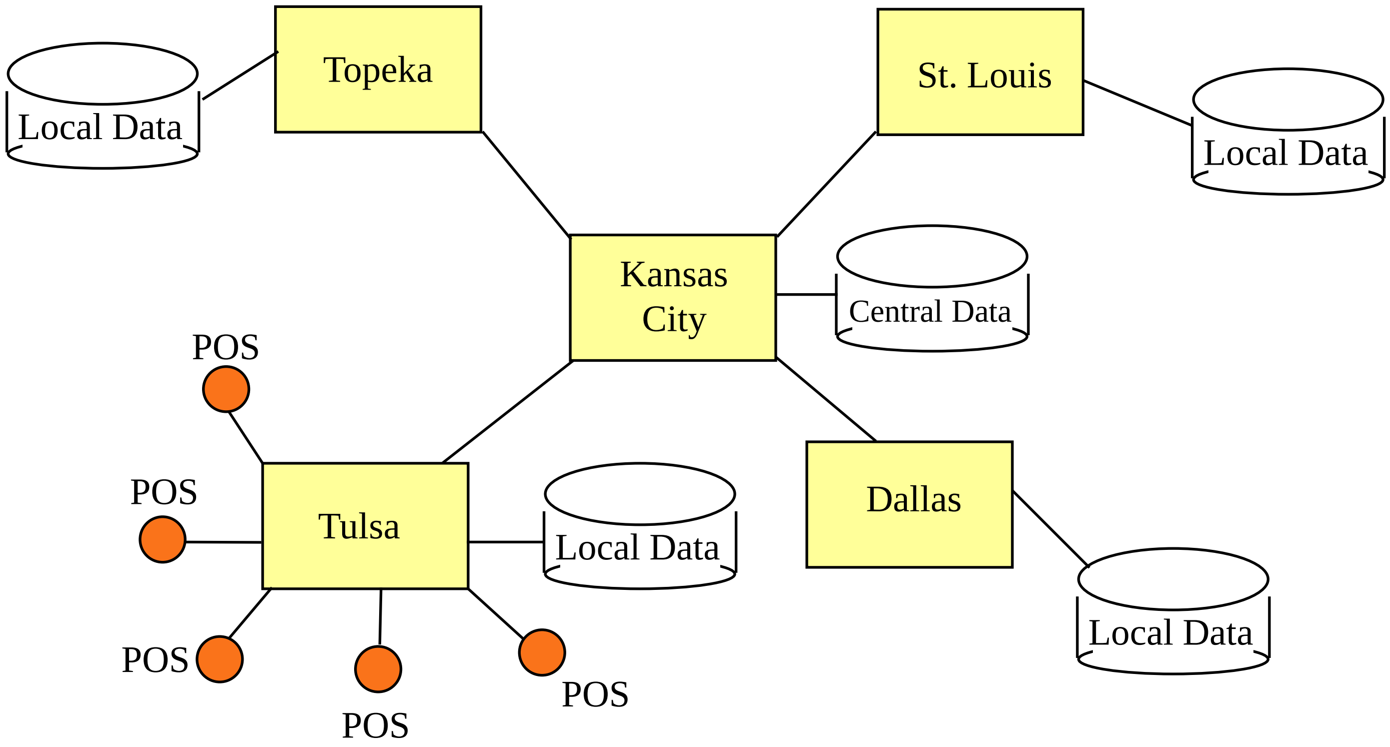
Bridges and Gateways Linking LANs & WANs



Star Topology

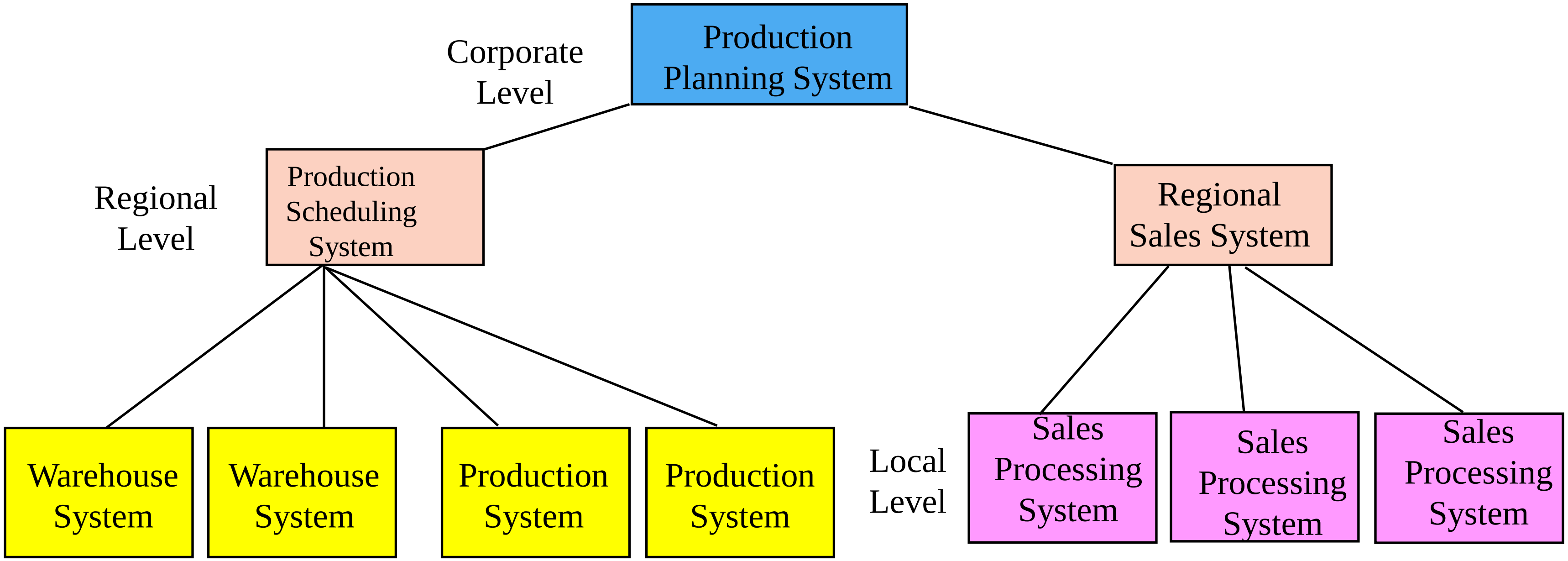
- A network of IPUs with a large central computer (the host).
- Host computer has direct connections to smaller computers, typically desktop or laptop PCs.
- Popular for mainframe computing.
- All communications must go through the host computer, except for local computing.

Star Network



Hierarchical Topology

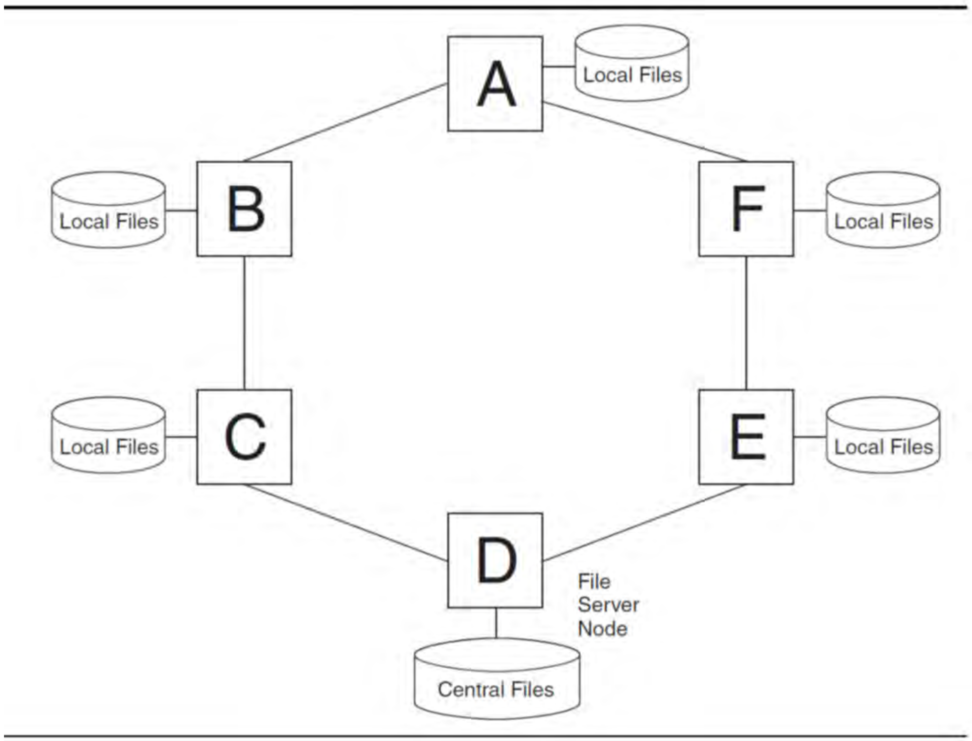
- A host computer is connected to several levels of subordinate smaller computers in a **master-slave** relationship.



Ring Topology

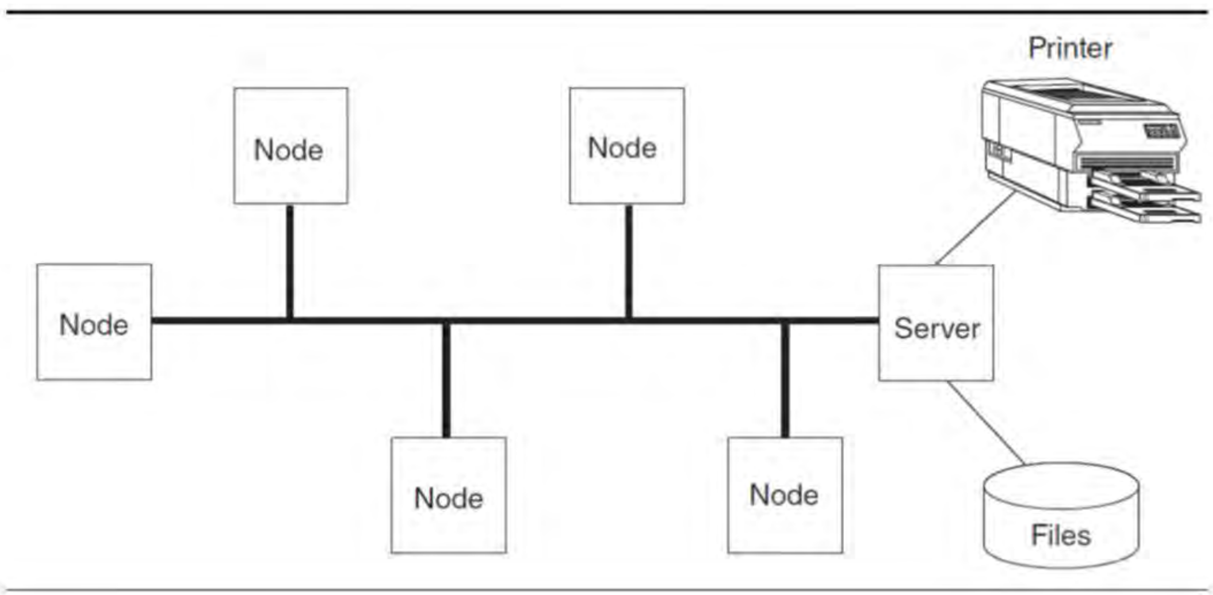
- Configuration eliminates the central site.
- All nodes in this configuration are of equal status (peers).
- Responsibility for managing communications is distributed among the nodes.
- Common resources that are shared by all nodes can be centralized and managed by a file server that is also a node.

Ring Topology



Bus Topology

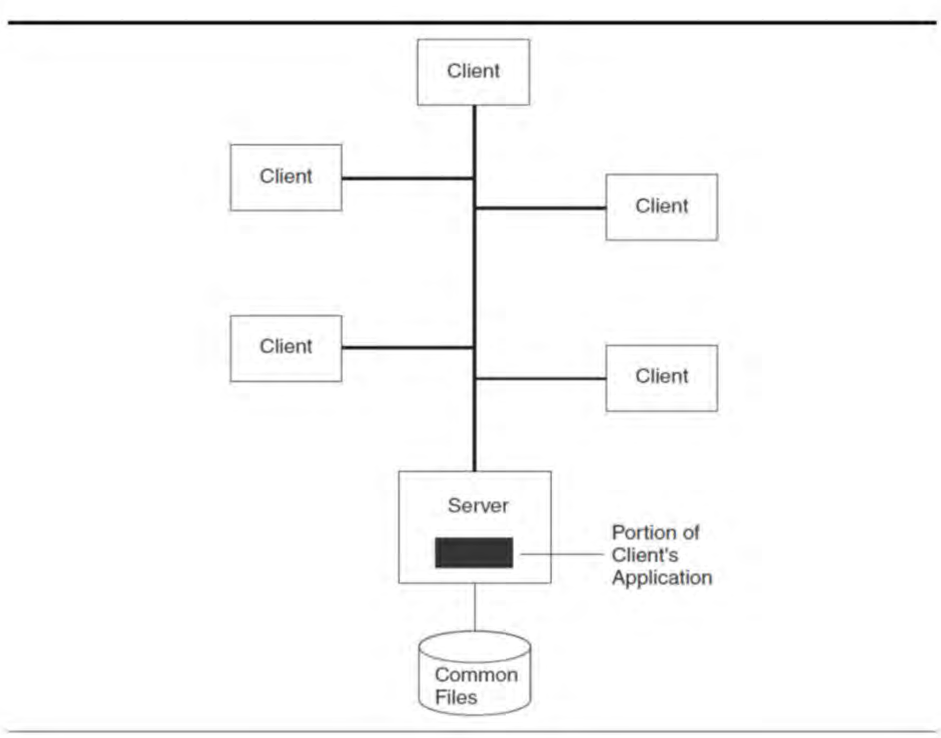
- Most popular LAN topology.



Client-Server Topology

- Configuration distributes the processing between the user's (client's) computer and the central file server.
- Both types of computers are part of the network, but each is assigned functions that it best performs.
- This approach reduces data communications traffic, thus reducing queues and increasing response time.

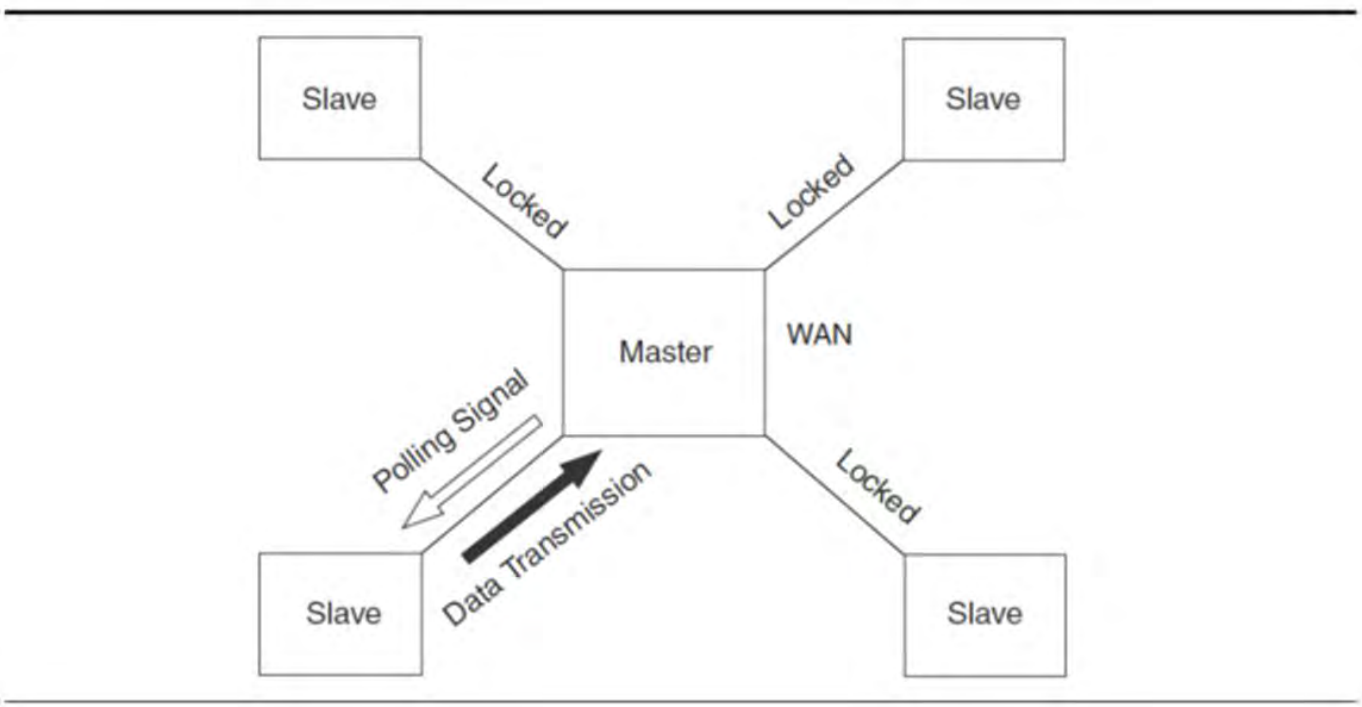
Client-Server Topology



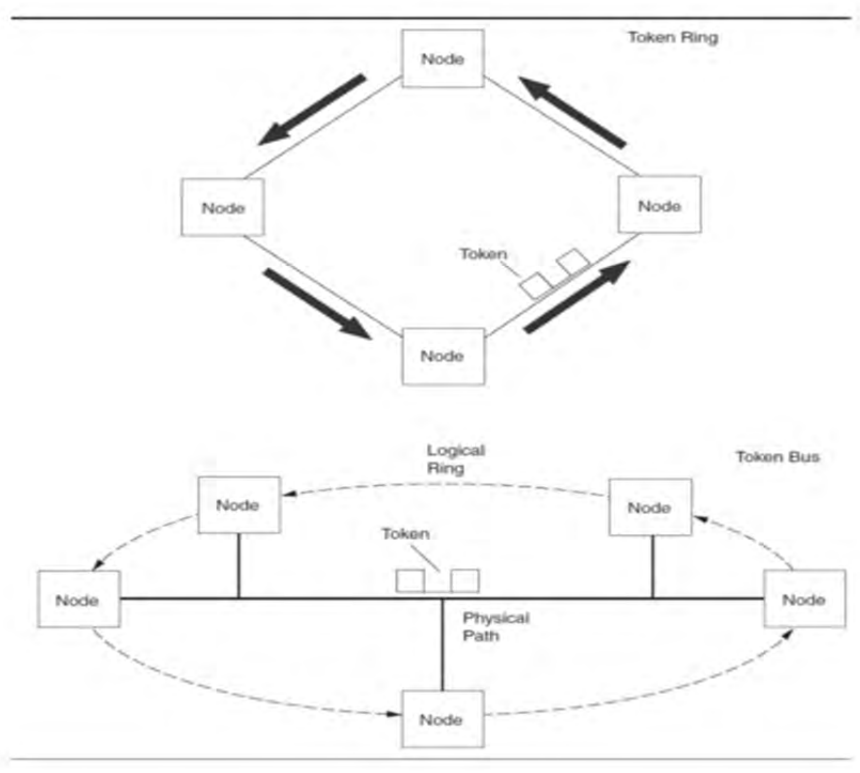
Network Control

- Purpose of network control is to:
  - Establish communications sessions.
  - Manage the flow of data across the network.
  - Detect and resolve data collisions between nodes.
  - Detect line failure of signal degeneration errors
- Two or more signals transmitted simultaneously will result in **data collision** which destroys messages.
  - **Polling** most popular technique for establishing a communication session in WANs.
  - **Token passing** involves transmitting special signal around the network. Only the node processing the token is allowed to transmit data.

Pooling Method of Controlling Data Collisions



Token-Passing Approach to Controlling Data Collisions



Carrier Sensing

- A random access technique that detects collisions when they occur.
- Technique is used with bus topology.
- Node wishing to transmit listens to determine if line is in use. If it is, it waits a pre-specified time to transmit.
- Collisions occur when nodes hear no transmissions, and then simultaneously transmit.
- Data collides and nodes instructed to hang up and try again.
- Ethernet is the best-know LAN using this standard.

Malicious & Destructive Programs

- **Virus** is a program that attaches itself to a legitimate program to penetrate the operating system and destroy programs, files and the operating system itself.
- **Worm** is used interchangeably with virus.
- **Logic bomb** is a destructive program triggered by some predetermined event or date.
- **Back door** (or trap door) is a software program that allows unauthorized access to a system.
- **Trojan horse** program purpose is to capture IDs and passwords.