IT Masters
itmasters.edu.au

Charles Sturt University

++++

Network+ Short Course

Presented by Matt Constable

Module 1

IT Masters
itmasters.edu.au

Charles Sturt University

Network+ Short Course

Based on subject :
ITE526: Internetworking Fundamentals

Part of the :
Master of Networking and Systems Administration
Master of Management (IT)

Overview

- **Introduction & Networking Concepts**
  - Course welcome & introduction.
  - Explain the purposes and uses of ports & protocols.
  - Explain devices, applications, protocols and services at their appropriate OSI layers.
  - Explain the concepts and characteristics of routing and switching.
  - Given a scenario, configure the appropriate IP addressing components.
  - Compare and contrast the characteristics of network topologies, types and technologies.
  - Given a scenario, implement the appropriate wireless technologies and configurations.
  - Summarize cloud concepts and their purposes.
  - Explain the functions of network services.

IT Masters
itmasters.edu.au

Charles Sturt University

Introductions

Matt Constable

- 20+ years in the IT industry
- Networking/Security/Wireless/VoIP
- Government, Education, Financial Services, Service Provider, Retail – Enterprise & Integration.
- B.Comp, M. Computer Security, various industry certs.
- I don’t have all the answers.
  - Everyone brings something to the table!

IT Masters
itmasters.edu.au

Charles Sturt University

Class Times

Webinars will run:

- ??
- Will be uploaded within 24 hours.
  - Youtube
  - Zoom Link
  - PDF copy of slides
  - Numerous other resources available throughout the course as applicable.

Contact

- Easiest way is via course forums.
  - Everyone can share in the Q & A.

Learning Resources

- Various resources on IT Masters Short Course System
- Weekly tasks
  - Quizzes
  - “Lab” Tasks
  - Range of individual and forum activities to help you learn; Please engage!

Study Tips

- Test yourself instead of re-reading notes – “retrieval practice”.
- Test yourself repeatedly.
- Talk out loud to yourself or a friend.
- Distinctiveness – How what you are is learning different, or the same, to something else – “compare & contrast”
- Apply to your own experience!
- BEWARE OF FAMILIARITY
  - Just because you are “familiar” with something…or have seen it before doesn’t mean you really *know* it…so practice, practice, practice.
- Read & study extensively!

IT Masters
itmasters.edu.au

Charles Sturt University

Week 1 – Networking Concepts

- Explain the purposes and uses of ports & protocols.
- Explain devices, applications, protocols and services at their appropriate OSI layers.
- Explain the concepts and characteristics of routing and switching.
- Given a scenario, configure the appropriate IP addressing components.
- Compare and contrast the characteristics of network topologies, types and technologies.
- Given a scenario, implement the appropriate wireless technologies and configurations.
- Summarize cloud concepts and their purposes.
- Explain the functions of network services.

Networking Concepts

How Networks Are Used

- Network services - the resources a network makes available to its users
  - Includes applications and the data provided by these applications
- Types of applications found on most networks:
  - Client-Server
  - File and Print Services
  - Communications Services

Client-Server Applications

- Client computer requests data or a service from a second computer, called the server
- List of several popular client-server applications:
  - Web service
  - Email services
  - FTP service
  - Telnet service
  - Remote Desktop
  - Remote applications

Client-Server Applications

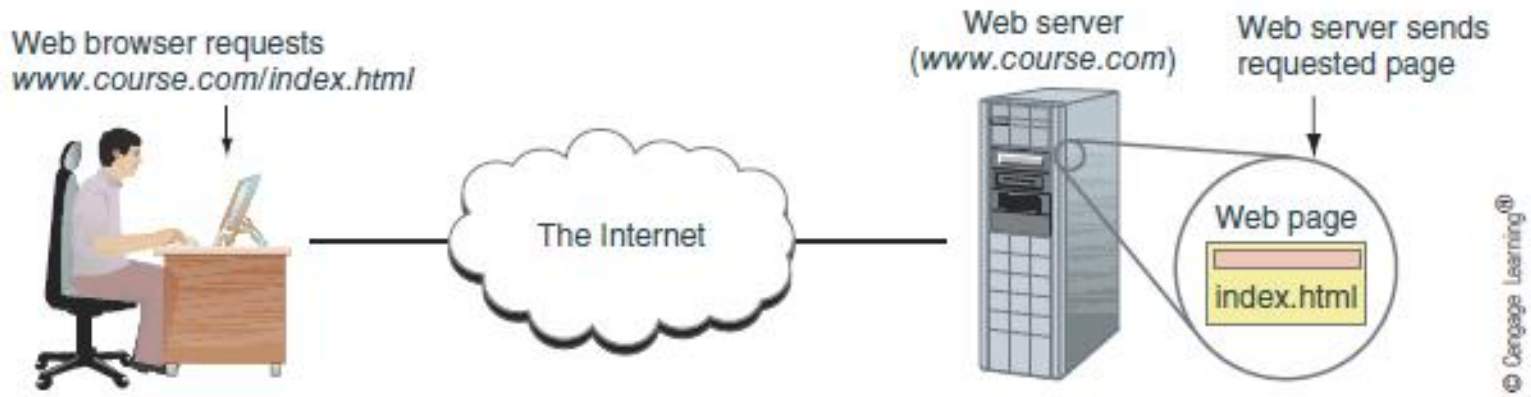


Figure 1-1 A Web browser (client application) requests a Web page from a Web server (server application); the Web server returns the requested data to the client

Client-Server Applications

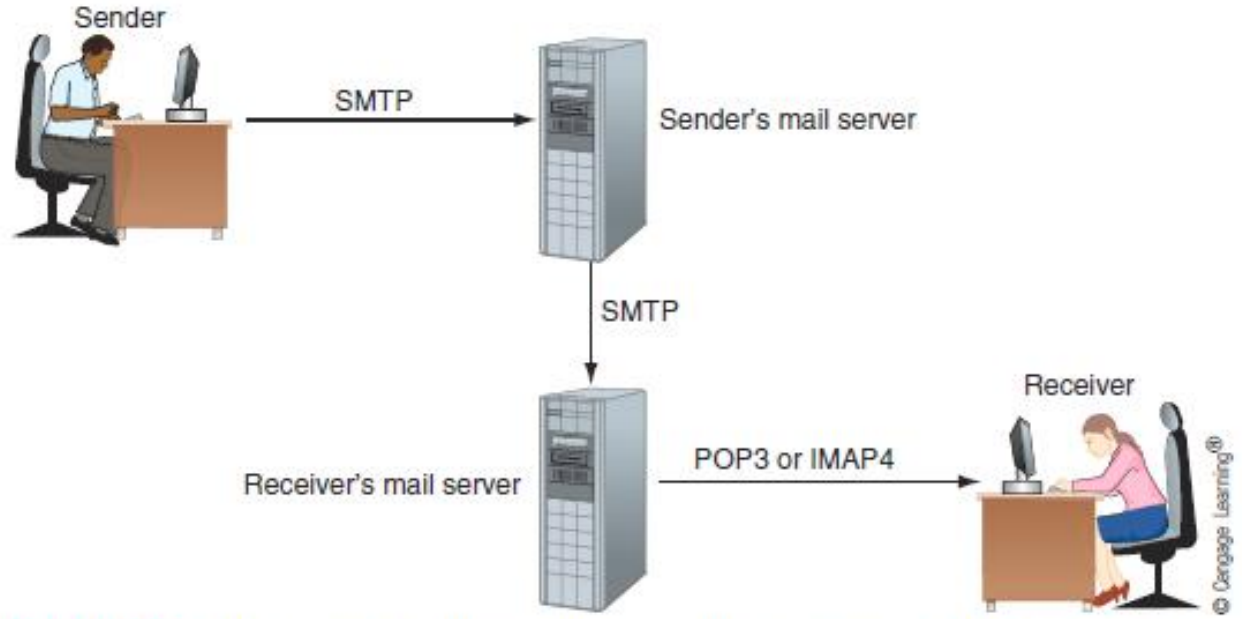


Figure 1-2 SMTP is used to send email to a recipient's mail server, and POP3 or IMAP4 is used by the client to receive email

File and Print Services

- File services - a server's ability to share data files and disk storage space
- File server - a computer that provides file services
- Print services - ability to share printers across a network
  - With one printer, less time is spent on maintenance and management

Communication Services

- Convergence - using the same network to deliver multiple types of communications services
- Unified communication (UC) - refers to the centralized management of multiple network-based communications
- Three types of communication services:
  - Conversational voice - VoIP (Voice over IP)
  - Streaming live audio and video
  - Streaming stored audio and video

Communication Services

- Voice and video transmissions are delay-sensitive
  - You don’t want to hear or see breaks in transmission
- Voice and video transmission are considered loss-tolerant
- Network administrators must pay attention to the quality of service (QoS) a network provides for voice and video
- Bandwidth - the amount of traffic, or data transmission activity, on the network

Controlling Network Access

- Topology - how parts of a whole work together
- Physical topology - mostly applies to hardware and describes how computers, other devices, and cables fir together to form the physical network
- Logical topology - has to do with software and describes how access to the network is controlled
  - How users and programs initially gain access to the network
- Network operating system - controls access to the entire network
  - Required by client-server models

Peer-to-Peer Model

- Peer-to-peer (P2P) network model - the OS of each computer on the network is responsible for controlling access to its resources
  - No centralized control
- Computers, called nodes or hosts, form a logical group of computers and users
  - May share resources
  - May prevent access to resources
- Each computer user has a Windows local account
  - Works only on that one computer

Peer-to-Peer

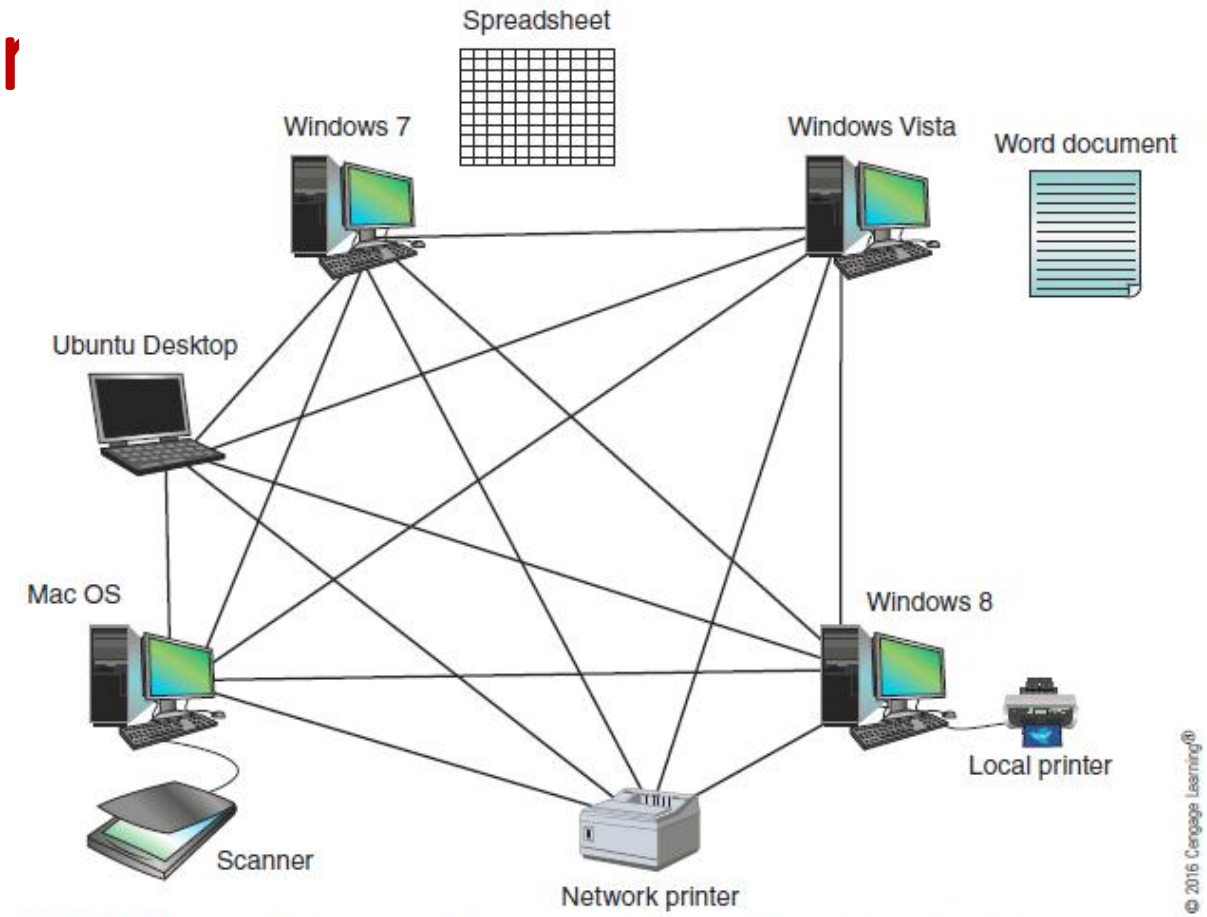


Figure 1-4 In a peer-to-peer network, no computer has more authority than another; each computer controls its own resources, and communicates directly with other computers

Peer-to-Peer Model

- Advantages
  - Simple configuration
  - Less expensive
    - Compared to other network models
- Disadvantages
  - Not scalable
  - Not necessarily secure
  - Not practical for large installations

Client-Server Network Model

- Resources are managed by the network operating system (NOS) via a centralized directory database
- Windows domain - a logical group of computers that a Windows Server can control
- Active Directory (AD) - the centralized directory database that contains user account information and security for the entire group of computers
- Global account (a.k.a. global username or network ID) - a domain-level account assigned by the network administrator and is kept in AD

Client-Server Network Model

- A user can sign on to the network from any computer on the network and gain access to the resources that AD allows
  - This process is managed by Active Directory Domain Services (AD DS)
- Clients don’t share their resources directly with each other
  - Access is controlled by entries in the centralized domain database

Client-Server N

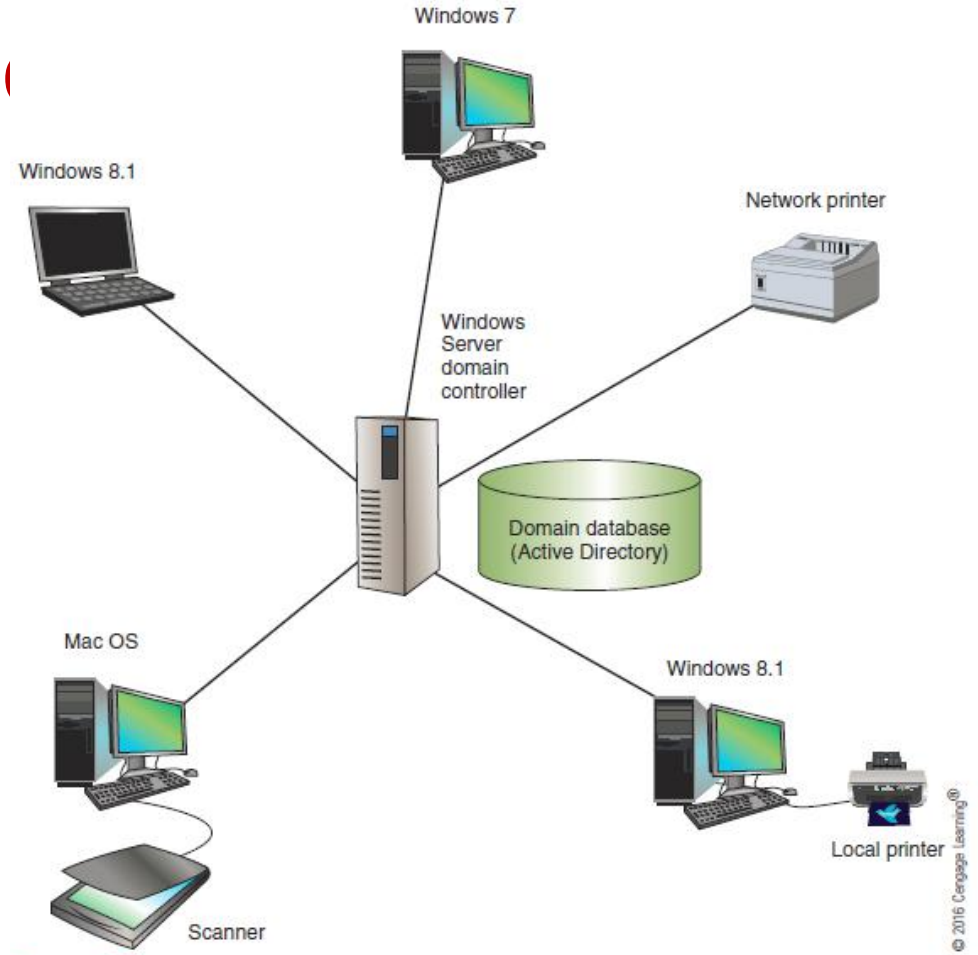


Figure 1-5 A Windows domain uses the client-server model to control access to the network, where security on each computer or device is controlled by a centralized database on a domain controller

Client-Server Network Model

- The NOS is responsible for:
  - Manages client data, resources
  - Ensures authorized user access
  - Controls user file access
  - Restricts user network access
  - Dictates computer communication rules
  - Supplies application to clients
- Server examples
  - Windows Server 2012 R2, Ubuntu Server, or Red Hat Linux

Client-Server Network Model

- Servers that have a NOS installed require:
  - More memory, processing, storage capacity
  - Equipped with special hardware
    - Provides network management functions
- Advantages relative to peer-to-peer networks
  - User credential assigned from one place
  - Multiple shared resource access centrally controlled
  - Central problem monitoring, diagnostics, correction capabilities
  - More scalable

Networking Hardware and Physical Topologies

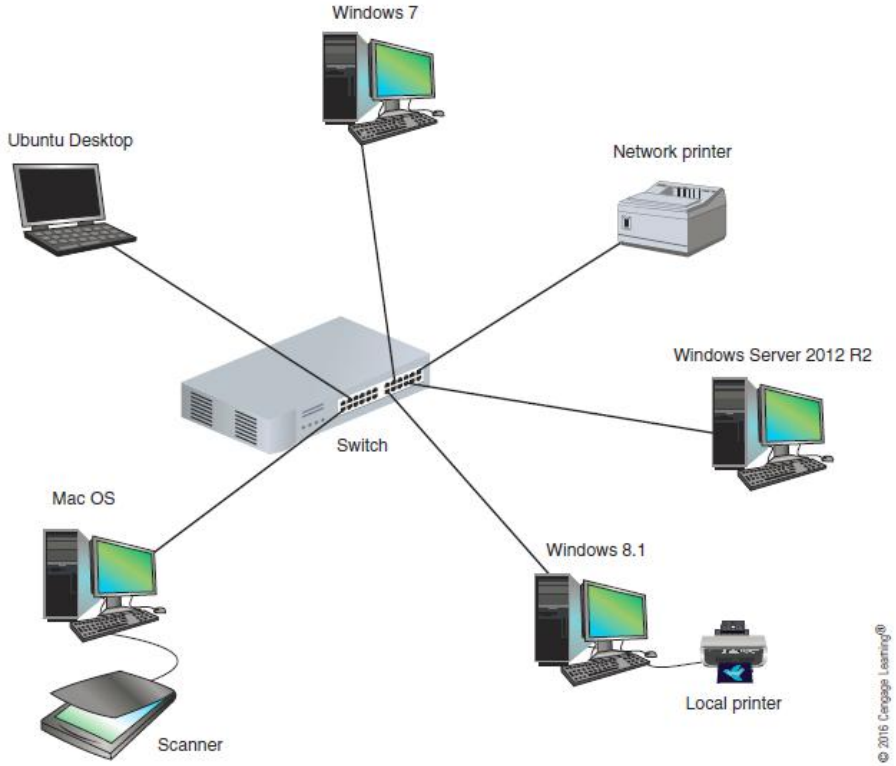


Figure 1-6 This LAN has five computers, a network printer, a local printer, a scanner, and a switch, and is using a star topology

LANs and Their Hardware

- Local area network (LAN) - usually contained in a small space
  - Such as an office or building
- Switch - receives incoming data from one of its ports and redirects it to another port or multiple ports
  - Will send the data to its intended destination
- Star topology - all devices connect to one central device (usually a switch)
- Network interface card (NIC) - a network port used to attach a device to a network

LANs and Their Hardware

- A LAN can have several switches
- Backbone - a central conduit that connects the segments (pieces) of a network
  - Might use higher transmission speeds and different cabling than network cables connected to computers
- Three switches daisy-chained together in a single line is said to use a bus topology
  - However, each switch is connected to computers via a star topology, making it a star-bus topology
  - A topology that combines topologies is known as a hybrid topology

LANs and Their Hardware

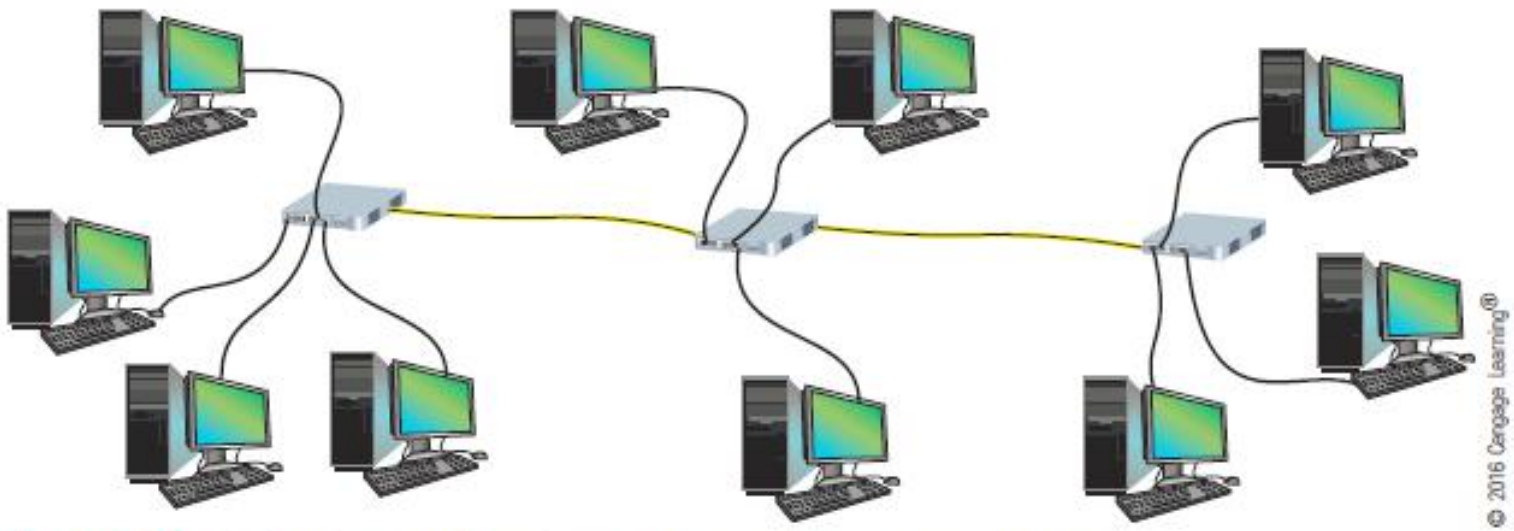


Figure 1-10 This local network has three switches, and is using a star-bus topology

LANs and Their Hardware

- Router - a device that manages traffic between two or more networks
  - Can help find the best path for traffic to get from one network to another
- Routers can be used in small home networks to connect the home LAN to the Internet
- Industrial-grade routers can have several network ports, one for each network it connects to
- Difference between router and switch:
  - Router is like a gateway between networks

LANs and Their Hardware

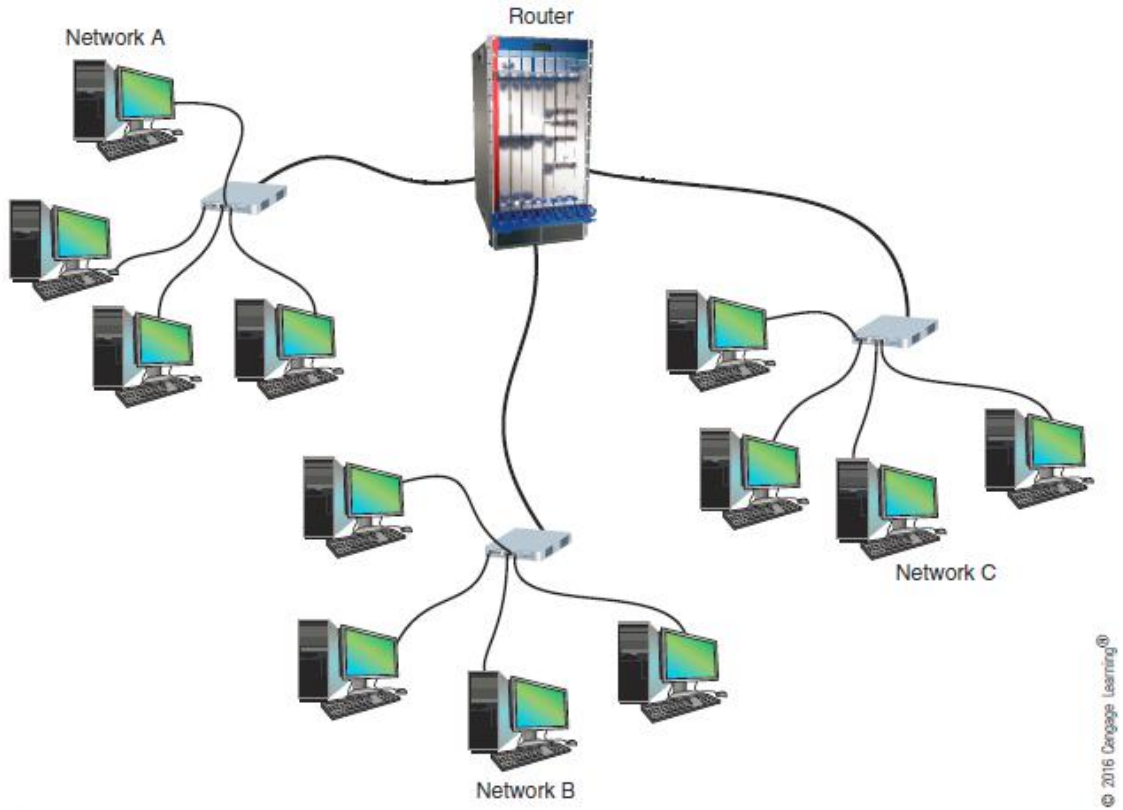


Figure 1-13 Three LANs connected by a router

MANs and WANs

- Metropolitan area network (MAN) - a group of connected LANs in the same geographical area
  - Also known as a campus area network (CAN)
- WAN (wide area network) - a group of LANs that spread over a wide geographical area
  - Internet is the largest and most varied WAN
- MANs and WANs often use different transmission methods and media than LANs
- PAN (personal area network) - smallest network
  - A network of personal devices

MANs and WAN

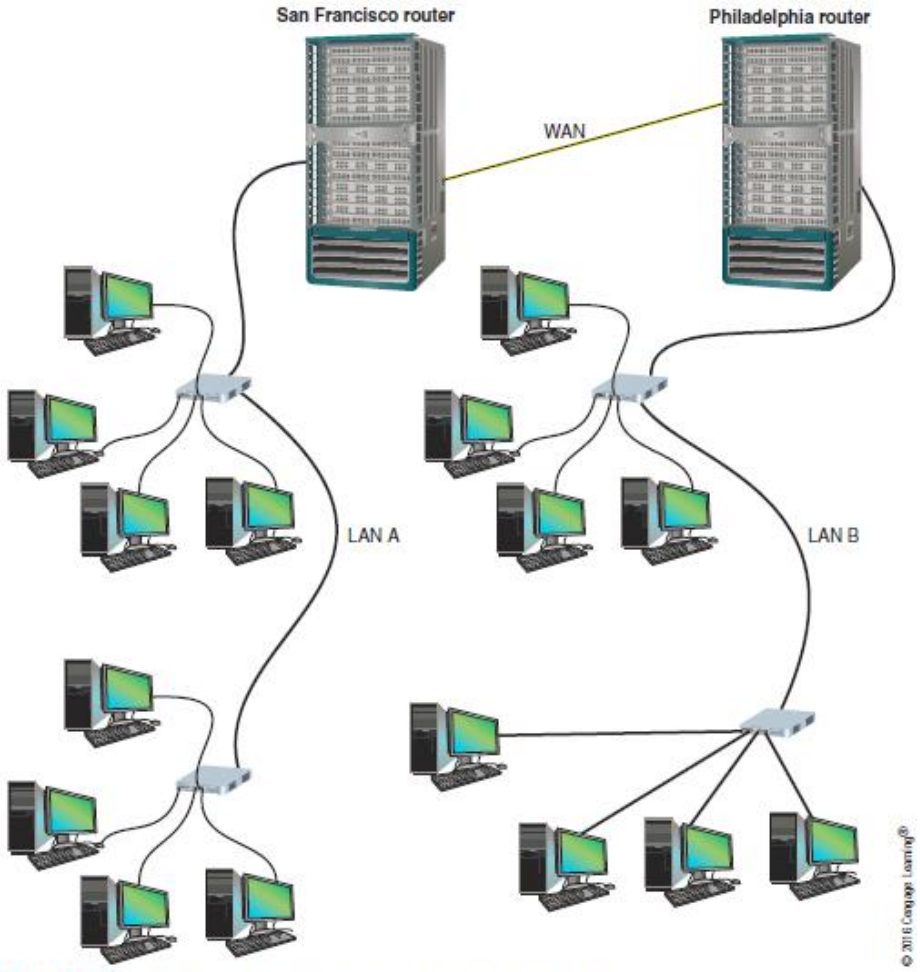


Figure 1-14 A WAN connects two LANs in different geographical areas

The Seven-Layer OSI Model

- OSI (Open Systems Interconnection) reference model - a seven-layer model developed to categorize the layers of communication
- Developed by ISO in the 1980s
- The layers are numbered in order, starting with Layer 1, the Physical layer at the bottom
  - Physical, Data Link, Network, Transport, Session, Presentation, Application

The OSI Model

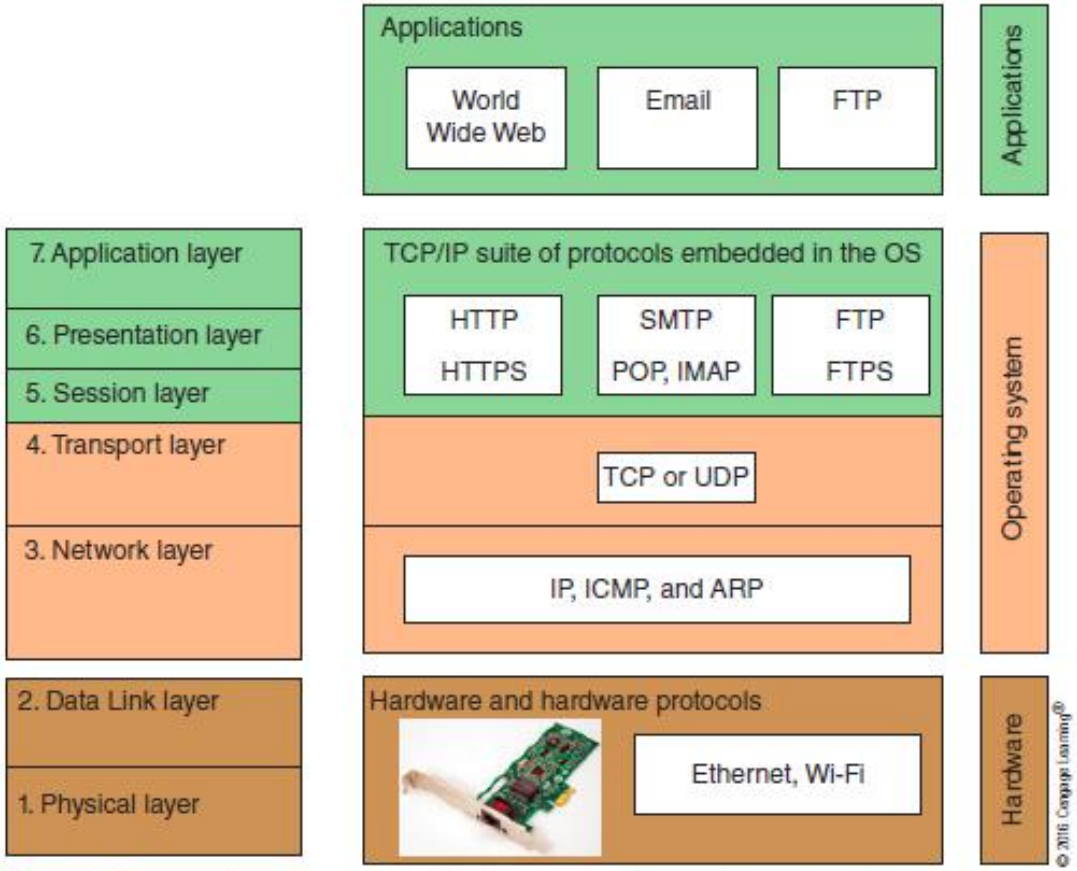


Figure 1-16 How software, protocols, and hardware map to the seven-layer OSI model

Layer 7: Application Layer

- Application layer - describes the interface between two applications, on separate computers
- Application layer protocols are used by programs that fall into two categories:
  - Provide services to a user, such as a browser and Web server
  - Utility programs that provide services to the system, such as SNMP that monitor and gather information about network traffic
- Payload - data that is passed between applications or utility programs and the OS

Layer 6: Presentation Layer

- Presentation layer - responsible for reformatting, compressing, and/or encrypting data in a way that the receiving application can read
- Example:
  - An email message can be encrypted at the Presentation layer by the email client or by the OS

Layer 5: Session Layer

- Session layer - describes how data between applications is synched and recovered if messages don't arrive intact at the receiving application
- The Application, Presentation, and Session layers are intertwined
  - Often difficult to distinguish between them
- Most tasks are performed by the OS when an application makes an API call to the OS
  - Application programming interface (API) call is the method an application uses when it makes a request of the OS

Layer 4: Transport Layer

- Transport layer - responsible for transporting Application layer payloads from one application to another
- Two main Transport layer protocols are:
  - TCP (Transmission Control Protocol) - makes a connection with the end host, checks whether data was received; called a connection-oriented protocol
  - UDP (User Datagram Protocol) - does not guarantee delivery by first connecting and checking whether data is received; called a connectionless protocol

Layer 4: Transport Layer

- Protocols add their own control information in an area at the beginning of the payload (called a header)
- Encapsulation - process of adding a header to the data inherited from the layer above
- The Transport layer header addresses the receiving application by a number called a port number
- If message is too large, TCP divides it into smaller messages called segments
  - In UDP, the message is called a datagram

Layer 3: Network Layer

- Network layer - responsible for moving messages from one node to another until reaches destination
- IP adds its own Network layer header to the segment or datagram
  - The entire Network layer message is called a packet
- IP address - assigned to each node on a network
  - Network layer uses it to uniquely identify each host
- IP relies on several routing protocols to find the best route for a packet to take to reach destination
  - ICMP and ARP are examples

Layer 2: Data Link Layer

- Layers 2 and 1 are responsible for interfacing with physical hardware on the local network
  - Protocols at these layers are programmed into firmware of a computer's NIC and other hardware
- Type of networking hardware or technology used on a network determine the Link Layer protocol used
  - Ethernet and Wi-Fi are examples
- The Link layer puts control information in a Link layer header and at the end of the packet in a trailer
  - Entire Link layer is called a frame

Layer 2: Data Link Layer

- MAC (Media Access Control) address - hardware address of the source and destination NICs
  - Also called a physical address, hardware address, or Data Link layer address
  - Embedded on every network adapter and are considered short-range addresses that can only find nodes on the local network

Layer 1: Physical Layer

- Physical layer - simplest layer and is responsible for sending bits via a wired or wireless transmission
- Can be transmitted as:
  - Wavelengths in the air
  - Voltage on a copper wire
  - Light (via fiber-optic cabling)

Protocol Data Unit or PDU

- Protocol data unit (PDU) - the technical name for a group of bits as it moves from one layer to the next and from one LAN to the next
  - Technicians loosely call this group of bits a message or a transmission

Table 1-1 Names for a PDU or message as it moves from one layer to another

OSI model	Name	Extremely technical name
Layer 7, Application layer Layer 6, Presentation layer Layer 5, Session layer	Payload or data	L7PDU
Layer 4, Transport layer	Segment (TCP) or datagram (UDP)	L4PDU
Layer 3, Network layer	Packet	L3PDU
Layer 2, Data Link layer	Frame	L2PDU
Layer 1, Physical layer	Bit	L1PDU

Summary of How the Layers Work Together

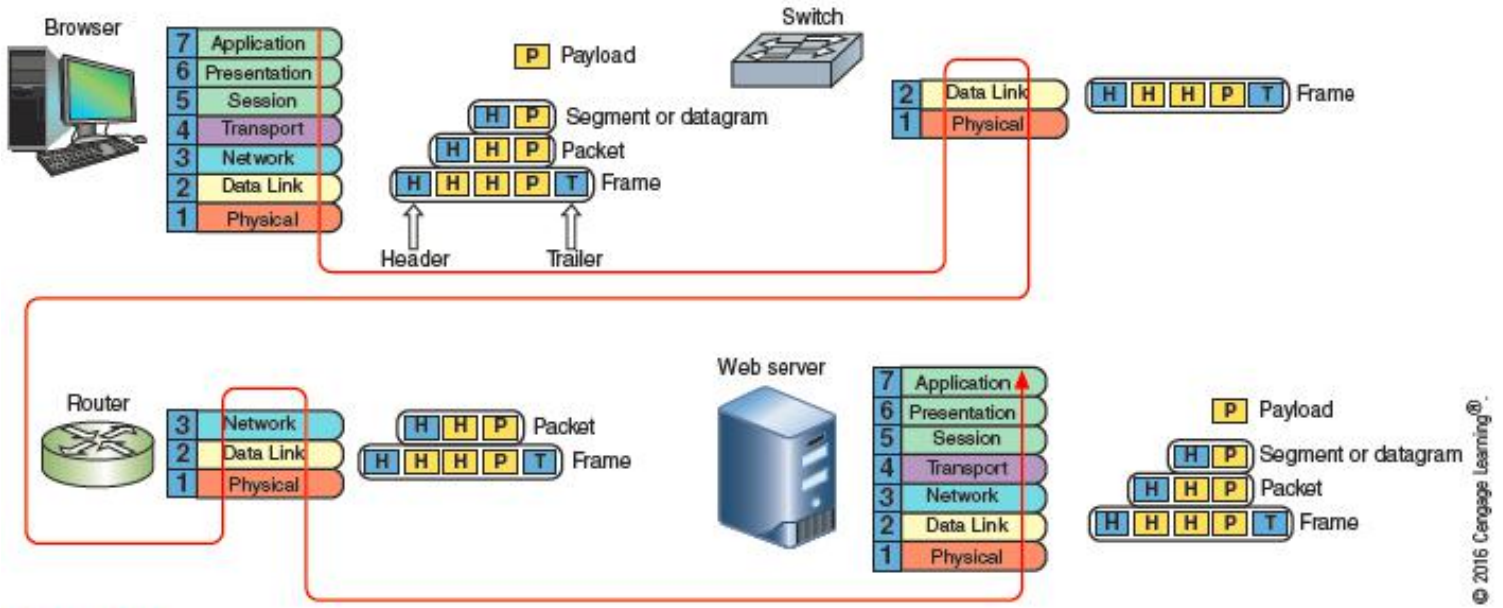


Figure 1-17 Follow the red line to see how the OSI layers work when a browser makes a request to a Web server

Summary of How the Layers Work Together

Table 1-2 Steps through the OSI layers during a browser-to-Web server transmission

Sending host	1. The browser, involving the Application, Presentation, and Session layers, creates an HTTP message or payload on its source computer and passes it down to the Transport layer.
	2. The Transport layer (TCP, which is part of the OS) encapsulates the payload by adding its own header and passes the segment down to the Network layer.
	3. IP at the Network layer in the OS receives the segment (depicted as two yellow boxes in the figure), adds its header, and passes the packet down to the Data Link layer.
	4. The Data Link layer on the NIC firmware receives the packet (depicted as three yellow boxes in the figure), adds its header and trailer, and passes the frame to the Physical layer.
	5. The Physical layer on the NIC hardware puts bits on the network.
Switch	6. The network transmission is received by a Data Link layer switch, which passes the frame up to the Data Link layer (firmware on the switch), which looks at the destination MAC address to decide where to send the frame.
	7. The pass-through frame is sent to the correct port on the switch and on to the router.
Router	8. The router has two NICs, one for each of the two networks to which it belongs. The Physical layer of the first NIC receives the frame and passes it up to the Data Link layer (NIC firmware), which removes the frame header and trailer and passes the packet up to IP at the Network layer (firmware program or other software) on the router.
	9. This Network layer IP program looks at the destination IP address and determines the next node en route for the packet and passes the packet back down to the Data Link layer on the second NIC. The Data Link layer adds a new frame header and trailer appropriate for this second NIC's LAN, including the MAC address of the next destination node. It passes the frame to its Physical layer (NIC hardware), which sends the bits on their way.
Destination host	10. When the frame reaches the destination host NIC, the Data Link layer NIC firmware receives it, removes the frame header and trailer, and passes the packet up to IP at the Network layer, which removes its header and passes the segment up to TCP at the Transport layer.
	11. TCP removes its header and passes the payload up to HTTP at the Application layer. HTTP presents the message to the Web server.

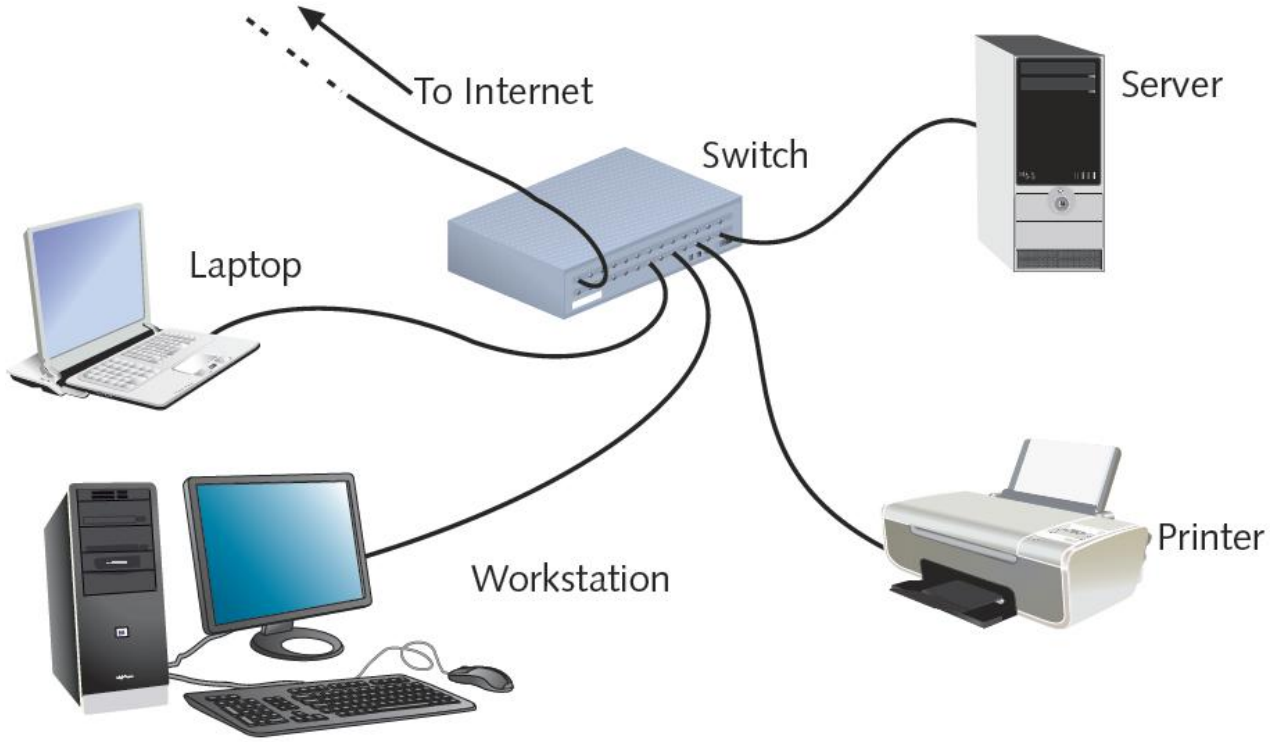
Switches

- Connectivity devices that subdivide a network
  - Segments
- Traditional switches
  - Operate at Data Link OSI model layer
- Modern switches
  - Can operate at Layer 3 or Layer 4
- Switches interpret MAC address information
- Common switch components
  - Internal processor, operating system, memory, ports

Switch Installation

- Follow manufacturer's guidelines
- General steps (assume Cat 5 or better UTP)
  - Verify switch placement
  - Turn on switch
  - Verify lights, self power tests
  - Configure (if necessary)
  - Connect NIC to a switch port (repeat for all nodes)
  - After all nodes connected, turn on nodes
  - Connect switch to larger network (optional)

Switch Installation (cont'd.)



Switching Methods

- Difference in switches
  - Incoming frames interpretation
  - Frame forwarding decisions making
- Four switching modes exist
  - Two basic methods discussed
    - Cut-through mode
    - Store-and-forward mode

Switching Methods (cont'd.)

- Cut-through mode
  - Switch reads frame's header
  - Forwarding decision made before receiving entire packet
    - Uses frame header: first 14 bytes contains destination MAC address
  - Cannot verify data integrity using frame check sequence
  - Can detect erroneously shortened packets (runts)
  - Runt detected: wait for integrity check

Switching Methods (cont'd.)

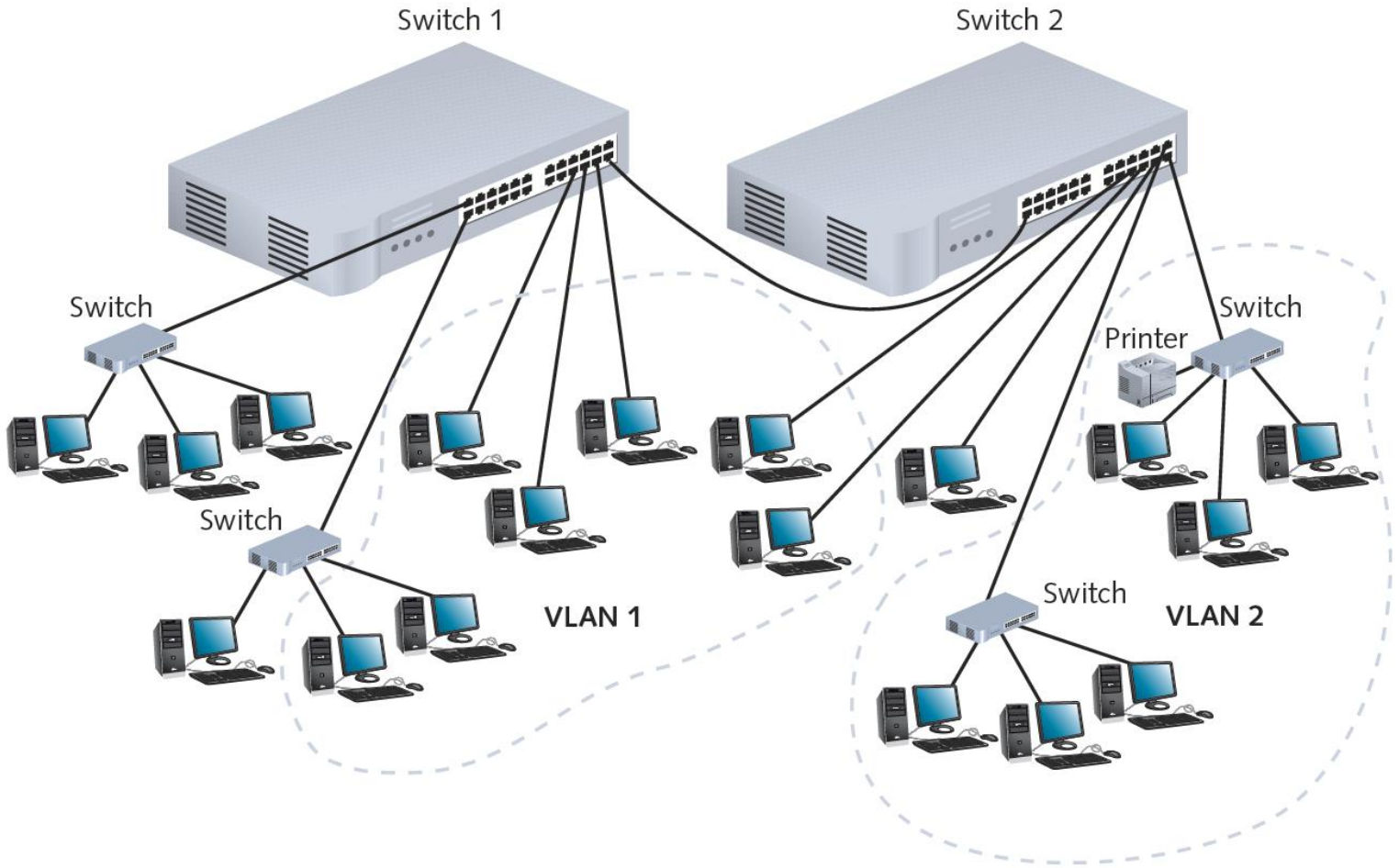
- Cut-through mode (cont'd.)
  - Cannot detect corrupt packets
  - Advantage: speed
  - Disadvantage
    - Data buffering (switch flooded with traffic)
  - Best use
    - Small workgroups needing speed
    - Low number of devices

Switching Methods (cont'd.)

- Store-and-forward mode
  - Switch reads entire data frame into memory
  - Checks for accuracy before transmitting information
  - Transmit data more accurately than cut-through mode
  - Slower than cut-through mode
  - Best uses
    - Larger LAN environments; mixed environments
  - Can transfer data between segments running different transmission speeds

VLANs and Trunking

- VLANs (virtual local area networks)
  - Logically separate networks within networks
    - Groups ports into broadcast domain
- Broadcast domain
  - Port combination making a Layer 2 segment
  - Ports rely on Layer 2 device to forward broadcast frames
- Collision domain
  - Ports in same broadcast domain
    - Do not share single channel


Switch 1
Switch 2
Switch
Switch
Printer
Switch
Switch
VLAN 1
VLAN 2

VLANs and Trunking (cont'd.)

- Advantage of VLANs
  - Flexible
    - Ports from multiple switches or segments
    - Use any end node type
  - Reasons for using VLAN
    - Separating user groups
    - Isolating connections
    - Identifying priority device groups
    - Grouping legacy protocol devices
    - Separating large network into smaller subnets

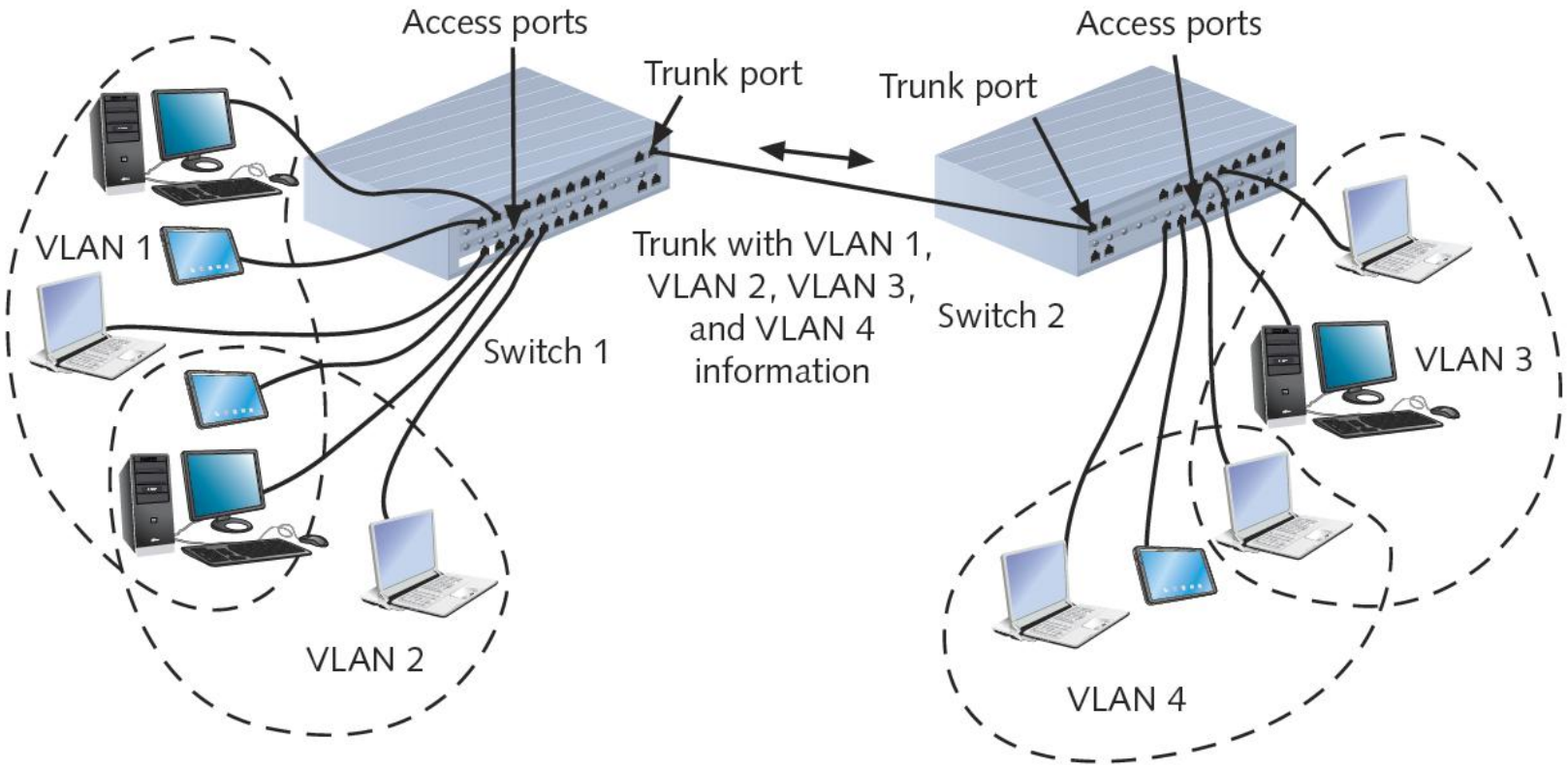
VLANs and Trunking (cont'd.)

- Switch typically preconfigured
  - One default VLAN
  - Cannot be deleted or renamed
- Create additional VLANs
  - Indicate to which VLAN each port belongs
  - Additional specifications
    - Security parameters, filtering instructions, port performance requirements, network addressing and management options
- Maintain VLAN using switch software

VLANs and Trunking (cont'd.)

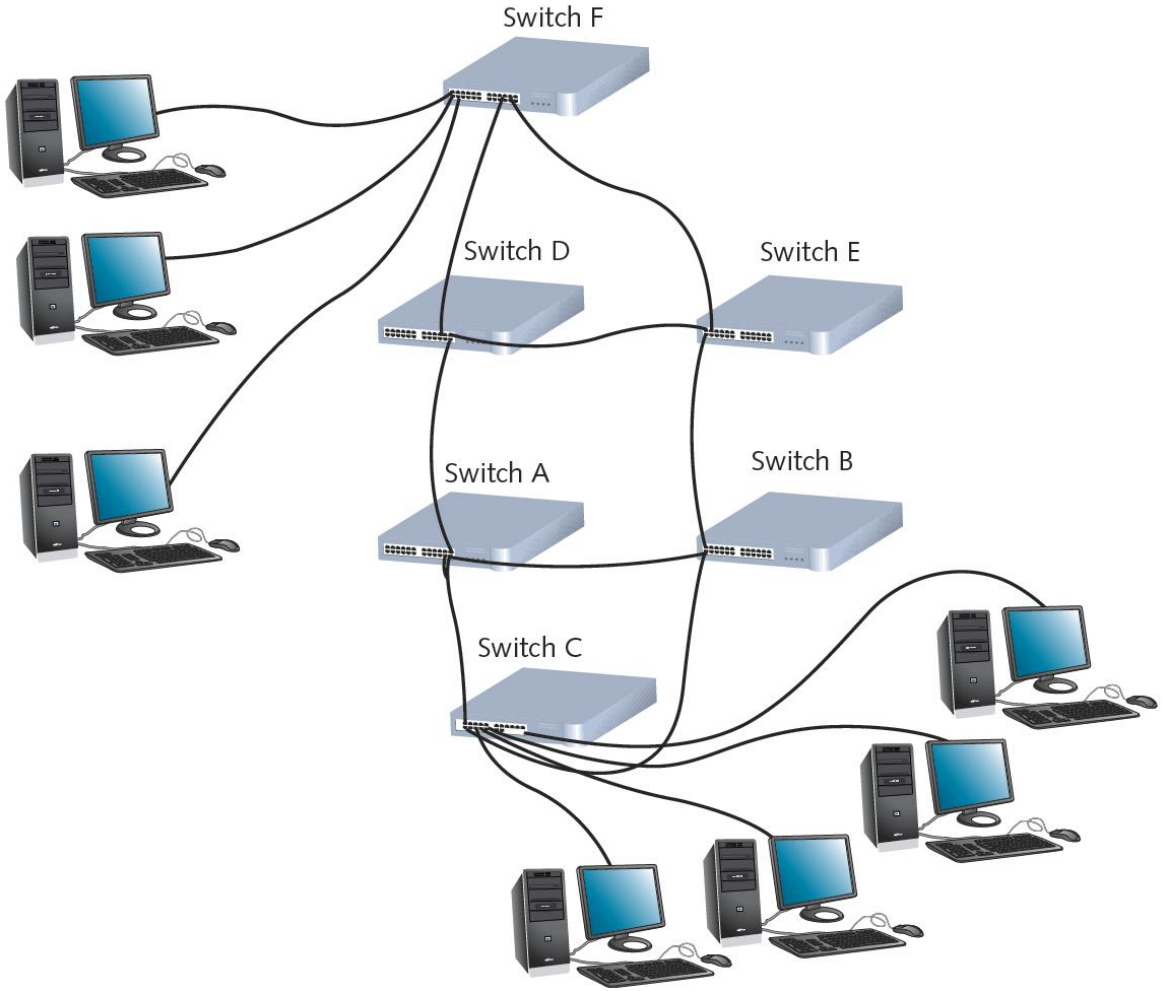
- Potential problem
  - Cutting off group from rest of network
    - Correct by using router or Layer 3 switch
- Trunking
  - Switch's interface carries traffic of multiple VLANs
- Trunk
  - Single physical connection between switches
- VLAN data separation
  - Frame contains VLAN identifier in header

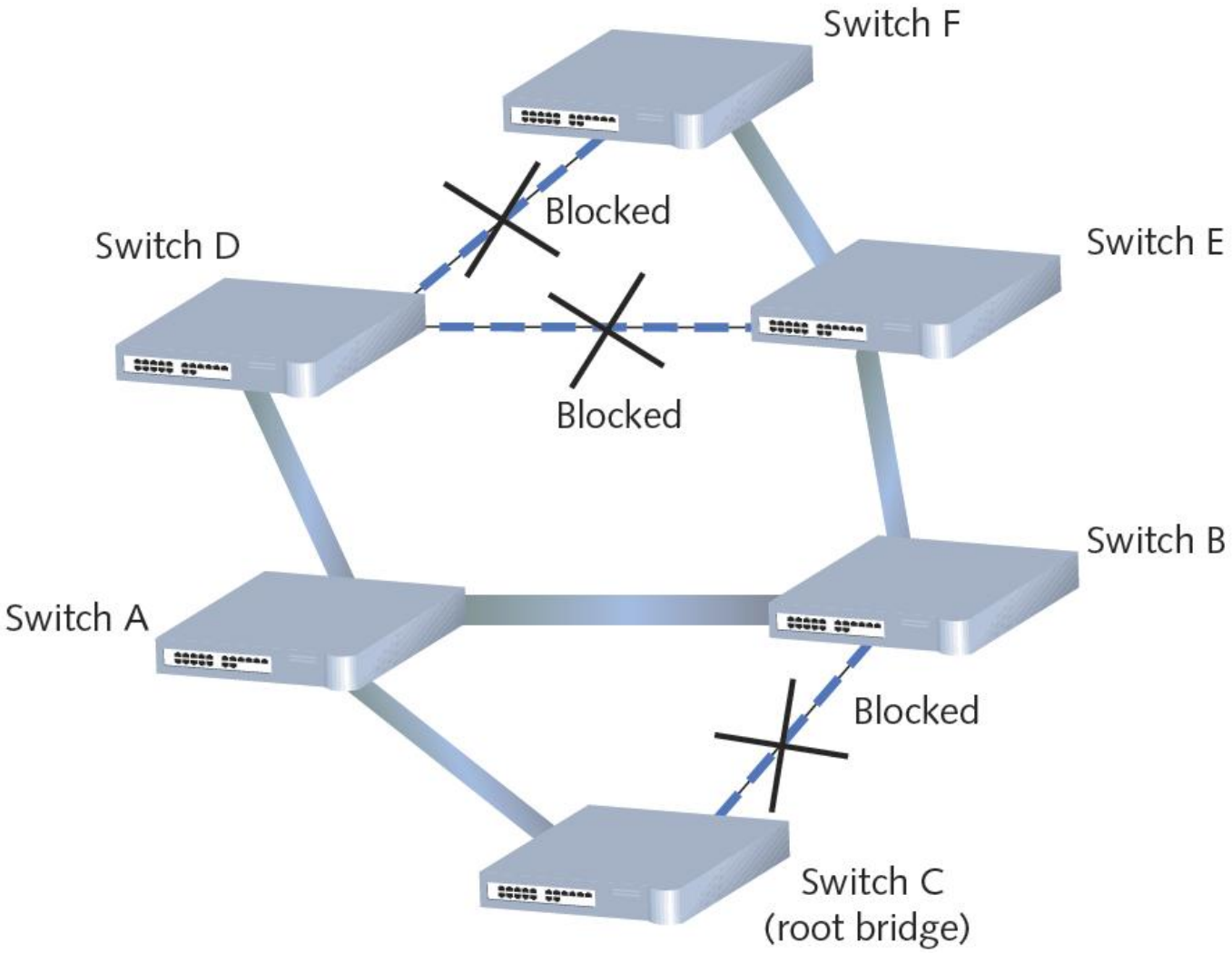
VLANs and Trunking (cont'd.)



STP (Spanning Tree Protocol)

- IEEE standard 802.1D
- Operates in Data Link layer
- Prevents traffic loops
  - Calculating paths avoiding potential loops
  - Artificially blocking links completing loop
- Three steps
  - Select root bridge based on Bridge ID
  - Examine possible paths between network bridge and root bridge
  - Disables links not part of shortest path


Switch F
Switch D
Switch E
Switch A
Switch B
Switch C


Switch F
Blocked
Switch D
Switch E
Blocked
Switch B
Switch A
Blocked
Switch C
(root bridge)

STP (cont'd.)

- History
  - Introduced in 1980s
    - Original STP too slow
  - RSTP (Rapid Spanning Tree Protocol)
    - Newer version
    - IEEE's 802.1w standard
- Cisco and Extreme Networks
  - Proprietary versions
- No enabling or configuration needed
  - Included in switch operating software

Content and Multilayer Switches

- Layer 3 switch (routing switch)
  - Interprets Layer 3 data
- Layer 4 switch
  - Interprets Layer 4 data
- Content switch (application switch)
  - Interprets Layer 4 through Layer 7 data
- Advantages
  - Advanced filtering
  - Keeping statistics
  - Security functions

Content and Multilayer Switches (cont'd.)

- Distinguishing between Layer 3 and Layer 4 switch
  - Manufacturer dependent
- Higher-layer switches
  - Cost more than Layer 2 switches
  - Used in network backbone

Routers

- Multiport connectivity device
  - Directs data between network nodes
  - Integrates LANs and WANs
    - Different transmission speeds, protocols
- Operate at Network layer (Layer 3)
  - Directs data from one segment or network to another
  - Logical addressing
  - Protocol dependent
- Slower than switches and bridges
  - Need to interpret Layers 3 and higher information

Routers (cont'd.)

- Traditional stand-alone LAN routers
  - Being replaced by Layer 3 routing switches
- New niche
  - Specialized applications
    - Linking large Internet nodes
    - Completing digitized telephone calls

Router Characteristics and Functions

- Intelligence
  - Tracks node location
  - Determine shortest, fastest path between two nodes
  - Connects dissimilar network types
- Large LANs and WANs
  - Routers indispensable
- Router components
  - Internal processor, operating system, memory, input and output jacks, management control interface

Router Characteristics and Functions (cont'd.)

- Multiprotocol routers
  - Multiple slots
  - Accommodate multiple network interfaces
- Inexpensive routers
  - Home, small office use

a b c

Figure 1. Routers of Cisco, Juniper and Huawei companies: a) Cisco ASR 9922; b) Juniper MX2020; c) Huawei NE5000E

Router Characteristics and Functions (cont'd.)

- Router capabilities
  - Connect dissimilar networks
  - Interpret Layer 3 addressing
  - Determine best data path
  - Reroute traffic

Router Characteristics and Functions (cont'd.)

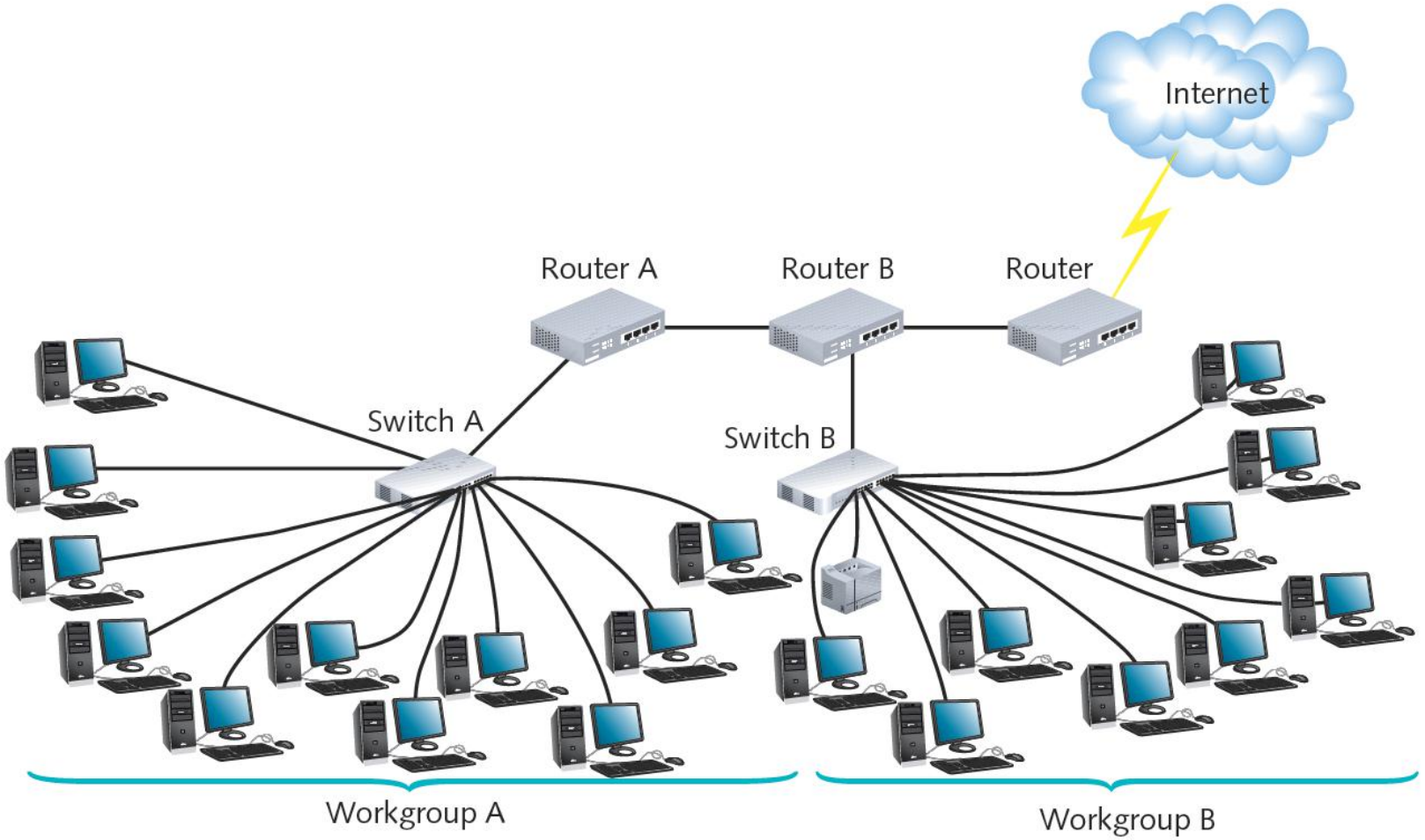
- Optional router functions
  - Filter broadcast transmissions
  - Enable custom segregation, security
  - Support simultaneous connectivity
  - Provide fault tolerance
  - Monitor network traffic
  - Diagnose problems and trigger alarms

Router Characteristics and Functions (cont'd.)

- Interior router
  - Directs data between nodes on a LAN
- Exterior router
  - Directs data between nodes external to a LAN
- Border routers
  - Connect autonomous LAN with a WAN
- Routing tables
  - Identify which routers serve which hosts

Router Characteristics and Functions (cont'd.)

- Static routing
  - Router configured to use specific path between nodes
- Dynamic routing
  - Automatically calculates best path between nodes
- Installation
  - Simple for small office or home office LANs
    - Web-based configuration
  - Challenging for sizable networks


Internet
Router A
Router B
Router
Switch A
Switch B
Workgroup A
Workgroup B

Routing Protocols

- Best path
  - Most efficient route from one node to another
  - Dependent on:
    - Hops between nodes
    - Current network activity
    - Unavailable link
    - Network transmission speed
    - Topology
  - Determined by routing protocol

Routing Protocols (cont'd.)

- Routing metric factors
  - Number of hops
  - Throughput on potential path
  - Delay on a potential path
  - Load (traffic)
  - Maximum transmission unit (MTU)
  - Cost
  - Reliability of potential path

Routing Protocols (cont'd.)

- Router convergence time
  - Time router takes to recognize best path
    - Change or network outage event
  - Distinguishing feature
    - Overhead; burden on network to support routing protocol

Routing Protocols (cont'd.)

- Distance-vector routing protocols
  - Determine best route based on distance to destination
  - Factors
    - Hops, latency, network traffic conditions
- RIP (Routing Information Protocol)
  - Only factors in number of hops between nodes
    - Limits 15 hops
  - Type of IGP (Interior Gateway Protocol)
    - Can only route within internal network
  - Slower and less secure than other routing protocols

Routing Protocols (cont'd.)

- RIPv2 (Routing Information Protocol Version 2)
  - Generates less broadcast traffic, more secure
  - Cannot exceed 15 hops
  - Less commonly used
- BGP (Border Gateway Protocol)
  - Communicates using BGP-specific messages
  - Many factors determine best paths
  - Configurable to follow policies
  - Type of EGP (Exterior Gateway Protocol)
  - Most complex (choice for Internet traffic)

Routing Protocols (cont'd.)

- Link-state routing protocol
  - Routers share information
    - Each router independently maps network, determines best path
- OSPF (Open Shortest Path First)
  - Interior or border router use
  - No hop limit
  - Complex algorithm for determining best paths
  - Each OSPF router
    - Maintains database containing other routers' links

Routing Protocols (cont'd.)

- IS-IS (Intermediate System to Intermediate System)
  - Codified by ISO
  - Interior routers only
  - Supports two Layer 3 protocols
    - IP
    - ISO-specific protocol
  - Less common than OSPF

Routing Protocols (cont'd.)

- Hybrid
  - Link-state and distance-vector characteristics
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
    - Most popular
    - Cisco network routers only
  - EIGRP benefits
    - Fast convergence time, low network overhead
    - Easier to configure and less CPU-intensive than OSPF
    - Supports multiple protocols
    - Accommodates very large, heterogeneous networks

Routing Protocols (cont'd.)

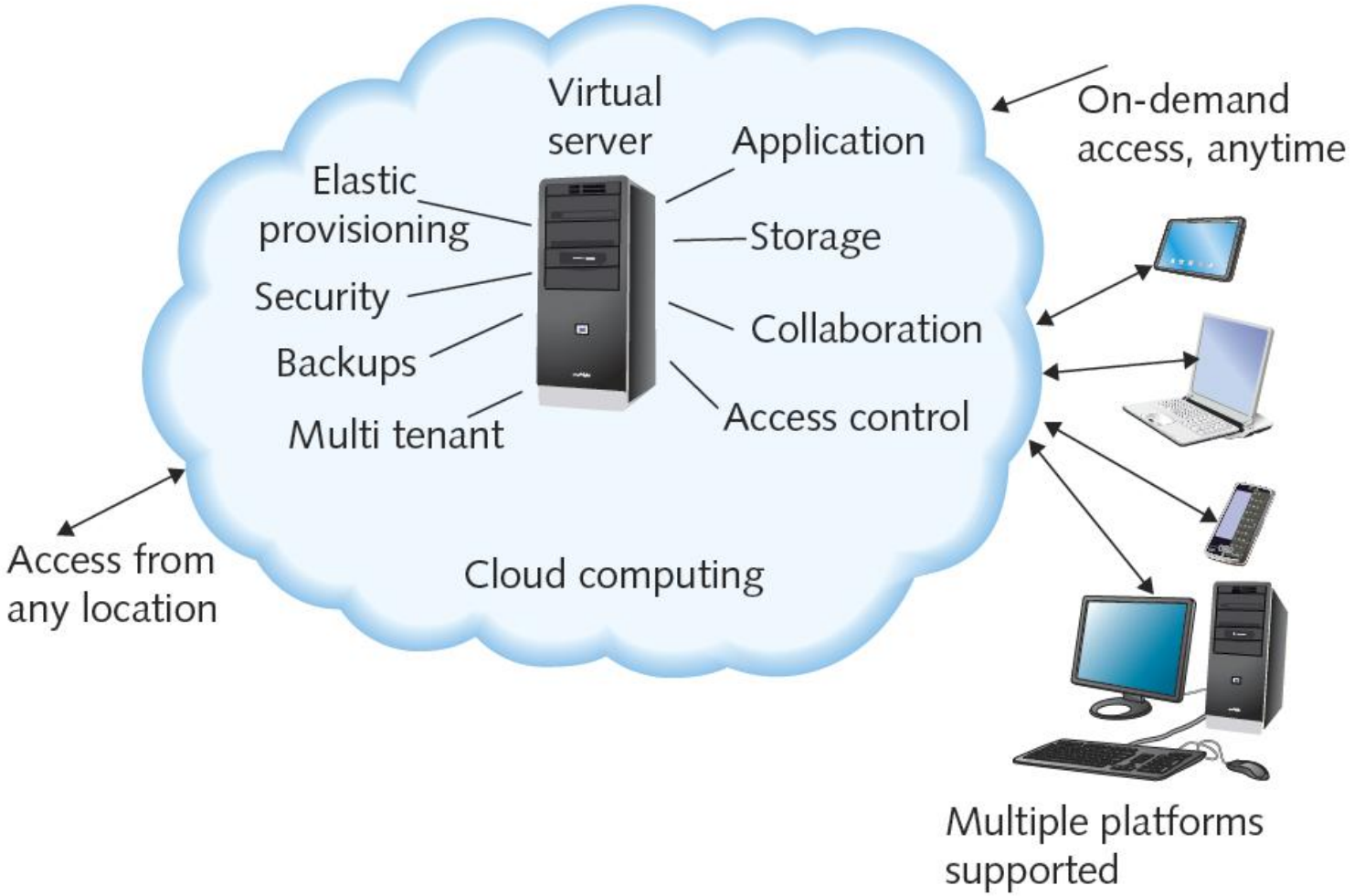
Routing protocol	Type	Location
RIP (Routing Information Protocol)	Distance-vector	Interior
RIPv2 (Routing Information Protocol version 2)	Distance-vector	Interior
BGP (Border Gateway Protocol)	Distance-vector	Exterior
OSPF (Open Shortest Path First)	Link-state	Interior or exterior
IS-IS (Intermediate System to Intermediate System)	Link-state	Interior
EIGRP (Enhanced Interior Gateway Routing Protocol)	Hybrid	Exterior or Interior

Gateways and Other Multifunction Devices

- Gateway
  - Combination of networking hardware and software
  - Connects two systems using different formatting, communications protocols, architecture
  - Repackages information
  - Resides on servers, microcomputers, connectivity devices, mainframes
- Popular gateways
  - E-mail gateway, Internet gateway, LAN gateway, voice/data gateway, firewall

Cloud Computing

- Internet frequently pictured as a cloud
- Cloud computing
  - Flexible provision of data storage, applications, and services
    - To multiple clients over a network
- Cloud computing distinguishing features
  - Self-service and on-demand
  - Elastic
  - Supports multiple platforms
  - Resource pooling and consolidation
  - Metered service



Example of cloud computing

Cloud Computing (cont'd.)

- Can provide virtual desktops
  - Operating environments hosted virtually
  - Different physical computer than one user interacts with
- NaaS (Network as a Service)
  - Service provider offers customers complete set of networking services
- Types of delivery
  - Public cloud
  - Private cloud

IT Masters
itmasters.edu.au

Charles Sturt University

Questions?

IT Masters
itmasters.edu.au

Charles Sturt University

++++

Network+ Short Course

Presented by Matt Constable

Module 2

IT Masters
itmasters.edu.au

Charles Sturt University

Network+ Short Course

Based on subject :
ITE526: Internetworking Fundamentals

Part of the :
Master of Networking and Systems Administration
Master of Management (IT)

Overview

- **Infrastructure**
  - Given a scenario, deploy the appropriate cabling solution.
  - Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them.
  - Explain the purposes and use case for advanced networking devices.
  - Explain the purposes of virtualization and network storage techniques.
  - Compare and contrast WAN technologies.

This Evenings Topics

- **WAN Essentials**
- **Virtualization Principles**
- **VPN Principles**

WAN Essentials

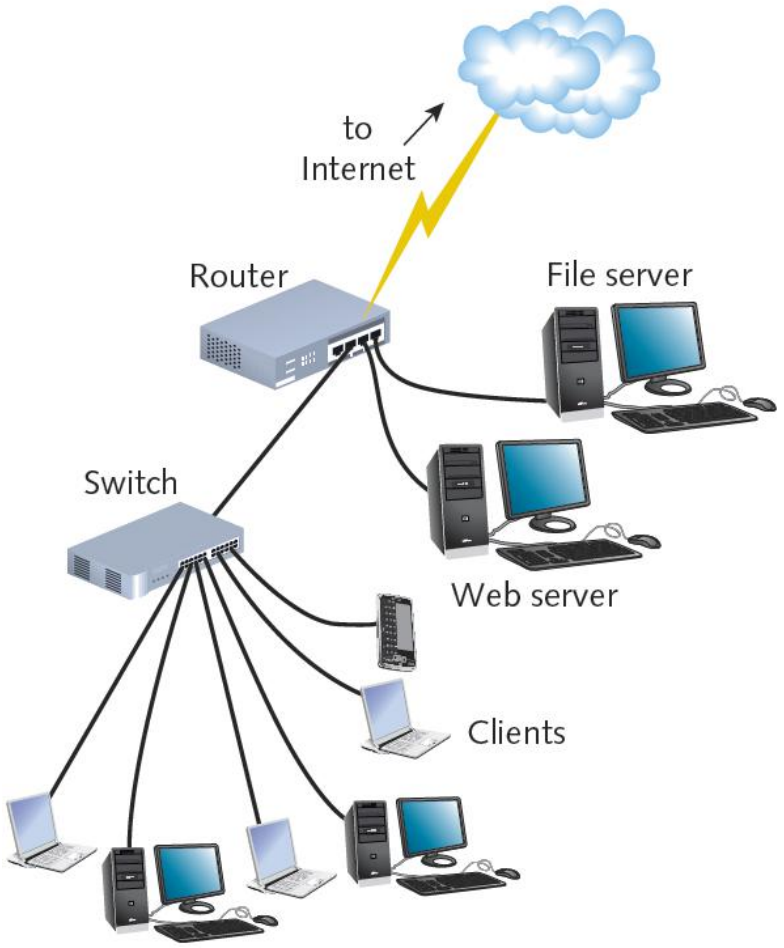
- WAN
  - Network traversing some distance, connecting LANs
  - Transmission methods depend on business needs
- WAN and LAN common properties
  - Client-host resource sharing
  - Layer 3 and higher protocols
  - Packet-switched digitized data

WAN Essentials

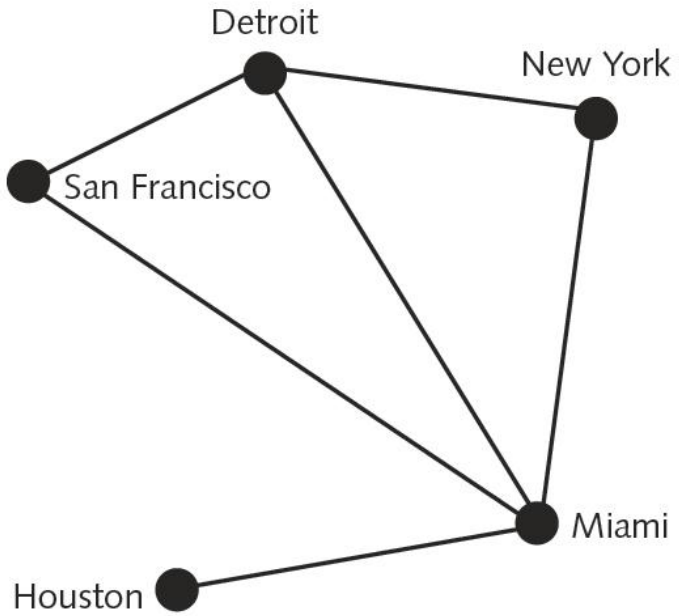
- WAN and LAN differences
  - Layers 1 and 2 access methods, topologies, media
  - LAN wiring: privately owned
  - WAN wiring: public through NSPs (network service providers)
    - Examples: AT&T, Verizon, Sprint
- WAN site
  - Individual geographic locations connected by WAN
- WAN link
  - WAN site to WAN site connection

WAN Topologies

- Differences from LAN topologies
  - Distance covered, number of users, traffic
  - Connect sites via dedicated, high-speed links
    - Use different connectivity devices
- WAN connections
  - Require Layer 3 devices
    - Routers
  - Cannot carry nonroutable protocols


to
Internet
Router
File server
Switch
Web server
Clients

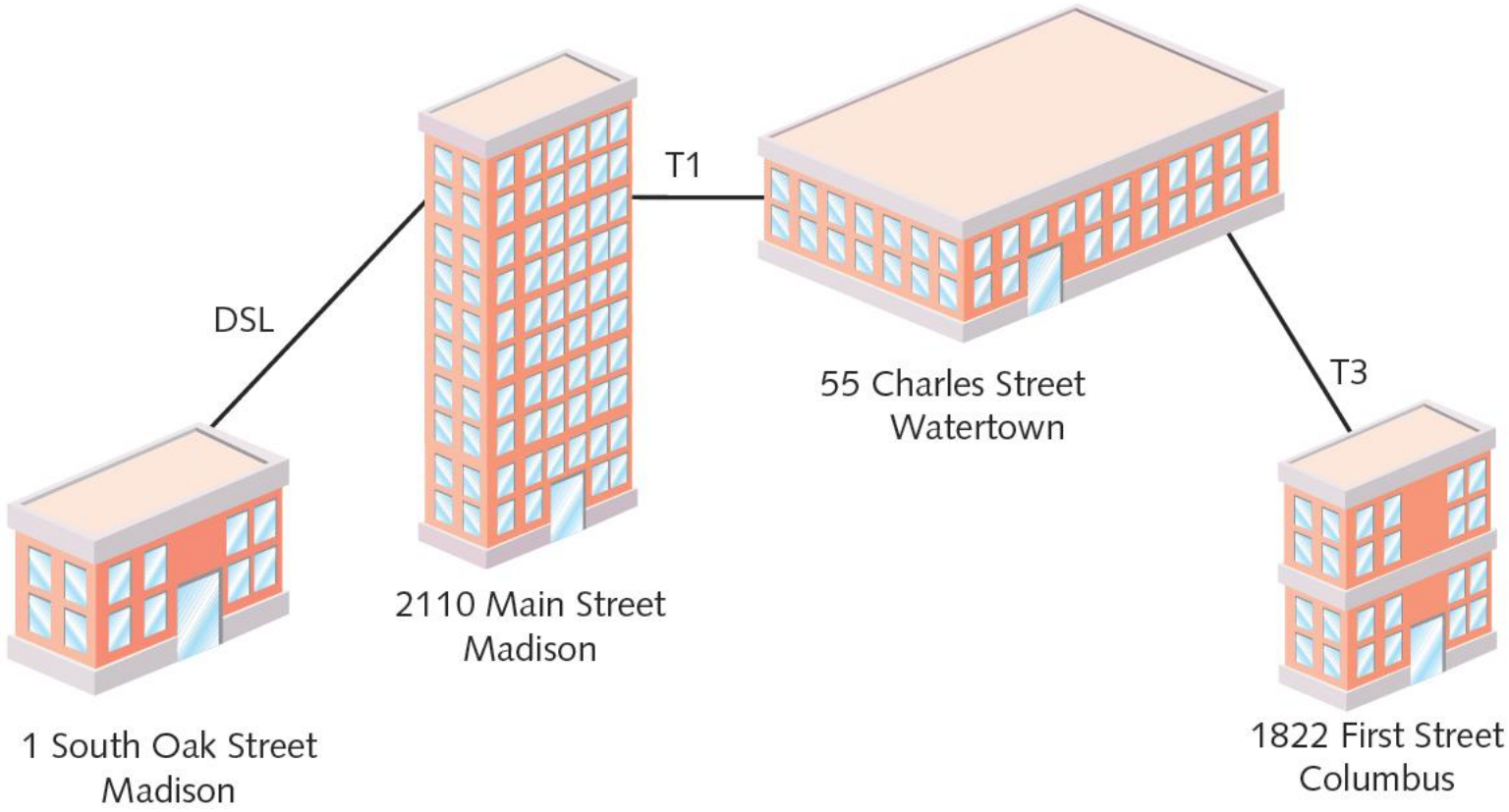
LAN


Detroit
New York
San Francisco
Miami
Houston

WAN

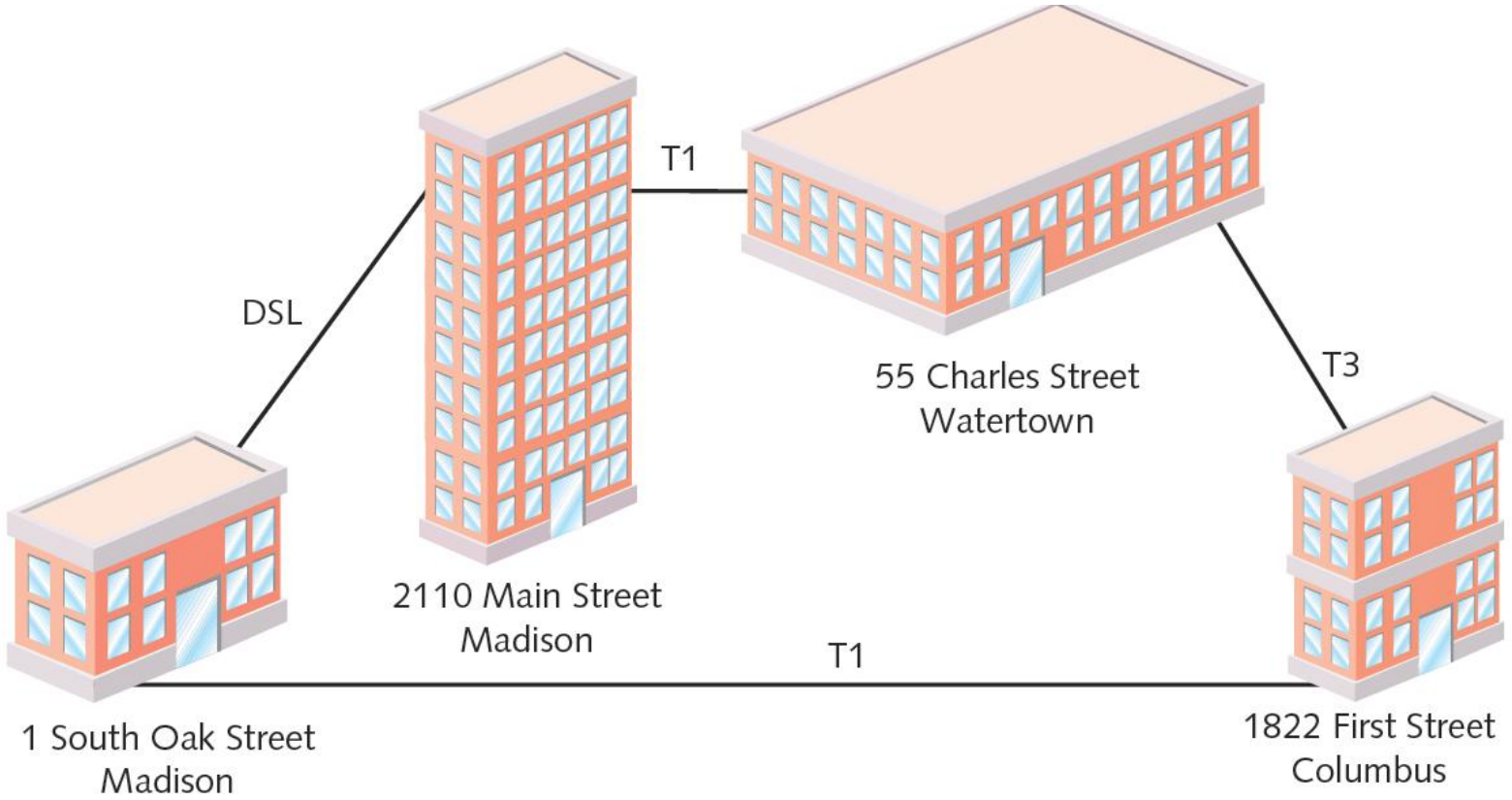
Bus

- Bus topology WAN
  - Each site connects serially to two sites maximum
  - Network site dependent on every other site to transmit and receive traffic
  - Different locations connected to another through point-to-point links
- Best use
  - Organizations requiring small WAN, dedicated circuits
- Drawback
  - Not scalable


T1
DSL
T3
55 Charles Street
Watertown
2110 Main Street
Madison
1 South Oak Street
Madison
1822 First Street
Columbus

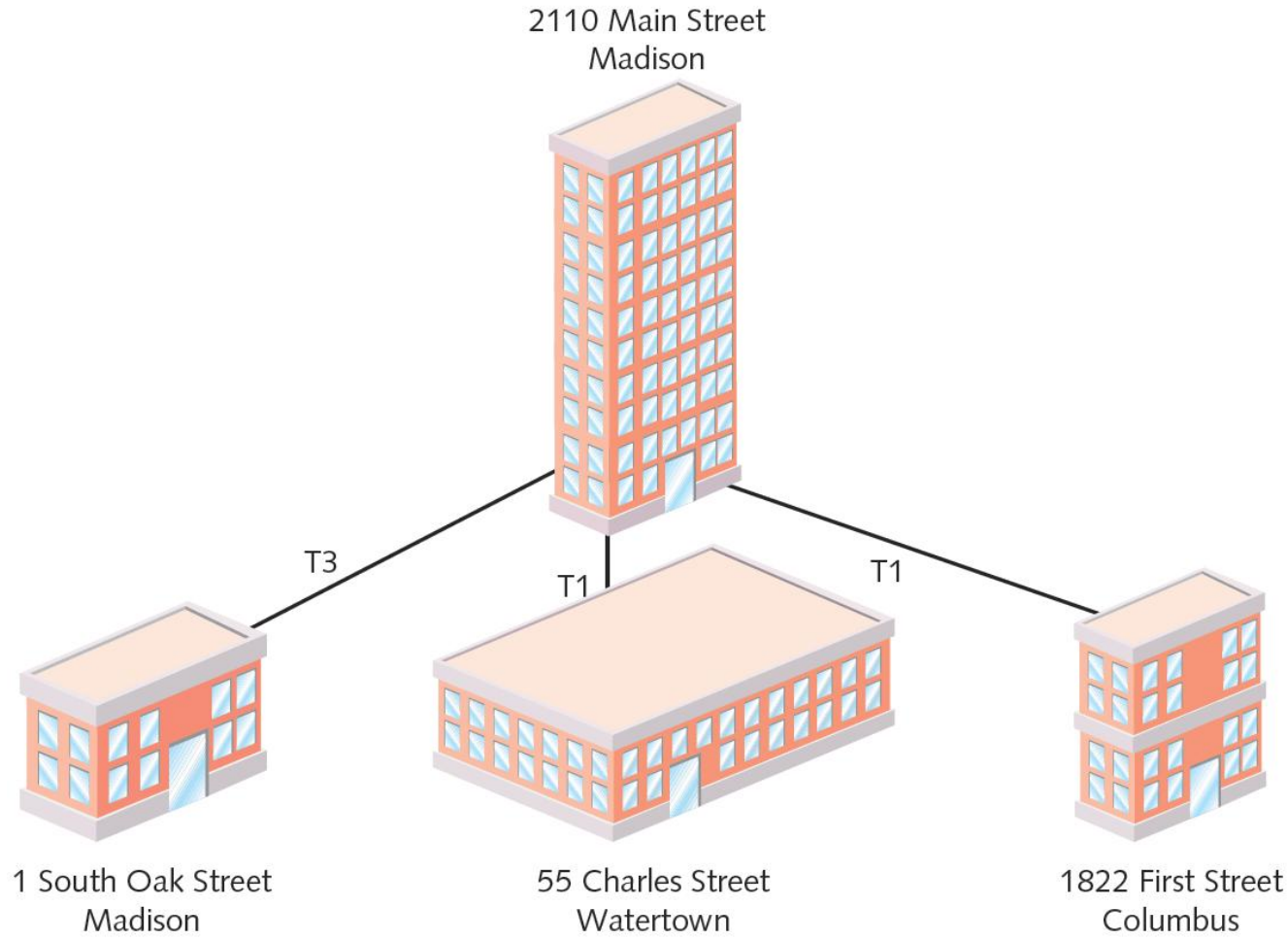
Ring

- Ring topology WAN
  - Each site connected to two other sites
  - Forms ring pattern
  - Connects locations
  - Relies on redundant rings
    - Data rerouted upon site failure
  - Expansion
    - Difficult, expensive
- Best use
  - Connecting maximum five locations


T1
DSL
55 Charles Street
Watertown
T3
2110 Main Street
Madison
T1
1 South Oak Street
Madison
1822 First Street
Columbus

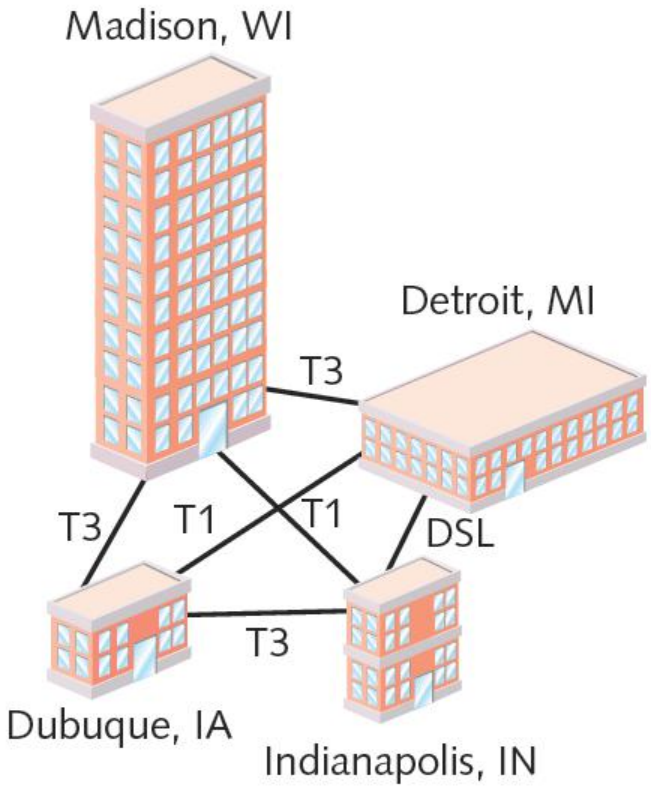
Star

- Star topology WAN
  - Single site central connection point
  - Separate data routes between any two sites
- Advantages
  - Single connection failure affects one location
  - Shorter data paths between any two sites
  - Expansion: simple, less costly
- Drawback
  - Central site failure can bring down entire WAN

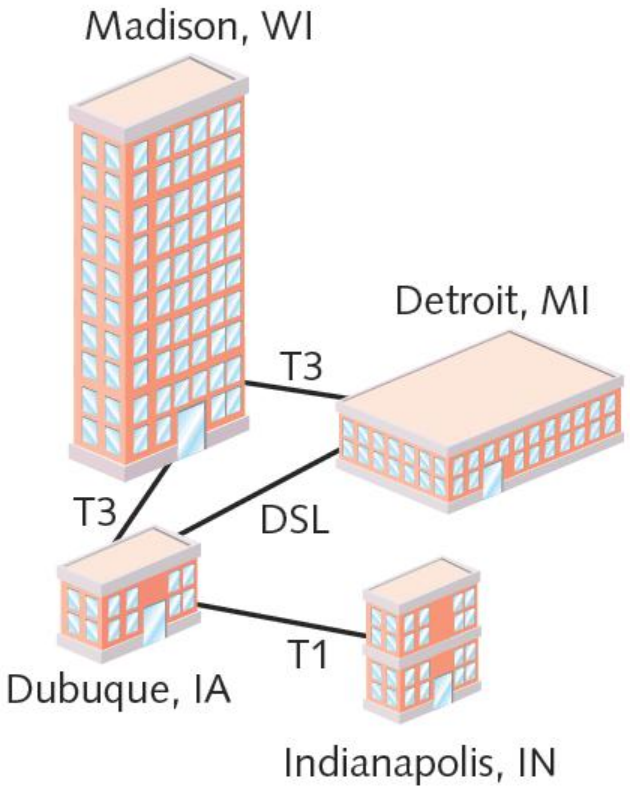

2110 Main Street
Madison
T3
T1
T1
1 South Oak Street
Madison
55 Charles Street
Watertown
1822 First Street
Columbus

Mesh

- Mesh topology WAN
  - Incorporates many directly interconnected sites
  - Data travels directly from origin to destination
  - Routers can redirect data easily, quickly
- Most fault-tolerant WAN type
- Full-mesh WAN
  - Every WAN site directly connected to every other site
  - Drawback: cost
- Partial-mesh WAN
  - Less costly



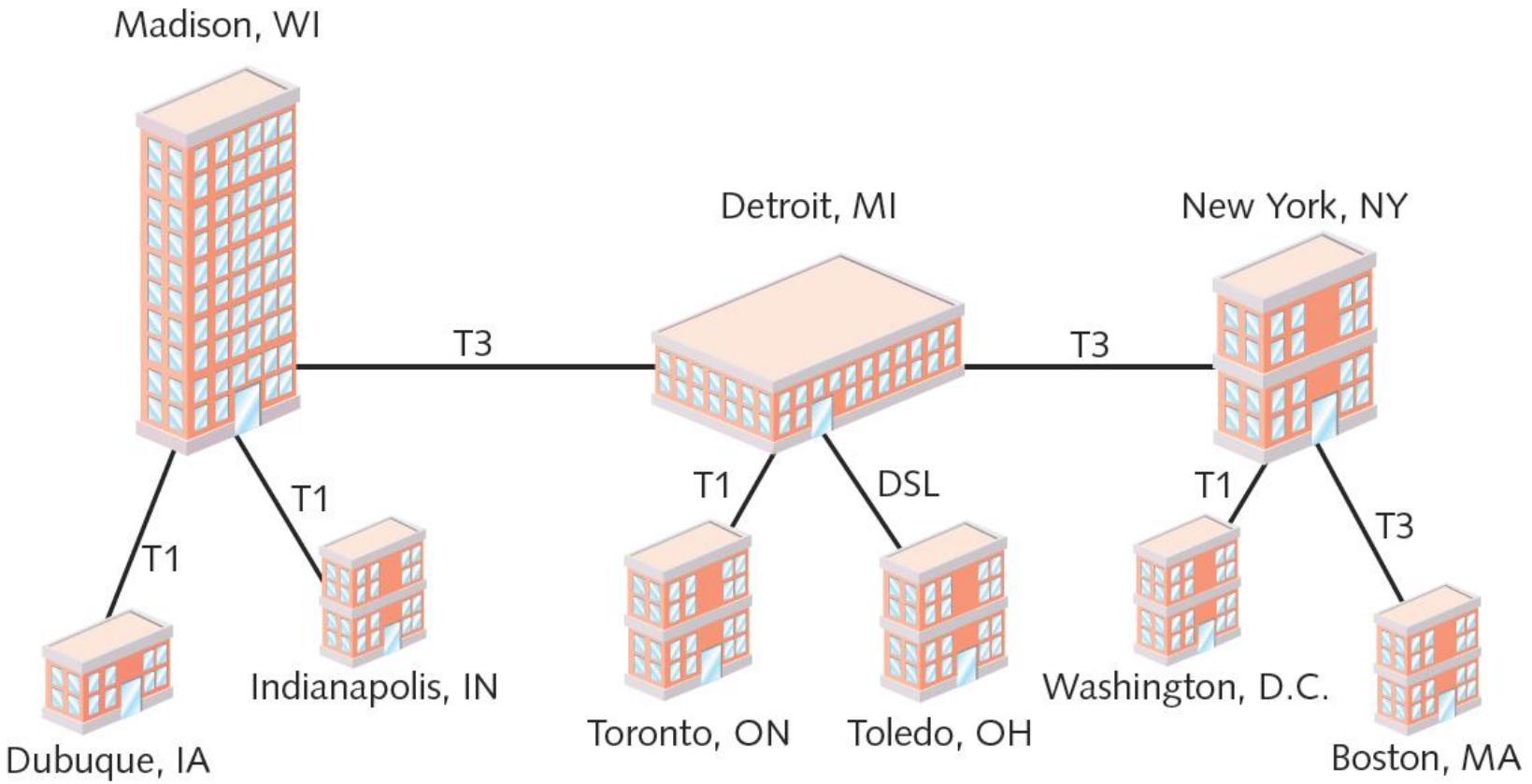
Full-mesh WAN



Partial-mesh WAN

Tiered

- Tiered topology WAN
  - Sites connected in star or ring formations
    - Interconnected at different levels
  - Interconnection points organized into layers
    - Form hierarchical groupings
- Flexibility
  - Allows many variations, practicality
  - Requires careful considerations
    - Geography, usage patterns, growth potential


Madison, WI
Detroit, MI
New York, NY
T3
T3
T1
T1
T1
DSL
T1
T3
Dubuque, IA
Indianapolis, IN
Toronto, ON
Toledo, OH
Washington, D.C.
Boston, MA

PSTN, X.25 & Frame-Relay

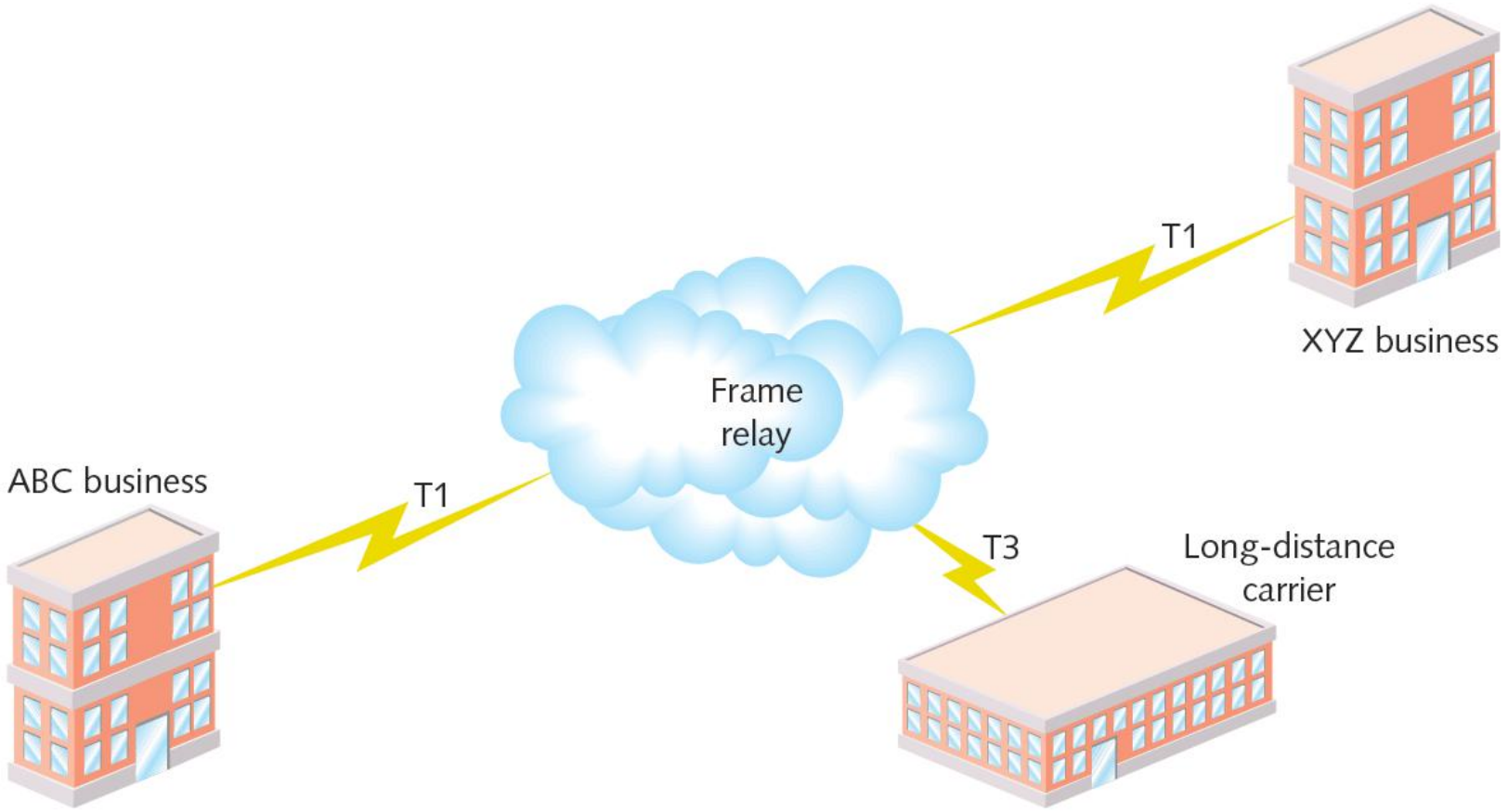
- All older style services.
- PSTN (Public Switched Telephone Network)
  - Dial-up connection
- X.25 ITU standard
  - Analog, packet-switching technology
    - Designed for long distance
  - Original standard: mid 1970s
    - Mainframe to remote computers: 64 Kbps throughput
  - Update: 1992
    - 2.048 Mbps throughput
    - Client, servers over WANs

PSTN, X.25 & Frame-Relay

- Frame relay
  - Updated X.25: digital, packet-switching
  - Protocols operate at Data Link layer
    - Supports multiple Network, Transport layer protocols
- Both perform error checking
  - Frame relay: no reliable data delivery guarantee
  - X.25: errors fixed or retransmitted
- Throughput
  - X.25: 64 Kbps to 45 Mbps
  - Frame relay: customer chooses

X.25 & Frame Relay

- Both use virtual circuits
  - Node connections with disparate physical links
    - Logically appear direct
  - Advantage: efficient bandwidth use
- Both configurable as SVCs (switched virtual circuits)
  - Connection established for transmission, terminated when complete
- Both configurable as PVCs (permanent virtual circuits)
  - Connection established before transmission, remains after transmission


ABC business
T1
Frame relay
T1
XYZ business
T3
Long-distance carrier

DSL (Digital Subscriber Line)

- Operates over PSTN
- Requires repeaters for longer distances
- Best suited for WAN local loop
- Supports multiple data, voice channels
  - Over single line
  - Higher, inaudible telephone line frequencies
- Uses advanced data modulation techniques
  - Data signal alters carrier signal properties
  - Amplitude or phase modulation

Types of DSL

- xDSL refers to all DSL varieties
  - ADSL, G.Lite, HDSL, SDSL, VDSL, SHDSL
- Two DSL categories
  - Asymmetrical and symmetrical
- Downstream
  - Data travels from carrier's switching facility to customer
- Upstream
  - Data travels from customer to carrier's switching facility

Types of DSL Quick Summary

DSL type	Maximum upstream throughput (Mbps)	Maximum downstream throughput (Mbps)	Distance limitation (feet)
ADSL ("full rate")	0.640	6.144	18,000
G.Lite (a type of ADSL)	0.512	1.544	25,000
HDSL or HDSL-2	1.544 or 2.048	1.544 or 2.048	18,000 or 12,000
SDSL	1.544	1.544	12,000
SHDSL	2.36 or 4.7	2.36 or 4.7	26,000 or 18,000
VDSL	1.6, 3.2, or 6.4	12.9, 25.9, or 51.8	1000–4500

Broadband Cable

- Cable companies connectivity option
- Based on TV signals coaxial cable wiring
  - Theoretical transmission speeds
    - 150 Mbps downstream; 10 Mbps upstream
  - Real transmission
    - 10 Mbps downstream; 2 Mbps upstream
    - Transmission limited (throttled)
    - Shared physical connections
- Best uses
  - Web surfing
  - Network data download

Broadband Cable

- Cable modem
  - Modulates, demodulates transmission, reception signals via cable wiring
  - Operates at Physical and Data Link layer
  - May connect to connectivity device

Figure 7-21 A cable modem
Courtesy Zoom Telephonics, Inc.

ATM (Asynchronous Transfer Mode)

- Functions in Data Link layer (Layer 2)
- Asynchronous communications method
  - Nodes do not conform to predetermined schemes
    - Specifying data transmissions timing
  - Each character transmitted
    - Start and stop bits
- Specifies Data Link layer framing techniques
- Fixed packet size
  - Packet (cell)
    - 48 data bytes plus 5-byte header

ATM

- Smaller packet size requires more overhead
  - Decrease potential throughput
  - Cell efficiency compensates for loss
- ATM relies on virtual circuits
  - ATM considered packet-switching technology
  - Virtual circuits provide circuit switching advantage
  - Reliable connection
- Allows specific QoS (quality of service) guarantee
  - Important for time-sensitive applications
- Speeds – 25-622Mbps

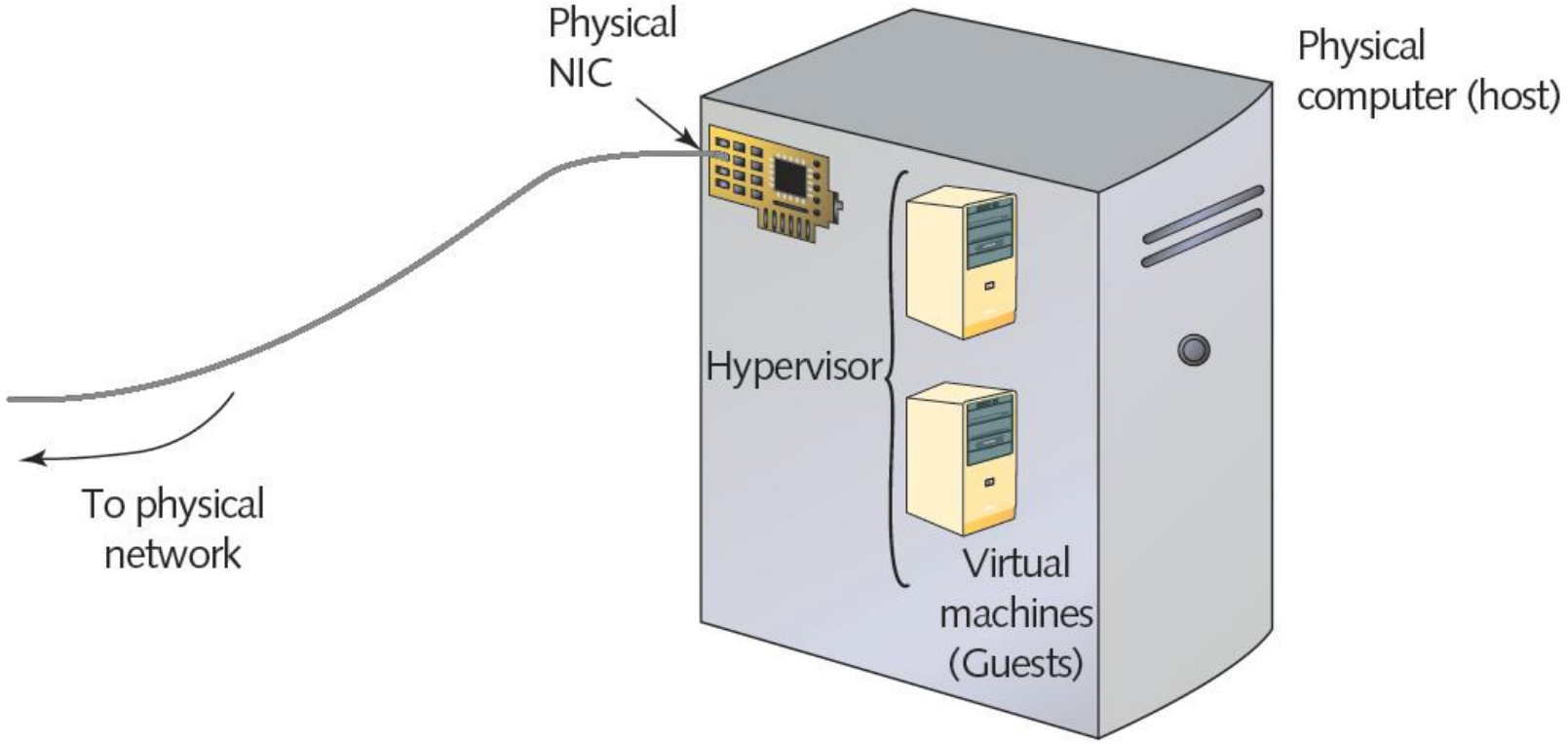
WAN Technologies Quick Reference

WAN technology	Typical media	Maximum throughput
Dial-up over PSTN	UTP or STP	56 Kbps theoretical; actual limit is 53 Kbps
X.25	UTP/STP (DS1 or DS3)	64 Kbps or 2.048 Mbps
Frame relay	UTP/STP (DS1 or DS3)	45 Mbps
BRI (ISDN)	UTP/STP (PSTN)	128 Kbps
PRI (ISDN)	UTP/STP (PSTN)	1.544 Mbps
T1	UTP/STP (PSTN), microwave, or fiber-optic cable	1.544 Mbps
Fractional T1	UTP/STP (PSTN), microwave, or fiber-optic cable	n times 64 Kbps (where *n* = number of channels leased)
T3	Microwave link or fiber-optic cable	45 Mbps
xDSL	UTP/STP (PSTN)	Theoretically, 1.544 Mbps–52 Mbps (depending on the type), but typical residential DSL throughputs are limited to 1.5 Mbps
Broadband cable	Hybrid fiber-coaxial cable	Theoretically, 56 Mbps downstream, 10 Mbps upstream, but actual throughputs are approximately 1.5–3 Mbps upstream and 256–768 Kbps downstream
BPL	Power line	Up to 1 Mbps actual throughput
ATM	Fiber-optic cable, UTP/STP (PSTN)	25 Mbps to 622 Mbps (depending on the customer's preferred bit rate)
SONET	Fiber-optic cable	51, 155, 622, 1244, 2488, 4976, 9952, or 39813 Mbps (depending on the OC level)

Virtualization

Virtualization

- Emulation of a computer, operating system environment, or application:
  - On a physical system
- Virtual machines (VMs)
  - Virtual workstations
  - Virtual servers
  - Can be configured to use different types of:
    - CPU
    - Storage drive
    - NIC



Elements of virtualization

Virtualization

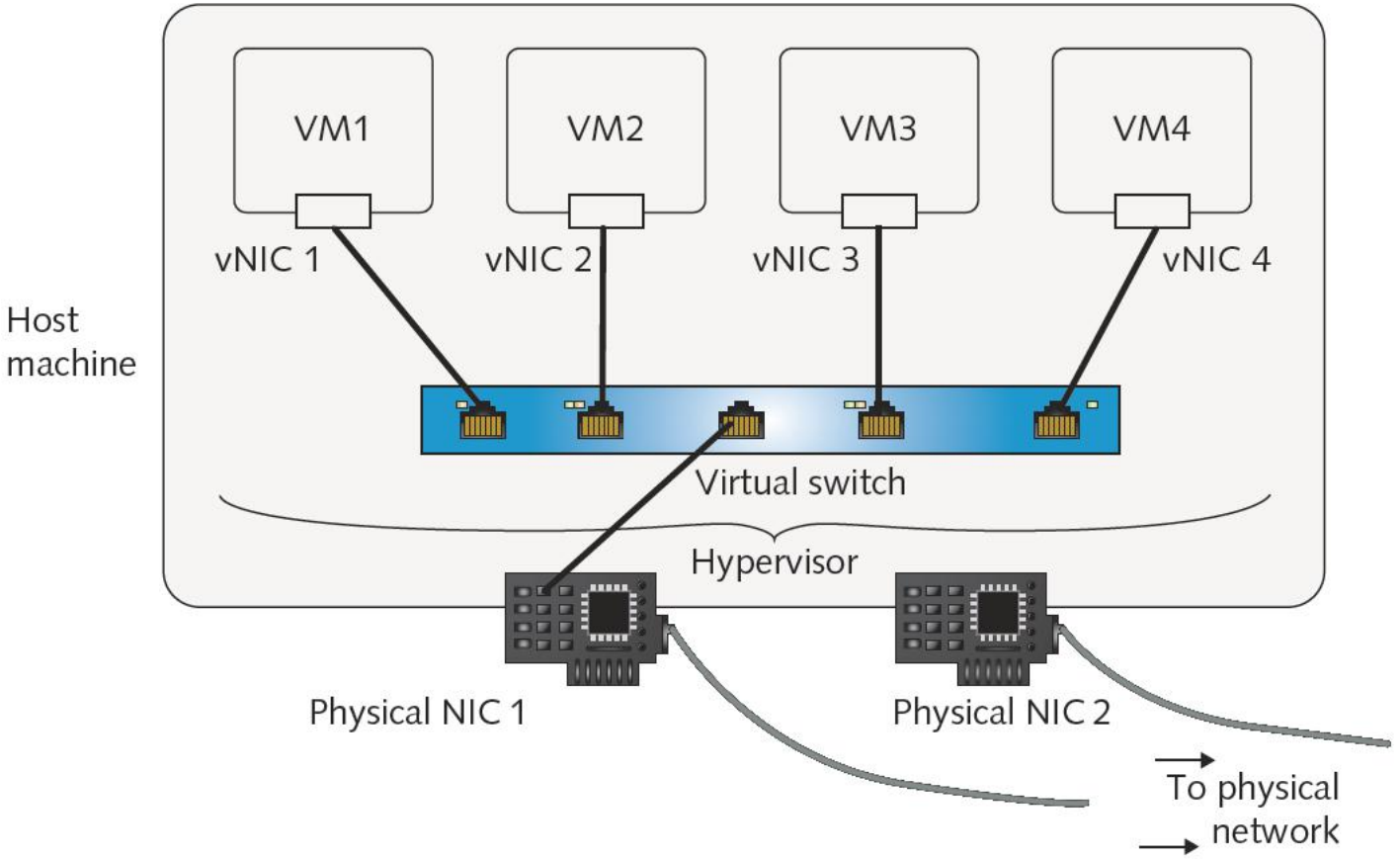
- Advantages
  - Efficient use of resources
  - Cost and energy savings
  - Fault and threat isolation
  - Simple backups, recovery, and replication
- Disadvantages
  - Compromised performance
  - Increased complexity
  - Increased licensing costs
  - Single point of failure

Virtual Network Components

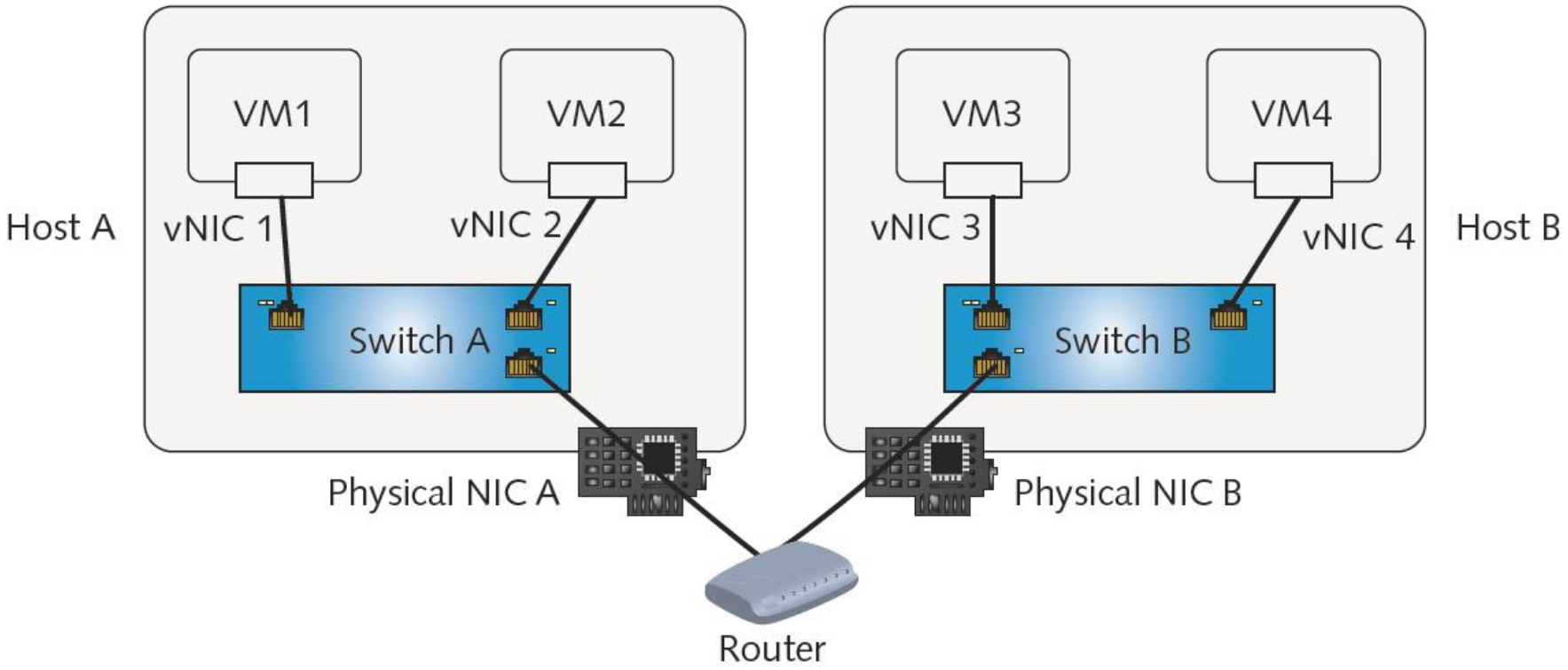
- Virtual network
  - Can be created to consist solely of virtual machines on a physical server
- Most networks combine physical and virtual elements

Virtual Switches and Bridges

- Virtual bridge or switch
  - Created when first VM's NIC is selected
  - Connects VM with host
  - Resides in RAM
- Virtual switch
  - Logically defined device
  - Operates at Data Link layer
  - Passes frames between nodes
- Virtual bridge
  - Connects vNICs with a network



Virtual servers on a single host connected with a virtual switch



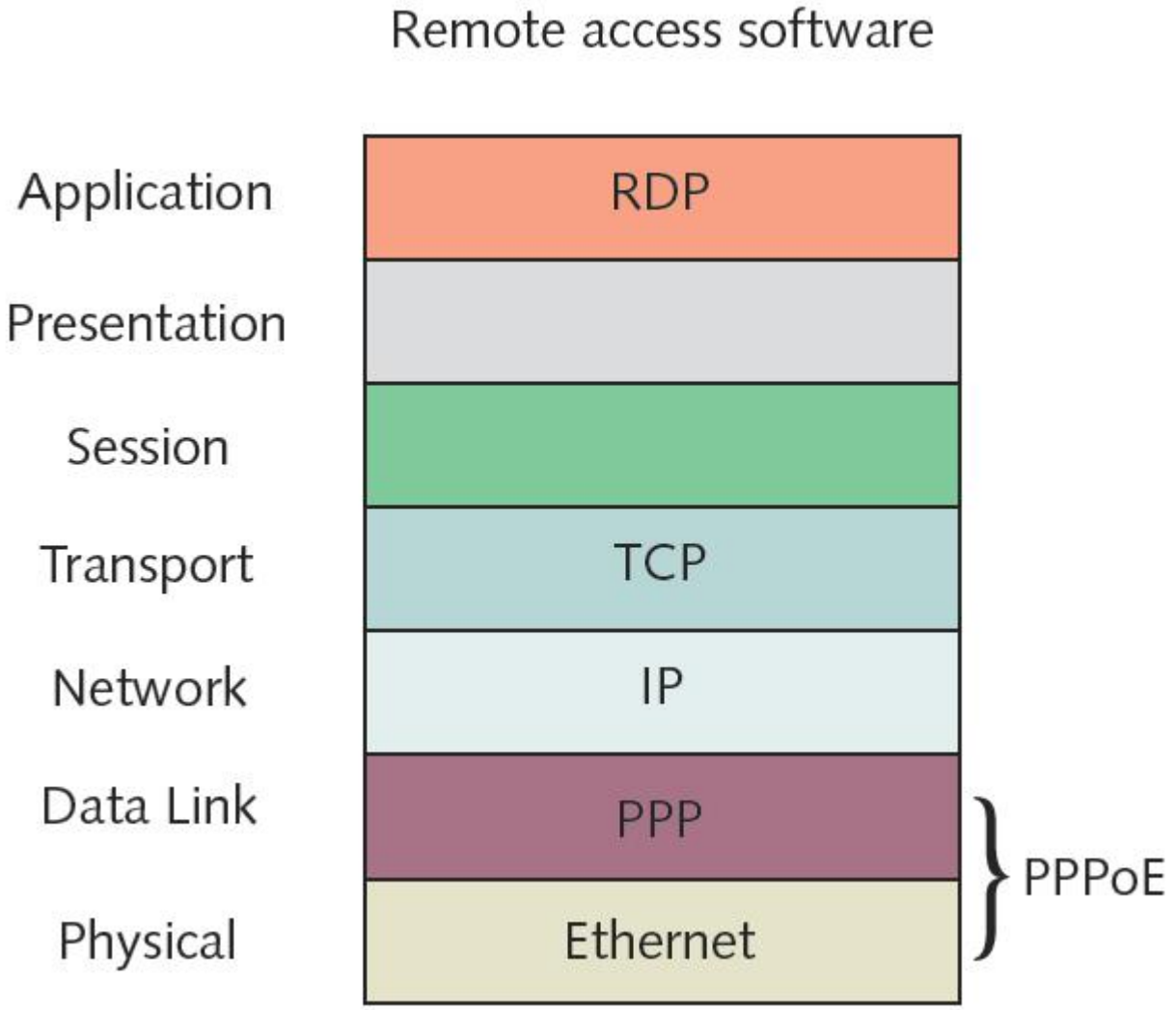
Virtual switches exchanging traffic through routers

Virtual Appliances

- Alternative to test servers for new software
- Virtual appliance includes:
  - Image of operating system, software, hardware specifications, and application configuration
- Most commonly virtual servers
- Popular functions
  - Firewall
  - E-mail solutions
  - Network management
  - Remote access

Remote Virtual Computing

- Allows workstation to remotely access and control another workstation
- Host may allow clients a variety of privileges
- Can send keystrokes and mouse clicks to the host
  - Receive screen output in return
- Thin client
  - Workstation that uses such software to access LAN
  - Requires very little hard disk space or processing power



Protocols used in a remote access Internet connection

Remote Virtual Computing

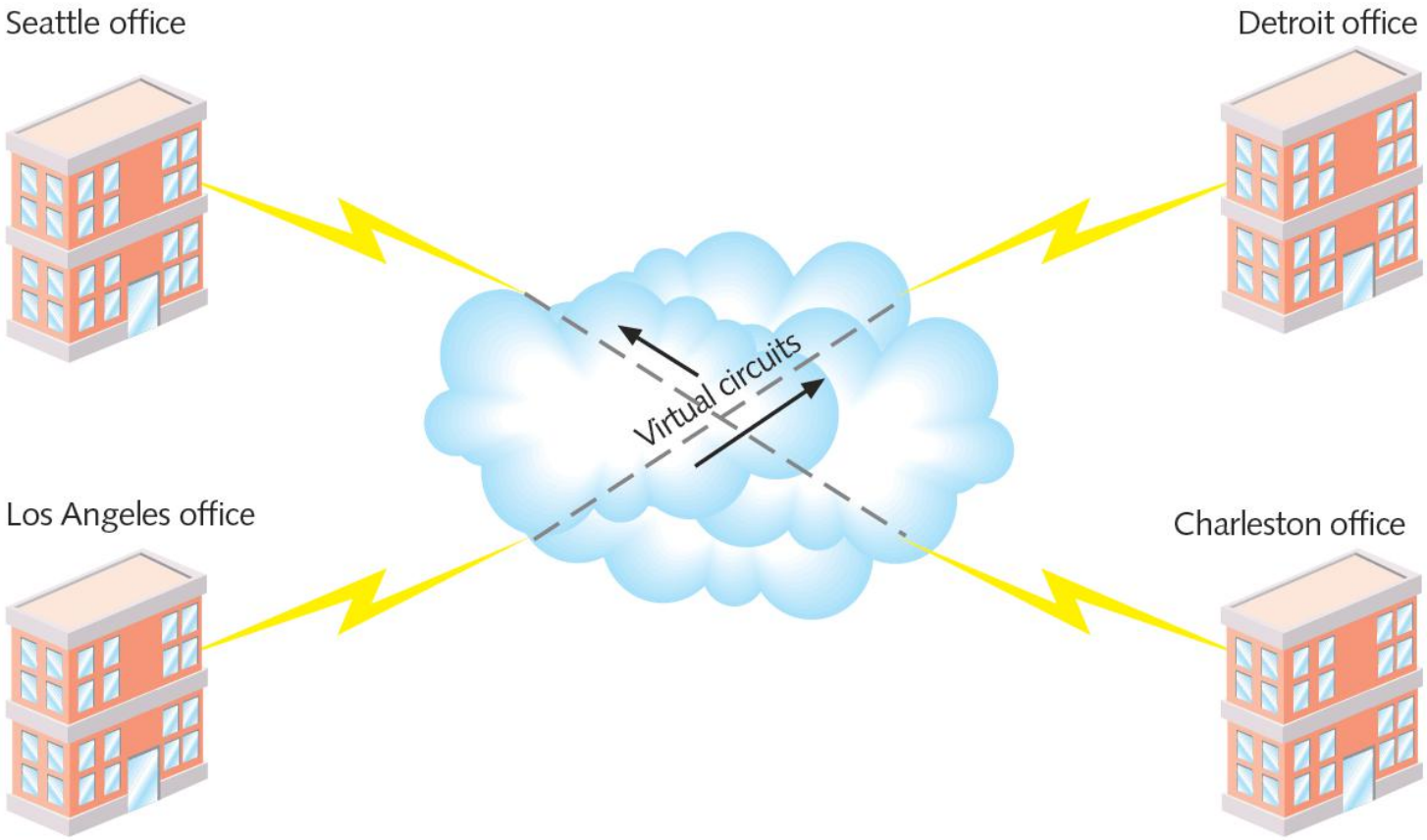
- Advantages
  - Simple to configure
  - Runs over any connection type
  - Single host can accept simultaneous connections from multiple clients
- Popular programs
  - Microsoft Remote Desktop
  - VNC (Virtual Network Computing)
  - ICA (Independent Computing Architecture)

Remote Virtual Computing

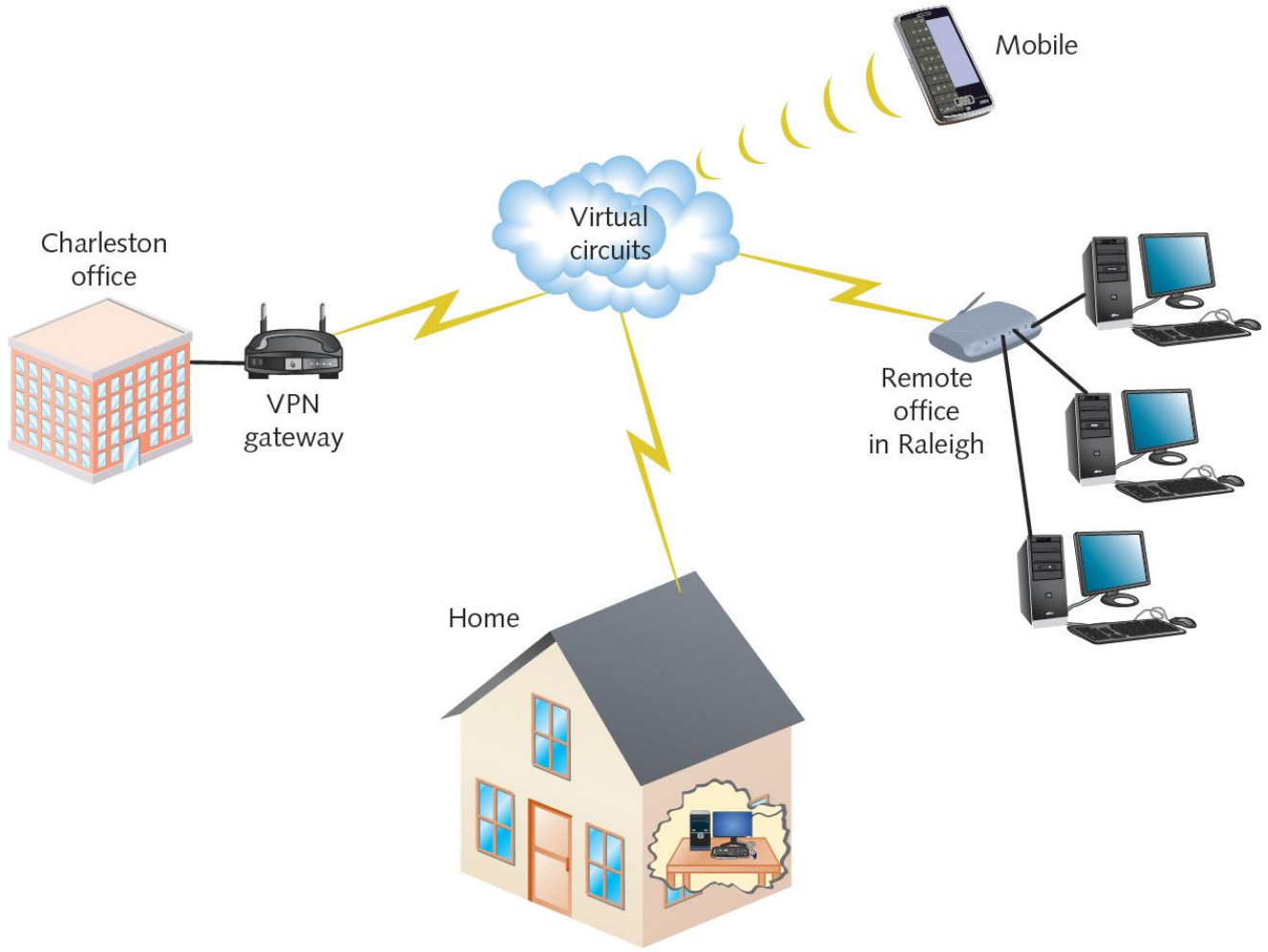
- Remote desktop
  - Comes with Windows client and server operating systems
- VNC (Virtual Network Computing)
  - Open source system
- ICA (Independent Computing Architecture)
  - Citrix System's XenApp
  - Can work with virtually any operating system or application
  - Easy to use

VPNs (Virtual Private Networks)

- Logically defined networks over public transmission systems
  - Isolated from other traffic on same public lines
- Requires inexpensive software
- Important considerations
  - Interoperability
  - Security
- Types
  - Site-to-site
  - Client-to-site



Site-to-site VPN



Client-to-site VPN (Remote Access VPN)

VPNs

- Enterprise-wide VPN
  - Can include elements of client-to-site and site-to-site models
- VPNs tailored to customer's distance, user, and bandwidth needs
- Two major types of tunneling protocols
  - PPTP (Point-to-Point Tunneling Protocol)
  - L2TP (Layer 2 Tunneling Protocol)

IT Masters
itmasters.edu.au

Charles Sturt University

Questions?

IT Masters
itmasters.edu.au

Charles Sturt University

++++

Network+ Short Course

Presented by Matt Constable

Module 3

IT Masters
itmasters.edu.au

Charles Sturt University

Network+ Short Course

Based on subject :
ITE526: Internetworking Fundamentals

Part of the :
Master of Networking and Systems Administration
Master of Management (IT)

Overview

- **Network Operations**
  - Given a scenario, use appropriate documentation and diagrams to manage the network.
  - Compare and contrast business continuity and disaster recovery concepts.
  - Explain common scanning, monitoring and patching processes and summarize their expected outputs.
  - Given a scenario, use remote access methods.
  - Identify policies and best practices.

What Are Integrity and Availability?

- Integrity
  - Soundness of network's programs, data, services, devices, connections
- Availability
  - How consistently and reliably a file or system can be accessed
- Uptime
  - Measure of time functioning normally between failures
  - Often expressed as percent uptime

Availability	Downtime per day	Downtime per month	Downtime per year
99%	14 minutes, 23 seconds	7 hours, 18 minutes, 17 seconds	87 hours, 39 minutes, 29 seconds
99.9%	1 minute, 26 seconds	43 minutes, 49 seconds	8 hours, 45 minutes, 56 seconds
99.99%	8 seconds	4 minutes, 22 seconds	52 minutes, 35 seconds
99.999%	.4 seconds	26 seconds	5 minutes, 15 seconds

Availability and downtime equivalents

What Are Integrity and Availability? (cont'd.)

- Integrity and availability compromised by:
  - Security breaches
  - Natural disasters
  - Malicious intruders
  - Power flaws
  - Human error
- Follow guidelines to keep network highly available
  - Industry or self-developed.

Malware

- Malicious software
- Program designed to intrude upon or harm system, resources
  - Examples: viruses, Trojan horses, worms, bots
- Virus
  - Replicating program intent to infect more computers
  - Copied to system without user knowledge
  - Replicates through network connections or exchange of external storage devices
- Well known how to protect against…..

Fault Tolerance

- Capacity for system to continue performing
  - Despite unexpected hardware, software malfunction
- Failure
  - Deviation from specified system performance level
    - Given time period
- Fault
  - Malfunction of one system component
  - Can result in failure
- Fault-tolerant system goal
  - Prevent faults from progressing to failures

Environment

- Consider network device environment
- Protect devices from:
  - Excessive heat, moisture
    - Use temperature, humidity monitors
  - Break-ins
  - Natural disasters

Power

- Blackout
  - Complete power loss
- Brownout
  - Temporary dimming of lights
- Causes
  - Forces of nature
  - Utility company maintenance, construction
- Solution
  - Alternate power sources

Power

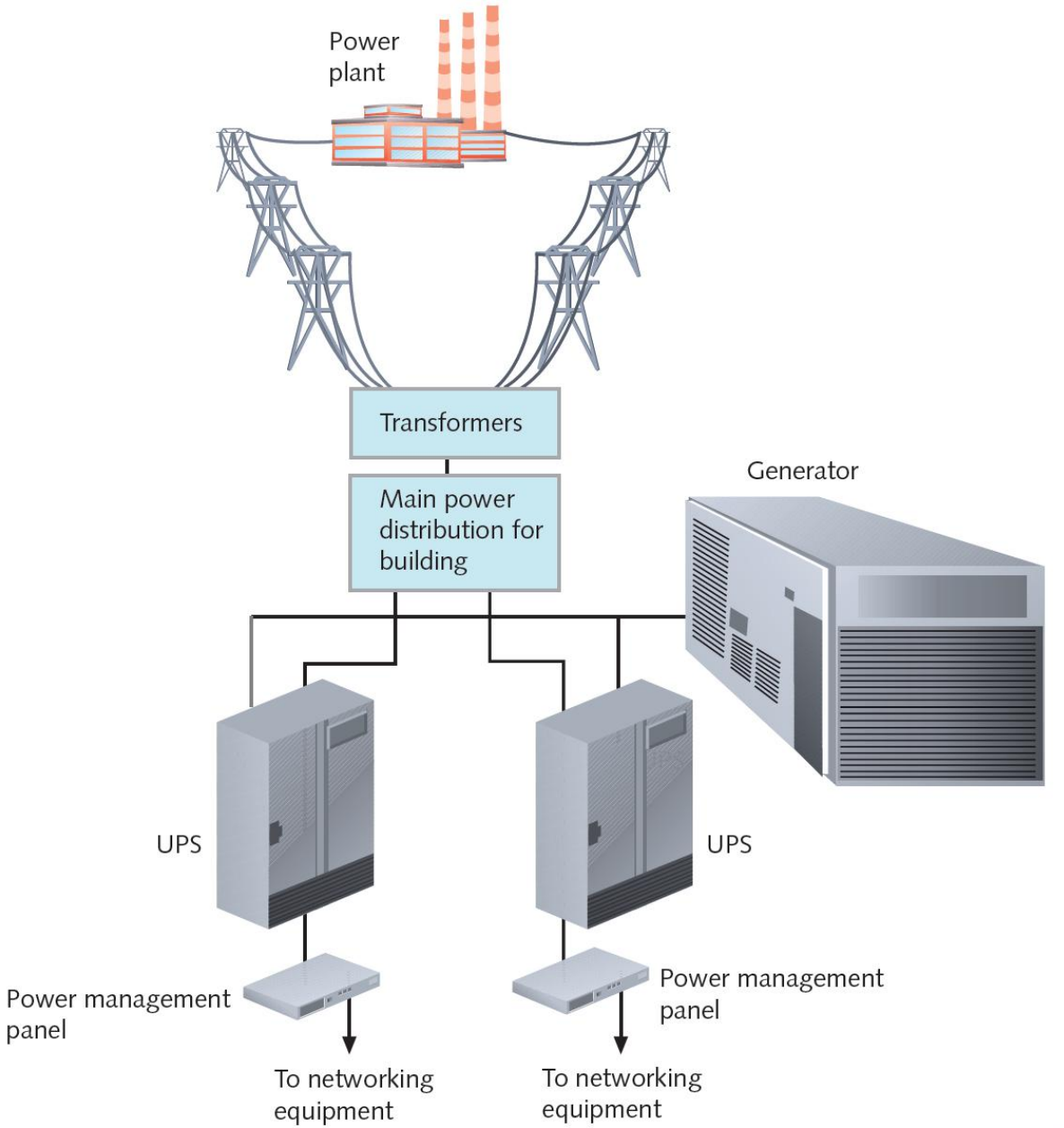
- Power flaws not tolerated by networks
- Types of power flaws that create damage
  - Surge
    - Momentary increase in voltage
  - Noise
    - Fluctuation in voltage levels
  - Brownout
    - Momentary voltage decrease
  - Blackout
    - Complete power loss

What can we do?

- Uninterruptible power supplies (UPSs)
  - Battery-operated power source
  - Directly attached to one or more devices
  - Attached to a power supply
  - Prevents harm to device, service interruption

What can we do?

- Generators
  - Powered by diesel, liquid propane, gas, natural gas, or steam
  - Do not provide surge protection
  - Provide electricity free from noise
  - Used in highly available environments
- Generator choice
  - Calculate organization’s crucial electrical demands
  - Determine generator’s optimal size


Power plant
Transformers
Main power distribution for building
Generator
UPS
UPS
Power management panel
Power management panel
To networking equipment
To networking equipment

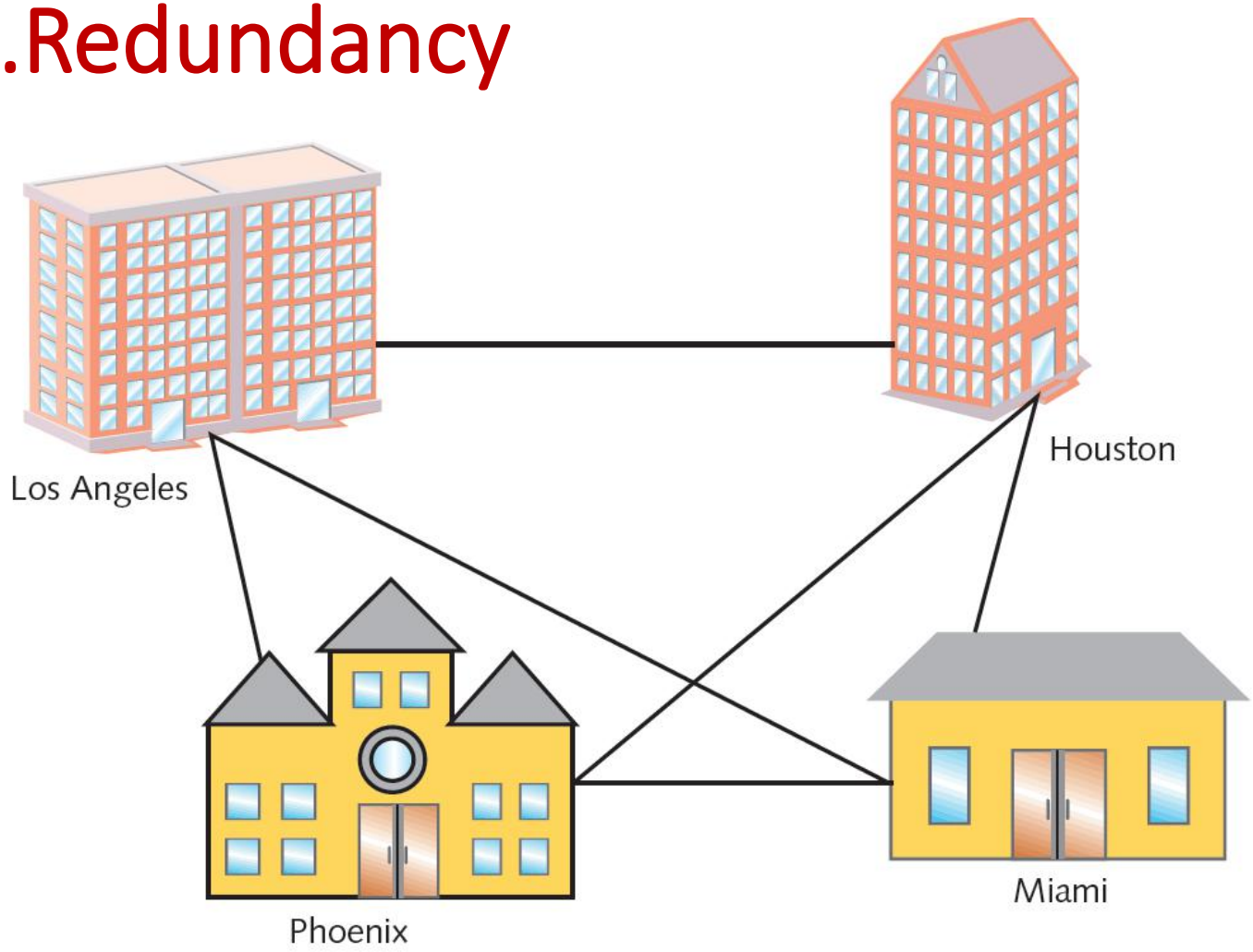
Network Design

- What is a good design?
- What do you want to achieve?
- Keep it as simple as possible!

Scenario…Redundancy

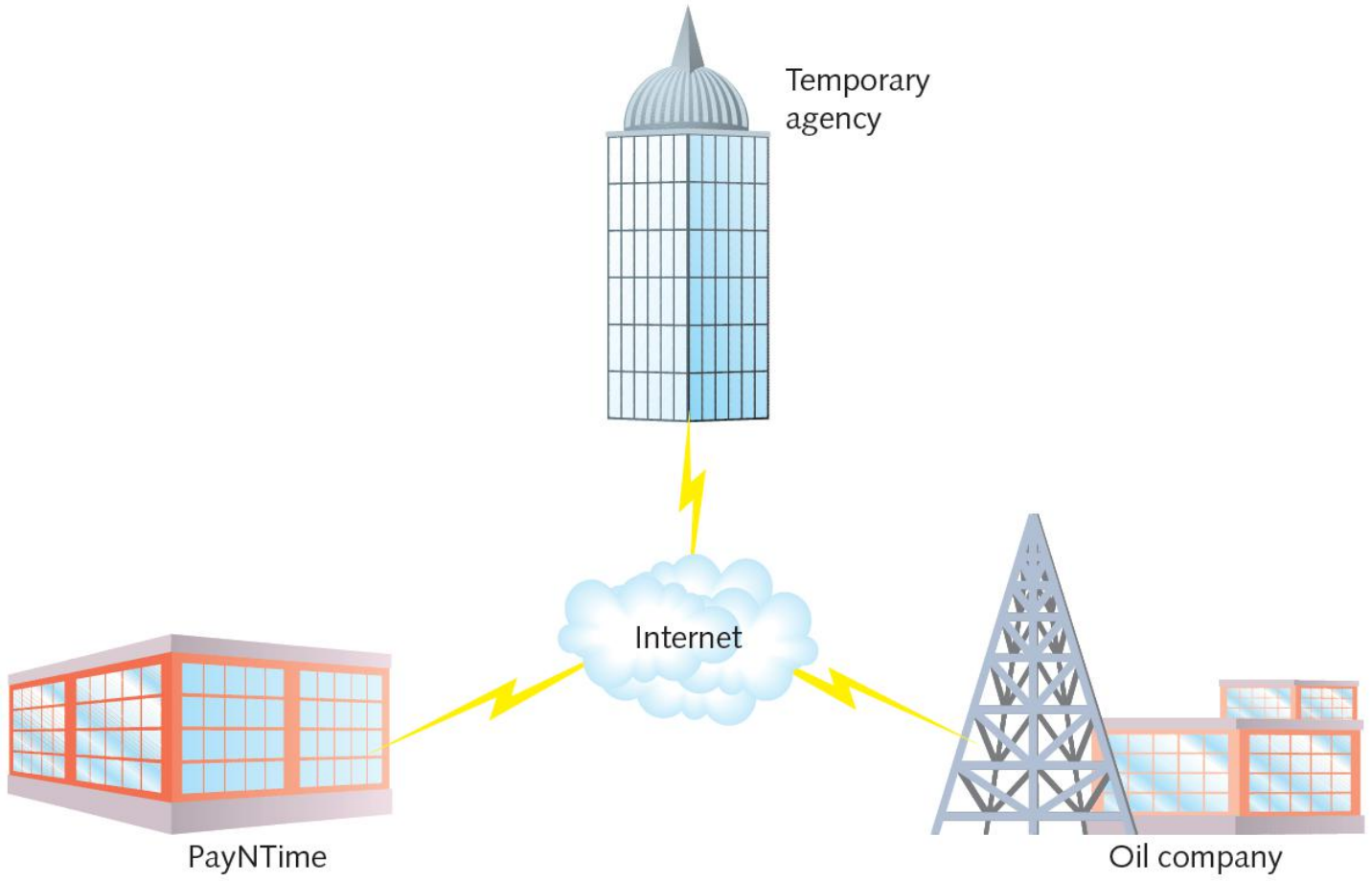
- Possible solutions: supply duplicate connection
  - Use different service carriers
  - Use two different routes
    - Critical data transactions follow more than one path
- Network redundancy advantages
  - Reduces network fault risk
    - Lost functionality, profits
- Disadvantage: cost

Scenario…Redundancy



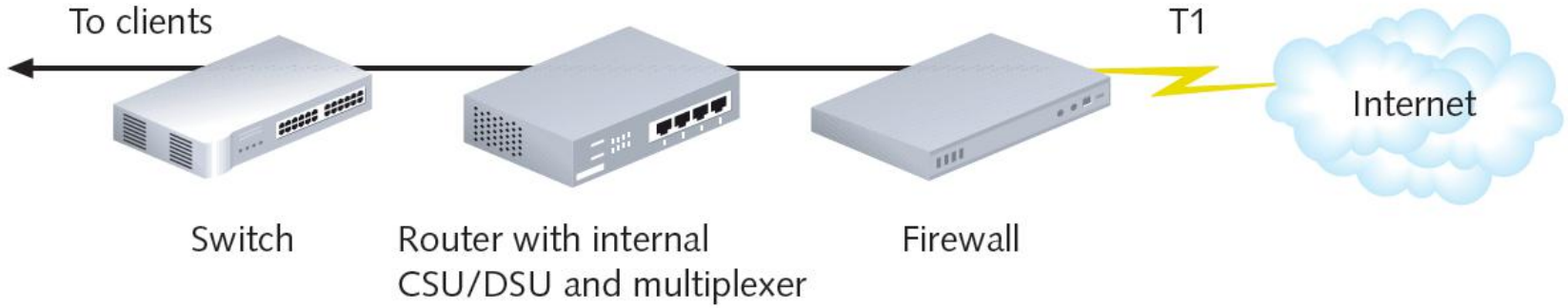
Scenario…Critcial Links

- Scenario: two critical links
  - Capacity, scalability concerns
  - Solution
    - Partner with ISP
    - Establish secure VPNs


Temporary agency
Internet
PayNTime
Oil company

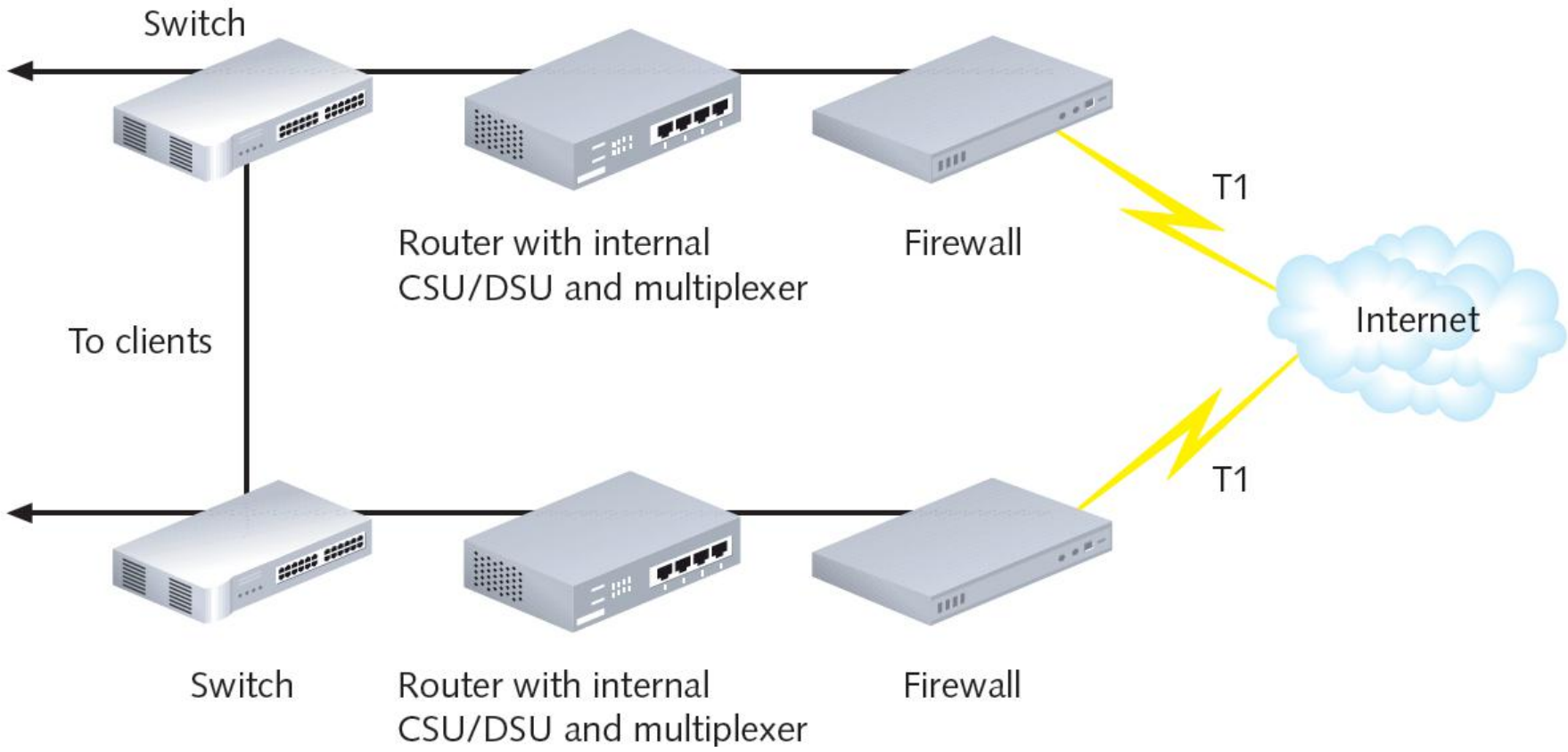
Scenario…Critical Links

- Scenario
  - Devices connect one LAN, WAN segment to another
    - Experience a fault
  - VPN agreement with national ISP
    - Single T1 link supports five customers



Scenario…Critical Links

- Problem with arrangement in previous slide…
  - Many single points of failure
    - T1 link failure
    - Firewall, router, CSU/DSU, multiplexer, or switch
- Solution
  - Redundant devices with automatic failover
  - Hot swappable devices
    - Immediately assume identical component duties
- Cold spare
  - Duplicate device on hand, not installed

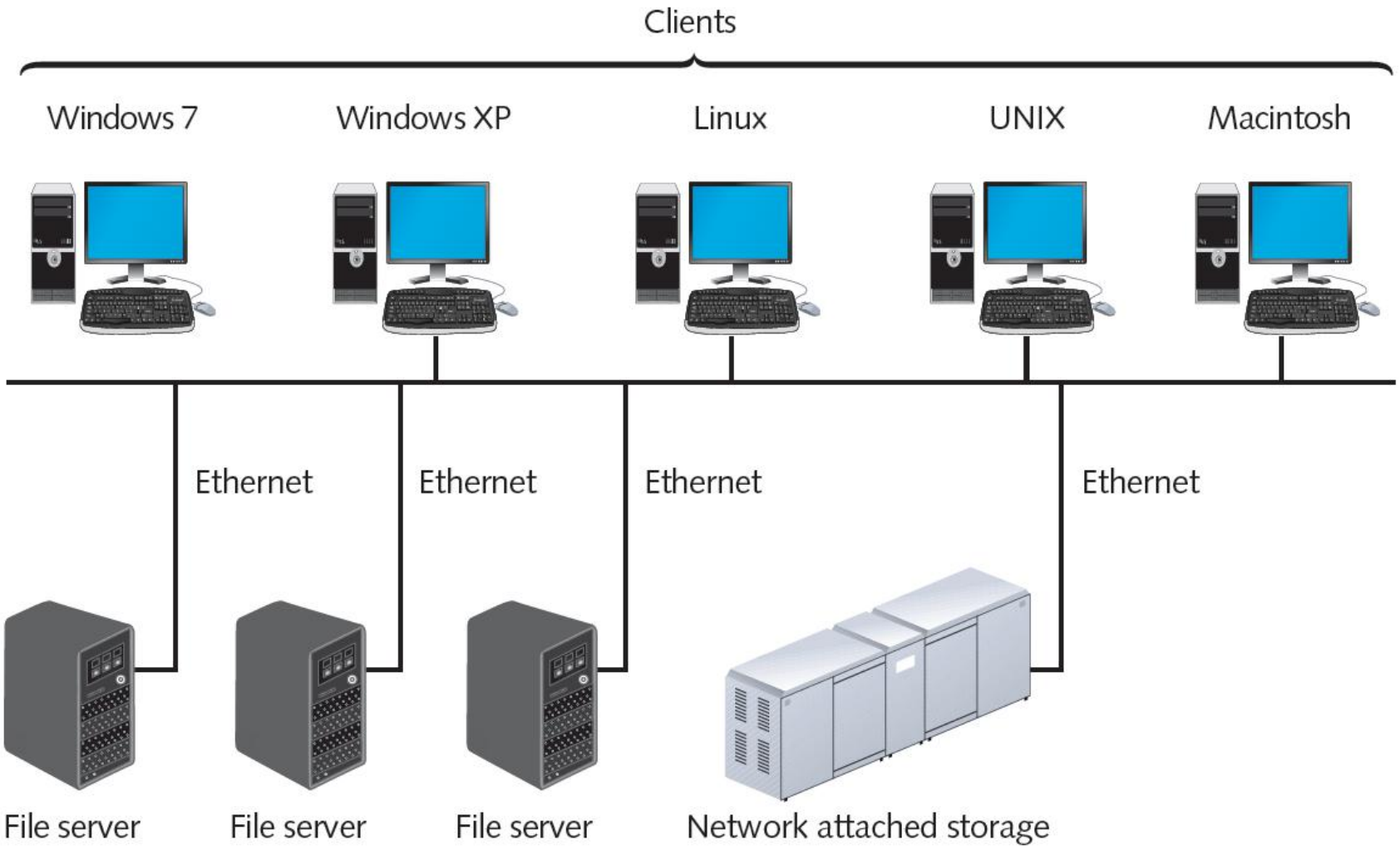

Switch
Router with internal
CSU/DSU and multiplexer
Firewall
T1
To clients
Internet
T1
Switch
Router with internal
CSU/DSU and multiplexer
Firewall

Servers

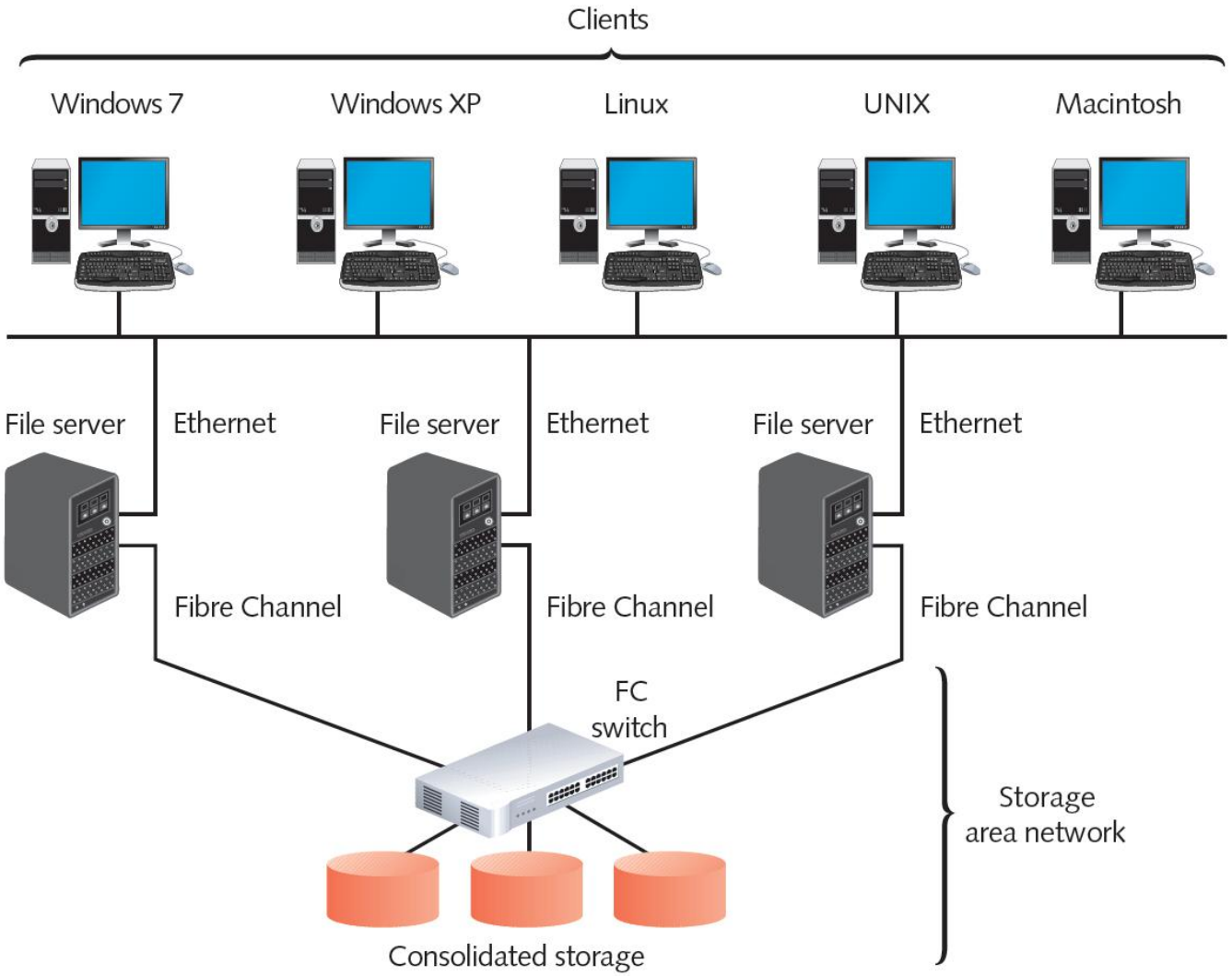
- Critical servers
  - Contain redundant components
    - Provide fault tolerance, load balancing
- Server mirroring
  - Fault-tolerance technique
  - One device, component duplicates another's activities
  - Uses identical servers, components
  - High-speed link between servers
  - Synchronization software
  - Form of replication
    - Dynamic copying of data from one location to another

Storage

- Data storage
  - Issues of availability and fault tolerance apply
- Various methods available
  - Ensure shared data and applications never lost or irretrievable
- RAID (Redundant Array of Independent [or Inexpensive] Disks)
  - Collection of disks
  - Provide shared data, application fault tolerance



Network attached storage on a LAN



Storage Area Network

Data Backup

- Backup
  - Copies of data or program files
  - Created for archiving, safekeeping
  - Store off site
- Without backup: risk losing everything
- Many backup options available
  - Performed by different software and hardware
  - Use different storage media types
- Can be controlled by NOS utilities, third-party software

Backup Media and Methods

- Approach to selecting backup media, methods
  - Ask questions to select appropriate solution
- Optical media
  - Media storing digitized data
  - Uses laser to write data, read data
  - Examples: CDs, DVDs, Tape
- Backup requirements
  - Recordable CD or DVD drive, software utility
- Blu-ray
  - Optical storage format

Backup Media and Methods

- DVD and Blu-ray DVD disadvantages
  - Writing data takes longer than other media
  - Requires more human intervention than other backup methods
- Tape backups
  - Copying data to magnetic tape
- Requirements
  - Tape drive connected to network
  - Management software
  - Backup media

Backup Media and Methods

- External disk drives (removable disk drives)
  - Storage device attached temporarily to computer
    - USB, PCMCIA, FireWire, CompactFlash port
  - Simple to use, save, share data
  - Temporary drive appears like any other drive
- Large data amount requirements
  - Backup control features, higher storage capacity, faster read-write access

Backup Media and Methods

- Network backups
  - Save data to another place on network
  - Different server, another WAN location
  - SAN, NAS storage device
- Online backup (cloud backup)
  - Saves data to another company's storage array using Internet
  - Implement strict security measures
  - Automated backup, restoration processes
- Evaluate online back up provider
  - Test speed, accuracy, security, recovery

Backup Strategy

- Devise a strategy to perform reliable backups
- Document in accessible area
- Address various questions
- Full backup
  - All data copied
- Incremental backup
  - Copy data changed since last full, incremental backup
- Differential backup
  - Copy only data changed since last backup

Disaster Recovery

- Disaster recovery
  - Restoring critical functionality, data
    - After enterprise-wide outage
    - Affecting more than single system, limited group
- Consider possible extremes
  - Not relatively minor outages, failures, security breaches, data corruption

Disaster Recovery Planning

- Account for worst-case scenarios
- Identify disaster recovery team
- Provide contingency plans
  - Restore and replace:
    - Computer systems
    - Power
    - Telephony systems
    - Paper-based files
- Plan contains various sections
- Lessen critical data loss risk

Disaster Recovery Contingencies

- Cold site
  - Components necessary to rebuild network exist
  - Not appropriately configured, updated, or connected
- Warm site
  - Components necessary to rebuild network exist
  - Some appropriately configured, updated, and connected
- Hot site
  - Components exist and match network's current state
  - All appropriately configured, updated, and connected

IT Masters
itmasters.edu.au

Charles Sturt University

Fundamentals of Network Management

Fundamentals of Network Management

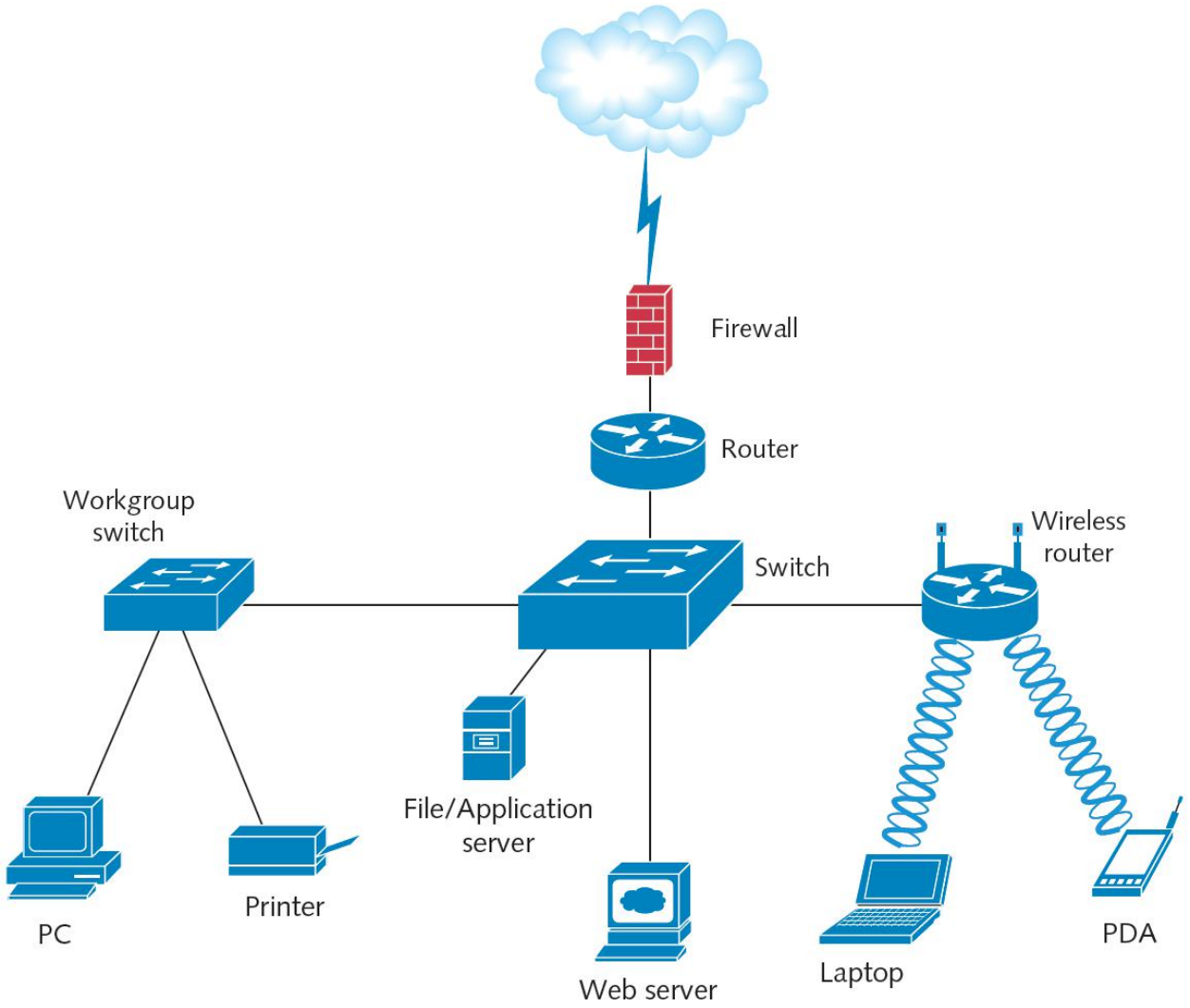
- Network management
  - Assess, monitor, and maintain all network aspects
  - Scope differs according to network's size and importance
  - Several network management disciplines
  - All share same goals
    - Enhance efficiency and performance
    - Prevent costly downtime and loss
  - Predict problems before they occur

Documentation

- Network aspects to document
  - Physical topology
  - Access method
  - Protocols
  - Devices
  - Operating systems
  - Applications
  - Configurations

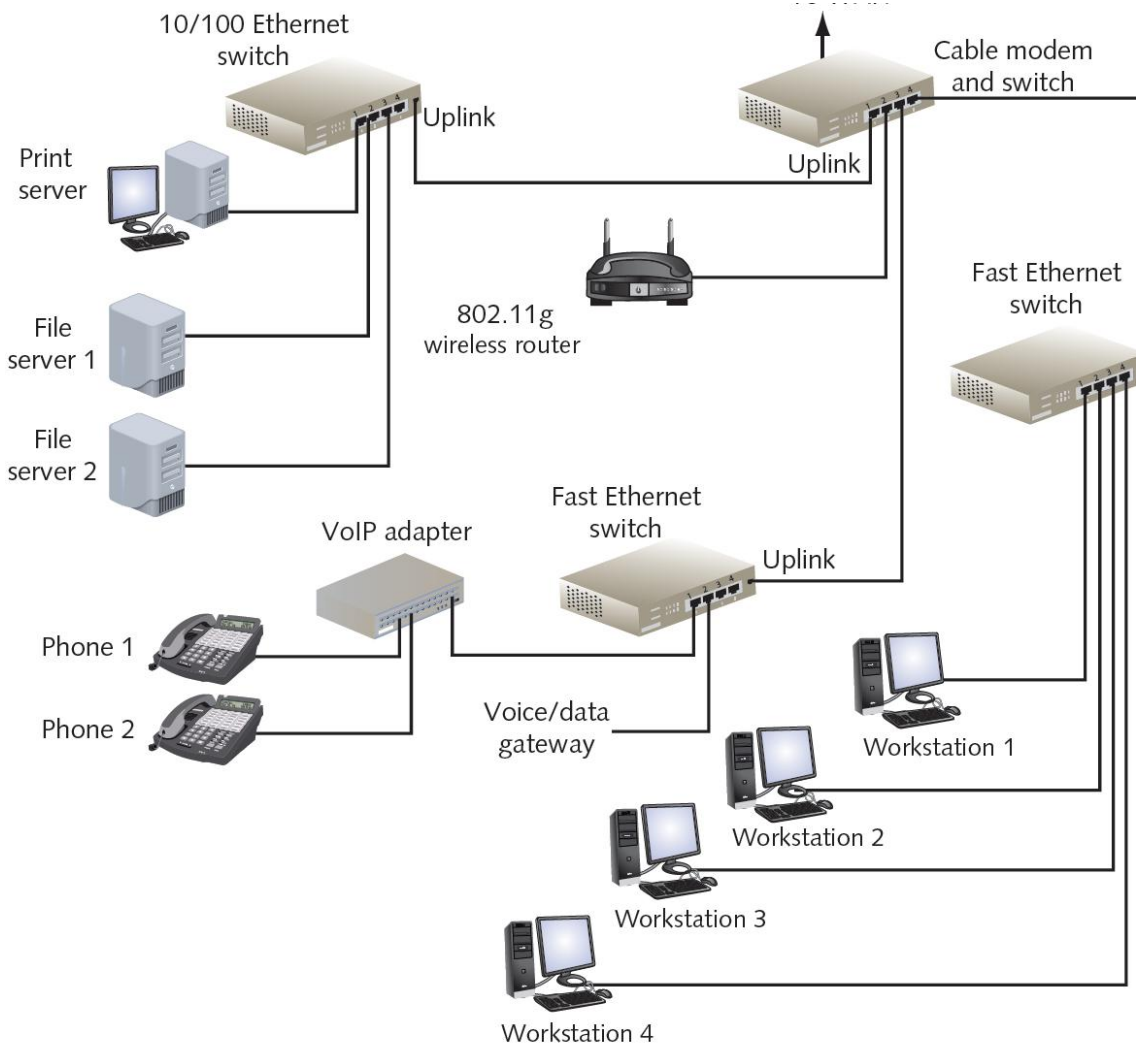
Documentation Set

- Configuration management
  - Collection, storage, assessment of configuration documentation
- Documenting all network aspects
  - Saves future work
- Network diagrams
  - Graphical representations of network's devices, connections
  - Use popular Cisco icons
  - Provide broad snapshot of network's physical or logical topology


Firewall
Router
Workgroup switch
Switch
Wireless router
File/Application server
PC
Printer
Web server
Laptop
PDA

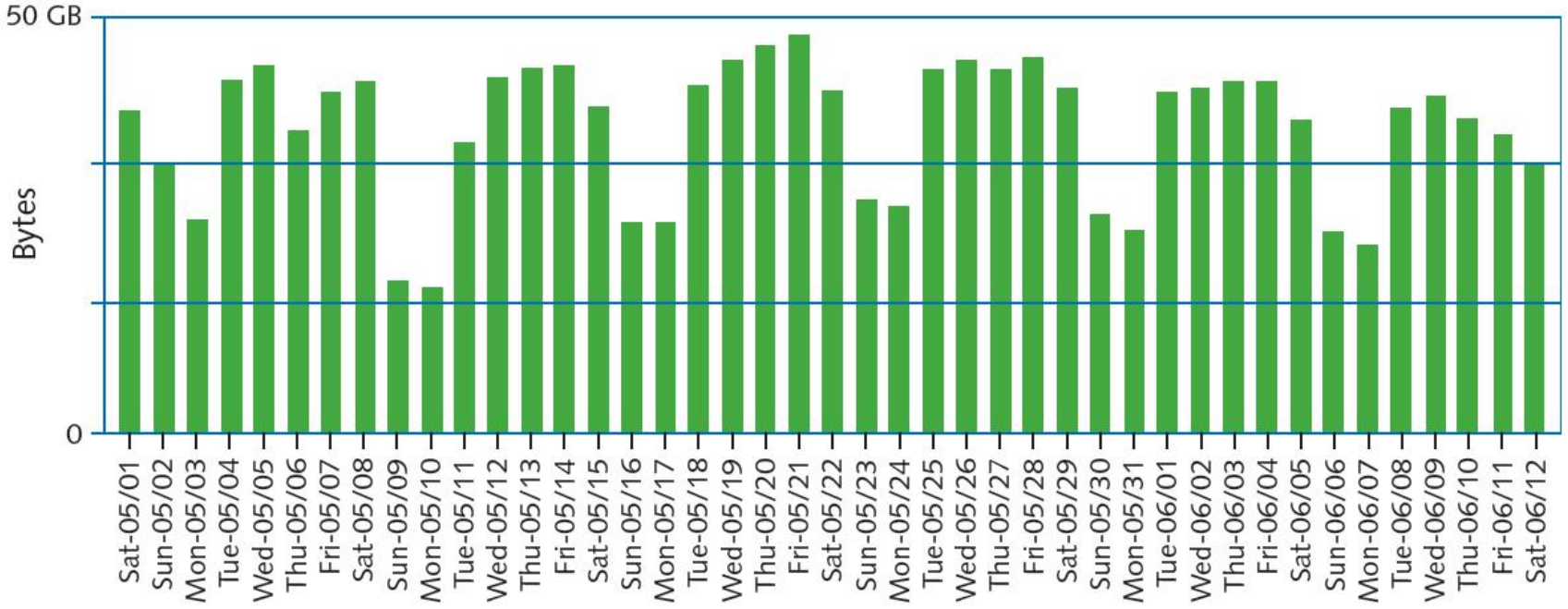
Documentation Set

- Wiring schematic
  - Graphical representation of network's wired infrastructure
  - Detailed form
    - Includes every wire connecting network devices
  - Less detailed form
    - Single line represents group of wires connecting several clients to a switch


10/100 Ethernet switch
Uplink
Cable modem and switch
Uplink
Print server
802.11g wireless router
Fast Ethernet switch
File server 1
File server 2
Fast Ethernet switch
VoIP adapter
Uplink
Phone 1
Phone 2
Voice/data gateway
Workstation 1
Workstation 2
Workstation 3
Workstation 4

Baseline Measurements

- Baseline
  - Report of network's current operation state
- Example baseline measurements
  - Network backbone utilization rate
  - Number of users logged on per day or per hour
  - Number of protocols running on network
  - Error statistics
    - Runts, collisions, jabbers, giants
  - Frequency of application use
  - Bandwidth usage


50 GB
Bytes
0
Sat-05/01
Sun-05/02
Mon-05/03
Tue-05/04
Wed-05/05
Thu-05/06
Fri-05/07
Sat-05/08
Sun-05/09
Mon-05/10
Tue-05/11
Wed-05/12
Thu-05/13
Fri-05/14
Sat-05/15
Sun-05/16
Mon-05/17
Tue-05/18
Wed-05/19
Thu-05/20
Fri-05/21
Sat-05/22
Sun-05/23
Mon-05/24
Tue-05/25
Wed-05/26
Thu-05/27
Fri-05/28
Sat-05/29
Sun-05/30
Mon-05/31
Tue-06/01
Wed-06/02
Thu-06/03
Fri-06/04
Sat-06/05
Sun-06/06
Mon-06/07
Tue-06/08
Wed-06/09
Thu-06/10
Fri-06/11
Sat-06/12

Why Basline?

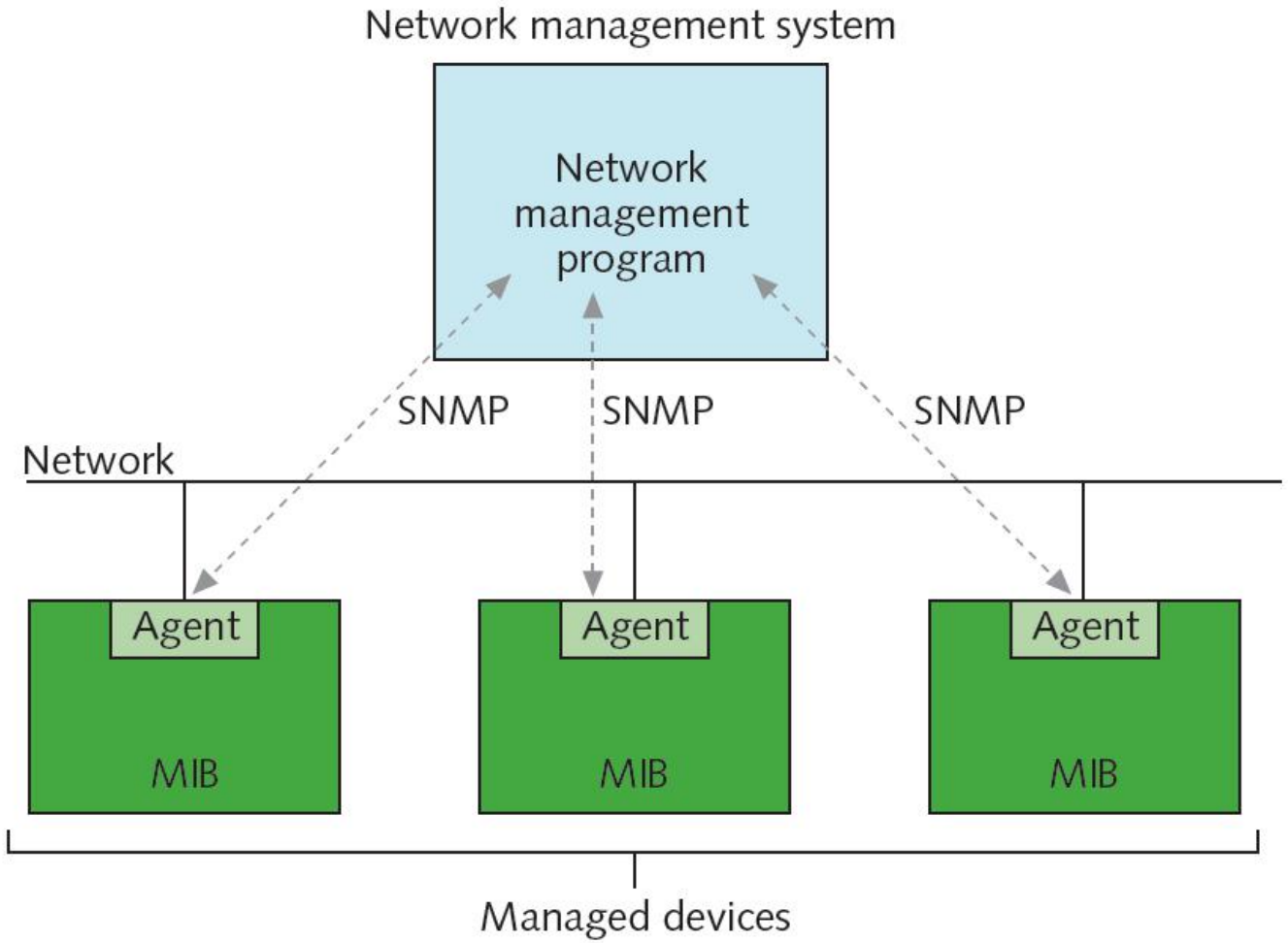
- Compare future and past performance
  - Most critical network, user functions
  - More data provides more accuracy
- Forecasting network traffic patterns
  - Difficult to predict users' habits, new technology effects, changes in resource demand
- Gathering baseline data
  - Software applications
    - Freeware
    - Expensive, customizable hardware and software
  - Determine use before selecting

Network Management Systems

- Enterprise-wide network management systems
  - Accomplish fault and performance management
  - All use similar architecture
  - Polling
    - Collecting data from multiple networked devices at regular intervals
  - Agent
    - Software routine
    - Collects information about device's operation
    - Provides information to network management application

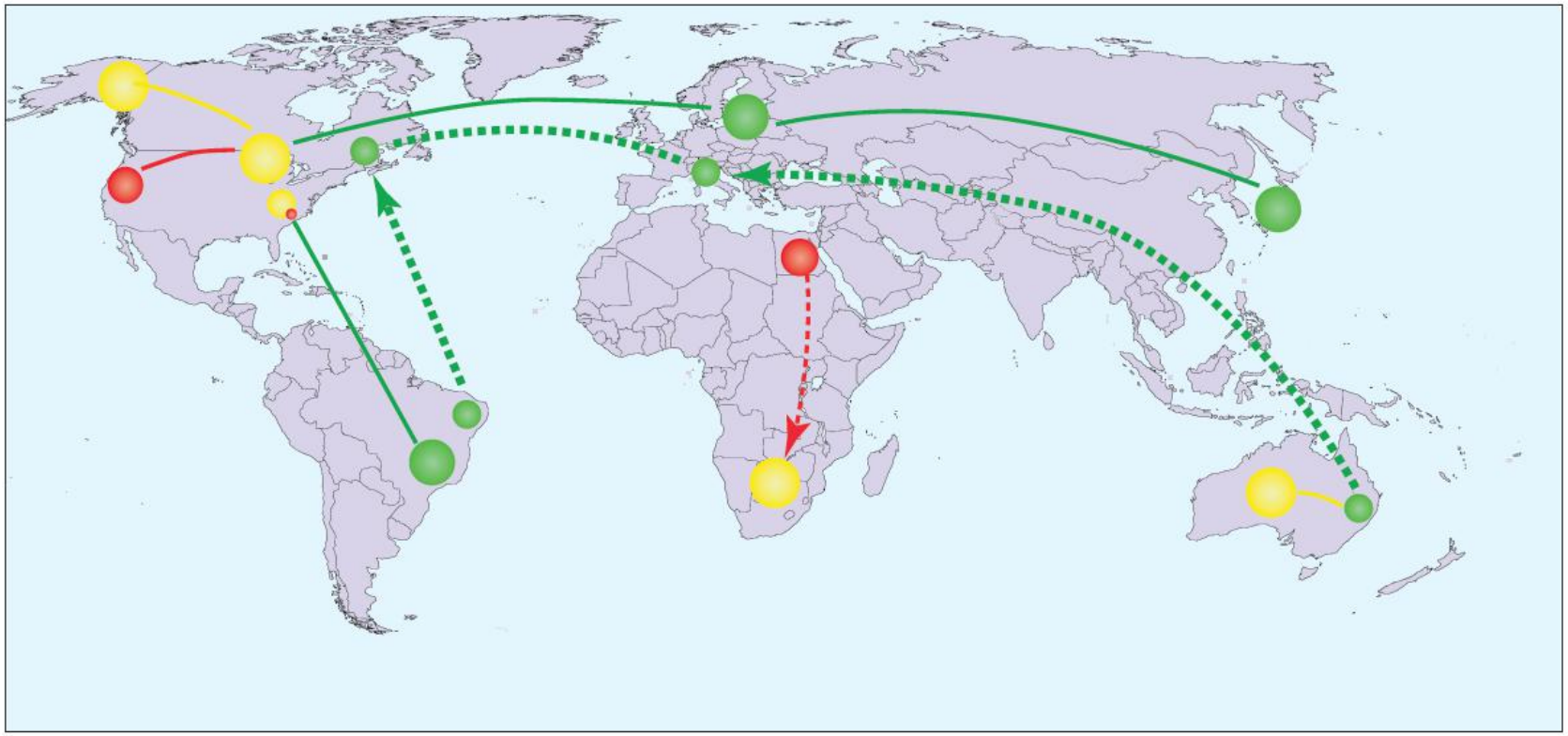
Network Management Software

- Various aspects of a device can be managed
  - Processor, memory, hard disk, NIC, and intangibles
- MIB (Management Information Base)
  - Contains managed devices definition, data
- SNMP (Simple Network Management Protocol)
  - Used to communicate managed device information
  - Part of TCP/IP suite
  - SNMPv3: most secure version of the protocol
  - SNMPv2 still widely used


Network management system
Network management program
SNMP
SNMP
SNMP
Network
Agent
MIB
Agent
MIB
Agent
MIB
Managed devices

Network Management Software

- Several ways to view and analyze data
- Network management applications
  - Flexible
  - Challenging to configure and fine-tune
  - Choose correct type and amount of information to collect
- Faults can trigger alarms
  - Also recorded in system and event logs



IT Masters
itmasters.edu.au

Charles Sturt University

Questions?

IT Masters
itmasters.edu.au

Charles Sturt University

++++

Network+ Short Course

Presented by Matt Constable

Module 4

IT Masters
itmasters.edu.au

Charles Sturt University

Network+ Short Course

Based on subject :
ITE526: Internetworking Fundamentals

Part of the :
Master of Networking and Systems Administration
Master of Management (IT)

Overview

- **Network Security**
  - Summarize the purposes of physical security devices.
  - Explain authentication and access controls.
  - Given a scenario, secure a basic wireless network.
  - Summarize common networking attacks.
  - Given a scenario, implement network device hardening.
  - Explain common mitigation techniques and their purposes.

Security

Security Assessment

- Examine network's security risks
  - Consider effects
- Different organization types
  - Different network security risk levels
- Posture assessment
  - Thorough network examination
  - Determine possible compromise points
  - Performed in-house by IT staff
  - Performed by third party

Security Risks

- Hacker
  - Individual who gains unauthorized access to systems
- Vulnerability
  - Weakness of a system, process, or architecture
- Exploit
  - Means of taking advantage of a vulnerability
- Zero-day exploit
  - Taking advantage of undiscovered software vulnerability
  - Most vulnerabilities are well known

Risks Associated with People

- Half of all security breaches
  - Human errors, ignorance, omissions
- Social engineering
  - Strategy to gain password
  - Phishing
    - Glean access, authentication information
    - Pose as someone needing information
- Many risks associated with people exist
- Easiest way to circumvent network security
  - Take advantage of human error

Risks Associated with Transmission and Hardware

- Physical, Data Link, and Network layer security risks
  - Require more technical sophistication
- Risks inherent in network hardware and design
  - Transmission interception
    - Man-in-the-middle attack
  - Eavesdropping
    - Networks connecting to Internet via leased public lines
  - Sniffing
    - Repeating devices broadcast traffic over entire segment

Risks Associated with Transmission and Hardware (cont'd.)

- Risks inherent in network hardware and design (cont'd.)
  - Port access via port scanner
    - Unused switch, router, server ports not secured
  - Private address availability to outside
    - Routers not properly configured to mask internal subnets
  - Router attack
    - Routers not configured to drop suspicious packets

Risks Associated with Transmission and Hardware (cont'd.)

- Risks inherent in network hardware and design (cont'd.)
  - Access servers not secured, monitored
  - Computers hosting sensitive data:
    - May coexist on same subnet as public computers
  - Insecure passwords
    - Easily guessable or default values

Risks Associated with Protocols and Software

- Includes Transport, Session, Presentation, and Application layers
- Networking protocols and software risks
  - TCP/IP security flaws
  - Invalid trust relationships
  - NOS back doors, security flaws
  - Buffer overflow
  - NOS allows server operators to exit to command prompt
  - Administrators default security options
  - Intercepting transactions between applications

Risks Associated with Internet Access

- Network security compromise
  - More often “from the inside”
- Outside threats still very real
  - Web browsers permit scripts to access systems
  - Users provide information to sites

Risks Associated with Internet Access (cont'd.)

- Common Internet-related security issues
  - Improperly configured firewall
    - Outsiders obtain internal IP addresses: IP spoofing
  - Telnets or FTPs
    - Transmit user ID and password in plain text
  - Newsgroups, mailing lists, forms
    - Provide hackers user information
  - Chat session flashing
  - Denial-of-service attack
    - Smurf attack: hacker issues flood of broadcast ping messages

An Effective Security Policy

- Minimize break-in risk
  - Communicate with and manage users
  - Use thoroughly planned security policy
- Security policy
  - Identifies security goals, risks, authority levels, designated security coordinator, and team members
  - Responsibilities of each employee
  - How to address security breaches
- Not included in policy:
  - Hardware, software, architecture, and protocols
  - Configuration details

Security Policy Goals

- Typical goals
  - Ensure authorized users have appropriate resource access
  - Prevent unauthorized user access
  - Protect unauthorized sensitive data access
    - Inside and outside
  - Prevent accidental hardware and software damage
  - Prevent intentional hardware or software damage
  - Create secure environment
    - Withstand, respond to, and recover from threat
  - Communicate employees' responsibilities

Security Policy Goals (cont'd.)

- Strategy
  - Form committee
    - Involve as many decision makers as possible
    - Assign security coordinator to drive policy creation
  - Understand risks
    - Conduct posture assessment
    - Rate severity and likelihood of each threat
  - Assign person responsible for addressing threats

Security Policy Content

- Outline policy content
  - Define policy subheadings
- Explain to users:
  - What they can and cannot do
  - How measures protect network's security
- User communication
  - Security newsletter
  - User security policy section
- Define what confidential means to the organization

Response Policy

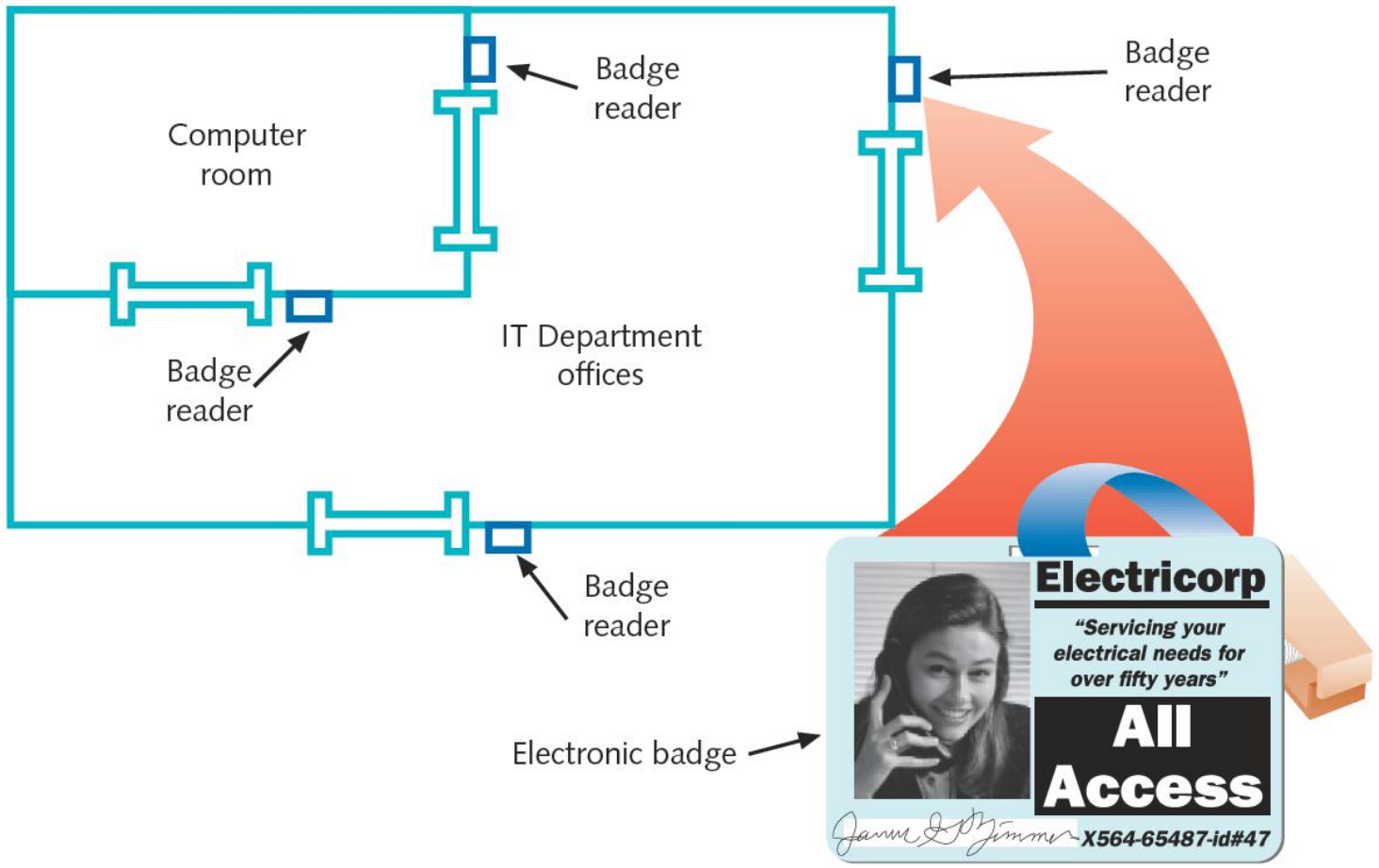
- Security breach occurrence
  - Provide planned response
- Identify response team members
  - Understand security policy, risks, and measures in place
  - Accept role with certain responsibilities
  - Regularly rehearse defense
    - Threat drill

Response Policy (cont'd.)

- Suggested team roles
  - Dispatcher
    - Person on call; first to notice; alerted to problem
  - Manager
    - Coordinates resources
  - Technical support specialist
    - One focus: solve problem quickly
  - Public relations specialist
    - Official spokesperson to public
- After problem resolution
  - Review process

Physical Security

- Restrict physical access to network components
  - Lock computer rooms, telco rooms, wiring closets, and equipment cabinets
- Locks can be physical or electronic
  - Electronic access badges
  - Locks requiring entrants to punch numeric code
  - Bio-recognition access


Computer room
Badge reader
Badge reader
IT Department offices
Badge reader
Badge reader
Electronic badge
Electricorp
"Servicing your electrical needs for over fifty years"
All Access
X564-65487-id#47

Physical Security (cont'd.)

- Physical barriers
  - Gates, fences, walls, and landscaping
- Closed-circuit TV systems monitor secured rooms
- Surveillance cameras
  - Data centers, telco rooms, data storage areas, facility entrances
  - Central security office capabilities
    - Display several camera views at once
    - Switch from camera to camera
  - Video footage used in investigation and prosecution

Physical Security (cont'd.)

- Security audit
  - Ask questions related to physical security checks
- Consider losses from salvaged and discarded computers
  - Hard disk information stolen
  - Solutions
    - Run specialized disk sanitizer program
    - Remove disk and use magnetic hard disk eraser
    - Pulverize or melt disk

Security in Network Design

- Breaches may occur due to poor LAN or WAN design
  - Address though intelligent network design
- Preventing external LAN security breaches
  - Restrict access at every point where LAN connects to rest of the world

Router Access Lists

- Control traffic through routers
- Router's main functions
  - Examine packets
  - Determine destination
    - Based on Network layer addressing information
- ACL (access control list)
  - Also called access list
  - Routers can decline to forward certain packets

Router Access Lists (cont'd.)

- ACL variables used to permit or deny traffic
  - Network layer protocol (IP, ICMP)
  - Transport layer protocol (TCP, UDP)
  - Source IP address
  - Source netmask
  - Destination IP address
  - Destination netmask
  - TCP or UDP port number

Router Access Lists (cont'd.)

- Router receives packet, examines packet
  - Refers to ACL for permit, deny criteria
  - Drops packet if deny characteristics match
  - Forwards packet if permit characteristics match
- Access list statement examples
  - Deny all traffic from source address with netmask 255.255.255.255
  - Deny all traffic destined for TCP port 23
- Separate ACL's for:
  - Interfaces; inbound and outbound traffic

Intrusion Detection and Prevention

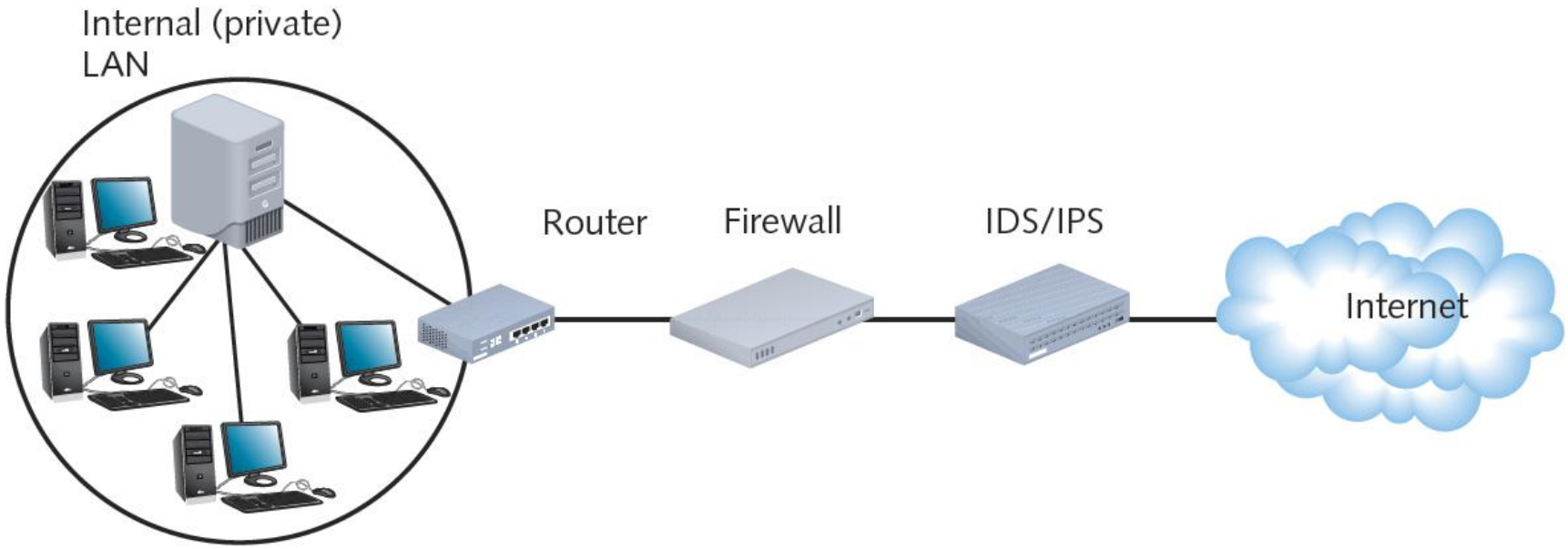
- Proactive security measure
  - Detecting suspicious network activity
- IDS (intrusion detection system)
  - Software monitoring traffic
    - On dedicated IDS device
    - On another device performing other functions
- Port mirroring
  - One port makes copy of traffic to second port for monitoring

Intrusion Detection and Prevention (cont'd.)

- IDS software detects many suspicious traffic patterns
  - Examples: denial-of-service, smurf attacks
- DMZ (demilitarized zone)
  - Network's protective perimeter
  - IDS sensors installed at network edges
- IDS at DMZ drawback
  - Number of false positives logged
- IDS can only detect and log suspicious activity

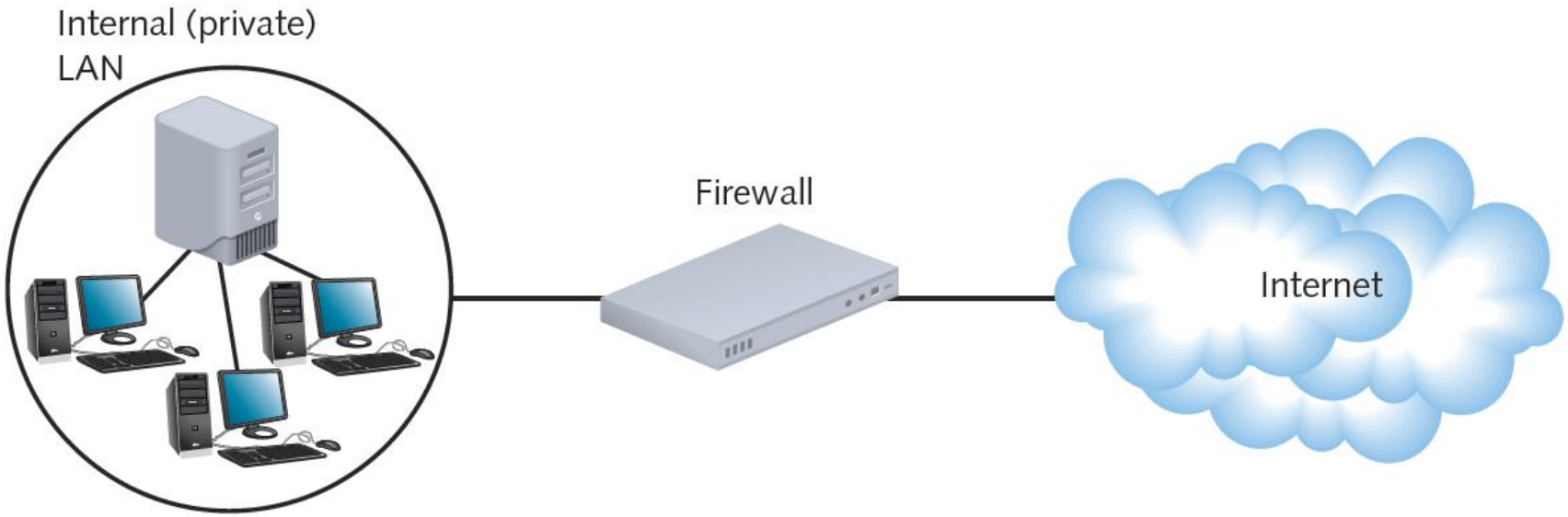
Intrusion Detection and Prevention (cont'd.)

- IPS (intrusion-prevention system)
  - Reacts to suspicious activity when alerted
  - Detects threat and prevents traffic from flowing to network
    - Based on originating IP address
- NIPS (network-based intrusion prevention)
  - Protects entire networks
- HIPS (host-based intrusion prevention)
  - Protects certain hosts


Internal (private)
LAN
Router
Firewall
IDS/IPS
Internet

Firewalls

- Specialized device or computer installed with specialized software
  - Selectively filters and blocks traffic between networks
  - Involves hardware and software combination
- Firewall location
  - Between two interconnected private networks
  - Between private network and public network (network-based firewall)


Internal (private)
LAN
Firewall
Internet

Firewalls (cont'd.)

- Packet-filtering firewall
  - Simplest firewall
  - Examines header of every entering packet
  - Can block traffic entering or exiting a LAN
- Firewall default configuration
  - Blocks most common security threats
  - Preconfigured to accept and deny certain traffic types
  - Network administrators often customize settings

Firewalls (cont'd.)

- Common packet-filtering firewall criteria
  - Source, destination IP addresses
  - Source, destination ports
  - Flags set in the IP header
  - Transmissions using UDP or ICMP protocols
  - Packet's status as first packet in new data stream, subsequent packet
  - Packet's status as inbound to, outbound from private network

Firewalls (cont'd.)

- Port blocking
  - Prevents connection to and transmission completion through ports
- Optional firewall functions
  - Encryption
  - User authentication
  - Central management
  - Easy rule establishment
  - Filtering based on data contained in packets

Firewalls (cont'd.)

- Optional firewall functions (cont'd.)
  - Logging, auditing capabilities
  - Protect internal LAN's address identity
  - Monitor data stream from end to end (stateful firewall)
- Tailoring a firewall
  - Consider type of traffic to filter
  - Consider exceptions to rules
- Packet-filtering firewalls
  - Cannot distinguish user trying to breach firewall from authorized user

Scanning Tools

- Used during posture assessment
  - Duplicate hacker methods
- NMAP (Network Mapper)
  - Designed to scan large networks
  - Provides information about network and hosts
  - Free to download
- Nessus
  - Performs more sophisticated scans than NMAP

Lures

- Honeypot
  - Decoy system that is purposefully vulnerable
  - Designed to fool hackers and gain information about their behavior
- Honeynet
  - Network of honeypots

NOS (Network Operating System) Security

- Restrict user authorization
  - Access to server files and directories
  - Public rights
    - Conferred to all users
    - Very limited
  - Group users according to security levels
    - Assign additional rights

Logon Restrictions

- Additional restrictions to strengthen security
  - Time of day
  - Total time logged on
  - Source address
  - Unsuccessful logon attempts

Passwords

- Choosing secure password
  - Guards against unauthorized access
  - Easy, inexpensive
- Communicate password guidelines
  - Use security policy
  - Stress importance of company's financial, personnel data security

Passwords (cont'd.)

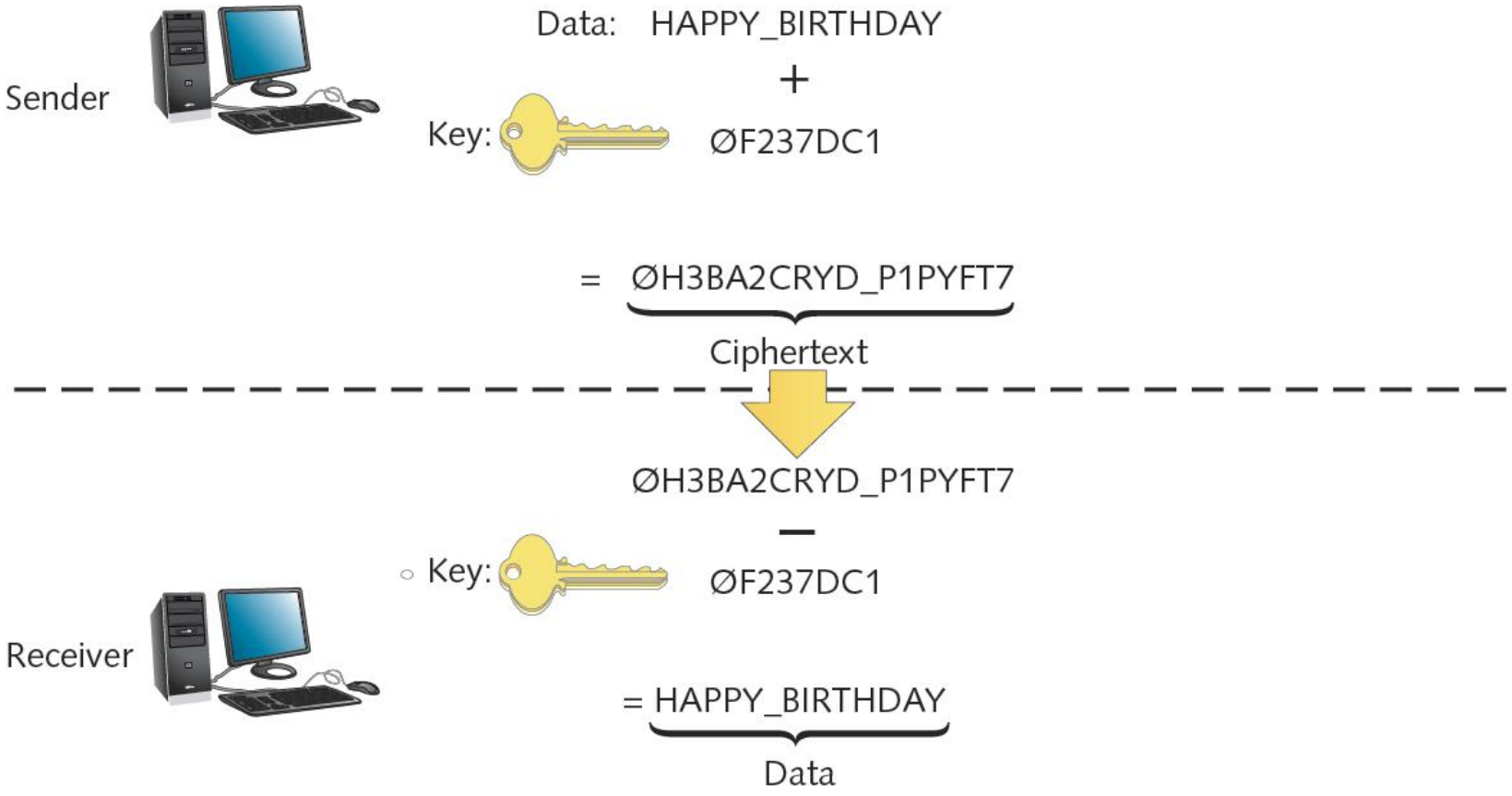
- Tips
  - Change system default passwords
  - Do not use familiar information or dictionary words
    - Dictionary attack
  - Use long passwords
    - Letters, numbers, special characters
  - Do not write down or share
  - Change frequently
  - Do not reuse
  - Use different passwords for different applications

Encryption

- Use of algorithm to scramble data
  - Format read by algorithm reversal (decryption)
- Designed to keep information private
- Many encryption forms exist
- Provides assurances
  - Data not modified between being sent and received
  - Data can be viewed only by intended recipient
  - Data was not forged by an intruder

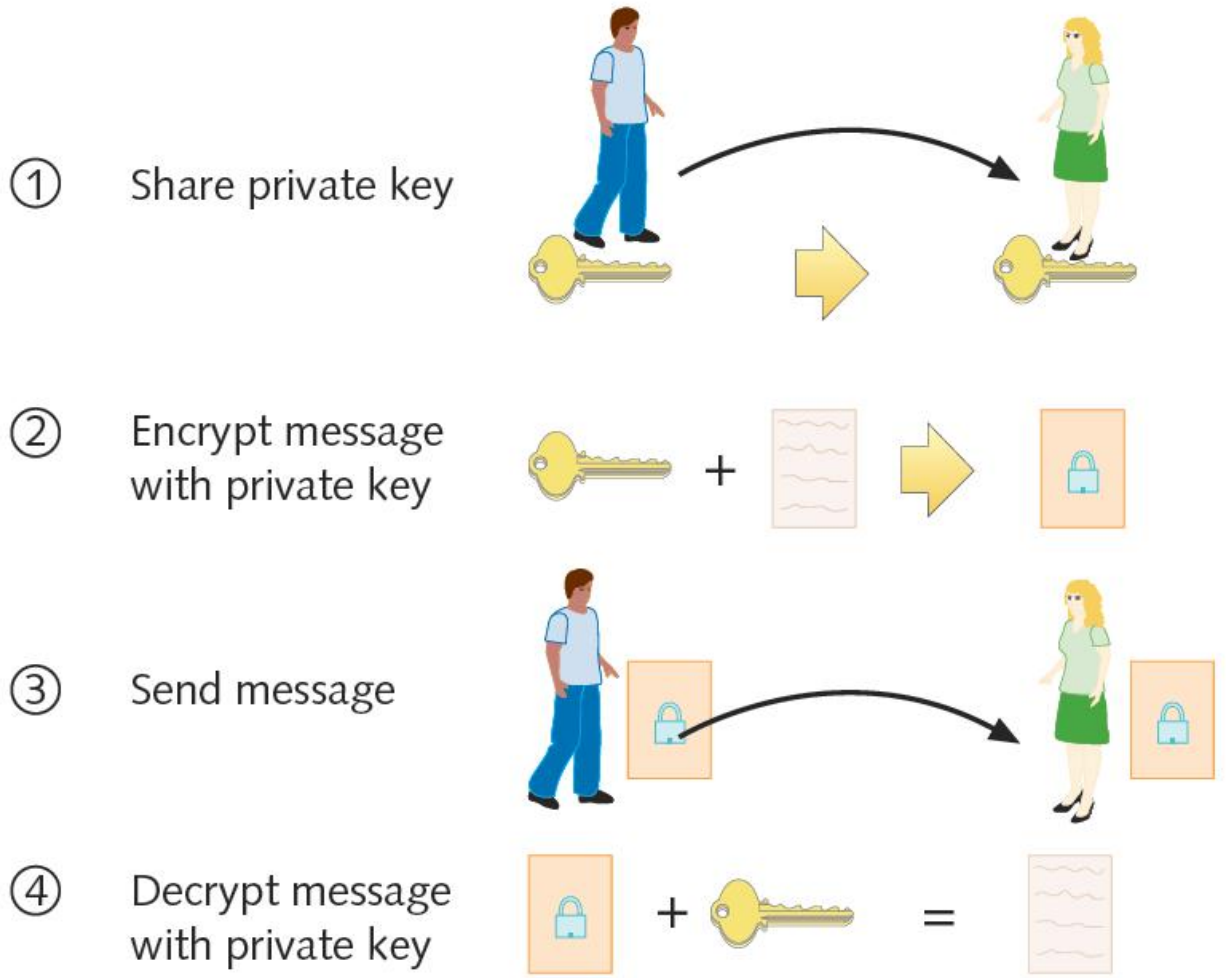
Key Encryption

- Key
  - Random string of characters
  - Woven into original data's bits
  - Generates unique data block
- Ciphertext
  - Scrambled data block
- Brute force attack
  - Attempt to discover key
  - Trying numerous possible character combinations


Sender
Data: HAPPY_BIRTHDAY
+
Key:
ØF237DC1
= ØH3BA2CRYD_P1PYFT7
Ciphertext
ØH3BA2CRYD_P1PYFT7
–
Key:
ØF237DC1
Receiver
= HAPPY_BIRTHDAY
Data

Key Encryption (cont'd.)

- Private key encryption
  - Data encrypted using single key
    - Known only by sender and receiver
  - Symmetric encryption
    - Same key used during both encryption and decryption
- DES (Data Encryption Standard)
  - Most popular private key encryption
  - IBM developed (1970s)
  - 56-bit key: secure at the time
- Triple DES
  - Weaves 56-bit key three times



Private key encryption

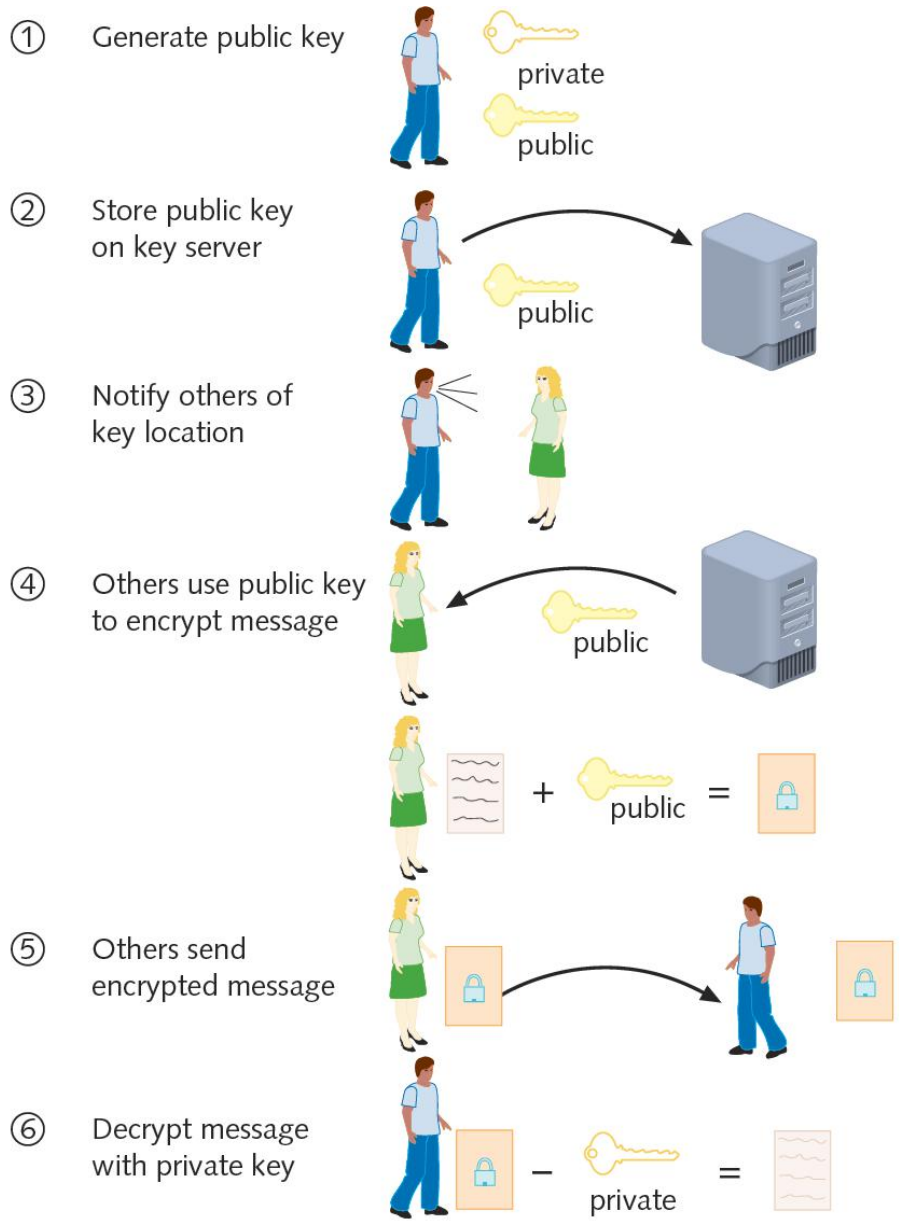
Key Encryption (cont'd.)

- AES (Advanced Encryption Standard)
  - Weaves 128, 160, 192, 256 bit keys through data multiple times
  - Popular form uses Rijndael algorithm
    - More secure than DES
    - Much faster than Triple DES
  - Replaced DES in high security level situations
- Private key encryption drawback
  - Sender must somehow share key with recipient

Key Encryption (cont'd.)

- Public key encryption
  - Data encrypted using two keys
  - Private key: user knows
  - Public key: anyone may request
- Public key server
  - Publicly accessible host
  - Freely provides users' public keys
- Key pair
  - Combination of public key and private key
- Asymmetric encryption
  - Requires two different keys

Public key encryption



Key Encryption (cont'd.)

- Diffie-Hellman (1975)
  - First public key algorithm
- RSA
  - Most popular
  - Key creation
    - Choose two large prime numbers, multiplying together
  - May be used in conjunction with RC4
    - Weaves key with data multiple times, as computer issues data stream

Key Encryption (cont'd.)

- RC4
  - Key up to 2048 bits long
  - Highly secure and fast
- Digital certificate
  - Password-protected, encrypted file
  - Holds identification information
  - Includes public key

Key Encryption (cont'd.)

- CA (certificate authority)
  - Issues, maintains digital certificates
  - Example: Verisign
- PKI (public key infrastructure)
  - Use of certificate authorities to associate public keys with certain users

PGP (Pretty Good Privacy)

- Secures e-mail transmissions
- Developed by Phil Zimmerman (1990s)
- Public key encryption system
  - Verifies e-mail sender authenticity
  - Encrypts e-mail data in transmission
- Administered at MIT
- Freely available
  - Open source and proprietary
- Also used to encrypt storage device data

SSL (Secure Sockets Layer)

- Encrypts TCP/IP transmissions
  - Web pages and Web form data between client and server
  - Uses public key encryption technology
- Web pages using HTTPS
  - HTTP over Secure Sockets Layer, HTTP Secure
  - Data transferred from server to client (vice versa) using SSL encryption
- HTTPS uses TCP port 443

SSH (Secure Shell)

- Collection of protocols
- Provides Telnet capabilities with security
- Guards against security threats
  - Unauthorized host access
  - IP spoofing
  - Interception of data in transit
  - DNS spoofing
- Encryption algorithm (depends on version)
  - DES, Triple DES, RSA, Kerberos, others

SCP (Secure CoPy) and SFTP (Secure File Transfer Protocol)

- SCP (Secure CoPy) utility
  - Extension to OpenSSH
  - Allows copying of files from one host to another securely
  - Replaces insecure file copy protocols (FTP)
  - Included with UNIX, Linux, and Macintosh OS X operating systems
- Windows operating systems
  - Some SSH programs include SCP utility
  - Separate freeware SCP application: WinSCP

IPSec (Internet Protocol Security)

- Defines encryption, authentication, key management for TCP/IP transmissions
- Enhancement to IPv4
- Native IPv6 standard
- Difference from other methods
  - Encrypts data
    - Adds security information to all IP packet headers
  - Transforms data packets
  - Operates at Network layer (Layer 3)

IPSec (cont'd.)

- Two phase authentication
  - Key management
    - Two nodes agree on common parameters for key use
    - IKE (Internet Key Exchange)
  - Encryption
    - AH (authentication header)
    - ESP (Encapsulating Security Payload)
- Used with any TCP/IP transmission
  - Most commonly runs on routers, connectivity devices in VPN context

Authentication Protocols (some…not all)

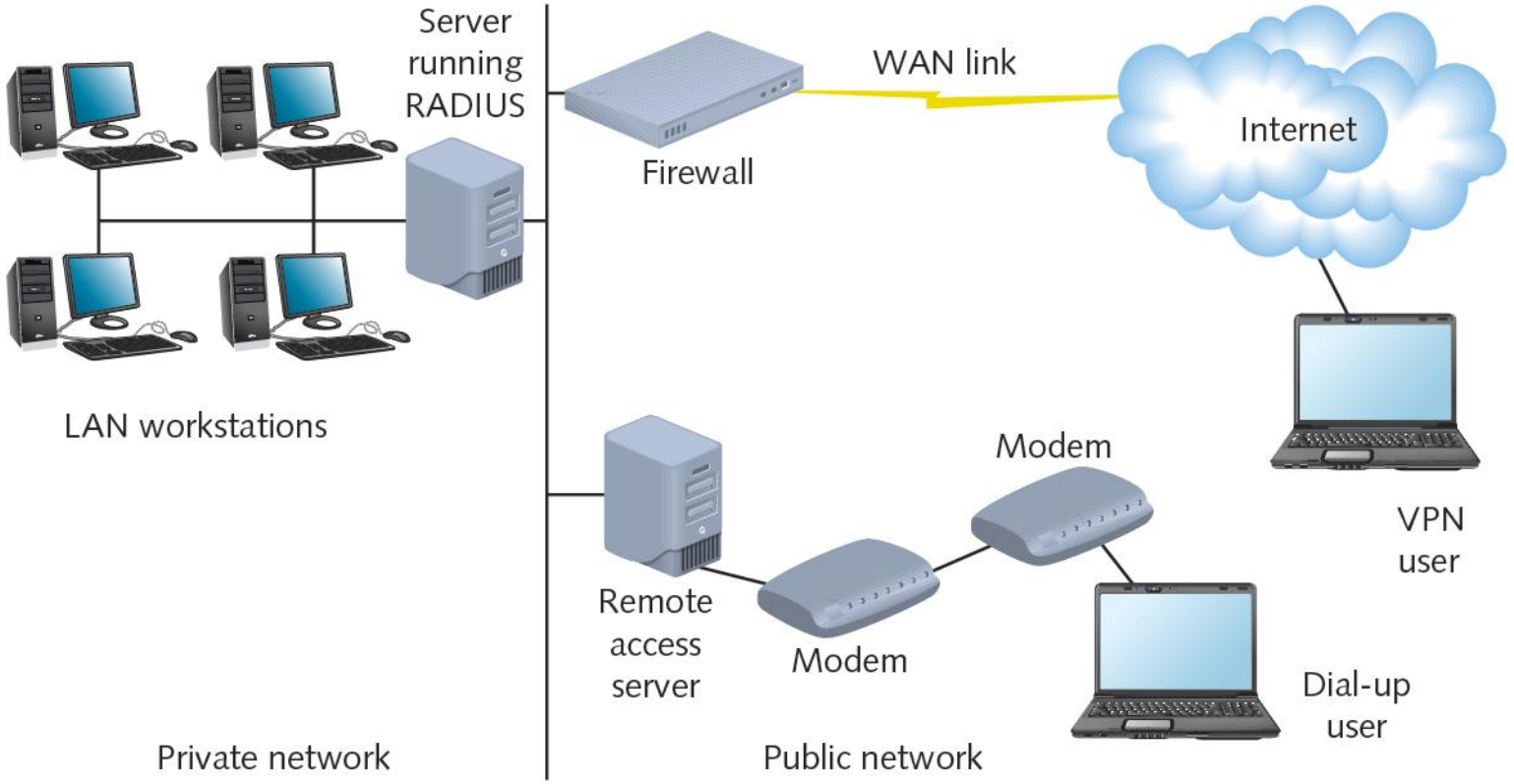
- Authentication
  - Process of verifying user's credentials
    - Grant user access to secured resources
- Authentication protocols
  - Rules computers follow to accomplish authentication
- Several authentication protocol types
  - Vary by encryption scheme:
    - And steps taken to verify credentials

RADIUS and TACACS+

- Centralized service
  - Often used to manage resource access
- AAA (authentication, authorization, and accounting)
  - Category of protocols that provide service
  - Establish client's identity
  - Examine credentials and allow or deny access
  - Track client's system or network usage

RADIUS and TACACS+ (cont'd.)

- RADIUS (Remote Authentication Dial-In User Service)
  - Defined by the IETF
  - Runs over UDP
  - Can operate as application on remote access server
    - Or on dedicated RADIUS server
  - Highly scalable
  - May be used to authenticate wireless connections
  - Can work in conjunction with other network servers



A RADIUS server on a network

RADIUS and TACACS+ (cont'd.)

- TACACS+ (Terminal Access Controller Access Control System Plus)
  - Separate access, authentication, and auditing capabilities
  - Differences from RADIUS
    - Relies on TCP at the Network layer
  - Proprietary protocol developed by Cisco Systems, Inc.
  - Typically installed on a router

Kerberos

- Cross-platform authentication protocol
- Uses key encryption
  - Verifies client identity
  - Securely exchanges information after client logs on
- Private key encryption service
- Provides significant security advantages over simple NOS authentication

IT Masters
itmasters.edu.au

Charles Sturt University

Questions?