Networks & Collaboration

- **Collaboration**
  - two or more people working together to achieve a common goal, result, or product
  - produces results greater than those that could be produced by any of the individuals working alone
  - coordination & communication and often makes use of computer networks

Networks & Collaboration

- Effectiveness driven by:
  - Communication skills and culture
    - Part of a group, giving critical feedback
  - Communication systems
    - Email, VPNs, instant messaging
  - Content management
    - Databases and content management
  - Workflow control
    - Process for creating/editing/using content

Networks Externality

- the larger the number of people using a network, the more valuable that network becomes ("network effect")
- When networks first started, people often look for the critical mass
  - Value for being part of the network > cost
- When networks hit critical mass, they usually grow at a faster rate
- Network growth may lead to congestion problems or the market may become saturated
  - Cycle of the network

Computer Network

- Network
  - Collection of computers
  - Communicate via transmission media
    - Physical: copper cable, optical fibre
    - Wireless
    - Radio Frequenicies
- Types
  - Local area network (LAN)
  - Wide area network (WAN)
  - Internet

LAN – Local Area Network

- Computers connected together at a *single* physical site
  - Any number of computers
  - One (small) geographic area
  - Property controlled by company operating network
    - company can run cabling as necessary

WAN – Wide Area Network

- Connect computers in *different* geographical areas
  - Physically separated sites
- Use a variety of communication networks
  - licensed by Government

The Internet and internets

- Network of networks
- Connect LANs, WANs, and other internets
- The Internet
  - Sending email and browsing the web
- internets
  - Private networks of networks

The Internet and internets

- Uses a variety of communication methods and conventions
  - Layered protocols provides a seamless flow of data
    - set of rules that communicating devices follow

History of the Internet

- That 60's problem:
  - Share data -> computers in many locations
  - Incompatible computers
    - operating systems, hardware, software
  - Primitive communications technology
- Solution:
  - ARPANET (Advanced Research Projects Agency NETwork)
    - 1969: requested by Department of Defense
    - Its technology spawned the Internet

Components of a LAN

- Switch
  - special purpose computer that receives and transmits messages on the LAN
  - May have more than one per LAN
- Network Interface Card (NIC)
  - hardware to connect each device to the cable
  - built-in NIC or expansion slot card
  - MAC (Media Access Controller) address
    - Unique identifier

LAN Network Protocol

- All Devices use same protocol
- Institute for Electrical & Electronics Engineers (IEEE)
  - Create & publish standards
  - LAN protocols from IEEE 802 committee
- IEEE 802.3 or Ethernet
  - Specifies
    - Hardware characteristics
    - Message packaging & processing
    - Operates at Layers 1 & 2 of TCP/IP-OSI architecture
- PCs support 10/100/1000 Ethernet NICs
  - 10, 100 or 1,000 Mbps
  - 1000/1024 & Bits/bytes

LANs with Wireless Connections

- Wireless NIC (WNIC)
- LAN operation
  - NICs - 802.3 protocol
  - WNICs - 802.11 protocol (Wi-Fi)
  - WNICS connect to Access Point (AP)
    - AP processes both standards

Connecting to the Internet

- The Internet is a Wide Area Network (WAN)
- Connecting computers at separate sites
  - Unable to use cable between sites
  - Obtain use of connections from licensed communications companies
  - Routers implement the protocol for WANs
    - Special purpose computers

Connecting to the Internet

- Individual Computer connection via router to an ISP
- Internet Service Provider (ISP)
  - Legitimate Internet address
  - Gateway to Internet
  - Fee for use of Internet
    - Pay for the Internet

Web vs Internet

- Web
  - Subset of the Internet
  - Consists of sites that process http
  - Use browser to surf the web
- Internet
  - Communications infrastructure
  - Supports all application layer protocols
    - http, smtp, ftp

Names & Addresses

- Rules exist for naming sites
  - Top-Level Domain (TLD)
    - .ca, .com, .org, .biz
- Address on the Internet
  - Uniform Resource Locator (URL)
- Logical Address (IP address)
  - Comprised of four sets of numbers separated by periods
- 198.103.238.30 = www.canada.ca

IP Addresses

- Two kinds:
  - Public
    - Used on Internet
    - Assigned by ICANN to ISPs & institutions
      - Internet Corporation for Assigned Names and Numbers
    - Each address is unique
  - Private
    - Used within private networks
    - Controlled by company operating network

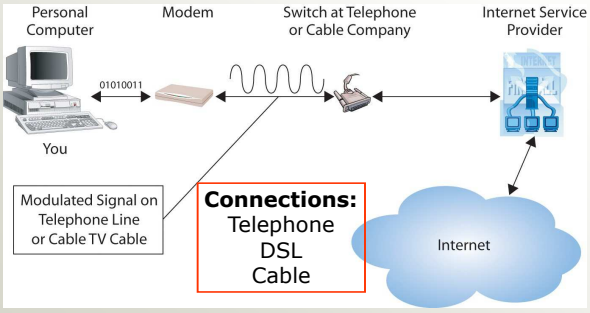
Dynamic Host Configuration Protocol Server

- IP Addresses assigned dynamically
- Assigns temporary IP address
  - Address used while connected to LAN
    - Plugged or wireless
  - When disconnected, IP made available
  - Re-assigns IP address as needed

Domain Name System

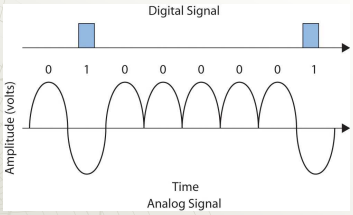
- Domain Name System (DNS)
  - Translates URL names into IP addresses
  - Resolves domain name
    - ICANN manages resolution system
- Domain Name Resolution
  - Conversion
  - domain name -> public IP address
  - Performed by Domain Name Resolvers

Connecting to an ISP



Analog vs Digital Signal

Digital Signal from Computer



Modem (modulator/demodular) completes conversion

Analog signal for transmission on telephone line or TV cable

Dial-Up Modems

- Uses telephone lines (twisted pair)
- Interferes with voice telephone service
- Converts between analog and digital
- Dial ISP for connection
- Max transmission speed = 56 kbps

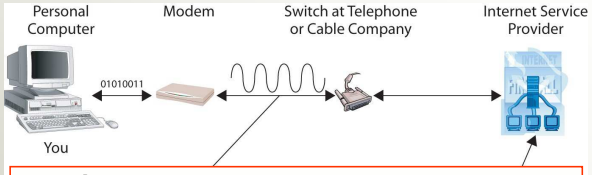
DSL Modems

- Digital Subscriber Line (DSL)
- Operates over telephone lines (twisted pair)
- No interference with voice service
- Faster data transmission than dial-up
- Connection always maintained
- Uses its own protocols
- Services and Speeds:
  - Asymmetric digital subscriber lines (ADSL)
    - 256kbps – 768kbps (upload/download different speeds)
  - Symmetrical digital subscriber lines (SDSL)
    - Up to 1.544mbps (upload/download same speed)

Cable Modems

- High-speed data transmission
- Cable television lines (coaxial cable)
  - Connects subscribers to distribution center
- High-capacity optical fiber cable
  - Connects neighbourhood distribution centers
- No interference with TV transmission
- Uses its own protocols
- Performance based on the # connected
  - Download speed up to 10Mbps
  - Upload speed up to 256 kbps

Connections



Speeds:
Narrowband (dial-up)
- Transmission speeds less then 56 kbps

Broadband (DSL, Cable)
- Transmission speeds in excess of 256 kbps

Wireless WAN

- **WWAN** differs from a wireless LAN
  - Covers a larger area
  - Use cellular networks to transfer data
- Radio waves used to connect Portable computer with a wireless WAN modem to a base station a wireless network
- Radio tower carries signal to a mobile switching centre, where the data are passed on to the appropriate network
- Wireless service provider then provides the connection to the Internet

Securing the Network: Firewalls

- Firewall:
  - Computer device that prevents unauthorized network access
  - Special-purpose computer or program
  - Organizations may have multiple firewalls
  - Used when connecting to The Internet
- Restricts access via
  - Port Number
  - Access control list (ACL)
  - Packet-filtering

Securing the Network: Firewalls

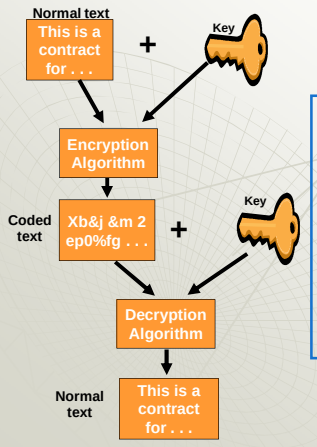
- Restricts access
  - Port Number
  - Indentifies a particular service
  - Ex: 80 for http, 25 for smtp
  - Filter out particular port #'s to restrict access
- Access control list (ACL)
  - Tracks IP addresses
  - Filter access to sites via IP address
  - Filter access from other sites via IP address

Securing the Network: Firewalls

- Packet-filtering firewalls
  - Examine source & destination address, & other data before allowing message to pass
  - Filter incoming & outgoing messages
  - Prohibit traffic from particular sites
  - Prohibit access to specific sites

Encryption

- Used for secure storage or communication
- Common encryption algorithms
  - DES – Data Encryption Standard & AES – Advanced Encryption Standard
    - U.S. government's standard for data encryption
  - 3DES – Triple Data Encryption Standard
    - Uses a key three times as long as Standard DES
    - Used for banks and other organizations that transmit highly sensitive data



- **Encryption** is the process of transforming normal text into coded text
- **Decryption** reverses this process.
- To encrypt or decrypt, both a key and an algorithm are needed.

Encryption

- Symmetric encryption
  - Use same key to encrypt and decrypt.
  - Advantages:
    - Much faster than asymmetric encryption.
  - Disadvantages:
    - Sender and receiver must both know the key
    - Both must ensure that the key is kept secret
    - If key becomes public, others will be able to decrypt
    - Both sides of a transaction use the same key – difficult to know who created the document

Encryption

- Asymmetric encryption
  - Use two keys:
    - **public key** is shared/exchanged publicly
    - **private key** is known only to the owner of that key
  - Message encoded with one, decoded with other
  - Advantages over symmetric keys:
    - Public key can be publicly distributed
    - Only one party has the private key, easy to know who created the document
    - Easy to implement over a network
  - Disadvantage is the speed.
    - Slower encryption method
    - Too slow for large amounts of data

Encryption

- HTTPS Protocol
  - Secure communication over Internet
    - http that uses SSL/TLS is //https
      - Encrypted using Secured Socket Layer (SSL)/Transport Layer Security (TLS) protocol
    - Encodes messages using Web site's public key, decoded with private key
  - Secure for sending sensitive data

Normal internet communications are not encrypted.

SSL/TLS

- Protocol uses both encryption methods
- Makes it safe to send sensitive data
- Asymmetric encryption transmits symmetric key
- Both parties then use the symmetric key
- Allows verification that communication is with a "true" Web site

SSL/TLS - Encryption

1. Computer obtains the public key of the website
2. Computer generates a key for symmetric encryption
3. Computer encodes that key using the website's public key. It sends the encrypted symmetric key to the website
4. Website decodes the symmetric key using its private key
5. From that point forward, computer and the website communicate using symmetric encryption

Digital Signatures

- Messages sent using plaintext
  - Can be intercepted and altered
- Digital signatures
  - Ensure no alteration of plaintext messages
  - Plaintext message hashed
    - Method that mathematically manipulates message to create bit string

Hashing

- **Hash** – transformation of plaintext of any length into a short code
- Differs from encryption:
  - Encryption always produces ciphertext similar in length to the plaintext, but hashing produces a hash of a fixed short length.
  - Encryption is reversible, but hashing is not; you cannot transform a hash back into its original plaintext.

Certificate Authority (CA)

- Organization that issues public/private keys and records the public key in a digital certificate.
- Common commercial certificate authorities are Thawte or Verisign. (WebCT)
- Certificate authority:
  - Hashes the information stored on a digital certificate
  - Encrypts that hash with its private key
  - Appends that digital signature to the digital certificate
- Provides a means for validating the authenticity of the certificate.

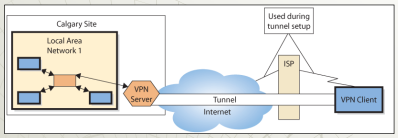
Digital Certificates

- Electronic document
  - created and digitally signed by a trusted third party.
- Certifies identity of the owner of a public key.
- Contains that party's public key.
- Browsers automatically obtain the digital certificate and use the public key contained in it to communicate with a website.
- Can be examined within your browser.
- Listed online in a publicly accessible repository

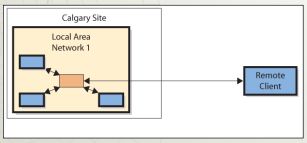
VPNs & Their Importance

- Virtual private network (VPN)
  - Use Internet or private network to create appearance of point-to-point connection
  - Tunnel connection
    - Client & server point-to-point connection
    - Private pathway over shared network
  - Secure with use of encrypted communications

Remote Access Using VPN



- Connection of a remote computer
- VPN software establishes connection
- VPN client/server have point-to-point connection
- Connection called a tunnel



VPN Communications

- Secure even over public internet
- VPN Client software encrypts message
- Encrypted message sent over Internet
- VPN server software decrypts message

Domains

Email address is:
user@hostname.sub.dom

- **username** is the person's "mailbox"
- **hostname** is the name of the host computer and is followed by one or more domains separated by periods:
  - host.domain
  - host.subdomain.domain
  - host.subdomain.subdomain.domain

E-mail?

- Messages & attachments sent
  - Broken down into pieces called: PACKETS
- Routers determine how to send messages
- System used to verify all packets received
  - Packets resent if necessary
- Messages & attachments reassembled at recipient's computer

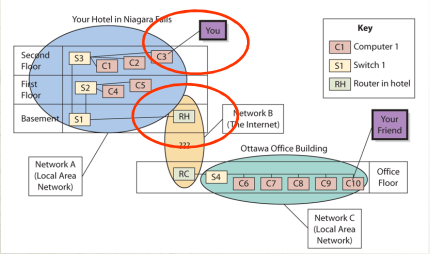
Communications Protocols

- Protocol
  - Standardized means
  - Used for coordinating activities
  - Sequence of ordered steps
- Communications protocols
  - Means for coordinating activities between communicating computers
    - Computers agree on protocol to use
  - Broken down into layers

Network Layers

- Developed by
  - Internet Engineering Task Force (IEFT)
- Transmission Control Program/Internet Protocol (TCP/IP) four-layer scheme
  - Layer 1
    - transmits data within a single network
  - Layers 2 & 3
    - data transmission across an internet
  - Layer 4
    - protocols allowing different applications to interact with each other and the individual

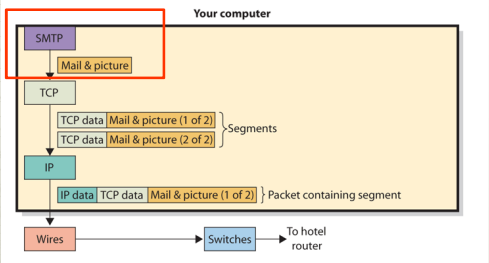
Sending an Email: Getting Connected



Getting Internet Access @ Hotel

- Search Hotel for DHCP server (Layer 1)
- RH server found
- Request RH for an IP address

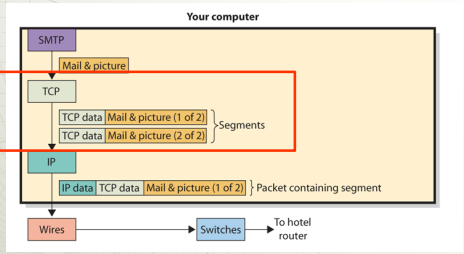
Sending an Email: Step 1



Pressing "Send/Receive"

- Generate & receive email (Layer 4)
- Simple Mail Transfer Protocol (SMTP)

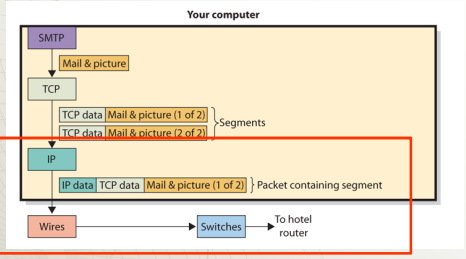
Sending an Email: Step 2



Break Apart Message & Get Ready for Transport

- Transmission Control Program (TCP) (Layer 3)
- Format and break message into segments

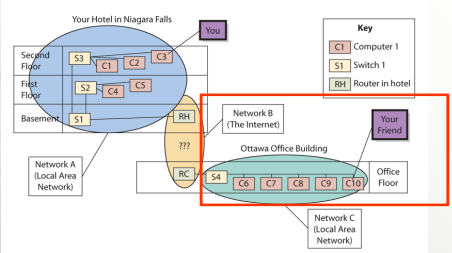
Sending an Email: Step 3



Send and Receive Packets

- Layer 2, Internet Protocol (IP)
- Packages message segments into Packet

Sending an Email: Step 4



Reassemble Packets and Display Message

- Packets arrive at destination
- Mail server reassembles message and gives to recipient

The Internet: Packet Switching Network

- Arpanet
  - 1st packet switching network
  - Provided access to many geographically separated computers
- Packet Switching Networks
  - Messages first disassembled into packets
  - Messages reassembled at the destination
  - Allowing for sharing of communication lines
  - Packets can be routed independently
    - Find their way to the destination
  - Provides for an efficient and resilient network

Your Phone Getting Smarter?

- Cellular telephones are no longer just phones, but rather mobile devices that provide a wide variety of services
- Built for communication and collaboration, and designed to be a networking machine

Smart Phones

- **Smart Phones**: iPhone, the E-series from Nokia, HTC Touch, Android or the latest BlackBerry from Research in Motion
  - Combine a powerful processor with sophisticated operating systems and cellular network technology
  - Provide a host of applications to their users including voice, text, email, web browsing, and much more

Smart Phones

- Design to be easy to use
- Networks
  - GSM
    - global systems for mobile communication
    - Rogers
  - CDMA
    - code division multiple access
    - Bell & Telus

Smart Phones

- Most operate on a 3G (4G)
- 3G is a group of standards for wireless communications
- 2G vs 3G
  - 3G provides higher data transfer rates and allows for simultaneous use of voice and data transfer
- Changing the way things are done
  - M-commerce
  - Working at home
- Security issues

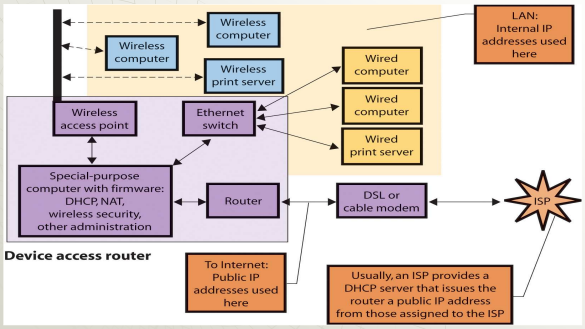
Search Engines and Web Crawlers

- Search engines
  - search for information on the Internet
  - 1st search engine Archie (1990)
  - Requires URLs and storage/retrieval method
- Web crawler software
  - browses the web to find URLs

Search Engines and Web Crawlers

- Search engine indexing
  - Index created for the results from the web crawling
- Search engines unable to "search" the entire web
- Each search engine uses its own search criteria
  - No two searches the same

Small Office Network



Accessing Programs in the Device Access Router

- Router has two IP addresses
  - Private address for local traffic
    - Assigned by manufacturer
    - Address used for internal routing
  - Public address for Internet traffic
    - Provided by ISP
    - Address valid on public Internet

DHCP on a Small Network

- Device access router provides DHCP server
- Computer contacts device to sign on
  - Obtains internal (private) IP address
- DHCP server keeps list with assigned address and MAC address
- Base station data also maintained
  - LAN MAC address is MAC address of Ethernet switch
  - MAC address is from router

Security Options

- Wired Equivalent Privacy (WEP)
  - Provides security over wireless networks
  - Each computer accessing LAN must enter symmetric key to encrypt data transmissions
  - Difficult to use in public places
- Wi-Fi Protected Access (WPA)
  - Improved version
  - Developed by IEEE 802.11 committee
- WPA2
  - Newer version

Security Option: MAC Address Filtering

- Prevents unauthorized access to LAN
- Requires MAC address of all authorized devices
- On Windows -> ipconfig
- On device access router input MAC Addresses into appropriate Filtering Security menu