Problem

- Ancient cities G and R have made a pact that each will come to the (military) aid of the other if one is in trouble.

G & R are 150 miles apart. How can they send a message for help quickly?
LOTRO: Beacon of Gondor

- Video: [http://www.youtube.com/watch?v=i6LGJ7evrAg](http://www.youtube.com/watch?v=i6LGJ7evrAg)
- Transmission medium: air - line of sight
- Data encoding: 1 bit – fire or no fire
- All receivers have to be listening
- Agreed upon interpretation of the signal at the endpoints
- Intermediate beacon wardens are always looking for a signal and relaying the signal
- One way communication
• Signaling technology can transmit complex sequences of bits - **packets**
• Each host or router obeys a set of rules for how to handle incoming/outgoing messages – communication **protocols**
• Communications can be multi-way
• **Bandwidth**: the number of bits that can be transferred per second (bps)
• **Latency**: the time it takes for a message to reach the destination after leaving the source
Local Area Networks

- Wired (UTP Cat5) or Wireless 802.11
- Connects hosts within a limited spatial region together to form a network
- All hosts within the network can “talk” to each other
- The network is often a shared medium: only one host can talk at one time and the rest listens.
Data Packet

- How messages are packaged for delivery on the network – like postal mail.
- Source and destination addresses
Network Abstractions

- Network communications are conceived as layers of abstractions.
- Each layer plays a specific role and is relatively independent of other layers.
- Each layer has its own packet format.
- Packets from higher layers are embedded in packets of lower layers – “encapsulation”.
TCP/IP Four Layer Model

**Application**
- Process to process: communicates data to other processes/applications on the same host or on other hosts
  - Eg. SMTP, FTP, SSH, HTTP

**Transport**
- Host to host: communicates data to other host on the same network or on other networks
  - Hides the topology of the network
  - Flow control, error correction, connection control
  - Eg. TCP, UDP

**Internet**
- Inter-network: communicates data to other networks
  - Deals with addressing and routing of datagrams to the next network
  - Eg. IPv4, IPv6

**Link**
- Transmit data to other network interfaces on the local network
  - Eg. Ethernet, WiFi 802.11
Data packet arrives from upper layer (Internet layer)
• If packet is too big, break packet into smaller fragments (`frames’)
• Embed data packet in a link layer packet with link layer header, sequence number, error correction code etc.
• Link layer packets gets transmitted on physical link
• Link layer protocol governs how transmission over physical link is done. Eg. Carrier sense multiple access

Bottom-up process is similar on the receiving host
Internet Layer

Data packet arrives from Transport layer
- Embed data packet in an IPv4 packet with IP header etc.
- Pass packet to Link layer

Data packet arrives from Link layer
- Check IP header if packet destination is for this host. If yes, strip header and pass to Transport layer
- Otherwise forward packet (routing)

Eg. IPv4
- Connects multiple networks together.
- Each network interface of a host is associated with an 32-bit IPv4 address
- IP address is not hardwired, but assigned in the software

Physical Network

Application
Transport
Internet
Link

Application
Transport
Internet
Link
IPv4 Addresses & Domain Name Service

- IP addresses are 32 bit numbers often written in 4 octets: 128.171.10.13
- Each address is also split into two parts
  - Prefix is the network address
  - Suffix is the host address within that network
- **Domain Name Servers** provide a service that translates more meaningful names to IP addresses
  - Uuninix.hawaii.edu = 128.171.24.197
  - www2.hawaii.edu = 128.171.224.150
IPv4 & Inter-network Routing

For routers

• Examine destination IP address
• Look up routing tables to determine outgoing network
• Pass packet to link layer of that outgoing network
• Best effort delivery – no guarantees!
Packet Routing Exercise
TCP provides a reliable communication channel between two host applications by addressing several issues:

- Data packets arriving out of order
- Data packets are corrupted
- Same packets arriving more than once
- Some packets are lost/discarded
- Traffic congestion control

TCP is used as the transport layer for applications such as TCP (connection-oriented) and UDP.

Each application on a host is associated with a port number, and an IP address + port number will identify an application end-point.
Your email client program downloads incoming emails from mail server (imap.gmail.com pop.gmail.com)

Outgoing emails are sent to mail server (smtp.gmail.com)

Mail servers handle the routing of emails using SMTP protocol which operates on port 25 or 587
  - Lookup IP address of destination hostname in the email address using DNS
  - Relaying email as packets to that IP address
Applications: HTTP

- Hyper-Text Transfer Protocol (port 80)
- Request-response protocol
- When [http://www2.hawaii.edu/~lipyeow/index.html](http://www2.hawaii.edu/~lipyeow/index.html) is entered into a web browser (http client)

```
GET /~lipyeow/index.html HTTP/1.1
host: www2.hawaii.edu
```

```
HTTP/1.1 200 OK
Date: Sun, 02 Sep 2012 00:35:40 GMT
Server: Apache
Last-Modified: Tue, 21 Aug 2012 01:27:18 GMT
ETag: "7d3e8-2950-4c7bc86e86980"
Accept-Ranges: bytes
Content-Length: 10576
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"> <HTML> ...
```
Internet Security

• All data transmitted on the network using the protocols described thus far are in plaintext

• Anyone with access to the physical network link can snoop on the bit sequences and decode according to the protocol stack!

• Anyone can read your emails if he/she has access to a link on which your email packets are transmitted

• Use encrypted connections eg. SSL/TLS
Secure HTTP -- HTTPS

- Use HTTP over a SSL/TLS layer (port 443)
- Negotiate a stateful encrypted connection to carry the HTTP messages.
- Use a trusted 3rd party (CA) to verify identity
- Use public key handshake to establish a session key
- Encrypt subsequent messages using session key