Internet Technology

01r. Lecture 1 Review: Key Terms

Paul Krzyzanowski
Rutgers University
Spring 2016
Basic principles & terminology

• The basic principles of data communication were established *long before* computer networking

• Let’s review some key terms we covered in the last lecture
Key terms (1)

- **Broadcast**
  - Send a message that will be received by everyone on the network

- **Unicast**
  - Send a message to one specific recipient

- **Synchronization**
  - Coordinate the delivery of messages.
  - E.g., agree to start, stop, or coordinate who transmits

- **Relay**
  - **Repeater**: regenerate the message to extend the network farther
Key terms (2)

• Control data vs. message data
  – Control data relates to the messaging protocol
    • synchronization, acknowledgements, flow control, priority, etc.
  – Message data is the actual data that you want to convey to the receiver

• Acknowledgement (also known as positive acknowledgement)
  – A control message sent from the receiver to the sender to indicate that a message has been received successfully

• Negative Acknowledgement
  – A form of error notification
  – A control message sent from the receiver or some network element to the sender to indicate that a message has NOT been delivered successfully
Key terms (3)

• Congestion
  – The inability of a network element to receive or transmit messages at the desired rate, leading to a buildup or possibly a loss of messages and a deterioration in the quality of service

• Flow control
  – Modifying the rate at which messages are sent to avoid congestion
  – This may includes control messages, such as "slow down"
Key terms (4)

• **Message encoding**
  – The techniques used to represent a message.
  – Before computers, this referred to, for example, the number of torches to display or positions of a semaphore for a specific message.
  – With digital techniques, this refers to the binary symbols used to represent the message and how those binary symbols are transmitted.

• **Best-effort message delivery**
  – An attempt to deliver messages reliably. If a message does not make it to the destination, try again: re-transmit
ARPANET

• ARPANET was a precursor to the Internet

• Inter-network – a network of networks
  – The devices on the ARPANET (and, later, the Internet) do not have to use the same (or compatible) networking hardware.
  – Routers interconnect the various networks together, creating a larger logical network

• Early key components of the ARPANET
  – IMP – Interface Message Processor. This evolved to the router.
    • This provided the hardware to route messages to their destination.
  – NCP – Network Control Protocol. This evolved to TCP/IP.
    • This provided the software for addressing, sending, and receiving messages.
Key design principles

Design principles of ARPANET, which became the design principles of the Internet

1. The Internet is a network of networks
   - No modification is needed to any underlying physical network to support the Internet
   - Different organizations may use different networking hardware

2. Assume unreliable networks
   - The network (collection of networks that a message takes) does not guarantee that a message will arrive at its destination or that messages will arrive in the order they were sent.
   - Software will be responsible for retransmitting lost or corrupt messages and for sequencing the messages in proper order.

3. Routers connect the networks that make up the Internet
   - Routers do not have to store information about past packets they’ve seen

4. There is no central control of the network
The network

• Two parts: the core & edge

• The edge
  – the devices (computers, TVs, phones) that connect to the network
  – These devices are called nodes, hosts, or end points

• The core
  – The network itself: the wires & radio waves that carry the messages and the routers that relay them toward their destination.
Local area network (LAN)

• The network within a small area (e.g., home, office)
• Compatible networking hardware
  – E.g., all ethernet (Wi-Fi bridges to ethernet and is compatible)
  – No routers needed to send messages from one node to another
• All nodes are peers: anyone can send a message to anyone else
• Generally high speed links with low latency
Local Area Network terms

• A NIC (Network Interface Component) connects a network to a device.

• Media: the communication links of the network
  – Unshielded Twisted Pair (e.g., ethernet), radio (e.g., Wi-Fi), coaxial cable (e.g., cable TV internet service), optical fiber (e.g., FiOS)

• Hubs & switches
  – Central point on a LAN for cables from the various nodes on the LAN
    • Consists of multiple ports. Port = connector for one cable.
  – Hub
    • Takes incoming data from one port and sends it to all other ports
  – Switch
    • Takes incoming data from one port and sends it only to the port where it needs to go. Better than a hub because it does not create extra network traffic for node. [Hubs are practically obsolete now; switches are pretty cheap]

• Routers
  – Used to move messages between local area networks
Local Area Network terms

• **Modem**
  – Stands for Modulator-Demodulator
  – Converts data between different analog formats (e.g., phone lines, cable TV, fiber optic cable)

• **Access link**
  – The interface between a LAN and the Internet
  – Common access links
    • DSL: digital subscriber line
      – DSL modem: places data packets on frequencies in the 4 kHz – 1 MHz range of a phone line
    • Cable TV
      – DOCSIS cable modem: places data packets on one or more 6 MHz wide channels. Each of these channels is the space that a single HDTV channel occupies and gives 38 Mbps of downstream service
    • Fiber to the Home (FTTH)
      – Verizon FiOS
Internet Service Providers

• Internet access is provided by a company called an Internet Service Provider (ISP)
  – There are thousands of ISPs

• ISPs are (roughly) organized into three tiers
  – **Tier 1**: top-level ISPs
    • Peer with each other
    • **Peering** = forward & receive traffic with another ISP at no cost
    • Keep a **global routing table**. For any destination address, a Tier 1 ISP will know which Tier 1 ISP can route the message
  – **Tier 2**: second level - regional
    • May peer with some networks – across regions or with competitors within a region
    • Purchases connectivity to the rest of the Internet from Tier 1 & other Tier 2 ISPs
  – **Tier 3**: third level – focus on retail and consumers
    • Purchases internet service from Tier 1 & Tier 2 ISPs
Packet Routing

• A packet going from a source node to a destination will typically pass through many networks (routers), both within an ISP and between ISPs
Sharing a network

• Lots of nodes & applications need to share a network

• Two options:
  1. Allow everyone to talk at the same time
     • …but use different frequency bands
     • FDM: Frequency Division Multiplexing
  2. Take turns
     • Two ways of doing this:
       1. Give each communication line a fixed time slot (e.g., you can transmit for 15 milliseconds every second)
         □ TDM: Time Division Multiplexing
       2. Let anyone transmit on variable-size time slots (more time for bigger packets)
         □ Packet switching
Circuit switching

• Requires connection setup
  – **Connection setup** figures out the path from source to destination
    • Each router in the path allocates memory buffers and time to ensure that
      it can handle the data traffic
  – Once the connection has been acknowledged, data transmission
    can occur

• Circuit switching offers
  – Guaranteed, fixed, bandwidth
  – Constant latency

• BUT … it does not use resources efficiently
  – The time slot is there whether you use it or not
Packet switching

• A data stream is broken into chunks called packets
• Each packet contains a destination address
• Routers do need to store state of past packets
  – They figure out a route when they get the packet

• Packet switching can lead to:
  – Variable latency
  – Congestion and possible packet loss
• BUT … it allows far more efficient use of the network
  – And network capacity is not limited by the number of nodes or applications that need to send data
• The Internet is built around packet switching
The end