Technology & Society

Wireless Networking

A Technical Overview

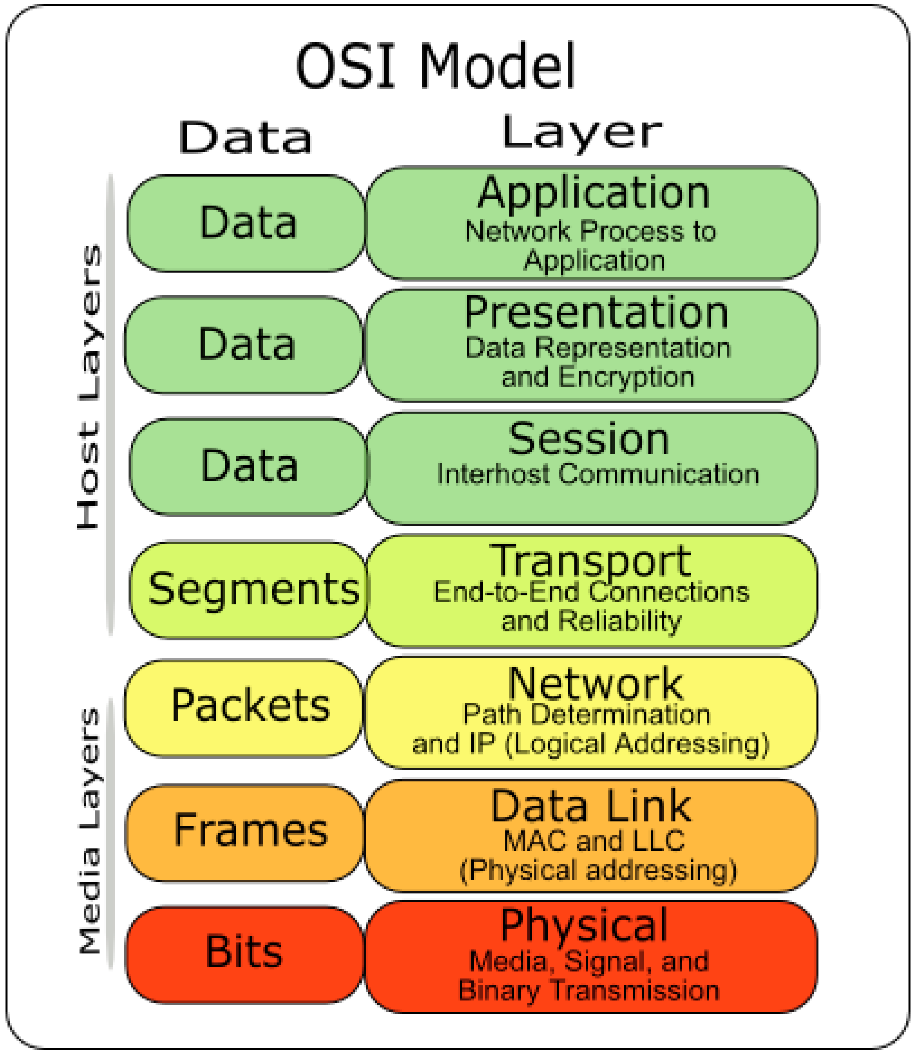
Stefan Karpinski

The OSI Model

- The outline for this talk is provided by the OSI model
  - OSI defines how different layers of technology interact in the Internet and other Internet-like systems
  - Using OSI as a theme for the talk will help to
    - place technologies within a framework
    - explain & clarify their relation to each other
  - Wireless technologies in particular present challenges to the OSI model
    - However, everything is still understood in reference to it

The OSI Model

- OSI stands for Open Systems Interconnect, from *c.* 1977
  - OSI reference model defines seven layers in networks



- *physical:* electricity, light, radio
- *data link:* Ethernet, 802.11, TDMA
- *network:* IP, ICMP, routing protocols
- *transport:* TCP, UDP, (routing data)
- *session & presentation:* unused[ish]
- *application:* web, email, video, ...

The Physical Layer

- Defines all electrical, physical specifications for devices.
  - Hubs and repeaters are physical-layer devices.
- Examples of physical media:
  - Wired — electricity (copper), light (fiber optics)
  - Wireless — radio, light (IR), sound, smoke, pigeons

The Data Link Layer

- Ensures correct transfer of data across a single "link"
  - Also called the *MAC* layer — medium access control
    - Allow multiple devices to share a physical medium
  - The classic example is Ethernet
    - Also, 802.11a/b/g, Bluetooth are all link protocols
  - Both Ethernet and 802.11 use same basic MAC technique:
    - They use CSMA — Carrier Sense Multiple Access

CSMA and Variants

- CSMA is stunningly simple:
  - Don't send data if you can hear someone else doing so
  - Instead, wait a random amount of time and try again

    [surprisingly, this is *not* the simplest MAC protocol]
- What happens if two transmissions collide?
  - Nothing. That's not the link layer's problem.

The Network Layer

- The "narrow waist" of the protocol stack…
  - Only one basic protocol: the **Internet Protocol** (*aka* IP)
    - Expects lower layer to get a bunch of bits across a link
    - Captures sender & addressee information about data
    - Gets the data from point the sender to the receiver
  - What happens if the data doesn't get there?
    - Nothing. That's not the network layer's problem.

From A to B…

- How does IP get data from point A to point B?
  - It uses *header* data at the front of the payload data
    - Included are source (from) and destination (to)
  - Each computer that receives the IP packet needs to know how to get it one hop closer to the destination

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options (optional)				

IP headers

From A to B…

- How do the intermediate computers know how to get an IP packet one hop closer?
  - There are special protocols to learn this
- The full path from A to B is called a route
- Intermediate computers are called routers
- In most networks, routers are part of the infrastructure
  - Ad-hoc networks have no infrastructure:
    - No specialized routers, just mobile nodes, forwarding data packets for each other — all nodes are routers

The Transport Layer

- Transparent transfer of data between hosts
  - Two major flavors:
    - Transmission Control Protocol [TCP]
      - end-to-end error recovery
      - in-order data delivery
      - congestion control
    - User Datagram Protocol [UDP]
      - ensures only (weak) datagram integrity
  - Each has its own protocol headers
    - Important fields: source & destination port numbers

Wired vs. Wireless

- Several assumptions are made in the TCP/IP stack that are true in wired networks, but untrue in wireless:
  - devices don't move around
    - IP routing does not handle transparent mobility well
  - the bit error rate (BER) for the physical medium is low
    - wired: less than 1/10000 typically
    - wireless: often as high as 1/1000 or even 1/100
  - corollary — dropped packets are due to congestion
  - there exists fixed routing infrastructure
    - not true in adhoc networks and sensor networks

Wired vs. Wireless

- The violated assumptions of wired networks make wireless networking particularly challenging
  - Example 1: TCP over Wi-Fi
    - dropped packets are common due to wireless medium
    - TCP thinks there's network congestion, backs off
  - Example 2: Mobile IP
    - if you want to keep the same IP address but move around you have to jump through all sorts of hoops

Cellular Networks

- How do cellular technologies fit into the OSI model?
  - GSM & CDMA are specs crossing multiple layers
  - Completely non-interoperable separate protocol stacks
- *Example:* GSM uses a T/FDMA "data link" protocol
  - But GSM also specifies
    - base-station structure & organization (~physical)
    - data switching & mobility support (~network/transport)
    - authentication, billing & services (~application)

Questions?