ICS 451: Today's plan

- Spanning Tree Protocol (continued)
- Virtual LANs
- 802.11
  - ad-hoc networks
- 802.11 security

SPT algorithm

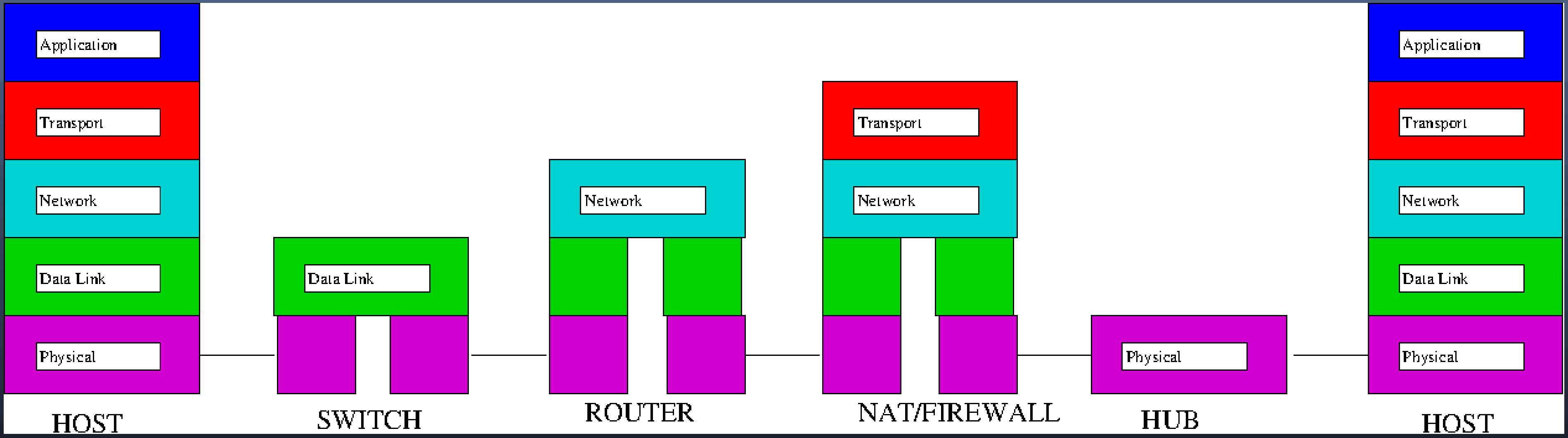
- when receiving <R, c, T, p> on interface q:
  - add the cost of q to the cost of c, then
  - save the BPDU as the latest for port q
  - if my ID < R, I am the root
    - set all my interfaces to *designated ports*
  - otherwise, I find the best saved BPDU *bv*
    - the port of *bv* is my *root port*
    - I compute my outgoing BPDU <R', c', T', _>
    - for each port, if my BPDU is better than the latest BPDU received from that port, I set that port to a *designated port*
    - otherwise, I *block* that port

STP details

- no traffic is forwarded during initial STP computation
- on link or switch failure, BPDUs eventually expire, and STP computation is restarted

- STP is almost plug-and-play
  - not enabled by default
    - perhaps not available on low-end switches
  - incurs additional traffic and delays
- STP supports redundant links!!!!

Hubs, Switches, Routers, NATs and layers



Virtual LANs

- a switch can be configured to group some of its interfaces into a Virtual LAN (VLAN)
- broadcasting (and STP) is only over the interfaces in the same VLAN
  - this can be combined with routing among the different VLANs
- VLANs over multiple switches require VLAN identifcation of received frames
  - additional header carries this ID (802.1q)
  - header also includes frame priority

802.11

- early marketing term “WiFi”
  - similar to “HiFi”, High Fidelity audio equipment
- over ISM license-free bands, mostly 2.45GHz
- designed to be similar to Ethernet
  - e.g. using MAC addresses
  - but has to deal with the wireless medium
    - acknowledgements required
- different speeds: 1, 2, 11, 54, 150 Mbps
  - at different frequencies: 2.45GHz, 5GHz

ISM Bands

- governments grant licenses to specific users to use the radio bands in specific ways
  - a form of FDM, avoids collisions
- some bands reserved for license-free uses
  - Industrial, Scientific, Medical (ISM) applications
  - may or may not be country dependent
  - the 2.45GHz (2.4 to 2.5 GHz) band used by microwave ovens is in ISM worldwide
- such uses have power limits
- and may have to accept interference

Wireless Medium

- not a uniform network as in a wired medium
  - not everyone receives the same packets
- cannot do collision detection (CD)
  - must acknowledge packets
    - except broadcast or multicast packets
- limited range (100m outdoors)
- easy to eavesdrop
  - attacker only needs to be “close enough”

Types of 802.11 networks

- ad-hoc networks:
  - all nodes are equivalent
  - peer to peer message passing
  - if devices are mobile, network changes over time
- infrastructure networks:
  - Wireless Access Points (WAPs) control network
  - all other nodes communicate through WAP(s)
  - often used to connect to Internet
    - very popular

802.11 data frame header fields

- frame control
  - data, ack, RTS/CTS, etc.
  - whether forwarded from a LAN
- duration
- 3 addresses:
  - host to server via WAP: (WAP, host, server)
  - server to host via WAP: (host, WAP, server)
- sequence control to remove duplicates

802.11 control frame header fields

- frame control
- duration
    - for RTS/CTS, duration of the entire exchange
- 1 or 2 addresses
    - acks only have a destination address
    - RTS/CTS have source and destination
- sequence control to remove duplicates

802.11 management frames

- beacon frames
  - supported speeds, Service Set ID (SSID)
  - if WAP sends no beacon frames, mobile device can request with probe request frames
- association request/response frames
  - requests contain SSID they want to join and parameters such as supported speeds

IP over 802.11

- Ethernet has different encapsulations, but usually IP is carried directly over Ethernet
- 802.11 has different encapsulations, and usually IP is encapsulated in an LLC/SNAP header
  - adds 6 bytes to the frame
- MTU is up to 2324 bytes
  - but usually limited to 1500 bytes for compatibility with Ethernet in infrastructure mode

802.11 security

- easy to eavesdrop, especially if unencrypted
  - no physical connection needed
- WEP (Wire Equivalent Privacy)
  - relatively easy to break, **do not use**
- WPA (WiFi Protected Access)
  - somewhat more secure, but still vulnerable
- WPA2
  - questionable security, but probably the best

other 802.11 security issues

- password guessing for weak passwords
  - dictionary attacks
- WiFi Protected Setup (WPS) was introduced to simplify secure configuration, but usually allows attacker to recover the WPS pin and have access to the network
- and more!

802.11 vs Ethernet

- ethernet is more secure, esp. with switches
  - but not completely secure, e.g. ARP attacks
- 802.11 supports mobility, no cabling needed
- ethernet can support higher data rates
  - switched ethernet has much fewer collisions
  - some ethernets have full-duplex links
  - generally lower latency
- 802.11 supports mobility!