ELEN E6761
Fall '00 - Lecture 2
IP Addressing, DNS & Hardware

Professor Dan Rubenstein

TA Info

- Vassilis Stachtos
  - e-mail: vs@comet.columbia.edu
  - Office: 801 CEPSR
  - Office Hr: Thurs, 4pm - 6pm
  - Mailbox: E2 (by the EE main office)
    - NOTE: recently changed (used to be E3)
  - Java?: will confirm before next assignment

Did you get my e-mail?

- You should have if you submitted the survey
- If not, please e-mail me (dsr100@columbia.edu) and (re)submit the survey
- Microsoft Word: if submitted in Word before my e-mail, then o.k. In future: No Microsoft Word!!!

HW info

- HW#1
  - not ready yet, will send it in an e-mail
  - due a week from the time of the e-mail
- HW#0… (go over math questions at end if there is time)
- PA#1 is due now!!!

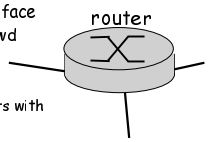
Overview of Today's Lecture

- DNS
  - Recursive Queries
  - Iterated Queries
  - Caching
- IP Addressing
  - Class-based
  - CIDR
- LAN Hardware / addressing
  - MAC address
  - Repeater
  - Hub
  - Bridge

5

Routers

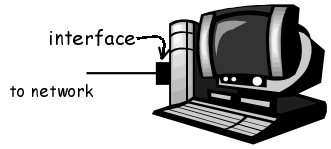
- Complex device that determines where to forward packets
  - Used in large-scale networks (i.e., it is typically not used to forward pkts within a LAN)
  - a packet arrives on one interface
  - leaves on other(s) heading twd desired destination(s)
  - routers must
    - determine where to fwd pkts with given destination address
    - use routing protocols to communicate with other routers



6

Addresses and Interfaces

- *interface:* connection between host or router and the physical network link
  - routers typically have multiple interfaces
  - hosts may have multiple interfaces
- Interfaces have addresses
  - Hosts don't have addresses(their interface does)
  - Routers don't have addresses (their interfaces do)



7

Internet addressing schemes

- A host interface has 3 types of addresses:
  - host name (Application Layer): e.g., medellin.cs.columbia.edu
  - IP address (Network Layer or Layer 3): e.g., 128.119.40.7
  - MAC address (Link Layer or Layer 2): e.g., E6-E9-00-17-BB-4B
- Actually, so do router interfaces:

traceroute cs.umass.edu (from medellin.cs.columbia.edu)

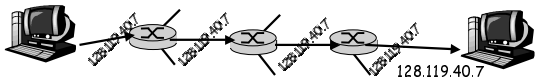
1 mudd-edge-1.net-columbia.edu (128.119.240.41)
2 nyser-gw.net.columbia.edu (128.59.16.1)
3 nn2k-gw.net.columbia.edu (128.59.1.6)
4 vbns-columbia1.nysernet.net (199.109.4.6)
5 jn1-at1-0-0-17.cht.vbns.net (204.147.132.130)
etc…

8

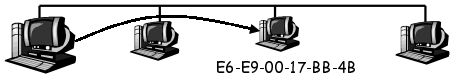
Why 3 Addressing Schemes?

- host names: convenient app-to-app communication

- IP: efficient large-scale network communication

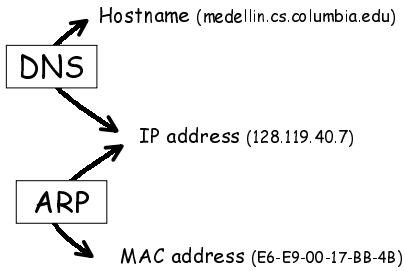


- MAC: quick-n-easy LAN forwarding



9

Translating between addresses



10

DNS: Domain Name System

People: many identifiers:
- SSN, name, Passport #

Internet hosts, routers:
- IP address (32 bit) - used for addressing datagrams
- "name", e.g., gaia.cs.umass.edu - used by humans

Domain Name System:
- *distributed database* implemented in hierarchy of many *name servers*
- *application-layer protocol* host, routers, name servers to communicate to *resolve* names (address/name translation)
  - note: core Internet function implemented as application-layer protocol
  - complexity at network's "edge" – interior routers don't maintain any DNS-related info

11

DNS name servers

Why not centralize DNS?
- single point of failure
- traffic volume
- distant centralized database
- maintenance

doesn't *scale!*

- no server has all name-to-IP address mappings

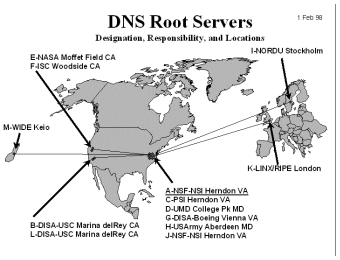
local name servers:
- each ISP, company has *local (default) name server*
- host DNS query first goes to local name server

authoritative name server:
- for a host: stores that host's IP address, name
- can perform name/address translation for that host's name

12

DNS: Root name servers

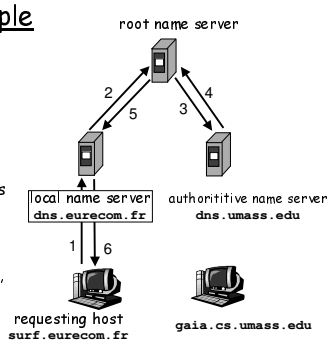
- contacted by local name server when can not resolve name
- root name server:
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server
- ~ dozen root name servers worldwide



Simple DNS example

host **surf.eurecom.fr** wants IP address of **gaia.cs.umass.edu**

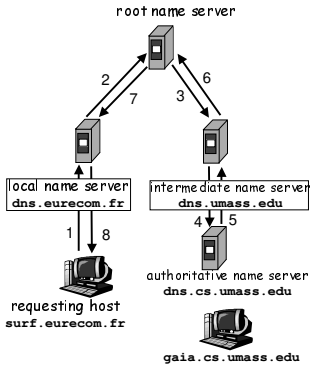
1. Contacts its local DNS server, **dns.eurecom.fr**
2. **dns.eurecom.fr** contacts root name server, if necessary
3. root name server contacts authoritative name server, **dns.umass.edu,** if necessary



DNS example

Root name server:

- may not know authoritative name server
- may know *intermediate name server:* who to contact to find authoritative name server



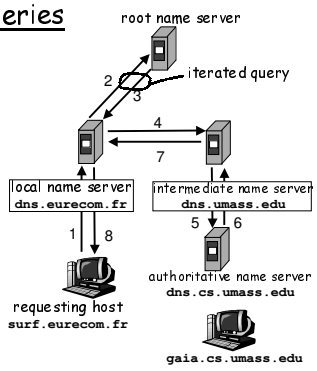
DNS: iterated queries

recursive query:

- puts burden of name resolution on contacted name server
- heavy load?

iterated query:

- contacted server replies with name of server to contact
- "I don't know this name, but ask this server"



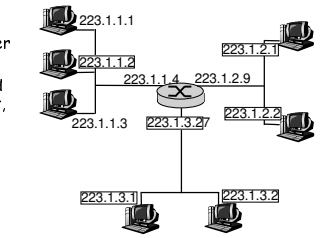
DNS: caching and updating records

- once (any) name server learns mapping, it *caches* mapping
  - To see the benefits of caching, compare time to "lookup" domain name:
    - e.g., www.cnn.com is almost always cached
    - e.g., something like www.meat.com usually not cached
  - cache entries timeout (disappear) after some time
- update/notify mechanisms under design by IETF
  - RFC 2136
  - http://www.ietf.org/html.charters/dnsind-charter.html

17

IP Addressing

- IP address: 32-bit identifier for host, router *interface*
  - IP addresses associated with interface, not host, router
- DHCP: Dynamic Host Configuration Protocol
  - some IP addresses left open
  - can be dynamically assigned (e.g., to a laptop) when interface connected



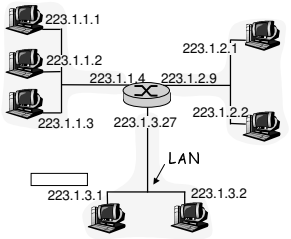
223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

18

IP Addressing

- IP address:
  - network part (high order bits)
  - host part (low order bits)
- *What's a network ?* (from IP address perspective)
  - device interfaces with same network part of IP address
  - can physically reach each other without intervening router (i.e., on the same LAN)



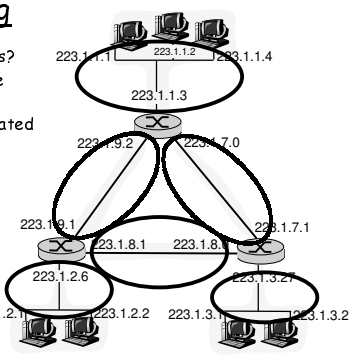
network consisting of 3 IP networks (for IP addresses starting with 223, first 24 bits are network address)

19

IP Addressing

How to find the networks?

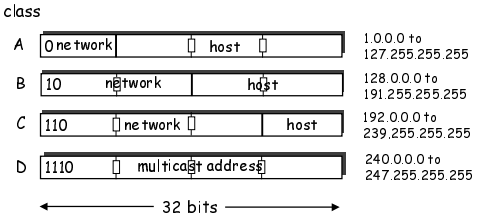
- Detach each interface from router, host
- create "islands of isolated networks"



Interconnected system consisting of six networks

20

IP Addresses: Class-based (Old)



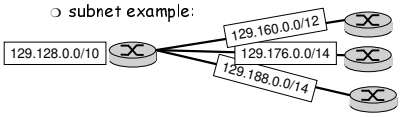
CIDR addressing (New)

- Classless Interdomain Routing
  - network part can be any # of bits
  - Format: a.b.c.d/x, where x indicates # of bits in network part (the prefix)

18 relevant bits

128.119.48.12/18 = 10000000 01110111 00 10000 00001100

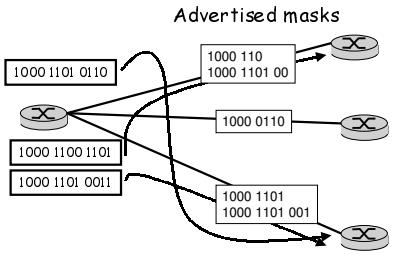
  - high order bits form the **prefix**
  - once inside the network, can **subnet**: divide remaining 24-x bits
  - subnet example:



Note: picture shows prefix masks, not interface addrs!

Routing with CIDR

- Packet should be sent toward the interface with the **longest matching prefix**



Hierarchical Routing

Our routing study thus far - idealization
all routers identical
network "flat"
… *not* true in practice

scale: with 50 million destinations:
- can't store all dest's in routing tables!
- routing table exchange would swamp links!

administrative autonomy
- internet = network of networks
- each network admin may want to control routing in its own network

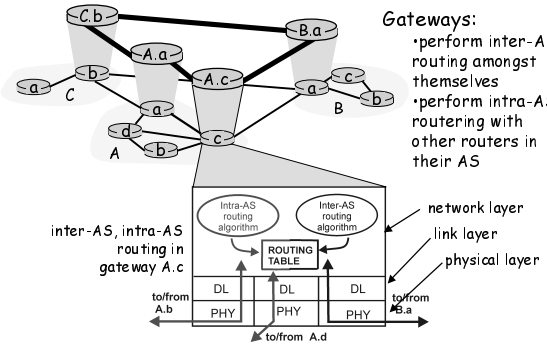
Hierarchical Routing

- aggregate routers into regions, "autonomous systems" (AS)
- routers in same AS run same routing protocol
  - "intra-AS" routing protocol
  - routers in different AS can run different intra-AS routing protocol
- NOTE: IP addressing format remains flat
  - e.g., Hierarchical routing protocols with CIDR addressing

gateway routers

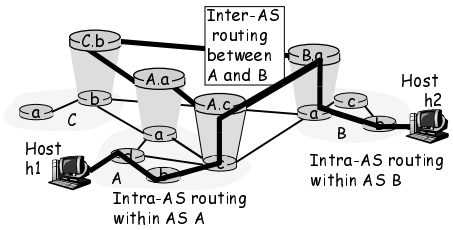
- special routers in AS
- run intra-AS routing protocol with all other routers in AS
- *also* responsible for routing to destinations outside AS
  - run *inter-AS routing* protocol with other gateway routers

Intra-AS and Inter-AS routing



Gateways:
- perform inter-AS routing amongst themselves
- perform intra-AS routering with other routers in their AS

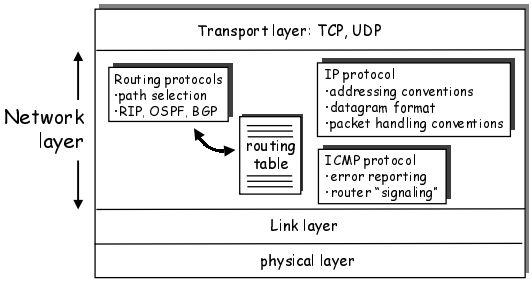
Intra-AS and Inter-AS routing



Future lecture: specific inter-AS and intra-AS Internet routing protocols

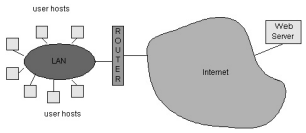
The Internet Network layer

Host, router network layer functions:



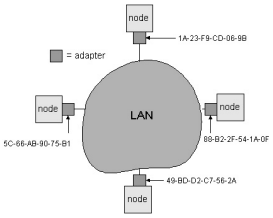
LAN technologies (Link Layer)

- MAC protocols used in LANs, to control access to the channel
- **Token Rings**: IEEE 802.5 (IBM token ring), for computer room, or Department connectivity, up to 16Mbps; FDDI (Fiber Distributed Data Interface), for Campus and Metro connectivity, up to 200 stations, at 100Mbps.
- **Ethernets**: employ the CSMA/CD protocol; 10Mbps (IEEE 802.3), Fast E-net (100Mbps), Giga E-net (1,000 Mbps); by far the most popular LAN technology



LAN Addresses and ARP

- **IP address**: drives the packet to destination **network**
- **LAN** (or MAC or Physical) **address**: drives the packet to the destination node's LAN interface card (adapter card) on the **local LAN**
- **48 bit MAC address** (for most LANs); burned in the adapter ROM
  - the address stays with the card
  - card's MAC address can't be changed

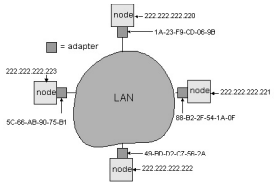


LAN Address (more)

- MAC address allocation administered by IEEE
- A manufacturer buys a portion of the address space (to assure uniqueness)
- Analogy:
  - (a) MAC address: like Social Security Number
  - (b) IP address: like postal address
- MAC flat address => portability
- IP hierarchical address NOT portable (address stays with the network, not the host interface)
- Broadcast LAN address: 1111……1111

ARP: Address Resolution Protocol

- MAC address ↔ IP address
- Each IP node (Host, Router) on the LAN has **ARP** module and Table
- ARP Table: IP/MAC address mappings for **some** LAN nodes
  - < IP address; MAC address; TTL>
  - < …… >
- TTL (Time To Live): timer, typically 20 min



ARP (more)

- Host A wants to send packet to destination IP addr XYZ on same LAN
- Source Host first checks own ARP Table for IP addr XYZ
- If XYZ **not** in the ARP Table, ARP module **broadcasts** ARP pkt:

  < XYZ, MAC (?) >

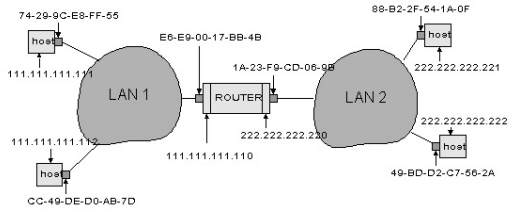
- ALL nodes on the LAN accept and inspect the ARP pkt
- Node XYZ responds with **unicast** ARP pkt carrying own MAC addr:

  < XYZ, MAC (XYZ) >

- MAC address **cached** in ARP Table
- Benefit of ARP: self-configuring (plug-n-play) – makes life easier for the sys-admin!!

Routing pkt to another LAN

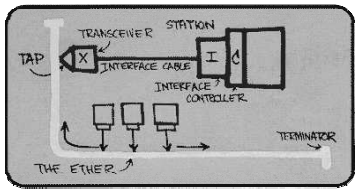
- Say, route packet from source IP addr <111.111.111.111> to destination addr <222.222.222.222>



- In routing table at source Host, find router 111.111.111.110
- In ARP table at source, find MAC address E6-E9-00-17-BB-4B, etc

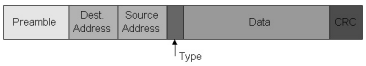
Ethernet

- Widely deployed because:
  - Cheap as dirt! $20 for 100Mbs!
  - First LAN technology
  - Simpler and less expensive than token LANs and ATM
  - Kept up with the speed race: 10, 100, 1000 Mbps
  - Many E-net technologies (cable, fiber etc). But they all share common characteristics



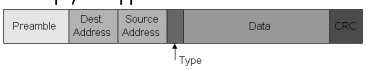
Ethernet Frame Structure

- Sending adapter encapsulates an IP datagram (or other network layer protocol packet) in **Ethernet Frame** which contains a Preamble, a Header, Data, and CRC fields
- **Preamble**: 7 bytes with the pattern 10101010 followed by one byte with the pattern 10101011; used for synchronizing receiver to sender clock (clocks are never exact, some drift is highly likely)



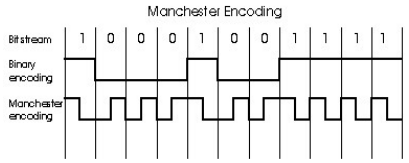
Ethernet Frame Structure (more)

- Header contains Destination and Source Addresses and a Type field
- **Addresses**: 6 bytes, frame is received by all adapters on a LAN and dropped if address does not match
- **Type**: indicates the higher layer protocol, mostly IP but others may be supported such as Novell IPX and AppleTalk)
- **CRC**: checked at receiver, if error is detected, the frame is simply dropped



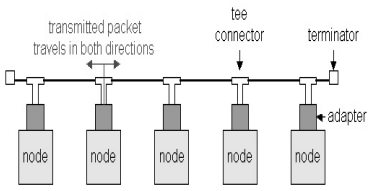
Baseband Manchester Encoding

- Baseband here means that no carrier is modulated; instead bits are encoded using Manchester encoding and transmitted directly by modified voltage of a DC signal
- Manchester encoding ensures that a voltage transition occurs in each bit time which helps with receiver and sender clock synchronization



Ethernet Technologies: 10Base2

- 10==10Mbps; 2==under 200 meters maximum length of a cable segment; also referred to as "Cheapnet"
- Uses thin coaxial cable in a bus topology
- Repeaters are used to connect multiple segments (up to 5); a repeater repeats the bits it hears on one interface to its other interfaces, ie a physical layer device only!

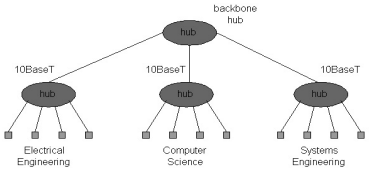


Hubs, Bridges, and Switches

- Used for extending LANs in terms of geographical coverage, number of nodes, administration capabilities, etc.
- Differ in regards to:
  - collision domain isolation
  - layer at which they operate
- Different than routers
  - hubs, bridges, and switches are plug and play
  - don't provide optimal routing of IP packets

Hubs

- Physical Layer devices: essentially repeaters operating at bit levels: repeat received bits on one interface to all other interfaces
- Hubs can be arranged in a hierarchy (or **multi-tier design**), with a **backbone** hub at its top



Hubs (more)

- Each connected LAN is referred to as a LAN **segment**
- Hubs **do not isolate** collision domains: a node may collide with any node residing at any segment in the LAN

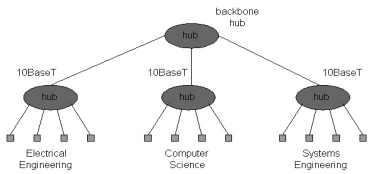
- Hub Advantages:
  - Simple, inexpensive device
  - Multi-tier provides graceful degradation: portions of the LAN continue to operate if one of the hubs malfunction
  - Extends maximum distance between node pairs (100m per Hub)
  - can disconnect a "jabbering adapter"; 10base2 would not work if an adapter does not stop transmitting on the cable
  - can gather monitoring information and statistics for display to LAN administrators

Hubs (more)

- Hub Limitations:
  - Always broadcasts pkts (i.e., no smarts about which link to send on)
  - Single collision domain results in no increase in max throughput; the multi-tier throughput same as the the single segment throughput
  - Individual LAN restrictions pose limits on the number of nodes in the same collision domain (thus, per Hub); and on the total allowed geographical coverage
  - Cannot connect different Ethernet types (e.g., 10BaseT and 100baseT)

10BaseT and 100BaseT

- 10/100 Mbps rate; latter called "fast ethernet"
- T stands for Twisted Pair
- 10BaseT and 100BaseT use Hubs



10BaseT and 100BaseT (more)

- Max distance from node to Hub is 100 meters
- 100BaseT does not use Manchester encoding; it uses 4B5B for better coding efficiency

45

Bridges

- **Link Layer devices**: they operate on Ethernet frames, examining the frame header and selectively forwarding a frame base on its destination
- Bridge i**solates collision** domains since it buffers frames
- When a frame is to be forwarded on a segment, the bridge uses CSMA/CD to access the segment and transmit
- Are also self-configuring (plug-n-play)

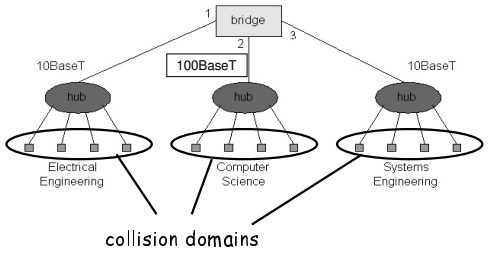
46

Bridges (more)

- Bridge advantages:
  - Isolates collision domains resulting in higher total max throughput, and does not limit the number of nodes nor geographical coverage
  - Can connect different type Ethernet since it is a store and forward device
  - Transparent: no need for any change to hosts LAN adapters

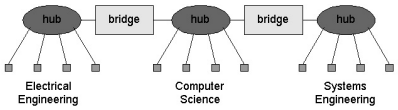
47

Backbone Bridge



48

Interconnection Without Backbone



- **Not recommended** for two reasons:
  - Single point of failure at Computer Science hub
  - All traffic between EE and SE must path over CS segment

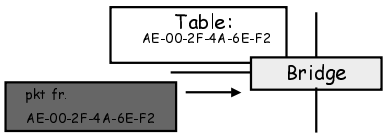
Bridge Filtering

- Bridges learn which hosts can be reached through which interfaces and maintain filtering tables
- A filtering table entry:
  (Node LAN Address, Bridge Interface, Time Stamp)
- Filtering procedure:

```
if destination is on LAN on which frame was received
    then drop the frame
    else { lookup filtering table
        if entry found for destination
            then forward the frame on interface indicated;
            else flood;   /* forward on all but the interface on
                             which the frame arrived*/
    }
```

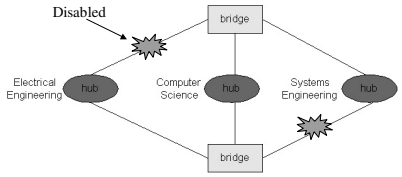

Bridge Learning

- When a frame is received, the bridge "learns" from the source address and updates its filtering table (Node LAN Address, Bridge Interface, Time Stamp)
- Stale entries in the Filtering Table are dropped (TTL can be 60 minutes)



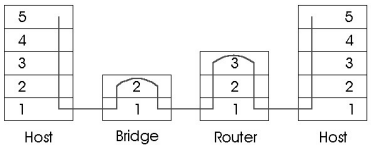
Bridges Spanning Tree

- For increased reliability, it is desirable to have redundant, alternate paths from a source to a destination
- With multiple simultaneous paths however, cycles result on which bridges may multiply and forward a frame forever
- Solution is organizing the set of bridges in a spanning tree by disabling a subset of the interfaces in the bridges:



Bridges vs. Routers

- Both are store-and-forward devices, but Routers are Network Layer devices (examine network layer headers) and Bridges are Link Layer devices
- Routers maintain routing tables and implement routing algorithms, bridges maintain filtering tables and implement filtering, learning and spanning tree algorithms



53

Routers vs. Bridges

- Bridges + and -

+ Bridge operation is simpler requiring less processing bandwidth

- Topologies are restricted with bridges: a spanning tree must be built to avoid cycles

- Bridges do not offer protection from broadcast storms (endless broadcasting by a host will be forwarded by a bridge: cost of plug-n-play)

54

Routers vs. Bridges

- Routers + and -

+ Arbitrary topologies can be supported, cycling is limited by TTL counters (and good routing protocols)

+ Provide firewall protection against broadcast storms

- Require IP address configuration (not plug and play)

- Require higher processing bandwidth

- Bridges do well in small (few hundred hosts) while routers are required in large networks (thousands of hosts)

55

Ethernet Switches

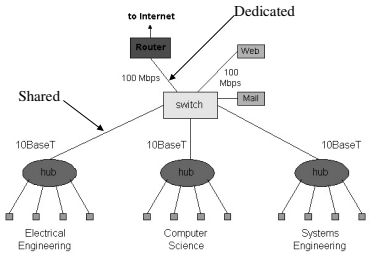
- A switch is a device that incorporates bridge functions as well as point-to-point 'dedicated connections'
- A host attached to a switch via a dedicated point-to-point connection; will always sense the medium as idle; no collisions ever!
- Ethernet Switches provide a combinations of shared/dedicated, 10/100/1000 Mbps connections

56

Ethernet

- Some E-net switches support cut-through switching: frame forwarded immediately to destination without awaiting for assembly of the entire frame in the switch buffer; slight reduction in latency
- Ethernet switches vary in size, with the largest ones incorporating a high bandwidth interconnection network

Ethernet Switches (more)



Gbit Ethernet

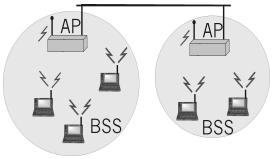
- Use standard Ethernet frame format
- Allows for Point-to-point links (switches) and shared broadcast channels (hubs)
- Uses Hubs called here "Buffered Distributors"
- Full-Duplex at 1 Gbps for point-to-point links

Hardware in the Layering Hierarchy

Network	Routers
Link	Bridges, Switches
Physical	Repeaters, Hubs

IEEE 802.11 Wireless LAN

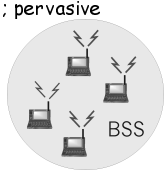
- Wireless LANs are becoming popular for mobile Internet access
- Applications: nomadic Internet access, portable computing, ad hoc networking (multihopping)
- IEEE 802.11 standards defines MAC protocol; unlicensed frequency spectrum bands: 900Mhz, 2.4Ghz
- **Basic Service Sets + Access Points => Distribution System**
- Like a bridged LAN (flat MAC address)



61

Ad Hoc Networks

- IEEE 802.11 stations can dynamically form a group without AP
- Ad Hoc Network: no pre-existing infrastructure
- Applications: "laptop" meeting in conference room, car, airport; interconnection of "personal" devices (see bluetooth.com); battelfield; pervasive computing (smart spaces)
- IETF MANET (Mobile Ad hoc Networks) working group



62

PPP: Point to point protocol

- LAN-like connectivity for a host (e.g., over a modem-line)
  - (when used w/ IP, assigns an IP address to the host
- Pkt framing: encapsulation of packets
- bit transparency: must carry any bit pattern in the data field
- error detection (no correction)
- multiple network layer protocols
- connection liveness
- Network Layer Address negotiation: Hosts/nodes across the link must learn/configure each other's network address

63

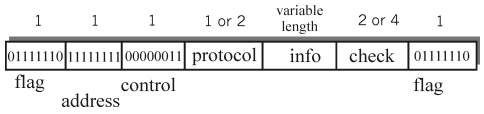
Not Provided by PPP

- error correction/recovery
- flow control
- sequencing
- multipoint links (e.g., polling)

64

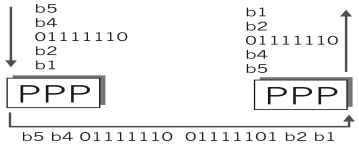
PPP Data Frame

- Flag: delimiter (framing)
- Address: does nothing (only one option)
- Control: does nothing; in the future possible multiple control fields
- Protocol: upper layer to which frame must be delivered (eg, PPP-LCP, IP, IPCP, etc)



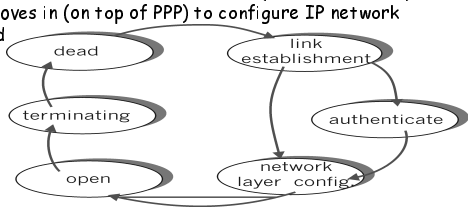
Byte Stuffing

- For "data transparency", the data field must be allowed to include the pattern <01111110> ; ie, this must not be interpreted as a flag
- to alert the receiver, the transmitter "stuffs" an extra < 01111110> byte after each < 01111110> data byte
- the receiver discards each 01111110 followed by another 01111110, and continues data reception



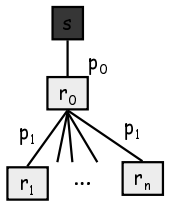
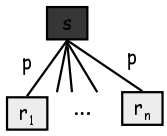
PPP Data Control Protocol

- PPP-LCP establishes/releases the PPP connection; negotiates options
- Starts in DEAD state
- Options: max frame length; authentication protocol
- Once PPP link established, IPCP (Control Protocol) moves in (on top of PPP) to configure IP network ad



HW#0

- Problem 5 model



- Problem 6 model