Networking Terms, Virtual LANS, and Network Layer Design Issues

CS158a

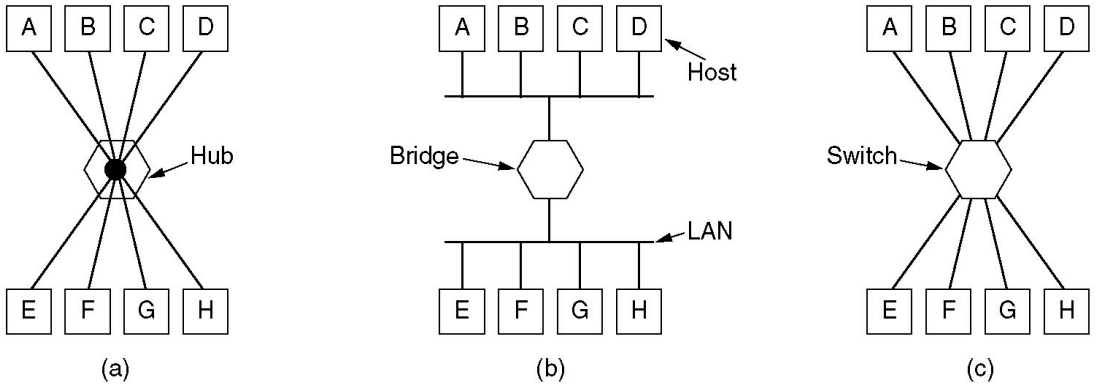
Chris Pollett

Apr 2, 2007.

Outline

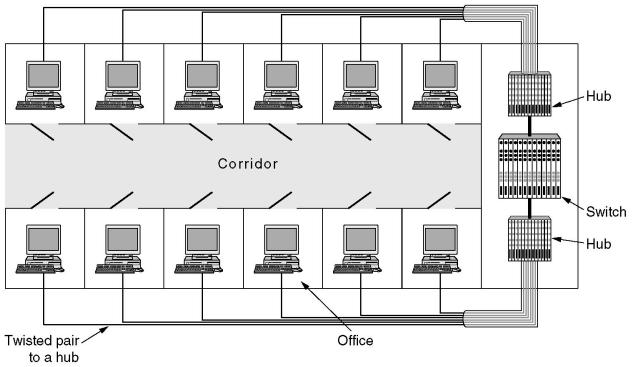
- Networking Terminology
- Virtual LANs
- IEEE 802.1Q
- Network Layer Design Issues

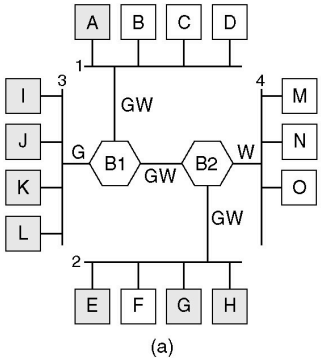
Networking Terminology

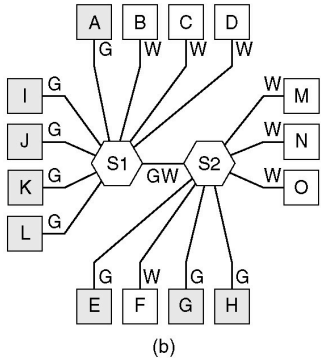


- **Repeater** -- operates at the Physical Layer, connecting two cable segments a signal input to one segment is amplified and output on the second cable. Classic Ethernet allowed up to 4 repeaters to extend its range.
- **Hubs** -- also operates at the physical layer, but has multiple input line that it joins. Frames arriving on anyone of these lines are output on all others. All input lines must operate at the same speed. Hubs do not amplify the signal.
- **Bridges** -- operate at the Data Link Layer and connect two or more LANs. When a frame arrives it extracts the 48 bit MAC destination address from the frame header and looks up its table to see where to send the frame. Like hubs, have line cards each able to hold 4 or 8 input lines all of a certain type (say Ethernet or Token ring). Can have cards for different network types and speeds. Each line is its own collision domain, in contrast to a hub.
- **Switches --**similar to a bridge however is more often used to connect individual computers rather than LANs. As a consequence often start forwarding frame as soon as header arrives. This is called a **cut-through switch**.

Virtual LANs

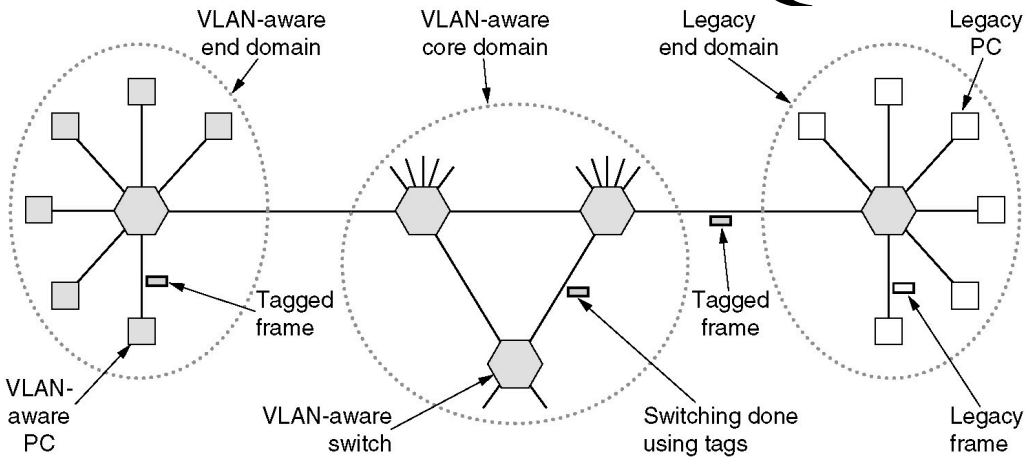






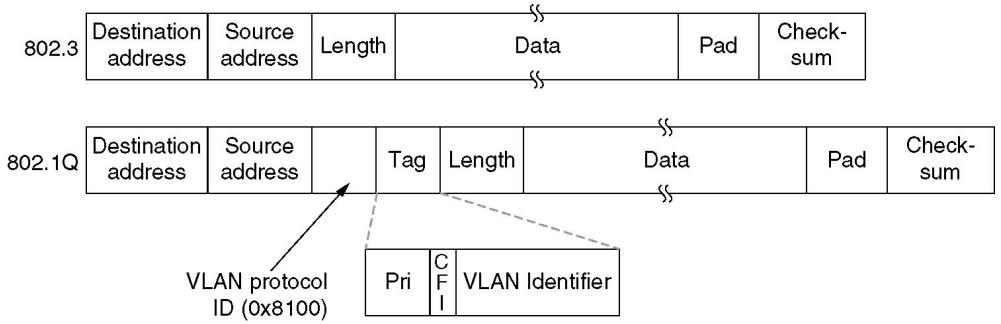
- Often one wants to create LANs of people who are in the same group, rather than who happens to have an office next to who.
- To do this one can run a twisted pair wire from each office to a central wiring closet.
- There one can plug people's wires into the hub for a given group.
- This improves security as only people within a group see the data on the ethernet.
- It also localizes loads within groups.
- Using switches rather than just hubs, one can set up the switches to create "virtual LANs". Traffic from a machine in such a virtual LAN is only seen by other machines in the virtual LAN.
- One can connect different floors or different building using multiple switches.

IEEE 802.1Q



- In order to fully need to get the VLAN idea to work between switches we need to be able to restrict traffic flow to correct switches only based on the VLAN the source and destination machines belong to.
- It would be useful to have a VLAN identifier to do this.
- However, it is hard to change the Ethernet standard since there are so many cards out there.
- It turns out only the bridges and switches need to know VLAN info, not every machine. As there are fewer of these, it is possible to upgrade them and change the Ethernet frame for them.
- This is what IEEE 802.1Q does.

IEEE 802.1Q Frame Format

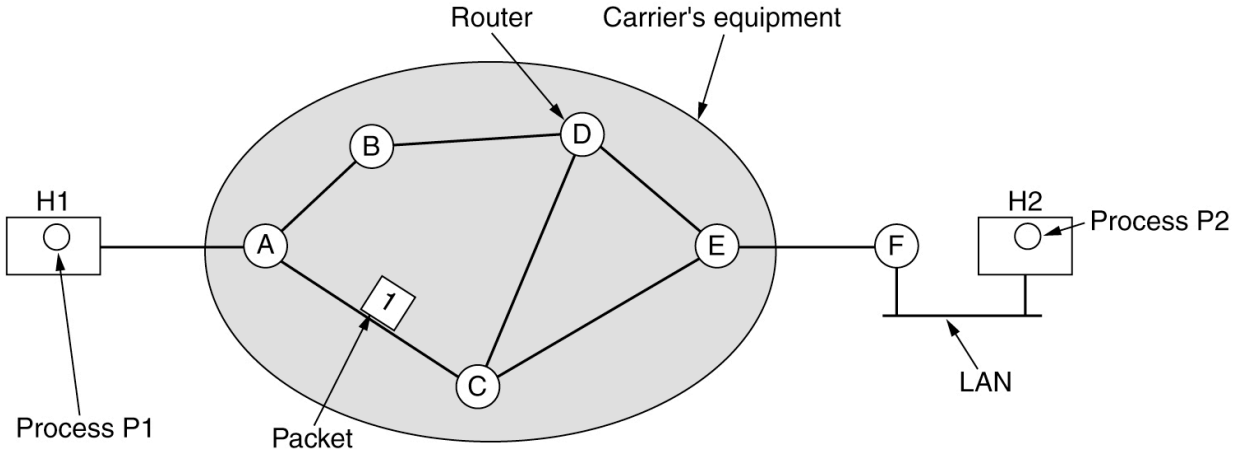


- The VLAN protocol ID is two bytes
- Pri - stands for priority, this is a non VLAN related feature.
- CFI -- Canonical Format Indicator. Not really used, supposed to be for things like little-endian versus big endian or token ring seeking token ring.
- Finally, there is a two byte VLAN identifier.

Network Layer Design Issues

- The network layer is concerned with getting packets from the source on the internet all the way to a destination computer.
- So it deals with end-toend communication.
- It must know the topology of the communication subnet (routers) and choose a route,
- It must avoid overloading communication lines if possible.
- It must also handle the case where the source and destination machine are on different networks.

Environment of the Network Layer Protocols



- The above picture is supposed to remind you of the context of the network layer.
- We have two machines on with potentially different LANs as well as the subnet between them.

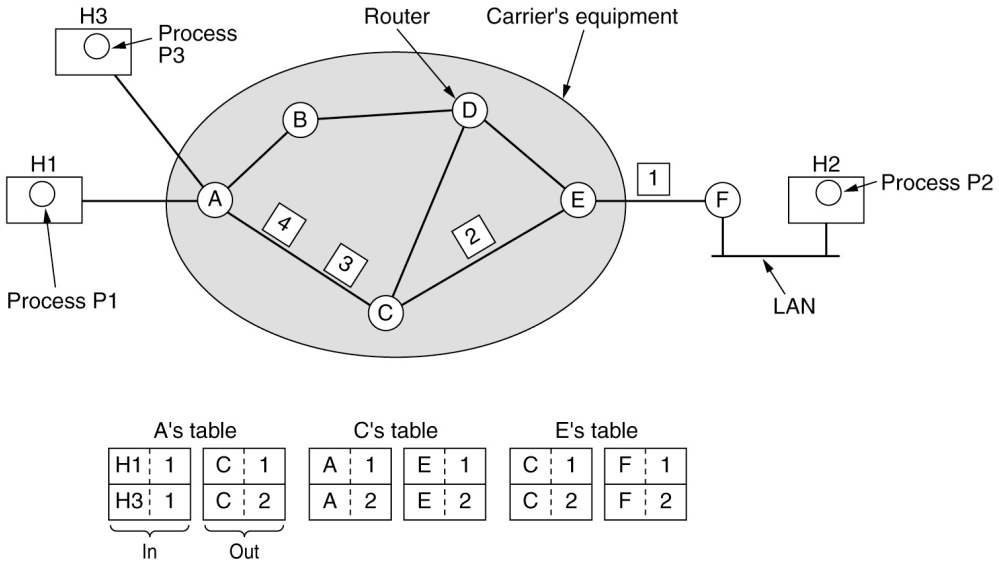
Requirements on the Services Provided to the Transport Layer

- The services should be independent of the router technology
- The transport layer should be shielded from the number, type, and topology of the routers present
- The network addresses made available to the transport layer should use a uniform numbering plan even across LANs and WANs.
- There are two camps on whether the network layer should offer connection-oriented (telephone) or connectionless services (internet community).

Implementation of Connectionless Services

- Packets are injected into the subnet individually and routed independent of each other
- These packets are called **datagrams** and the subnet is called a **datagram subnet**.
- If the message is longer than the maximum packet length it must be split into packets.
- These packets are then routed individually (so they can take different routes).
- Each router along the route has a routing table consisting of a pairs (dest, which connected router to send on) This table can change based on traffic according to some routing algorithm.

Implementation of Connection-Oriented Services



- In a connection oriented set-up a path from the source to the destination is set-up first.
- This path is called a **virtual circuit**.
- Each router maintains in and out connection identifiers for each connection
- These IDs are used in the router table to store the next hop for packet to be used and what the outgoing connection ID should be.

Comparison of Virtual Circuit and Datagram Subnets

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC