

CS4461

From MTU LUG wiki

CS4461 Computer Networks Final Exam Study Guide

Chapter 4 - The Network Layer

Virtual Circuit Networks:

Virtual Circuit networks consist of

- path between src and dst hosts
- VC numbers, one number for each link along the path
- Entries in the forwarding table in each router along the path

Packets carry VC numbers in the header. Each router in the VC must rewrite this header since they may differ depending on the router.

In a Virtual Circuit network the routers must maintain connection state information for the ongoing connections. Each time a new connection is started a new entry in the forwarding table needs to be created.

Virtual Circuit Phases

- VC setup:
 - the sending transport layer contacts the network layer
 - specifies the receiver's address
 - waits for the network to set up the VC.
 - The network layer determines the path between src and dst
 - the series of links and routers through which all packets of the VC will travel.
 - The network layer then adds an entry in the forwarding table in each router along the path.
- Data Transfer: VC is established and data begins to flow
- VC teardown:
 - src or dst informs network layer of its desire to terminate the VC.
 - The network layer then updates forwarding tables to delete the routes.

Datagram Networks:

Each time an end system wants to send a packet it stamps the dst address on the packet and sends it to the network. The packet is sent through a series of routers. Each router uses the dst address to forward the packet.

- lookup the appropriate output link interface in the table
- forward the packet out the chosen interface

Matches the prefix of the dst address and chooses output link based on that.

Longest Prefix Matching Rule

- find the longest matching entry in the table
- forward the packet to the link interface associated with that prefix

Problem - contiguous blocks of address space are getting smaller meaning forwarding tables get larger.

No connection state information is maintained, but forwarding state information is. This happens on a specified interval of time rather than each time a connection is started and ended.

Problem - Forwarding tables can be modified before all the info is transmitted so the paths of individual packets may differ and packets may arrive out of order.

The Internet Protocol (IP):

Datagram Format

- Version Number: 4 bits specify the IP protocol version.
 - Router uses this to determine how to interpret the remainder of the packet
- Header Length: 4 bits to specify where in the IP datagram the data begins. (typically 20)
- Type of Service: TOS bits set to determine priority
- Datagram Length: Total length of the IP datagram (header plus data) measured in bytes
 - field is 16 bits long so max is 65535 bytes (typically 1500 bytes)
- Identifier, flags, fragmentation offset: IP fragmentation stuff
- Time-to-live: TTL ensures that datagrams don't cycle forever in routing loops
 - Decreased by 1 each time it goes through a router
 - Must be dropped when it hits 0
- Protocol: Used only at the dst to indicate the specific transport layer protocol
- Header checksum: Aids routers in detecting bit errors
- Src and Dst IP addresses: src creates a datagram
 - puts its own IP in the src IP address field
 - puts dst IP address into the dst IP address field
- Options: allow for the IP header to be extended
- Data: the payload of the packet contains the transport-layer segment to be delivered

Link State Routing Algorithm:

The network topology and all link costs are known and available as input to the LS algorithm. Dijkstra's algorithm is popular.

Problem - oscillations in updates. A solution would be to mandate that no 2 routers can run the LS algorithm at the same time.

Popular LS Algorithm in use: OSPF

Distance Vector Routing Algorithm:

The DV algorithm is iterative and *distributed* meaning that each node receives information from one or more of its directly connected neighbors. It is iterative in that it continues until no more information is exchanged between neighbors.

Link-Cost change and Link Failure:

- At time t0, y detects the link-cost change
- updates its distance vector
- informs its neighbors of the change
- At time t1, z receives the update from y and updates its table
- it compares a new least cost to x
- sends its new distance vector to its neighbors
- At time t2, y receives z's update and updates its table
- y's least costs do not change
- y sends no messages to z
- Algorithm stabilizes

Popular DV Algorithm In Use: RIP

Border Gateway Protocol:

BGP is an inter-AS routing protocol. BGP provides each AS a means to

- Obtain subnet reachability information from neighboring ASs
- Propagate the reachability information to all routers internal to the AS
- Determine "good" routes to subnets based on the reachability information and on AS policy

Essentially BGP allow for a subnet to shout out "OMG I'M OVER HERE!!!!!! 11 lone"

Chapter 5 - The Link Layer

Purpose: To move a datagram over an individual link. The link layer has the end to end job of moving network layer datagrams over a *single link* in the path.

Possible services offered by a link-layer protocol include:

- Framing: Encapsulate the network-layer datagram within a link-layer frame
- Link Access: A medium access control (MAC) protocol specifies the rules by which a frame is transmitted onto the link.
- Reliable Delivery: When a protocol provides a reliable delivery service it guarantees to move each network-layer datagram across the link without error
- Flow Control: The nodes on each side of a link have a limited amount of frame buffering capacity.
- Error Detection: A node's receiver can incorrectly decide that a bit in a frame is zero when it was transmitted as a one and vice versa.
- Error Correction: Receiver not only detects whether errors have been introduced in the frame but also determines exactly where in the frame the errors have occurred.
- Half-duplex and full-duplex: With full-duplex the nodes at both ends of a link may transmit packets at the same time.

Channel Partitioning Protocols

Time division multiplexing

- The Good
 - Eliminates Collisions
 - Perfectly fair
- The Bad
 - Each node is limited to an average of the bandwidth even if its the only one taking
 - A particular node is the only one with something to say. It can't say it all at once it must take breaks

Code division multiplexing

- The Good
 - Different nodes can transmit simultaneously

Random Access Protocols

When there is a collision, each node involved in the collision repeatedly retransmits its frame until the frame gets through without a collision. It doesn't necessarily retransmit right away however. It waits a random amount of time to retransmit thus decreasing the probability of future collisions on the same frame.

Carrier Sense Multiple Access With Collision Detection (CSMA/CD)

- An adapter may begin to transmit at any time
- An adapter never transmits a frame when it senses that some other adapter is transmitting
- A transmitting adapter aborts its transmission as soon as it detects that another adapter is also transmitting
- Before attempting a retransmission, an adapter waits a random time that is typically small compared with the time to transmit a frame

How CSMA/CD works in a specific adapter

1. The adapter obtains a network-layer datagram from its parent node
 - prepares an ethernet frame
 - puts the frame in an adapter buffer
2. If the adapter senses that the channel is idle it starts to transmit the frame
 - if it senses the channel is busy then it waits until it senses no signal energy and then starts to transmit
3. While transmitting the adapter monitors for the presence of signal energy coming from other adapters
 - if the adapter transmits the entire frame without detecting signal energy from other adapters, the adapter is finished with the frame
4. If the adapter detects signal energy from other adapters while transmitting it stops transmitting its frame and instead transmits a 48-bit jam signal
5. After aborting the adapter enters an exponential backoff phase
 - After experiencing the n th collision in a row for this frame the adapter chooses a value for K at random from $\{0, 1, 2, \dots, 2^m - 1\}$
 - where $m = \min(n, 10)$
 - The adapter then waits $K \cdot 512$ bit times then returns to step 2.

Purpose of the jam signal is to ensure that all the other adapters are aware of the collision.

At 10Mbps a bit time is 0.1 microseconds.

The Ethernet standard imposes limits on the distance between any two nodes. These limits ensure that if adapter A chooses a lower value of K than all the other adapters involved in a collision, then adapter A will be able to transmit its frames without experiencing a new collision. It is possible that an adapter can sneak in a new frame while other adapters are in the exponential backoff state.

Taking Turns Protocols: Most popular is Token Ring.

Retrieved from "<http://lug.mtu.edu/mediawiki/index.php?title=CS4461&oldid=4234>"

Categories: Michigan Technological University | MTU Classes

- This page was last modified on 30 September 2005, at 18:17.
- This page has been accessed 8,262 times.