

CSIS 625 Week 10

Telephony, SONET, Network Layer
Copyright 2002-2003 – Daniel R. Oelke

For use by students of CSIS 625 for purposes of this class only.

I. Overview

A. Telephone Technology

1. Pick up of topics not covered earlier

B. SONET

C. Network Layer

1. Network layer role
2. Routing algorithms
3. Multicast

II. Telephone Network

A. Pay Phone Service

1. Public Phone Service
 - a. Both phone and line are owned by LEC
 - b. No monthly rental charges
 - c. Accessed by everybody
2. Semipublic Service
 - a. Rent a line and set, place phone in controlled location
 - b. Minimum rate guaranteed to the LEC -- controlled by tariffs
3. Private Service
 - a. buy or rent a set, rent a line (flat fee) and/or share of profits
 - b. placed in restricted location

B. WATS

1. Wide Area Telecommunications Services
2. Primarily a billing service that allows reduced rate for long-distance and local telecommunications
3. Initially, WATS was implemented in the form of bands that separated the country into 5 regions
4. Currently WATS rates can be negotiated between any geographical localities
5. 800/888 Service
 - a. Reverse-billing WATS
 - b. Recipient pays for the call, and not the call initiator

C. PBX Systems

1. PBX -- Private Branch Exchange
2. Typically a small-capacity (up to 5K lines) digital switch that provides add-on services not available through LEC
3. Add-on services include, but are not limited to voice mail, transferring, conference calling, etc.
4. Interfaces to the LEC via leased trunks
5. Typically utilizes digital phone sets
6. Up to the customer to maintain the wiring and the equipment

D. Centrex Service

1. A PBX-like service offered through LECs
2. LEC “partitions” a Class 5 switch, dedicating some of its processing and voice capacity to Centrex customers
3. Partitioning is typically virtual, or software-only
4. Provides the same services as PBXs
5. Customer does not have to maintain the wiring or the equipment -- LEC does it for the customer
6. Customer has an option of adding own services (voice processing, etc) to Centrex, just like to any PBX

E. Key Systems

1. Same features as PBXs
2. Aimed at smaller customers
3. Uses dial-up lines instead of trunks to interface with LEC
4. Modern PBXs are typically packaged as either Key Systems or PBXs, the only difference being the LEC interface

III.SONET & SDH

A.Definition

1. SONET - Synchronous Optical NETWORK
 - a. ANSI/Bellcore standard
2. SDH - Synchronous Digital Hierarchy
 - a. ITU (European) standard
3. Both standards are practically identical
4. Standards for a synchronous digital transmission system of TDM traffic over fiber networks.
5. Standards based system for data rates above a T3.

B.SONET/SDH Hierarchy

1. STS - Synchronous Transport Signals
 - a. 51.84Mbps - base level of SONET hierarchy
2. STM - Synchronous Transport Module
 - a. 155.52Mbps - base level of SDH hierarchy
 - b. Exactly equal to STS-3
3. STS/OC/STM
 - a. STS-n and OC-n are identical -
 - (1) OC-n names are used for optical interconnects
 - (2) STS-n names are used for electrical interconnects
 - b. OC-n is exactly n times the rate of an OC-1 signal.
 - c. STM-1 signal is exactly 3 times the rate of an STS-1 signal
 - d. STM-n is exactly n times the rate of an STM-1 signal
 - e. Table of Rates
 - (1) STS-1 = OC-1 = = 51.84Mbps
 - (2) STS-3c = OC-3 = STM-1 = 155.52Mbps
 - (3) STS-12c = OC-12 = STM-4 = 622.08Mbps
 - (4) STS-48c = OC-48 = STM-16 = 2.488Gbps
 - (5) STS-192c = OC-192 = STM-64 = 9.953Gbps
 - (6) STS-768c = OC-768 = STM-256 = 39.813Gbps

C.STS frame format

1. An STS-1 frame consists of 810 bytes (octets) sent in 125 μ s.
 - a. $810 * 8 * 8000 = 51.84\text{Mbps}$

2. The 810 bytes are arranged as 90 columns x 9 rows
 - a. 3 columns are overhead
 - b. 87 columns are actual data

D. ADM, Terminal, Repeater

1. SONET/SDH terminal - a mux/demux that creates a SONET signal and terminates paths.
2. SONET/SDH ADM (Add/Drop Multiplexer) - a mux/demux that can separate individual STS-n signals from a higher level signal.
3. SONET/SDH repeater- a physical level regenerator that also terminates section level overhead to allow section level management.

E. SONET/SDH - Path/Section/Line

1. In Sonet/SDH systems a strong designation of levels of overhead are kept.
2. Section is lowest level
 - a. Repeater to repeater
3. Line is middle layer
4. Path is top/longest layer
 - a. from entrance to SONET system to exit of SONET system
5. SONET/SDH - Section & Line Overhead
 - a. The section overhead is the first 3 rows of the first 3 columns (9 bytes) per frame.
 - b. The line overhead is the lower 6 rows of the first 3 columns (18 bytes) per frame.

F. SONET/SDH Physical layer

1. Fiber optic link, using NRZ encoding
 - a. light present is a 1
 - b. no light is a 0
2. To keep enough transitions, a scrambling mechanism is used.

G. SONET/SDH Virtual Tributaries

1. Virtual Tributaries are a method to map a lower speed signal (like a T1 or E1) into a portion of an STS-n payload.
2. VT1.5 - 27 bytes/frame => 1.728Mbps
 - a. Used for T1s
3. VT2 - 36 bytes/frame => 2.304Mbps
4. VT3 - 54 bytes/frame => 3.456Mbps
5. VT6 - 108 bytes/frame => 6.912Mbps

H. STS concatenated signals

1. Multiple STS-1s can be grouped together into a single higher bit rate facility.
2. Extra overhead bytes are ignored.
3. Technically, any number of STS-1s can be grouped, but the only groupings normally supported are:
 - a. STS-3C, STS-12C, STS-48C
4. Generally a grouping must fall on a boundary of the same size inside of the OC-n carrier
 - a. A STS-3C must fall on a boundary of 3
 - b. STS-12C must fall on a boundary of 12
5. Typically used for situations where ATM or Packets are sent over a SONET network.

IV. Network Layer

A. Vocabulary

1. internet - a collection of networks connected by bridges or routers
2. Internet - THE world wide collection of networks using TCP/IP as their network protocol that people use for communicating.
3. End System (ES) - a node on one of the networks in an internet that supports end-user services (OSI model terminology)
4. Intermediate System (IS) - a node that connects two networks to permit communications between end systems on the different networks. (OSI model terminology)
5. IP - Internet Protocol - the network layer protocol used on the Internet.
6. Router - a device that uses the network layer information for forwarding packets from one network to another.
7. Bridge - a device that uses data link layer information for forwarding packets from one network to another.
8. Gateway is kind of like a router in that it connects multiple networks - but it does so at the application layer, instead of at the network layer.
9. Repeater - a device that connects multiple network segments at the physical layer
 - a. Converts analog to digital, retimes & reshapes signal, convert back to physical layer transmission scheme
10. Amplifier - A device that increases the amplitude of a analog signal fed into it.

B. Network Layer Role

1. Provide a link between networks
 - a. These networks may be of different data link and/or physical layers
2. Provide routing and delivery of data between nodes on different networks
3. When there are many networks connected in multiple ways, the algorithms to determine how a packet gets from end to end get “interesting”

C. Connection oriented vs. connectionless

1. Connection Oriented
 - a. Assumed that all networks provide a connection oriented form of service
 - b. May be virtual circuits on the networks
 - c. IS systems splice together connections between the networks.
 - d. This system is rarely used in real systems
2. Connectionless
 - a. packet-switching instead of virtual circuits
 - b. At each router a forwarding decision is made independently for each packet

D. Routing Characteristics

1. Routing algorithms and protocols are supposed to get packets from one node to another. How well they do this is judged on a number of factors
 - a. Correctness – packets get where they are supposed to
 - b. Simplicity – Able to implement this (simple makes equipment cheaper)
 - c. Robustness – Being able to deal with network problems
 - d. Stability – Making sure that things don't change too rapidly causing more problems
 - e. Fairness – everyone gets the same amount (or what they paid for)
 - f. Optimality – bandwidth of links is well used.
 - g. Efficiency – make sure that processing is minimal so that delay is minimal

E. Least Cost Routing

1. The goal of most routing protocols is to get information between two points in the “best” way.
2. Best may be defined by a number of things
 - a. Number of network hops (easy to measure)
 - b. Amount of delay from various links
 - (1) Can be physical delay from transmission rate and distance
 - (2) Can add in congestion (queuing time)
 - c. Cost in \$ to send packets over a given link
 - d. Usually is not physical distance

F. Adaptive vs. Non-adaptive routing

1. Adaptive Routing
 - a. Each router as it processes each packet makes a decision about how to send the packet to its destination
 - b. This can change when the network changes
 - (1) Link failures
 - (2) Congestion
2. Non-Adaptive routing
 - a. Once a pathway is established, all packets for a destination go along that one route.

G. Fragmentation and Reassembly

1. Network layer (as well as other layers sometimes) provides segmentation and reassembly.
2. Makes bigger packets of data into smaller ones that the underlying layer can handle.
3. Each header has fields
 - a. Length
 - b. Offset value
 - c. “More” flag

H. Packet Time to Live

1. Packets may end up in a routing loop going around and around
 - a. May be just bounced between two nodes
2. To keep packets from using network bandwidth forever, most network protocols have a packet lifetime specified by the originator.
3. TTL – Time to live. - A number set by the packet originator and decremented by each hop along a path.
 - a. When this counter reaches 0, the packet is discarded
 - b. Used to limit the damage of routing loops.

I. Gateway

1. A gateway is kind of like a router in that it connects multiple networks - but it does so at the application layer, instead of at the network layer.
2. A special kind of application that transfers information from one application format to another.

V. Routing algorithms

A. Theoretical view of Routing Algorithms.

1. There are many different ways to determine the best path for a packet to take through a network.
2. Routing algorithms are the steps taken to find the best path
3. Routing protocols are a description of how this routing information is discovered and disseminated in the network.

4. Type of Routing Algorithms
 - a. Fixed Routing
 - b. Flooding
 - c. Random Routing
 - d. Distance Vector Routing
 - e. Link State Routing

B. Fixed Routing

1. A simple method where a human goes to each router and programs it with tables that tell it where every packet goes.
 - a. May have a central network controller that disseminates the information
2. Very simple and stable.
3. Does not react well to network congestion or link failures.
 - a. May have alternate paths for each destination to accommodate link failures.

C. Flooding Routing

1. Very simple method where every node sends packets to every other node it is connected to.
2. Must have a mechanism to kill off packets
 - a. Nodes could remember every packet it has sent
 - b. A TTL counter in the packet can be implemented
3. Multiple copies will be received by the recipient so packet must have unique tag that allows duplicates to be discarded.
4. Advantages:
 - a. Requires no central authority.
 - b. All links are tried – packets will get through if there is any way possible.
 - (1) Very robust – good for emergency messages in a military network.
 - c. At least one packet will have used minimum hop count
 - (1) May be used to find path for virtual circuit
 - d. All nodes receive the packet
 - (1) May be used to disseminate important information (like route updates)
5. Disadvantage
 - a. Very high network load for the traffic given
6. Actually used in some routing protocols and in the peer-to-peer application Gnutella.

D. Random Routing

1. Send a packet to one random outgoing path for retransmission.
2. Same idea as flooding, but with less traffic load on the network.
3. Advantages
 - a. No central authority
 - b. Relatively robust
 - c. Less traffic than flooding
4. Disadvantages
 - a. Still a heavy traffic load
 - b. Most packets do not use the least hop path.

E. Distance Vector Routing

1. A type of adaptive routing
2. Each router periodically shares its knowledge about the entire network.
 - a. This is sent only to the router's direct neighbors.

- b. This information is shared at a regular basis
- 3. When a router receives information from its neighbor, it updates its routing table.
 - a. The routing table has Network ID, cost, next hop.
 - b. When a lower cost path is found, the old route is discarded and the new route added.

F. Link State Routing

- 1. A type of adaptive routing
- 2. Each router shares its knowledge about it's neighbors (not the entire routing table)
- 3. Information about it's neighbors is sent to all routers
 - a. Uses a flooding technique
- 4. Information is sent out when there is a change (not periodically)
- 5. When a router receives information, it uses it to update its routing table
 - a. The routing table has Network ID, cost, next hop.

G. Dijkstra Algorithm

- 1. To calculate the the lowest cost path between two nodes, the routers use Dijkstra's algorithm.
- 2. The algorithm builds a tree structure of the network using itself as the root.
 - a. All nodes that can be reached from the root are attached (all neighbors) – temporarily.
 - b. The node are sorted by order of cost to reach them.
 - c. Starting with lowest cost temporarily attached node, make it permanent part of the tree.
 - d. Consider all nodes attached from the chosen node and add them temporarily.
 - e. Repeat last two steps until all nodes are attached permanently

VI. Routing in practice

A. Vocabulary

- 1. Autonomous system
 - a. A group of networks and routers where all the routers exchange information using a common routing protocol.
 - b. All of these routers are managed by a single organization
 - c. Except where there is a failure, all routers are “connected”
- 2. IRP – Interior Router Protocol – A routing protocol used within a single autonomous system.
 - a. Also known as Intra-Domain Routing protocol
- 3. ERP – Exterior router protocol – A routing protocol used for exchanging routing information outside of an autonomous system.
 - a. Also known as Inter-Domain Routing Protocol

B. Typically an ERP is simpler than an IRP

- 1. Exchanges only summary information of reachability
- 2. IRP has more detailed information on least-cost path to reach any given node.

C. BGP – Border Gateway Protocol

- 1. An Exterior router protocol.
- 2. Designed to allow routers (“gateways” in the standard) of different autonomous systems to exchange information.
- 3. BGP-4 Defined in RFC 1771
- 4. 3 major functions/procedures
 - a. Neighbor acquisition
 - b. Neighbor reachability

- c. Network reachability
- 5. Distributes information for each neighbor
 - a. List of routers needed to get to the neighbor
 - b. IP address of the router that is the next hop
 - c. List of networks served by this router

D. RIP – Routing Information Protocol

- 1. An early TCP/IP routing protocol.
- 2. Now used as an Interior routing protocol only
- 3. Depreciated in use for the most part
 - a. Since it was one of the first, it still shows up in a lot of systems.
- 4. Each router broadcasts it's entire route table.
- 5. A Distance Vector routing protocol
- 6. Has problem's scaling as the number of routers and links grows very large

E. OSPF – Open Shortest Path First

- 1. An upgrade from RIP
- 2. An Interior routing protocol
- 3. Based on Link State Routing
- 4. Cost to traverse a link may be set to anything that the network administrator desires.
 - a. May be delay, data rate, \$, etc.
 - b. Some “costs” may be artificially inflated, or reduced to help steer traffic down a certain path.

F. IS-IS Routing

- 1. An OSI stack based system – now adopted for TCP/IP networks

VII. Multicast Traffic

A. Definition: Multicast - to send the same data to multiple destinations, but not send multiple copies and not broadcast it to everyone.

B. Useful for:

- 1. Radio/TV broadcasts where users “tune in”
- 2. Teleconferencing – IETF meetings are often sent this way
- 3. Distributed updates of information (software updates, database updates, etc)

C. Uses special set of network (and sometimes data link layer) addresses.

D. On a single broadcast LAN, often sent as a broadcast to a special address that allows network interfaces to listen (or ignore) as they choose

E. On some systems that are not multicast aware, it can be sent multiple times – also called multiple unicast.

F. Special requirements of multicast

- 1. Routers must be multicast aware.
- 2. Router will possibly forward a packet out multiple ports rather than just one.
- 3. Each multicast aware router must keep track of networks or interfaces that have are “joined” to a particular multicast session.
- 4. Routers must handle nodes, or networks, leaving and joining a multicast session.
 - a. Keep alive messages ensure that nodes who leave improperly are removed from the multicast group
- 5. Routing protocol and algorithms needed for routers to determine the shortest path to all group members.
- 6. IGMP – Internet Group Management Protocol

- a. The TCP/IP protocol for managing multicast traffic
- b. Defined in RFC 1112 (version 1) and RFC 2236 (version 2)