Internetworking and Transport Layer Issues

- Fundamentals of Internetworking
  - Concept of Universal Network
- Fundamentals of Transport Protocols
  - Connection Management
  - Flow and Error Control

Fundamentals Of Internetworking

- Internetworking techniques allow users of different networks to cooperate across network boundaries
- Cooperation is motivated by
  - Exchange of Electronic mail
  - Banking and remote transaction
  - Rapid dissemination of pertinent information
  - Market forecasting
- In essence, Internetworking is motivated by the fact that value to user of many networks is strongly correlated with the number of other users that can be reached

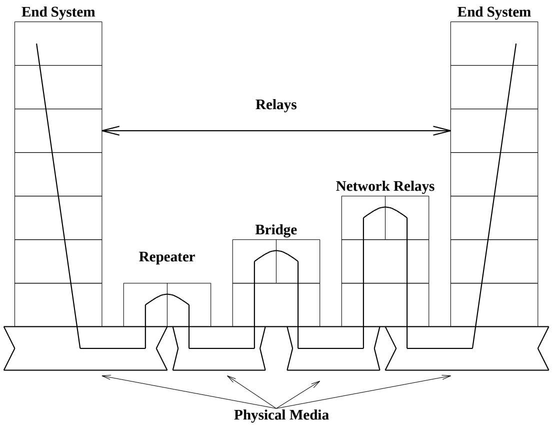
Requirements for Network Interconnection

- The main goal of internetworking is to provide transparent access to all facilities of each network by users of other networks
  - Concept of universal or metanetwork
- A few requirements are necessary
  - Provide communication between networks, at least the equivalent of the OSI physical or data link layer
  - Provide routing between users
  - Provide an accounting service to keep track of the use of various network resources

Relays, Bridges, Routers and Gateways

- A layer n relay is a device that interconnects two systems not directly connected to each other (OSI Ref. Model)
  - Layer n relay shares a common layer n with other systems, but does not participate in layer n+1 protocol
- Current terminology, however
  - Repeater : Physical layer relay
  - Bridge : Data link layer relay
  - Router : Network layer relay
  - Gateway : Any relay at higher layer than network layer
- Terminology is non uniformly used in the literature

Relays, Bridges, Routers and Gateways



Network Interconnection Issues

- **Development of appropriate approaches depend upon resolution of a variety of issues**
  - **Addressing and Naming issues**
  - **Routing techniques, Error Control, Flow Control**
  - **Information Quanta, Packet Sizes**
  - **Connection-oriented versus connectionless**
  - **Timings, Interrupts**
  - **Access Control**
- **Appropriate answers depend on degree of compatibility among protocols**

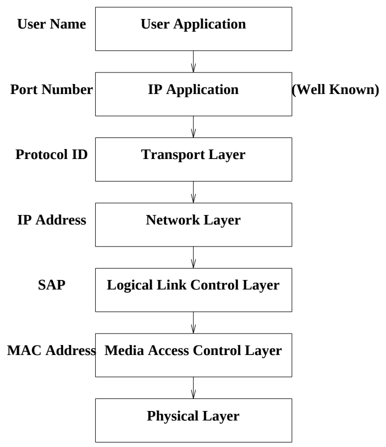
Naming And Addressing In An internet Environment

- **Communication between users require several forms of addressing**
  - **Typically,**
    - **Physical Address**
    - **Data Link Address**
    - **Network Address**
  - **And**
    - **Higher layer addresses for end to end communications**

Naming and Addressing

- **A name is a binding from a domain of labels to a range of objects**
- **In computer networks, we often need to bind names to addresses**
  - **Example: The host ra.cs.pitt.edu is bound to the internet address "130.49.2.28"**
- **At each router in a network we need to bind the destination name to an address which is the next machine to which the packet should be sent**

Complete Naming Scheme Internet



Internetworking Standards

- **Three standards for Internetworking are available**
  - **X.75, which provides internetworking of X.25 Networks**
  - **DoD Internet Protocol, best effort service**
  - **ISO IP, datagram service**

Transport Layer Protocols

- **The main objective is to provide an interface between higher application-oriented layers and underlying network**
  - **The interface is a set of primitives that provides the end user with a message transport facility independent of the quality of the service provided by the underlying network.**

Transport Layer Protocols

- **The basic elements of a transport protocol depend on the service type provided by the underlying network**
  - **The spectrum of network services varies from a flawless, error free service with no resets, to an unreliable service that may cause packet loss and packet duplication**
- **Depending on the network environment different transport protocols emphasize different features.**

Features of Transport Protocols

- The basic features of a transport protocol include:
  - Connection management,
  - Addressing,
  - Multiplexing,
  - Error control,
  - Flow control

Connection management

- Connection management involves the establishment and termination of a transport level connection
- Several issues need to be resolved to establish a connection
  - Finding the Transport Service Access Point (TSAP) of the process with which the connection is to be established
  - Agreeing on the parameters of the connection
    - Initial sequence number, quality of service parameters, ...

Connection management

- Problems may occur during connection establishment:
  - Network may loose, delay or duplicate packets
    - Duplicate packets may surface after the original connection is closed causing it to be re-established and generating undesired traffic

Finding TSAPs

- The remote process may have a ''well known'' port number
  - Port 21 of Transmission Control Protocol (TCP) is reserved for File Transfer Protocol (FTP)
  - Port 69 of User Datagram Protocol (UDP) is reserved for Trivial File Transfer Protocol (TFTP)

Finding TSAPs

- The TSAP of the remote process is not known
  - The remote process is not a well-known process, or is not currently running
- Help of a ''well known'' server process is needed
  - The sever process creates the desired process, if needed, and attaches it to a TSAP
    - The TSAP is ephemeral because it is released when the process terminates
  - The sever process informs the calling node of the TSAP of the desired remote process
  - A connection is established between the calling process and the remote process using the newly ephemeral TSP

Dealing with Delayed Packets

- Delayed old packets with the same sequence number can confuse the receiving node (i.e., when the network recovers from a crash, for example)
- A numbre of solutions are possible to prevent confusion:
  - The network limits the lifetime of packets of at most T units of time
  - Each node decrements the Time-To-Live (TTL) field by 1, and the node discards the packet if its TTL reaches 0
  - Upon recovering from a crash, a node waits T units of time before resuming transmission
  - Since the lifetime of a packet is time units, this guarantees that all the old copies of packets are discarded from the network

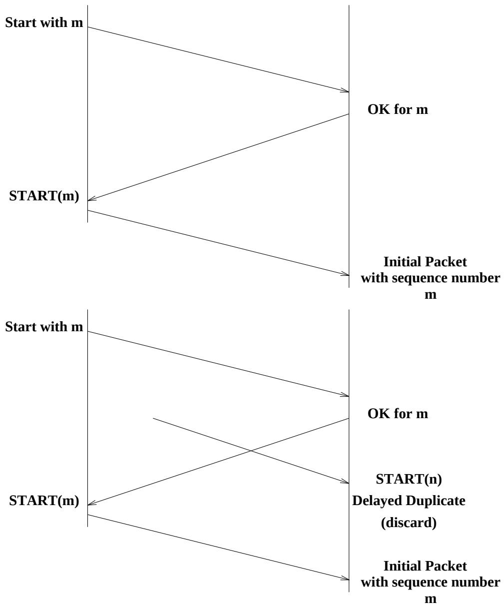
Connection Parameter Negotiation

- Agreeing on connection parameters can be achieved, with a high probability of success, by a procedure called ''three-way handshake''
- Through the exchange of three messages, both sides of the connection that the proper connection has been established.
  - It is a reliable way to verify that a connection establishment is indeed being carried out
- The same technique is usually used to terminate a connection.

Connection Parameter Agreement
Initial Sequence Number

- Host A wants to establish a connection and start transmitting messages to host B
  - Confusion is possible because of old session initialization packets that might still be in the network
- Suppose that host A wants to start transmitting a packet numbered m.
  - An old packet may arrive at the destination indicating an initial packet numbre $m \neq n$
- Three-way hand-shake guarantees that the hosts agree on the initial sequence number, and more generally on the parameters of the connection

Connection Parameter Agreement



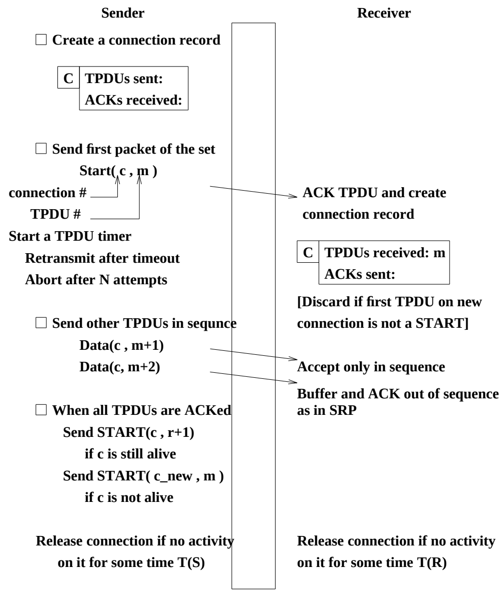
Connection Parameter Agreement

- **Errors can occur when a host fails**
  - **Host A is sending packets to Host B, using stop-and-wait protocol**
  - **Host B fails in the middle transmission**
  - **Upon recovery, Host B requests that Host A restarts after the last packet Acked**
  - **If B passed the packet to the user before sending ACK to A, when the crash occured**
    - **User will get two copies**
  - **If B sent the ACK to A first, when the crash occured**
    - **User will miss a packet**

Timer-Based Connection Management

- **An alternative method for handling delayed copies of packets is ''Timer-Based''**
  - **Records, both at the sender and receiver, are established to keep track of the connection progress**
  - **The connection is released when there is no activity for a period of time**
    - **The period of time at the sender may not be the same as the one at the receiver**

Timer-Based Connection Management
Selective Repeat Protocol



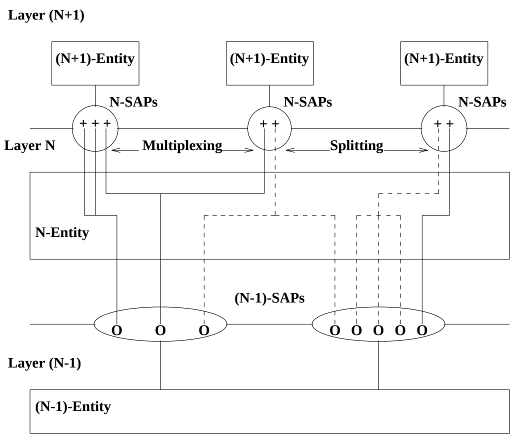
Timer-Based Connection Management

- Assuming Selective Repeat Protocol, the parameters T(S) and T(R) can be selected so that:
  - N $\times$ timeout + max_TPDU_lifetime << T(R) << T(S)
    - N is the number of attempts before aborting the connection
- This guarantees that no delayed packet can appear after the receiver releases the connection

Multiplexing

- Multiplexing provides a cost effective mechanism to manage network connections
- Two forms of multiplexing are commonly used :
  - Upward multiplexing allows several transport connections to share the same network connection
  - Downward multiplexing allows the transport layer to split the traffic of a single transport connection among several network connections in a round-robin fashion
- Multiplexing increases the throughput and improves the performance of the transport layer

Multiplexing and Splitting Via Connection End Points (CEP)



Error control

- Error control requires:
  - Detecting errors,
  - Detecting duplicate packets
- The techniques to control errors include sequence numbers, positive acknowledgment, and timeout mechanisms
  - Recovery of lost packets is achieved by retransmission

Flow Control

- The flow control mechanisms aims at regulating the amount of traffic between the transport entities involved in the communication
  - A common scheme for flow control is end-to-end window control based on a credit mechanism

Conclusion

- Discussed Transport Layer Main Issues
- Discussed Internetworking Main Issues