Chapter 12

Network Protocols
Outline

- Protocol: Set of defined rules to allow communication between entities
- Open Systems Interconnection (OSI)
- Transmission Control Protocol/Internetworking Protocol (TCP/IP)
- Internet Protocol next Generation (IPnG or IPv6)
- Extension of TCP over wireless
## OSI Model

<table>
<thead>
<tr>
<th>Layer</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 1</td>
<td>Physical</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Data link</td>
</tr>
<tr>
<td>Layer 3</td>
<td>Network</td>
</tr>
<tr>
<td>Layer 4</td>
<td>Transport</td>
</tr>
<tr>
<td>Layer 5</td>
<td>Session</td>
</tr>
<tr>
<td>Layer 6</td>
<td>Presentation</td>
</tr>
<tr>
<td>Layer 7</td>
<td>Application</td>
</tr>
</tbody>
</table>

### 7 layer OSI model
OSI Model (Cont’d)

- OSI model proposed by ISO
- Model divided into seven layers, each performing a specific task
- The seven layers are:
  - Application
  - Presentation
  - Session
  - Transport
  - Network
  - Data Link
  - Physical
Physical Layer Functions

- Performs services requested by the Data Link layer.
- Concerned with the physical characteristics of interfaces and media.
- Representation of bits, transmission rate, synchronization of bits.
- Link configuration.
- Physical topology, and transmission mode.
Data Link Layer Functions

- Provides functional and procedural means to transfer data between network entities.
- Responds to service requests from the network layer and issues requests to the physical layer.

Concerned with:
- Framing.
- Physical addressing.
- Flow Control.
- Error Control.
- Access Control.
Network Layer Functions

- Provides for transfer of variable length sequences from source to destination via one or more networks.
- Responds to service requests from the transport layer and issues requests to the data link layer.
- Concerned with:
  - Logical addressing.
  - Network routing.
  - Flow Control.
  - Error Control.
  - Segmentation and reassembly.
Transport Layer Functions

- Provides transparent data transfer between end users.
- Responds to service requests from the session layer and issues requests to the network layer.
- Concerned with:
  - Service-point addressing.
  - Segmentation and reassembly.
  - Connection control; Flow Control.
  - Error Control.
Session Layer Functions

- Provides mechanism for managing a dialogue between end-user application processes.
- Responds to service requests from the presentation layer and issues requests to the transport layer.
- Supports duplex or half-duplex operations.
- Concerned with:
  - Dialogue control.
  - Synchronization.
Presentation Layer Functions

- Relieves application layer from concern regarding syntactical differences in data representation with end-user systems.
- Responds to service requests from the application layer and issues requests to the session layer.
- Concerned with:
  - Translation.
  - Encryption.
  - Compression.
Application Layer Functions

- Interfaces directly to and performs common application services for application processes.
- Issues service requests to the Presentation layer.
- Specific services provided:
  - Network virtual terminal.
  - File transfer, access and management.
  - Mail services.
  - Directory services.
TCP/IP Model

- TCP/IP protocol consists of five layers.
- The lower four layers correspond to the layer of the OSI model.
- The application layer of the TCP/IP model represents the three topmost layers of the OSI model.
OSI and TCP/IP Models

<table>
<thead>
<tr>
<th>OSI layers</th>
<th>TCP/IP layers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>DNS</td>
</tr>
<tr>
<td>Presentation</td>
<td>FTP, Telnet, SMTP</td>
</tr>
<tr>
<td>Session</td>
<td>Application</td>
</tr>
<tr>
<td>Transport</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>Network</td>
<td>IP, OSPF, DHCP, ICMP, IGMP</td>
</tr>
<tr>
<td>Data link</td>
<td>Lower level vendor...</td>
</tr>
<tr>
<td>Physical</td>
<td></td>
</tr>
</tbody>
</table>
Internet Protocol (IP)

- Provides connection-less, best-effort service for delivery of packets through the inter-network.
- Best-effort: No error checking or tracking done for the sequence of packets (datagrams) being transmitted.
- Upper layer should take care of sequencing.
- Datagrams transmitted independently and may take different routes to reach same destination.
- Fragmentation and reassembly supported to handle data links with different maximum – transmission unit (MTU) sizes.
Internet Control Message Protocol (ICMP)

- Companion protocol to IP.
- Provides mechanisms for error reporting and query to a host or a router.
- Query message used to probe the status of a host or a router.
- Error reporting messages used by the host and the routers to report errors.
Internet Group Management Protocol (IGMP)

- Used to maintain multicast group membership within a domain.
- Similar to ICMP, IGMP query and reply messages are used by routers to maintain multicast group membership.
- Periodic IGMP query messages are used to find new multicast members within the domain.
- A member sends an IGMP join message to the router, which takes care of joining the multicast tree.
Dynamic Host Configuration Protocol (DHCP)

- Used to assign IP addresses dynamically in a domain.
- Extension to Bootstrap Protocol (BOOTP)
- Node Requests an IP address from DHCP server.
- Helps in saving IP address space by using same IP address to occasionally connecting hosts.
Internet Routing Protocols

- **Intradomain Routing**
  - Distance Vector.
    - Routing Information Protocol (RIP)
      - Distance information about all the nodes is conveyed to the neighbors.
  
- **Link State**
  - Open Shortest Path First (OSPF)
    - Neighbor information is conveyed to all the nodes in the network.
Internet Routing Protocols (Cont’d)

- **Interdomain Routing**
  - **Exterior Gateway Protocol (EGP)**
    - Forces treelike topology onto the Internet.
    - Single Backbone and autonomous systems are connected in parents and children, not peers.
  - **Border Gateway Protocol (BGP)**
    - Assumes Internet as arbitrarily interconnected set of Autonomous systems.
    - Based on Path vector routing protocol.
Transmission Control Protocol (TCP) over Wireless

- Internet employs TCP/IP protocol stack.
- Most of the applications require reliable transmission layer (mostly TCP).
- Wireless network must support existing applications.
- Packet loss can occur because of random errors as well as due to congestion.
- Decreases efficiency due to TCP’s Congestion avoidance.
- Many other problems like mobility support, demands modification in TCP.
Solutions for Wireless Environment

- **TCP-SACK**
  - Selective Acknowledgement and Selective Retransmission.
  - Sender can retransmit missing data due to random errors/mobility.

- **WTCP Protocol**
  - Separate flows for wired (Sender to BS) and wireless (BS to MS) segments of TCP connections.
  - Local Retransmission for mobile link breakage
  - BS sends ACK to sender after Timestamp modification, to avoid change in round trip estimates.

- **Freeze-TCP Protocol**
  - Mobile detects impending handoff.
  - Advertises Zero Window size, to force the sender into Zero Window Probe mode.
Solutions for Wireless Environment (Cont’d)

- Explicit Band State Notification (EBSN)
  - Local Retransmission from BS to shield wireless link errors.
  - EBSN message from BS to Source during local recovery.
  - Source Resets its timeout value after EBSN.

- Fast Retransmission Approach
  - Tries to reduce the effect of MS handoff.
  - MS after handoff sends certain number of duplicate ACKs.
  - Avoids coarse time-outs at the sender, Accelerates retransmission.
Solutions for Wireless Environment (Link Layer Protocols)

- **Transport Unaware Link Improvement Protocol (TULIP)**
  - Provides Service Aware Link Layer.
  - Reliable Service for TCP packets, unreliable service for UDP Packets.

- **AIRMAIL Protocol**
  - Asymmetric Reliable Mobile Access in Link Layer.
  - Uses combination of FEC and ARQ for loss recovery.

- **Snoop Protocol**
  - Transport layer aware Snoop Agent at BS.
  - Agent monitors all TCP segments destined to MS, caches it in buffer.
  - Also monitors ACKs from MS.
  - Loss detected by duplicate ACKs from MS or local time-out.
  - Local Retransmission of missing segment if cached
  - Suppresses the duplicate ACKs.
Solutions for Wireless Environment (Split TCP Approach)

- **Indirect-TCP (I-TCP)**
  - Split the connection into wired component and wireless component.
  - Specialized support for mobile applications for wireless side. Wired side is left unchanged.

- **M-TCP Protocol**
  - Split the connection into wired component and wireless component.
  - BS relays ACKs for sender only after receiving ACKs from MS.
  - In case of frequent disconnections, Receiver can signal Sender to enter in persist mode by advertising Zero Window size.
Internet Protocol Version 6 (IPv6)

Designed to address the unforeseen growth of the internet and the limited address space provided by IPv4

Features of IPv6:

• **Enhanced Address Space:** 128 bits long, can solve the problem created by limited IPv4 address space (32 bits).

• **Resource Allocation:** By using “Flow Label”, a sender can request special packet handling.

• **Modified Address Format:** Options and Base Header are separated which speeds up the routing process.

• **Support for Security:** Encryption and Authentication options are supported in option header.
IPv6 Header Format

<table>
<thead>
<tr>
<th>Version</th>
<th>Traffic Class</th>
<th>Flow Label</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payload Length</td>
<td>Next Header</td>
<td>Hop Limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Format of IPv6

<table>
<thead>
<tr>
<th>Name</th>
<th>Bits</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>4</td>
<td>IPv6 version number.</td>
</tr>
<tr>
<td>Traffic Class</td>
<td>8</td>
<td>Internet traffic priority delivery value.</td>
</tr>
<tr>
<td>Flow Label</td>
<td>20</td>
<td>Used for specifying special router handling from source to destination(s) for a sequence of packets.</td>
</tr>
<tr>
<td>Payload Length</td>
<td>16, unsigned</td>
<td>Specifies the length of the data in the packet. When set to zero, the option is a hop-by-hop Jumbo payload.</td>
</tr>
<tr>
<td>Next Header</td>
<td>8</td>
<td>Specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field.</td>
</tr>
<tr>
<td>Hop Limit</td>
<td>8, unsigned</td>
<td>For each router that forwards the packet, the hop limit is decremented by 1. When the hop limit field reaches zero, the packet is discarded. This replaces the TTL field in the IPv4 header that was originally intended to be used as a time based hop limit.</td>
</tr>
<tr>
<td>Source Address</td>
<td>128</td>
<td>The IPv6 address of the sending node.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>128</td>
<td>The IPv6 address of the destination node.</td>
</tr>
</tbody>
</table>
Differences between IPv4 and IPv6

- Expanded Addressing Capabilities
- Simplified Header Format
- Improved Support for Options and Extensions
- Flow Labeling Capabilities
- Support for Authentication and Encryption
Network Transition from IPv4 to IPv6

• Dual IP-Stack: IPv4-hosts and IPv4-routers have an IPv6-stack, this ensures full compatibility to not yet updated systems.

• IPv6-in-IPv4 Encapsulation (Tunneling): Encapsulate IPv6 datagram in IPv4 datagram and tunnel it to next router/host.