TKK Tietoliikennelaboratorio
HUT Communications Laboratory

S-72.423
Telecommunication Systems
2004

Exercise 5. Solutions

S-72.423 Exercise 5. Solutions

The Internet

1. List the higher layer internet protocols and the applications they support.

   Solution

   The Internet protocol suite includes many application-layer protocols that represent a wide variety of applications, including the following:

   - *File Transfer Protocol (FTP)*—Moves files between devices
   - *Simple Network-Management Protocol (SNMP)*—Primarily reports anomalous network conditions and sets network threshold values
   - *Telnet*—Serves as a terminal emulation protocol
   - *X Windows*—Serves as a distributed windowing and graphics system used for communication between X terminals and UNIX workstations
   - *Network File System (NFS), External Data Representation (XDR), and Remote Procedure Call (RPC)*—Work together to enable transparent access to remote network resources
   - *Simple Mail Transfer Protocol (SMTP)*—Provides electronic mail services
   - *Domain Name System (DNS)*—Translates the names of network nodes into network addresses

2. Describe IP routing in few sentences.

Solution

IP routing protocols are dynamic. Dynamic routing calls for routes to be calculated automatically at regular intervals by software in routing devices. This contrasts with static routing, where routers are established by the network administrator and do not change until the network administrator changes them.

An IP routing table, which consists of destination address/next hop pairs, is used to enable dynamic routing. An entry in this table, for example, would be interpreted as follows: to get to network 172.31.0.0, send the packet out Ethernet interface 0 (E0).

IP routing specifies that IP datagrams travel through internetworks one hop at a time. The entire route is not known at the onset of the journey, however. Instead, at each stop, the next destination is calculated by matching the destination address within the datagram with an entry in the current node's routing table.

Each node's involvement in the routing process is limited to forwarding packets based on internal information. The nodes do not monitor whether the packets get to their final destination, nor does IP provide for error reporting back to the source when routing anomalies occur. This task is left to another Internet protocol, the Internet Control-Message Protocol (ICMP), which is discussed in the following section.

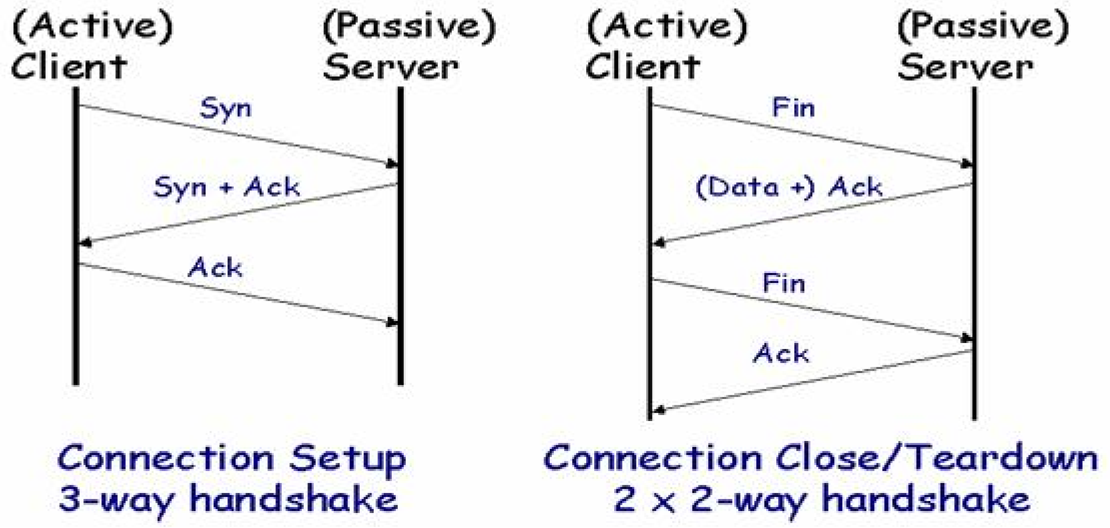
3. Describe the TCP connection establishment.

Solution

To use reliable transport services, TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using a "three-way handshake" mechanism.

A three-way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. This mechanism also guarantees that both sides are ready to transmit data and know that the other side is ready to transmit as well. This is necessary so that packets are not transmitted or retransmitted during session establishment or after session termination.

Each host randomly chooses a sequence number used to track bytes within the stream it is sending and receiving. Then, the three-way handshake proceeds in the following manner:



The first host (Host A) initiates a connection by sending a packet with the initial sequence number (X) and SYN bit set to indicate a connection request. The second host (Host B) receives the SYN, records the sequence number X, and replies by acknowledging the SYN (with an ACK = X + 1). Host B includes its own initial sequence number (SEQ = Y). An ACK = 20 means the host has received bytes 0 through 19 and expects byte 20 next. This technique is called *forward acknowledgment*. Host A then acknowledges all bytes Host B sent with a forward acknowledgment indicating the next byte Host A expects to receive (ACK = Y + 1). Data transfer then can begin.

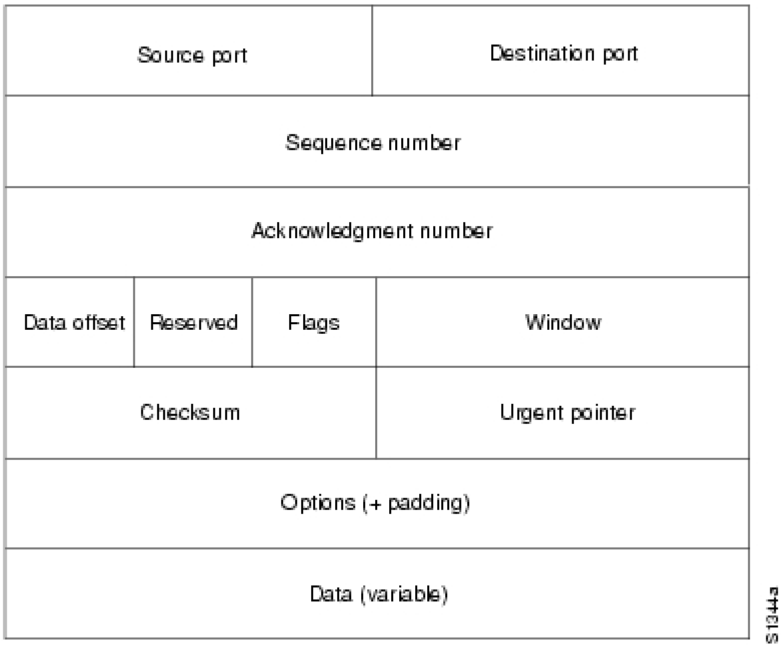
4. **IPv4**

- Show in a figure the TCP packet format and describe the fields that comprise it.
- What happens if there is no Time-to-Live counter in IPv4 IP packet?
- What are the benefits of using IP subnet addressing?

Solution

-
    - *Source Port* and *Destination Port*—Identifies points at which upper-layer source and destination processes receive TCP services.

- *Sequence Number*—Usually specifies the number assigned to the first byte of data in the current message. In the connection-establishment phase, this field also can be used to identify an initial sequence number to be used in an upcoming transmission.
- *Acknowledgment Number*—Contains the sequence number of the next byte of data the sender of the packet expects to receive.
- *Data Offset*—Indicates the number of 32-bit words in the TCP header.
- *Reserved*—Remains reserved for future use.
- *Flags*—Carries a variety of control information, including the SYN and ACK bits used for connection establishment, and the FIN bit used for connection termination.
- *Window*—Specifies the size of the sender's receive window (that is, the buffer space available for incoming data).
- *Checksum*—Indicates whether the header was damaged in transit.
- *Urgent Pointer*—Points to the first urgent data byte in the packet.
- *Options*—Specifies various TCP options.
- *Data*—Contains upper-layer information.



<table>
<tr><td colspan="3">Source port</td><td>Destination port</td></tr>
<tr><td colspan="4">Sequence number</td></tr>
<tr><td colspan="4">Acknowledgment number</td></tr>
<tr><td>Data offset</td><td>Reserved</td><td>Flags</td><td>Window</td></tr>
<tr><td colspan="3">Checksum</td><td>Urgent pointer</td></tr>
<tr><td colspan="4">Options (+ padding)</td></tr>
<tr><td colspan="4">Data (variable)</td></tr>
</table>

- *Time-to-Live*—maintains a counter that gradually decrements down to zero, at which point the datagram is discarded. ***This keeps packets from looping endlessly.***

- Subnetting provides the network administrator with several benefits:
  - Extra flexibility,
  - More efficient use of network addresses,
  - The capability to contain broadcast traffic (a broadcast will not cross a router).

5. **IPv6**

- What is the main reason for IPv6 being developed?

- What is the new broadcast methods included in IPv6?

- How many bits does the new expanded addressing provide?

Solution

See http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ipv6.htm

- The main issue surrounding IPv6 is addressing, or the lack of addressing. Many people believe that we are nearly out of the four billion addresses available in IPv4.
-
  - i. Unicast:
    Unicast is a communication between a single host and a single receiver. Packets sent to a unicast address are delivered to the interface identified by that address.
  - ii. Multicast:
    Multicast is communication between a single host and multiple receivers. Packets are sent to all interfaces identified by that address.
  - iii. Anycast:

Packets sent to an anycast address or list of addresses are delivered to the nearest interface identified by that address. Anycast is a communication between a single sender and a list of addresses.

- The expanded addressing moves us from 32-bit address to a 128-bit addressing method