Subnetting

Subnetting & Masks

- IP address is depleting faster than expected:
  - All network, even one with 2 hosts, need at least class C address.
  - A network with 256 hosts need class B address.
- Also, the more there is networks, the bigger the routing table gets.
- Solution is subnetting.
  - A network can be divided into subnets.
  - Outside routers still view them as one large network.
  - Only, the local routers see them as separate networks.

Subnet Masks

- Now in each routing table both the network number and the mask is stored.
- An AND operation is performed before looking up for the next hop.
- For distant networks, the mask is of type A, B, or C. But for local network, the mask is longer.

Example of Subnet

- H3 in 128.96.33.0 sees everything in 128.96.34.0 as one single network.
- Network 128.96.34.0 is class B address and can have about 256x256 hosts in one large network.
- But the administrator of 128.96.34.0 has divided its network into two physical networks 128.96.34.0 and 128.96.34.128 with mask 255.255.255.128.

IP Datagram Forwarding: with IP

- What is Bit Mask?
  - R2’s routing table

- IP - Internet Protocol
  - Addressing Scheme
  - Address Resolution
  - Datagram Forwarding
    - Encapsulation, Fragmentation & Reassembly
- TCP - Transmission Control Protocol
  - Connection startup & shutdown
  - Reliability: ordering, missing data handling
Encapsulation

- Datagrams have to travel via a physical network. But, a physical network has its own frame format. A Datagram, therefore must be encapsulated.

  - The destination address in the frame header is the address of the next hop.

Transmission across Internet

Encapsulation applies to one network at a time. However, in Internet the journey requires series of transmission over many different networks.

MTU and Datagram Size

- Each Network on its way generally has their own maximum transmission unit size (MTU). How can IP routers overcome this obstacle?

Fragmentation

- Datagrams are fragmented into multiple segments, if it faces a Network with MTU smaller than the datagram size.
- Each fragment has the same format as the datagram, except a bit flag which indicates that it is a fragment, not the entire datagram.
- FRAGMENTOFFSET field indicates where in the original datagram the fragment data belongs.

Reassembly

- Because each fragment has a copy of the original header, and an indication flag that it is a fragment, the original datagram can be reassembled at the end.

Datagram Identification

- Individual fragments can arrive out of order. How IP reassembles out of order fragments?
  - Sender inserts an unique number in IDENTIFICATION field. This with FRAGMENT OFFSET helps in restoring out of order.
- IP does not guarantee delivery and thus fragments can be lost. How IP handles such loss?
  - The same two fields helps in identifying a missing fragment.
  - After receiving the first FRAGMENT, receiver starts a timer. If the entire datagram does not arrive within a specified time, it discards all fragments.
  - But, it does not notify the sender!
What if a fragment needs to be fragmented again?

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Offset Field Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQ</td>
<td>Sequence number of fragment</td>
<td>in units of 8 bytes</td>
</tr>
<tr>
<td>ID</td>
<td>Unique fragment ID</td>
<td></td>
</tr>
<tr>
<td>Offset</td>
<td>Location of fragment data within packet</td>
<td></td>
</tr>
<tr>
<td>More</td>
<td>Indicates if more fragments follow</td>
<td></td>
</tr>
</tbody>
</table>

Example of TCP Fragments

Before Fragmentation

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Offset Field Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQ</td>
<td>Sequence number of fragment</td>
<td>in units of 8 bytes</td>
</tr>
<tr>
<td>ID</td>
<td>Unique fragment ID</td>
<td></td>
</tr>
<tr>
<td>Offset</td>
<td>Location of fragment data within packet</td>
<td></td>
</tr>
<tr>
<td>More</td>
<td>Indicates if more fragments follow</td>
<td></td>
</tr>
</tbody>
</table>

ICMP: An Error Control/Reporting Message Protocol

- IP is a best effort mechanism. But provides no guarantee of delivery.
- However, it is not careless!
- ICMP is a mechanism by which network elements can pass information about the source/cause of errors, and also warn each other about potential problems.
- ICMP defines 5 error messages and 4 information messages.

ICMP: Error Messages

- **SOURCE QUENCE**
  - sent by overworked routers to the sources of discarded datagrams.
- **TIME EXCEEDED**
  - sent by router for packets whose TIME TO LIVE field has expired.
- **DESTINATION UNREACHABLE**
  - sent by routers who could not find forwarding address.
- **REDIRECT**
  - if a router thinks, not him, but some other router should have received the packet.
- **FRAGMENTATION REQUIRED**
  - if the fragment as required permission is not given to a router, it can request source to send fragmented datagrams

ICMP: Informational Messages

- **ECHO/ REQUEST/REPLY**
  - An echo request message can be sent to any ICMP host in a network. It sends replies.
  - Ping!
- **ADDRESS MASK REQUEST/REPLY**
  - A host, when boots can request for the correct address mask for the network. The router in the network send the correct 32 bit address mask.
ICMP Packets over IP

Some Example of ICMP Services

- **Ping**
  - send a datagram with ICMP echo request.

- **Trace a Route**
  - send IP packets with TIME TO LIVE set to 1, 2, 3, etc.

- **Path MTU Discovery**
  - set a FLAG bit in IP messages so that it cannot be fragmented by routers.
  - Send large messages and wait for FRAGMENT REQUIRED ICMP message to come back.
  - Do experiment with various data sizes!