Application  
Transport  
Network  
Link  
Physical

you are here

Transport
(process-to-process)

Network
(host-to-host)

Link
(node-to-node)
Network Layer

- The network layer provides communication between two end hosts. Its two main functions are routing (which path to take) and forwarding (who to forward a packet to). Network layer is implemented in all end hosts and intermediate routers.
- A packet can pass through different link layers technology (WiFi, Ethernet etc.) on its way to the destination.
- The Internet’s network layer consists of IP (handles addressing, packet format), ICMP (for information and error reporting), and routing protocols.
Internet Protocol (IP)

- Each IP datagram has a 20-byte header, consisting of header fields such as version number, datagram length, header checksum (similar to UDP/TCP checksum for only for IP header), time-to-live (decrease by one for every hop travelled, datagram is dropped when becomes 0 to prevent infinite loop), and upper-layer protocol ID (which protocol should deal with this packet).

IP Addresses

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>Site A</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>Site B</td>
</tr>
<tr>
<td>172.16.0.1</td>
<td>Site C</td>
</tr>
</tbody>
</table>
Fragmentation

Network (host-to-host)

Transport (process-to-process)

Link (node-to-node)
Fragmentation

- Due to different maximum packet size at the link layer, routers may have to fragment IP datagrams before forwarding them. IP headers contain necessary information so that the destination host can put the fragments back together.
- IP header contains an ID field (increase by one for every packet sent by the sending host), a fragment bit (1 if more fragments to come, 0 if this is the last), and an offset (position in the original datagram, in units of 8-byte chunks).
IP Address

associated with an interface

4,294,967,296
IP Addresses

- An IP address is associated with an interface (the boundary between a node and a physical link), not host. It is common for a host/router to have multiple IP addresses.
- IP address is a 32-bit ID, which must be globally unique across the Internet.
- IP addresses are organized into hierarchy, with IANA (Internet Assigned Numbers Authority) controlling the 1st level assignment.

Subnet

Subnet Mask
A subnet is a logical grouping of nodes in a network, normally defined using a subnet mask of the form a.b.c.d/x. The value x indicates the number of bits in the prefix of the IP address that is constant for all nodes in the subnet. The rest of the bits (32-x) are variables.

Classfull addressing divides the space of IP addresses into classes, where x can only be either 8, 16, or 24. Classless Interdomain Routing allows much more flexible management of IP addresses with no restrictions on x.

DHCP

Dynamic Host Configuration Protocol

Forwarding Table
Forwarding Table

- Forwarding table in a router stores pairs of (destination subnet, outgoing interface).
- Destination subnet is identified by subnet mask or prefix of IP addresses, and the longest prefix matching rule is used in case there are multiple entries that match the same destination address.
- To view routing table, on UNIX based system, run "netstat -rn", on Windows XP, run "route print".

NAT
Network Address Translation

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
Network Address Translation

- NAT mitigates the problem of IP address starvation by allowing hosts in a LAN to use private IP addresses (10/24, 172.16/12, 192.168/16). A NAT-enabled router maps a (IP address, port) pair of a connection to a port on the router. The outside world (WAN) only sees the IP address of the NAT router and talks to router (as if they are talking to the host inside LAN).
- The router modifies the network and transport-layer header packets between the LAN and WAN as the packets pass through the router.

ICMP

- ICMP is used by hosts and routers to communicate network-layer information to each other. ICMP messages are carried inside IP datagrams (so it lies above of IP in the stack). Each ICMP message has a type and a code field, which indicates what the message is for.
ICMP
Internet Control Message Protocol

ICMP
(type, code)

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>What?</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>0</td>
<td>echo request</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>echo reply</td>
</tr>
</tbody>
</table>
ping

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>What?</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>cannot reach host</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>cannot reach port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>What?</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>0</td>
<td>TTL expired</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>bad IP header</td>
</tr>
</tbody>
</table>
traceroute