LAB EXERCISE - 8

Trace IP/ICMP using Wireshark

Not all link-layer protocols can carry network-layer packets of the same size. Some protocols can carry big datagrams, whereas other protocols can carry only little packets. For example, Ethernet frames can carry up to 1,500 bytes of data, whereas frames for some wide-area links can carry no more than 576 bytes. The maximum amount of data that a link-layer frame can carry is called the maximum transmission unit (MTU). Because each IP datagram is encapsulated within the link-layer frame for transport from one router to the next router, the MTU of the link-layer protocol places a hard limit on the length of an IP datagram.

Each of the links along the route between sender and destination can use different link-layer protocols, and each of these protocols can have different MTUs.
When a router receives an IP datagram from one link, and checks for forwarding table to determine the outgoing link, and observes that this outgoing link has an MTU that is smaller than the length of the IP datagram, it fragments the data in the IP datagram into two or more smaller IP datagrams, encapsulate each of these smaller IP datagrams in a separate link-layer frame; and send these frames over the outgoing link. Each of these smaller datagrams is referred to as a fragment.

Fragments need to be reassembled before they reach the transport layer at the destination. Usually this is done by the destination host. When a destination host receives a series of datagrams from the same source, it needs to determine whether any of these datagrams are fragments of some original, larger datagram. If some datagrams are fragments, it must further determine when it has received the last fragment and how the fragments it has received should be pieced back together to form the original datagram. To allow the destination host to perform these reassembly tasks, the designers of IP (version 4) put *identification*, *flag*, and *fragmentation offset* fields in the IP datagram header.

When a datagram is created, the sending host stamps the datagram with an identification number as well as source and destination addresses. When a router needs to fragment a datagram, each resulting datagram (that is, fragment) is stamped with the source address, destination address, and identification number of the original datagram.

When the destination receives a series of datagrams from the same sending host, it can examine the identification numbers of the datagrams to determine which of the datagrams are actually fragments of the same larger datagram.

Because IP is an unreliable service, one or more of the fragments may never arrive at the destination. For this reason, in order for the destination host to be absolutely sure it has received the last fragment of the original datagram, the last fragment has More flag bit set to 0, whereas all the other fragments have this flag bit set to 1.
Also, in order for the destination host to determine whether a fragment is missing and also to be able to reassemble the fragments in their proper order, the offset field is used to specify where the fragment fits within the original IP datagram.

Figure below illustrates an example. A datagram of 4,000 bytes (20 bytes of IP header plus 3,980 bytes of IP payload) arrives at a router and must be forwarded to a link with an MTU of 1,500 bytes. This implies that the 3,980 data bytes in the original datagram must be allocated to three separate fragments (each of which is also an IP datagram). Suppose that the original datagram is stamped with an identification number of 777. The characteristics of the three fragments are shown in Table. The values in Table reflect the requirement that the amount of original payload data in all but the last fragment be a multiple of 8 bytes, and that the offset value be specified in units of 8-byte chunks.

At the destination, the payload of the datagram is passed to the transport layer only after the IP layer has fully reconstructed the original IP datagram. If one or more of the fragments does not arrive at the destination, the incomplete datagram is discarded and not passed to the transport layer.

Fragment	Bytes	ID	Offset	Flag
1st fragment	1,480 bytes in the data field of the IP datagram	identification = 777	offset = 0 (meaning the data should be inserted beginning at byte 0)	flag = 1 (meaning there is more)
2nd fragment	1,480 bytes of data	identification = 777	offset = 185 (meaning the data should be inserted beginning at byte 1,480. Note that 185 · 8 = 1,480)	flag = 1 (meaning there is more)
3rd fragment	1,020 bytes (= 3,980–1,480–1,480) of data	identification = 777	offset = 370 (meaning the data should be inserted beginning at byte 2,960. Note that 370 · 8 = 2,960)	flag = 0 (meaning this is the last fragment)

PING

Ping is a computer network tool used to test whether a particular host is reachable across an IP network. It allows a user to verify that a particular IP address exists or not and whether it can accept requests. Ping is used diagnostically to ensure that a host computer the user is trying to reach is actually operating. It can be used for troubleshooting to test connectivity and determine response time. It is also used to self test the network interface card of the computer.
Ping works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. It measures the round-trip time and records any packet loss, and prints

when finished a statistical summary of the echo response packets received, the minimum, mean, max and in some versions the standard deviation of the round trip time.

ICMP

ICMP, is used by hosts and routers to communicate network-layer information to each other. The most typical use of ICMP is for error reporting..
ICMP messages are carried as IP payload. when a host receives an IP datagram with ICMP specified as the upper-layer protocol, it demultiplexes the datagram's contents to ICMP, just as it would demultiplex a datagram's content to TCP or UDP.

ICMP messages have a type and a code field, and contain the header and the first 8 bytes of the IP datagram that caused the ICMP message to be generated in the first place (so that the sender can determine the datagram that caused the error). The well-known ping program sends an ICMP type 8 code 0 message to the specified host. The destination host, seeing the echo request, sends back a type 0 code 0 ICMP echo reply