Chapter 8

Active Measurement

8.1 Basic components of Active Probing Infrastructure

The basic components of active probing infrastructure are shown in Figure 8.1. In each probing experiment, sender creates and transmits a probe stream, which traverses some route in the network and terminates at the receiver. The probe sequence numbers available from the payloads, the packet arrival and departure timestamps define the raw outcome of the experiment. The monitor at sender and receiver records them. In case of round-trip measurements, the sender and receiver are two processes running on a single computer with a single Internet address. Each of these components is a potential source of errors, which involve timing in some form. These can be broken down into errors due to reference timing sources hardware issues such as interrupt cycles, which drive process scheduling, and software issues including the performance of algorithms for software clock correction (ref. [66], [67], [68], [69], [70]).
8.2 Infrastructure Used for Measurement at ssgmce.org

Wide Area Network (WAN) infrastructure used to support measurement and analysis at ssgmce.org is shown in Figure 8.2. The measurements are carried on Intel P-IV PC with Red-Hat Linux 7.2 and Windows Millennium operating systems. Ping and Traceroute are the measurement tools used. The measurement node is connected to Gigabit backbone. The various devices used in the WAN are Router (CISCO 2620), Modem (V.35 Patton) at network room, G703 Modem at Shegaon PBX and G703 to V.35 converter at Khamgaon PBX.

The various sites such as www.yahoo.com, www.aajtak.com etc. that are accessed frequently at ssgmce domain are chosen for pinging. In our procedure, pinging is done twice a minute. The user can choose the packet size and time for pinging. The raw data is then processed using GNU plot utility of Linux, graphs between packet loss v/s time of day and RTT v/s time of day are generated using the collected data.
8.3 Measuring Tools

Ping

"Ping" is one of the most useful network debugging tools available. It takes its name from a submarine sonar search - you send a short sound burst and listen for an echo - a ping - coming back. In an IP network, 'ping' sends a short data burst - a single packet - and listens for a single packet in reply. This tests the most basic function of an IP network which is delivery of single packet.

We call the ping program that sends the echo request as the client, and the host being pinged as the server. Most TCP/IP implementations supports the Ping server directly in the kernel - the server is not a user process. Unix implementations of ping set the identifier field in the ICMP message to the process ID of the sending process. This allows ping to identify the return response if there are multiple instances of ping.
running at the same time on the same host. The sequence number starts at 0 and is incremented every time a new echo request is sent. Ping prints the sequence number of each returned packet, allowing us to see if the packets are missing, recorded, or duplicated. Ping is able to calculate the round-trip time by sorting the time at which it sends the echo request in the data portion of the ICMP messages.

By Using Ping We Get

Ping places a unique sequence number on each packet it transmits, and reports, which sequence numbers it receives back. Thus, one can determine if packets have been dropped, duplicated, or reordered.

Ping checksums each packet it exchanges. It detects some forms of damaged packets.

Ping places a timestamp in each packet, which is echoed back and can easily be used to compute how long each packet exchange took - the Round Trip Time (RTT).

Ping reports other ICMP messages that might otherwise get buried in the system software. It reports, for example, if a router is declaring the target host unreachable.

Limitation

Some routers may silently discard undeliverable packets. Others may believe a packet has been transmitted successfully when it has not been. (This is especially common over Ethernet, which does not provide link-layer acknowledgments). Therefore, ping may not always provide reasons why packets go unanswered.

Ping can not tell one why a packet was damaged, delayed, or duplicated. It cannot tell one where this happened either, although one may be able to deduce it.

Ping cannot give one a blow-by-blow description of every host that handled the packet and everything that happened at every step of the way. It is an unfortunate fact that no software can reliably provide this information for a TCP/IP network.
Ping Options

- **c count**
  
  Send count packets and then stop. This option is convenient for scripts that periodically check network behavior.

- **I pre-load**
  
  Send pre-load packets as fast as possible, and then fall into a normal mode of behavior. Good for finding out how many packets your routers can quickly handle, which is in turn good for diagnosing problems that only appear with large TCP window sizes.

- **n numeric**

  Numeric output only.

Sample Ping Output

Following are the ten-packets exchanged over the loop back interface. One line is printed for every reply received. Note that for each sequence number, a single reply is received, and they are all in order. The IP TTL values are reported.

PING www.yahoo.com

64 bytes from 144.228.202.1: icmp_seq=0 ttl=254 time=35.653 ms
64 bytes from 144.228.202.1: icmp_seq=1 ttl=254 time=28.797 ms
64 bytes from 144.228.202.1: icmp_seq=2 ttl=254 time=28.559 ms
64 bytes from 144.228.202.1: icmp_seq=3 ttl=254 time=39.533 ms
64 bytes from 144.228.202.1: icmp_seq=4 ttl=254 time=28.621 ms
64 bytes from 144.228.202.1: icmp_seq=5 ttl=254 time=28.159 ms
64 bytes from 144.228.202.1: icmp_seq=6 ttl=254 time=848.810 ms
64 bytes from 144.228.202.1: icmp_seq=7 ttl=254 time=828.579 ms
64 bytes from 144.228.202.1: icmp_seq=8 ttl=254 time=753.865 ms
Traceroute

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route one’s packets follow (or finding the miscreant gateway that is discarding one’s packets) can be difficult. Traceroute utilizes the IP protocol ‘time to live’ field and attempts to elicit an ICMP TIME EXCEEDED response from each gateway along the path to some host. The only mandatory parameter is the destination host name or IP number. The default probe datagram length is 38 bytes, but this may be increased by specifying a packet size (in bytes) after the destination host name. "Traceroute" is a network debugging utility that attempts to trace the path a packet takes through the network - its route.

How Traceroute Work

Traceroute transmits packets with small TTL values. The TTL (Time To Live) is an IP header field that is designed to prevent packets from running in loops. Every router handles a packet subtracts one from the packet’s TTL. If the TTL reaches zero, the packet has expired and is discarded. Traceroute depends on the common router practice of sending an ICMP time exceeded message, back to the sender when this occurs. By using small TTL values, which quickly expire, traceroute causes routers along a packet’s normal delivery path to generate these ICMP messages, which identify the router. A TTL value of one should produce a message from the first router; a TTL value of two generates a message from the second; etc.

In a typical traceroute session, a group of packets with TTL=1 are sent. A single router should respond, using the IP address of the interface it transmits the ICMP Timeout messages, which should be the same as the interface over which it received
the original packets. Also, round trip times are reported for each packet in the group.
Traceroute reports any additional ICMP messages (such as destination unreachable) using a rather cryptic syntax e.g. -! N means network unreachable. ! H means host unreachable, etc. Once this first group of packets has been processed (this can take around 10 seconds), the second group (TTL=2) begins transmitting, and the whole process repeats.

Figure 8.3: How traceroute works.

Limitation

1. Changing Paths

We are not tracing the path of one packet, but of many. Hopefully, all those packets will follow the same route, but this is by no means assured. What if a link fails during the traceroute. Our packets may be rerouted, and traceroutes output becomes a confused combination of two separate routes.

2. No Sending Addresses

We only see one IP address from each router - the address closest to us. To put it another way, traceroute can't tell us about over which which interfaces routers are sending the packets. It only shows the interfaces packets are being received. The sending interfaces can often be deduced by matching each router with the next one in line - typically only one interface could be used between them.
CHAPTER 8. ACTIVE MEASUREMENT

3. Routing problems

Routing problems may cause the router not to have a route back to the sender, or to have a route through some interface other than the one it received the packet on. In these cases, we will either receive no reply at all (no route), or a reply showing an IP address that never handled the original packet (it was handled by some other interface on the same router).

4. Buggy TCP/IP implementations

Traceroute depends on a rather obscure feature that often doesn’t work correctly. Some of the problems people have found: code that fails to decrement TTL, code that incorrectly forward packets with zero TTL, code that does not generate ICMP Timeouts, and code that sends ICMPs with the same TTL as the original packet.

MEASUREMENT METHODOLOGY

The investigator used ping to measure the response time (round trip time in milliseconds (ms)), the packet loss percentage, the variability of the response time both short term (time scale of seconds) as well longer time scales, and the lack of reachability, i.e. no response for a succession of pings.

1. Loss

The loss is a good measure of the quality of the link (in terms of its packet loss rates) for many TCP based applications. Loss is caused by congestion, which in turn causes queues (e.g. in routers) to fill and packets to be dropped. The network delivering an imperfect copy of the packet may also cause losses. This is usually caused by bit errors in the links or in network devices.
2. RTT

The response time or Round Trip Time (RTT) when plotted against packet size can give an idea of ping data rate. This becomes increasingly difficult as one goes to high performance links, since the packet range is relatively small (Typically < 1500 bytes), and the timing resolution is limited. The RTT is related to the distance between the sites plus the delay at each hop along the path between the sites. The distance effect can be roughly characterized by the speed of light in fiber, and is roughly given by $\text{distance}/(0.6 \times c)$ where $c$ is the velocity of light. Putting this together with the hop delays, the RTT $R$ is roughly given by:

$$R = 2 \times (\text{distance}/(0.6 \times c) + \text{hops} \times \text{Delay})$$ (8.1)

where the factor of 2 is due to the fact that we are measuring the front and back times for the round-trip.

8.4 Results

Figures 8.4 and 8.5 show the latency plots as well as the packet loss plots for Thursday, 30th Jan 03 from midnight 0:00 AM to 10:00 AM for the path ssgmce.net - www.yahoo.com.

The latency plots show the characteristic that the RTT for this particular path is varying in 'BURSTS'. The particular characteristic to be noted is that although RTT variations are large, but the packet loss percentage for this particular path during the similar period is quite low, except for very few and occasional 100 percent packet loss bursts. The average packet loss could be predicted around 4 percent during this period.
This could be analysed that, the traffic during this period was bit heavy, but not so much so as to cause heavy packet loss during this period. Therefore the network was
capable of handling the traffic although it had become slower due to the increased traffic. The low packet loss percentage indicates good behavior of the network and capability to handle large traffic without any significant changes or problems to the end user. The width of the bursts was quite the same during the period from 1:00AM to 2:30 AM and during the period from 4:00AM to 5:00AM. But increased latency burst width was observed during the period from 6:30 AM to 9:30 AM with 100 percent Packet loss occurring once during this period.

As the packet loss has been quite low and almost constant during this period we can say that the path has been quite constant during this period with not much variation in the number of hops. The average RTT in this period was around 270 ms.