Traceroute

Command in Windows:

tracert

Network administrators and system administrators use this tool most commonly in their day to day activities. Its basically a network diagnostic tool.

There are three main primary objectives of traceroute tool.

The entire path that a packet travels through

Names and identity of routers and devices in packet's path

Network Latency or more specifically the time taken to send and receive data to each device on the path

It's a tool that can be used to query the path that your data will take to reach its destination, without actually sending your data.

Each IP packet that you send on the internet has got a field called as TTL. TTL stands for Time To Live. Although its called as Time To Live, it's not actually the time in seconds, but it's something else.

TTL is not measured by the no of seconds but the no of hops. It's the maximum number of hops that a packet can travel through across the internet, before its discarded.

Hops are nothing but the computers, routers, or any devices that comes in between the source and the destination.

What if there was no TTL at all?

If there was no TTL in an IP packet, the packet will flow endlessly from one router to another and on and on forever searching for the destination. TTL value is set by the sender inside his IP packet (the person using the system, or sending the packet, is unaware of these things going on under the hood, but is automatically handled by the operating system).

If the destination is not found after traveling through too many routers in between (hops) and TTL value becomes 0 (which means no further travel) the receiving router will drop the packet and informs the original sender.

Original sender is informed that the TTL value exceeded and it cannot forward the packet further.

But how will the routers in between determine the TTL value limit has reached?

Each router that comes in between the source and destination will go on reducing the TTL value before sending to the next router. This means, if i have a default TTL value of 30, then my first router will reduce it to 29 and then send that to the next router across the path. The receiving router will make it 28 and send to the next and so on. If a router receives a packet with TTL of 1 (which means no more further traveling, and no forwarding), the packet is discarded. But the router which discards the packet will inform the original sender that the TTL value has exceeded.

The information send by the router receiving a packet with TTL of 1 back to the original sender is called as "ICMP TTL exceeded messages". Of course in internet when you send something to a receiver, the receiver will come to know the address of the sender.

Hence when an ICMP TTL exceeded message is sent by a router, the original sender will come to know the address of the router.

OUTPUT:

```
C:\Users\itsme>tracert www.thapar.edu

Tracing route to www.thapar.edu [14.139.242.109]
over a maximum of 30 hops:

  1    31 ms     1 ms     1 ms  dsldevice.lan [192.168.1.254]
  2     6 ms     8 ms     6 ms  100.75.0.1
  3     *       64 ms     9 ms  172.17.10.61
  4    10 ms    10 ms    10 ms  192.168.241.37
  5    18 ms     *        9 ms  192.168.252.137
  6    28 ms    11 ms     8 ms  192.168.241.62
  7    77 ms    15 ms    18 ms  aes-static-125.34.144.59.airtel.in [59.144.34.125]
  8    21 ms    19 ms    16 ms  182.79.149.2
  9    31 ms    13 ms    17 ms  115.248.156.25
 10    16 ms    17 ms    19 ms  124.124.195.101
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15   175 ms    55 ms    52 ms  14.139.242.109

Trace complete.

C:\Users\itsme>
```

Where the hops exist?

1. 192.168.1.254

```
NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
```

2. 100.75.0.1

```
NetRange:       100.64.0.0 - 100.127.255.255
CIDR:           100.64.0.0/10
NetName:        SHARED-ADDRESS-SPACE-RFCTBD-IANA-RESERVED
NetHandle:      NET-100-64-0-0-1
Parent:         NET100 (NET-100-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:Internet Assigned Numbers Authority (IANA)
RegDate:        2012-03-13
Updated:        2016-04-11
```

3. 172.17.10.61

```
NetRange:       172.16.0.0 - 172.31.255.255
CIDR:           172.16.0.0/12
NetName:        PRIVATE-ADDRESS-BBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-172-16-0-0-1
Parent:         NET172 (NET-172-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
```

4. 192.168.241.37

```
NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
```

5. 192.168.252.137

```
NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
```

6. 192.168.241.62

```
NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
```

7. 59.144.34.125

```
inetnum:          59.144.0.0 - 59.145.255.255
netname:          BHARTI-IN
descr:            BHARTI INFOTEL LTD.
descr:            ISP Division , Long Distance Group - Telesonic
descr:            234 , Okhala Phase III
descr:            NEW DELHI
descr:            INDIA
country:          IN
org:              ORG-BAL1-AP
admin-c:          NA40-AP
tech-c:           NA40-AP
abuse-c:          AB914-AP
status:           ALLOCATED PORTABLE
remarks:          ----------------------------------------------------
remarks:          To report network abuse, please contact mnt-irt
remarks:          For troubleshooting, please contact tech-c and admin-c
remarks:          Report invalid contact via www.apnic.net/invalidcontact
remarks:          ----------------------------------------------------
mnt-by:           APNIC-HM
mnt-lower:        MAINT-IN-BBIL
mnt-routes:       MAINT-IN-BBIL
mnt-irt:          IRT-BHARTI-TELEMEDIA-IN
last-modified:    2020-05-16T21:37:18Z
source:           APNIC
```

8. 182.79.149.2

```
inetnum:          182.64.0.0 - 182.79.255.255
netname:          BHARTI-IN
descr:            Bharti Airtel Limited
descr:            Transport Network Group
descr:            234, Okhla Phase III
country:          IN
org:              ORG-BAL1-AP
admin-c:          NA40-AP
tech-c:           NA40-AP
abuse-c:          AB914-AP
status:           ALLOCATED PORTABLE
remarks:          ----------------------------------------------------
remarks:          To report network abuse, please contact mnt-irt
remarks:          For troubleshooting, please contact tech-c and admin-c
remarks:          Report invalid contact via www.apnic.net/invalidcontact
remarks:          ----------------------------------------------------
notify:           ipspamsupport@Airtel.com
mnt-by:           APNIC-HM
mnt-lower:        MAINT-IN-BBIL
mnt-routes:       MAINT-IN-BBIL
mnt-irt:          IRT-BHARTI-TELEMEDIA-IN
last-modified:    2020-05-16T21:37:21Z
source:           APNIC
```

9. 115.248.156.25

```
inetnum:          115.248.0.0 - 115.255.255.255
netname:          RCOM
descr:            Reliance Communications Ltd
descr:            Dhirubai Ambani Knowledge City
descr:            Thane Belapur Road, KoparKhairane
descr:            Navi Mumbai - 400710
descr:            India
country:          IN
org:              ORG-RCL5-AP
admin-c:          AH406-AP
tech-c:           AH406-AP
remarks:          ------------------------------------------------------
remarks:          To report network abuse, please contact mnt-irt
remarks:          For troubleshooting, please contact tech-c and admin-c
remarks:          Report invalid contact via www.apnic.net/invalidcontact
remarks:          ------------------------------------------------------
mnt-irt:          IRT-RELIANCE-COMMUNICATIONS-IN
mnt-by:           APNIC-HM
mnt-lower:        MAINT-IN-SN
mnt-routes:       MAINT-IN-SN
status:           ALLOCATED PORTABLE
last-modified:    2018-10-16T04:20:40Z
source:           APNIC
```

10.124.124.195.101

```
inetnum:          124.124.0.0 - 124.124.255.255
netname:          RCOM-STATIC
descr:            This space is statically assigned.
country:          IN
admin-c:          AH406-AP
tech-c:           AH406-AP
status:           ALLOCATED NON-PORTABLE
mnt-by:           MAINT-IN-SN
last-modified:    2010-09-17T14:26:38Z
source:           APNIC
```

11.14.139.242.109

```
inetnum:          14.139.242.96 - 14.139.242.111
netname:          NMEICT-Thaper-University-Patiala
descr:            Thapar University, Patiala
country:          IN
admin-c:          NNA22-AP
tech-c:           AM768-AP
status:           ASSIGNED NON-PORTABLE
notify:           ar_a@thapar.edu
mnt-by:           MAINT-RSMANI-NKN-IN
mnt-lower:        MAINT-IN-NKNINST1
mnt-routes:       MAINT-RSMANI-NKN-IN
mnt-irt:          IRT-NMEICT-THAPER-UNIVERSITY-PATIALA
last-modified:    2014-03-18T04:28:33Z
source:           APNIC
```

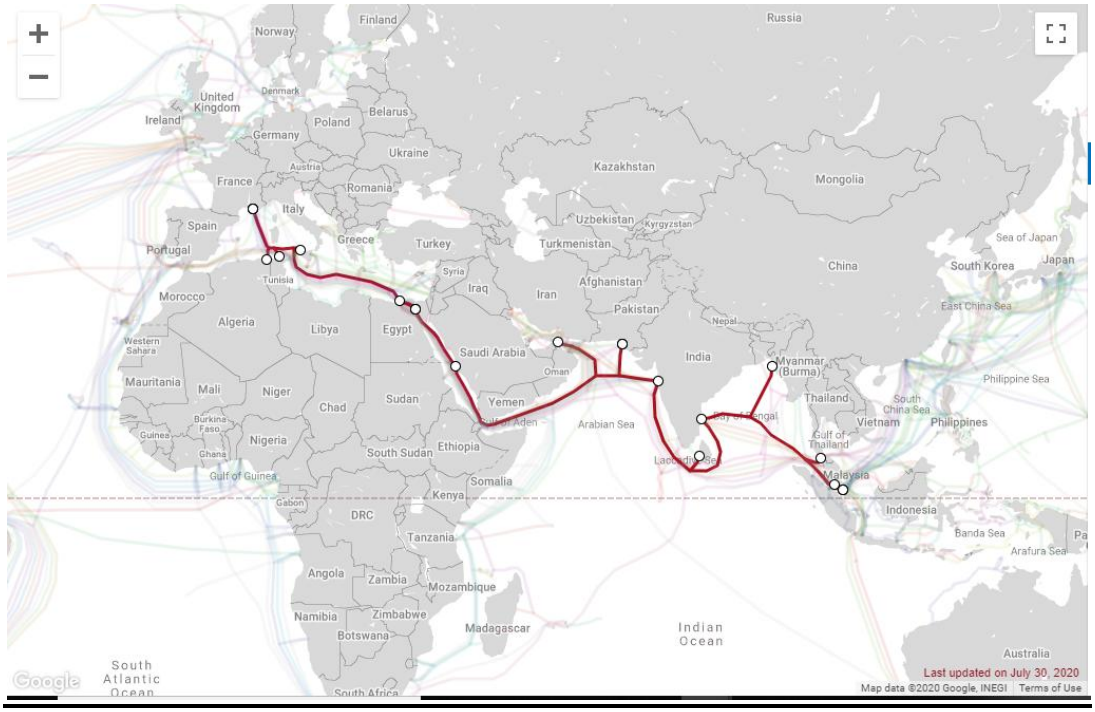
How it Works?

- ➔ My Source address will make a packet with destination ip address of www.thapar.edu and a destination port number between 33434 to 33534. And the important thing it does it to make the TTL Value 1
- ➔ Of course my packet will reach my gateway server. On seeing receiving the packet my gateway server will reduce the TTL by 1 (All routers/hops in between does this job of reducing the TTL value by 1). Once the TTL is reduced by the value of 1 (1-1= 0), the TTL value becomes zero. Hence my gateway server will send me back a TTL Time exceeded message. Please remember that when my gateway server sends a TTL exceeded message back to me, it will send the first 28 byte header of the initial packet i send.
- ➔ On receiving this TTL Time exceeded message, my traceroute program will come to know the source address and other details about the first hop (Which is my gateway server.).
- ➔ Now the traceroute program will again send the same UDP packet with the destination of www.thapar.edu, and a random UDP destination port between 33434 to 33534. But this time i will make the initial TTL 2. This is because my gateway router will reduce it by 1 and then forwards that same packet which send to the next hop/router (the packet send by my gateway to its next hop will have a TTL value of 1).

- ➔ On receiving UDP packet, the next hop to my gateway server will once again reduce it to 1 which means now the TTL has once again become 0. Hence it will send me back a ICMP Time exceeded message with its source address, and also the first 28 byte header of the packet which i send.
- ➔ On receiving that message of TTL Time Exceeded, my traceroute program will come to know about that hop/routers IP address and it will show that on my screen.
- ➔ Now again my traceroute program will make a similar UDP packet with again a random udp port with the destination address of www.thapar.edu. But this time the ttl value is made to 3, so that the ttl will automatically become 0, when it reaches the third hop/router(Please remember that my gateway and the next hop to it, will reduce it by 1). So that it will reply me with a TTL Time exceeded message, and my traceroute program will come to know about that hop/routers IP address.
- ➔ On receiving that reply, the traceroute program will once again make a UDP packet with TTL value of 4 this time. If i gets a TTL Time exceeded for that also, then my traceroute program will send a UDP packet with TTL of 5 and so on.
- ➔ When the original receiver (www.thapar.edu) gets my UDP packet, it will send me a "ICMP Destination/PORT Unreachable" message. This is bound to happen because we are always sending a random UDP port between 33434 to 33534. Hence my Traceroute program will come to know that we have reached the final destination and will stop sending any further packets.

Submarine Cable Map

➔ SeaMeWe-4



- Cable Length: 20,000 km
- Owners: Bangladesh Submarine Cable Company Limited (BSCCL), Orange, Singtel, Telecom Italia Sparkle, Tata Communications, Telekom Malaysia, Airtel (Bharti), Sri Lanka Telecom, Etisalat, Saudi Telecom, CAT Telecom Public Company Limited, Tunisia Telecom, Verizon, Pakistan Telecommunications Company Ltd., Telecom Egypt, Algerie Telecom

Landing Points

- Alexandria, Egypt
- Annaba, Algeria
- Bizerte, Tunisia
- Chennai, India
- Colombo, Sri Lanka
- Cox’s Bazar, Bangladesh
- Fujairah, United Arab Emirates
- Jeddah, Saudi Arabia
- Karachi, Pakistan
- Marseille, France
- Melaka, Malaysia
- Mumbai, India
- Palermo, Italy
- Satun, Thailand
- Suez, Egypt
- Tuas, Singapore