CS315: Lab Assignment 1

Chidurala Tejaswini
220010012@iitdh.ac.in

12 January 2024

Q1. Answers for Task 1: Background

(i) ping www.google.com

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ ping www.google.com
PING www.google.com (142.250.196.36) 56(84) bytes of data.
64 bytes from maa03s45-in-f4.1e100.net (142.250.196.36): icmp_seq=1 ttl=116 time=31.6 ms
64 bytes from maa03s45-in-f4.1e100.net (142.250.196.36): icmp_seq=2 ttl=116 time=34.6 ms
64 bytes from maa03s45-in-f4.1e100.net (142.250.196.36): icmp_seq=3 ttl=116 time=36.6 ms
64 bytes from maa03s45-in-f4.1e100.net (142.250.196.36): icmp_seq=4 ttl=116 time=40.4 ms
64 bytes from maa03s45-in-f4.1e100.net (142.250.196.36): icmp_seq=6 ttl=116 time=34.0 ms
64 bytes from maa03s45-in-f4.1e100.net (142.250.196.36): icmp_seq=7 ttl=116 time=32.2 ms
64 bytes from maa03s45-in-f4.1e100.net (142.250.196.36): icmp_seq=8 ttl=116 time=30.9 ms
^C
--- www.google.com ping statistics ---
8 packets transmitted, 7 received, 12.5% packet loss, time 7774ms
rtt min/avg/max/mdev = 30.913/34.333/40.369/3.058 ms
```

Figure 1: Output for ping

- A ping is a Command Prompt command that can be used to test a connection between one computer and another.
- On running the command (here, in WSL) `ping www.google.com` ,Ping measures the **round-trip time** for messages sent from the originating host to a destination computer that are echoed back to the source.
- Round-trip time (RTT) is the duration in milliseconds (ms) it takes for a network request to go from a starting point to a destination and back again to the starting point.
- Each response includes sequence number, TTL, and RTT in milliseconds.On the linux terminal, such messages keep getting sent, and RTT values are displayed, until termination via `Ctrl+C`
- On termination, it displays statistics on the packets sent, received, and lost.

(ii) traceroute www.google.com

The traceroute command in Linux prints the route that a packet takes to reach the host. When running `traceroute www.google.com` , we would get a report with 5 columns of information. The output of traceroute typically shows 5 columns:

1. Hop Number: Sequence number of the hop.
2. IP Address/Hostname: Address or hostname of the device at that hop.
3. RTT 1: Round-trip time for the first signal packet.
4. RTT 2: Round-trip time for the second signal packet.
5. RTT 3: Round-trip time for the third signal packet.

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ traceroute www.google.com
traceroute to www.google.com (142.250.193.164), 30 hops max, 60 byte packets
 1  TEJASWINICHIDURALA.mshome.net (172.24.128.1)  0.820 ms  0.771 ms  0.756 ms
 2  10.200.224.2 (10.200.224.2)  3.024 ms  3.008 ms  2.992 ms
 3  10.240.0.1 (10.240.0.1)  2.515 ms  2.500 ms  2.914 ms
 4  internet.iitdh.ac.in (10.240.240.1)  3.283 ms  2.872 ms  3.158 ms
 5  * * *
 6  * * *
 7  103.120.29.72.static-delhi.powertel.in (103.120.29.72)  30.409 ms  34.219 ms  30.199 ms
 8  72.14.209.113 (72.14.209.113)  30.145 ms  30.132 ms  29.835 ms
 9  142.251.230.177 (142.251.230.177)  32.459 ms  31.868 ms *
10  142.251.55.233 (142.251.55.233)  30.910 ms  30.640 ms  31.803 ms
11  maa05s26-in-f4.1e100.net (142.250.193.164)  31.892 ms  31.871 ms  31.851 ms
```

Figure 2: Output for traceroute

(iii) arp

The `arp` Command is a TCP/IP utility and Microsoft Windows command for viewing and modifying the local Address Resolution Protocol (ARP) cache, which contains recently resolved MAC addresses of Internet Protocol (IP) hosts on the network.

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
TEJASWINICHIDURALA.msho  ether   00:15:5d:ef:49:3a   C                     eth0
```

Figure 3: A section of the output for arp

(iv) ifconfig

- The `ifconfig` (interface configurator) used to initialize an interface, assign IP Address to interface and enable or disable interface on demand.
- Using this command, we can view the IP Address and Hardware / MAC address assign to interface.
- The output from ifconfig has three main parts:
    1. **Status Line**: This line contains the interface name and status flags currently associated with the interface. Also, it includes MTU (Maximum Transmission Unit) and the index number of the interface. This line determines the current state of the interface.
    2. **IP address information line**:This line includes the IPv4/IPv6 address that is configured for the interface. For an IPv4 address, the configured netmask and broadcast address are also displayed.
    3. **MAC Address Line**: For an IPv4 address, the third line shows the MAC address (Ethernet layer address) that is assigned to the interface.

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.24.138.36  netmask 255.255.240.0  broadcast 172.24.143.255
        inet6 fe80::215:5dff:fe1c:e142  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:1c:e1:42  txqueuelen 1000  (Ethernet)
        RX packets 752  bytes 391271 (391.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 714  bytes 107362 (107.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 549  bytes 138531 (138.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 549  bytes 138531 (138.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 4: Output for ifconfig

(v) hostname

The `hostname` command is used to retrieve the host name of a computer or network node in a network. Hostnames are specific names or character strings that refer to a host and make it usable for the network and people.

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ hostname
TEJASWINICHIDURALA
```

Figure 5: Output for hostname

(vi) Look at the following files in your linux system and write what the files are for?

`/etc/hostname`

This file stores the system's host name, which is the FQDN (Fully Qualified Domain Name) of the system.

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ cat /etc/hostname
TEJASWINICHIDURALA
```

Figure 6: Contents of the hostname

`/etc/hosts`

The /etc/hosts is an operating system file that translate hostnames or domain names to IP addresses.

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ cat /etc/hosts
# This file was automatically generated by WSL. To stop automatic generation of this file, add the following entry to /etc/wsl.conf:
# [network]
# generateHosts = false
127.0.0.1       localhost
127.0.1.1       TEJASWINICHIDURALA.     TEJASWINICHIDURALA

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Figure 7: Contents of the hosts

`/etc/resolv.conf`

his file contains the list of name servers that are used by your host for DNS resolution. If you are using DHCP(Dynamic Host Configuration Protocol), this file is automatically populated with DNS record issued by DHCP server.

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ cat /etc/resolv.conf
# This file was automatically generated by WSL. To stop automatic generation of this file, add the following entry to /etc/wsl.conf:
# [network]
# generateResolvConf = false
nameserver 10.255.255.254
```

Figure 8: Contents of the resolv.conf files

`/etc/protocols`

The /etc/protocols file contains information regarding the known protocol. For each protocol, a single line should be present with the following information:
`official-protocol-name` `protocol-number` `aliases` . # is used for comments regarding the protocols.

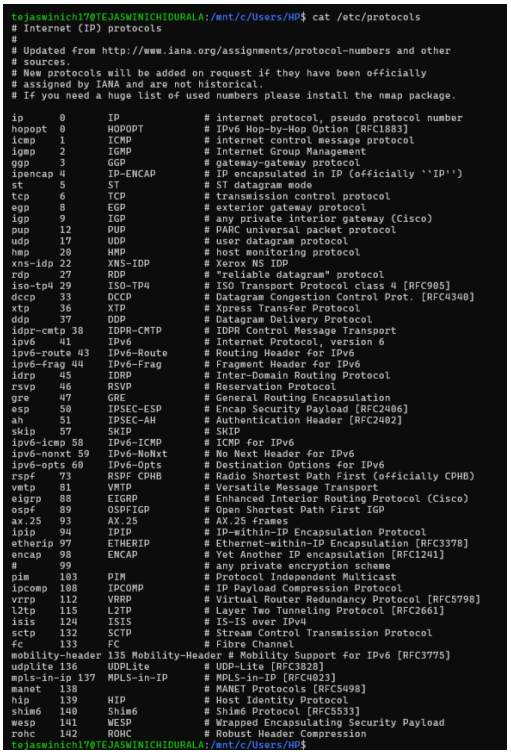

Figure 9: A section of the contents of the protocols file

`/etc/services`

The /etc/services file contains a list of network services and ports mapped to them. Most Internet services are assigned a specific port for their use. When a client opens a connection across the network to a server, the client uses the port to specify which service it wishes to use. This file serves as a small local database to store this information. For each service, this file specifies the service's 'well-known port number', and notes whether the service is available as a TCP (connection-oriented) or UDP (connectionless) service.

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ cat /etc/services
# Network services, Internet style
#
# Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
#
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
domain          53/tcp                          # Domain Name Server
domain          53/udp
bootps          67/udp
bootpc          68/udp
tftp            69/udp
gopher          70/tcp                          # Internet Gopher
finger          79/tcp
http            80/tcp          www             # WorldWideWeb HTTP
kerberos        88/tcp          kerberos5 krb5 kerberos-sec     # Kerberos v5
kerberos        88/udp          kerberos5 krb5 kerberos-sec     # Kerberos v5
iso-tsap        102/tcp         tsap            # part of ISODE
```

Figure 10: A section of the contents of the services file

Q2. Answers for Task 2: Warm-Up Questions

(i) What is your machine's hostname and IP address? How did you get this information?

My machine's hostname is `TEJASWINICHIDURALA` ,using command hostname or cat /etc/hostname. And the IP address assigned to it is `172.24.138.36` was obtained using the `ifconfig` command, next to the eth0 label.

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ hostname
TEJASWINICHIDURALA
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.24.138.36  netmask 255.255.240.0  broadcast 172.24.143.255
        inet6 fe80::215:5dff:fe1c:e142  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:1c:e1:42  txqueuelen 1000  (Ethernet)
        RX packets 950  bytes 405556 (405.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 862  bytes 116446 (116.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 739  bytes 201439 (201.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 739  bytes 201439 (201.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 11: eth0 section of ifconfig output

(ii) What is the next hop router's IP address and MAC address? How did you get this information?

The next hop router's IP address is `172.24.128.1` .Its MAC Address is `00:15:5d:ef:49:3a` . This information is found using the `arp` command. On my Windows system, the same is done using

`ipconfig` and `arp -a` .

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ traceroute google.com
traceroute to google.com (142.250.195.110), 30 hops max, 60 byte packets
 1  TEJASWINICHIDURALA.mshome.net (172.24.128.1)  0.645 ms  0.550 ms  0.708 ms
 2  10.200.224.2 (10.200.224.2)  8.786 ms  7.848 ms  8.466 ms
 3  10.240.0.1 (10.240.0.1)  8.523 ms  8.435 ms  8.339 ms
 4  internet.iitdh.ac.in (10.240.240.1)  11.227 ms  11.152 ms  11.126 ms
 5  * * *
 6  * * *
 7  103.120.29.72.static-delhi.powertel.in (103.120.29.72)  30.811 ms  30.213 ms  30.205 ms
 8  72.14.209.113 (72.14.209.113)  29.501 ms  32.448 ms  32.195 ms
 9  142.250.209.75 (142.250.209.75)  32.887 ms 142.251.54.79 (142.251.54.79)  32.016 ms 142.250.209.75 (142.250.209.75)  33.093 ms
10  142.251.55.71 (142.251.55.71)  31.751 ms  31.997 ms  32.295 ms
11  maa03s39-in-f14.1e100.net (142.250.195.110)  33.798 ms  33.855 ms  36.310 ms
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
TEJASWINICHIDURALA.msho  ether   00:15:5d:ef:49:3a   C                     eth0
```

(iii) What is the local DNS server's IP address? How did you get this information?

The local DNS server's IP address is `10.255.255.254` . This was obtained by looking at the contents of `/etc/resolv.conf` .

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ grep "nameserver" /etc/resolv.conf
nameserver 10.255.255.254
```

Figure 12: Name Server IP Address

(iv) What do the numbers in the file /etc/protocols represent?

The (1-byte) numbers in the file `/etc/protocols` represents the protocol number, which is used to identify the protocol.

(v) What is the port number associated with applications: ssh, ftp, nfs, smtp (email)? How did you get this information?

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ grep "ssh" /etc/services
ssh             22/tcp                          # SSH Remote Login Protocol
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ grep "ftp" /etc/services
ftp-data        20/tcp
ftp             21/tcp
tftp            69/udp
ftps-data       989/tcp                         # FTP over SSL (data)
ftps            990/tcp
venus-se        2431/udp                        # udp sftp side effect
codasrv-se      2433/udp                        # udp sftp side effect
gsiftp          2811/tcp
zope-ftp        8021/tcp                        # zope management by ftp
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ grep "nfs" /etc/services
nfs             2049/tcp                        # Network File System
nfs             2049/udp                        # Network File System
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ grep "smtp" /etc/services
smtp            25/tcp          mail
submissions     465/tcp         ssmtp smtps urd # Submission over TLS [RFC8314]
```

Figure 13: Applications Port Numbers

The port numbers for the applications given are as follows:

- ssh: port 22
- ftp: port 21
- nfs: port 2049
- smtp: 25

This is obtained using the `/etc/services` file, in combination with the grep tool.

(vi) How many of these questions can you answer for the phone running on android/iOS?

In theory, we should be able to obtain all of the required answers for a phone as well. The only thing is that we would need some kind of terminal-like setup to find these things. We'd have to use some application that gets such details!

Q3. Answers for Task 3

(i) The Unix utility Ping can be used to find the RTT to various Internet hosts. Read the man page for ping, and use it to find the RTT to the following websites. `www.amazon.in` and `www.iitb.ac.in`

(a) Explain the results that you obtain; For example, the success and failure of the Ping

We have obtained results of values for `www.amazon.in` , while not for `www.iitb.ac.in` , since the website may have blocked ping requests. This shows that we are able to form a connection to `www.amazon.in` , but not with `www.iitb.ac.in` .

(b) What are the reasons for the values of RTTs that you see?

```
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ ping www.amazon.in
PING d1elgm1ww0d6wo.cloudfront.net (52.84.8.199) 56(84) bytes of data.
64 bytes from server-52-84-8-199.maa51.r.cloudfront.net (52.84.8.199): icmp_seq=1 ttl=245 time=40.4 ms
64 bytes from server-52-84-8-199.maa51.r.cloudfront.net (52.84.8.199): icmp_seq=2 ttl=245 time=40.7 ms
64 bytes from server-52-84-8-199.maa51.r.cloudfront.net (52.84.8.199): icmp_seq=3 ttl=245 time=41.1 ms
64 bytes from server-52-84-8-199.maa51.r.cloudfront.net (52.84.8.199): icmp_seq=4 ttl=245 time=41.1 ms
^C
--- d1elgm1ww0d6wo.cloudfront.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 40.382/40.821/41.142/0.313 ms
tejaswinich17@TEJASWINICHIDURALA:/mnt/c/Users/HP$ ping www.iitb.ac.in
PING www.iitb.ac.in (103.21.124.133) 56(84) bytes of data.
^C
--- www.iitb.ac.in ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5658ms
```

Figure 14: Output of ping

The initial value is quite high since it tries to find the path to locate the destination. The later RTT values fluctuate due to traffic and other factors. Multiple Ping requests are sent, to check consistency along the connection.

(ii) Read the man page for the Unix utility Traceroute and use it for the website `www.amazon.in`

(a) Explain what you see. Whenever successful, draw a network map from your machine to the destination, which includes the hop addresses obtained from Traceroute.

After running the `$ traceroute www.amazon.in` command, the observed route took `30` hops to reach `www.amazon.in` . Some intermediate gateways did not provide details, indicated by asterisks (*). Below is the network map observed:

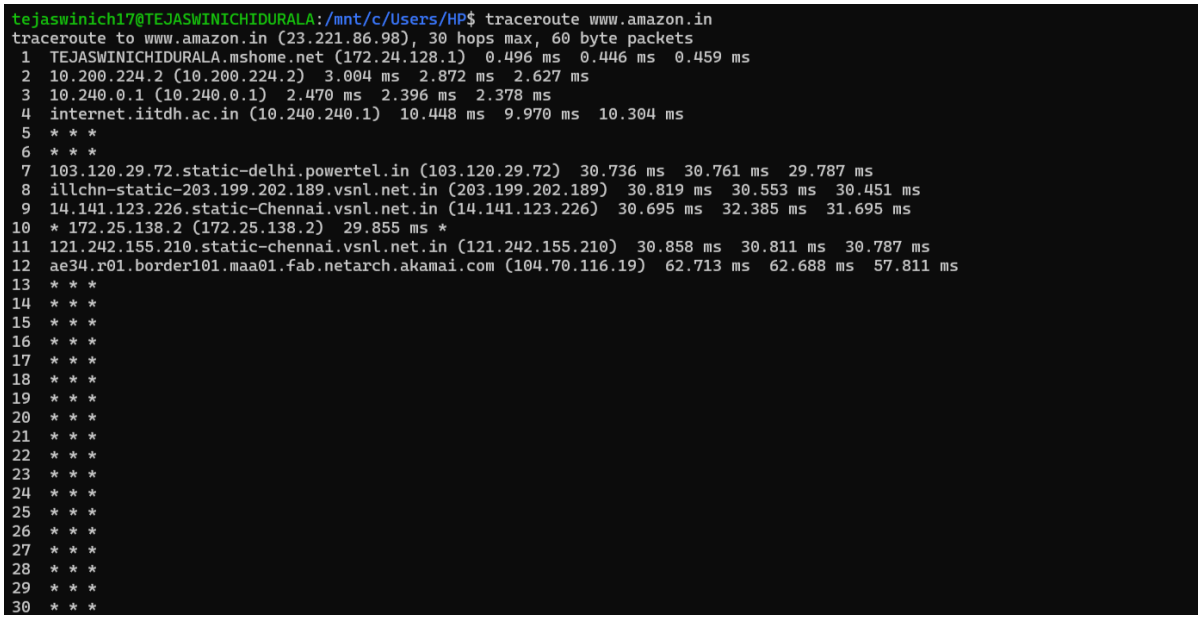

Figure 15: Output of traceroute

The network map shows the hop sequence: We observe that it took `30` hops for the packet to reach www.amazon.in. A network map would look like:
172.24.128.1(Device) → 10.200.224.2 → 10.240.0.1 → 103.120.29.72 → 203.199.202.189 → 14.141.123.226 → 172.25.138.2 → 121.242.155.210 → 104.70.116.19 (Destination IP) and asterisks(*) imply that gateways did not provide details like ip address.

(b) How can you change the maximum hop number?

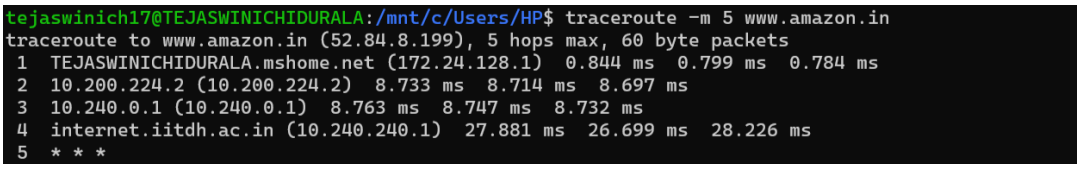

Figure 16: Output of maximum hop number

You can change the maximum hop number in `traceroute` by using the `-m` (default is 30).
`traceroute -m <max_hops> <destination>`

- `-m <max_hops>` : Specifies the maximum hop count
- `<destination>` : The target hostname or IP address (e.g.www.google.com)

For `$ traceroute -m 5 www.amazon.in` where `<max_hops>` =5 and `<destination> =www.amazon.in`

(c) What do the three timestamps signify in the result of Traceroute?

The three timestamps signify the RTT (Round-Trip Time) values (in milliseconds) for 3 signal packets that reach a certain point in the list of hops (and return back).

(d) What is the use of TTL (Time To Live) field in ICMP packets?

TTL field is a counter that decreases in value after each hop of the packet. It is a time limit imposed on the data packet to be in-network before being discarded. It is an 8-bit binary value set in the Internet Protocol (IP) Header by the sending host. The purpose of a TTL is to prevent data packets from being circulated forever in the network.