Troubleshooting en perdida de paquetes

Troubleshooting quiere decir "Solución de problemas o Recursos para solucionar problemas", para esta seccion lo aplicaremos para la perdida de paquetes de red.

Cuando se administra un servidor o un equipo este puede llegar a tener problemas de red, los cuales van desde lo fisico a lo virtual(configuracion) en las distribuciones linux estas cuentan con herramientas para poder intuir el posible error que lo provoca.

Comando ping

Este comando nos permite checar si existe comunicación entre un equipo remoto y el nuestro.

```
#sintaxis para pedir ciertas veces si existe conexion en un equipo remoto
ping -c <numero de veces de consulta> <ip>
#ejemplo
ping -c 4 8.8.8.8
```

El resultado que nos da el comando anterior demuestra que existe conexion con el equipo remoto 8.8.8.8 ya que en los parametros de la parte inferior dice que de 4 paquetes tramitidos, estos fueron recividos en su totalidad en un tiempo de 300 ms.

```
[user@linux ~]$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=22.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=23.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=22.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=22.3 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 22.192/22.735/23.645/0.580 ms
```

Para fines didacticos se activo del firewall en modo panico para simulara un fallo con la conexion el resultado que produce seria que los 4 paquetes que fueron enviados, todos estos no fueron recibidos tal y como se muestra a continuacion.

```
[user@linux ~]# ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3085ms
```

existe ocasiones que de 4 paquete enviados 2 son recibidos y 2 son perdidos, lo cual se puede llegar a deducir que existe intermitencia en la conexion.

Comando mtr

Este comando nos permite ver los saltos(traceroute) que realiza el ordenador al host remoto al cual se desea comunicar por ejemplo.

```
          My traceroute [v0.95]
fedora (10.0.2.15) -> 8.8.8.8 (8.8.8.8)          2022-10-06T15:00:27-0500
keys: Help Display Mode    Restart statistics  order of fields quit
                                Packets            Pings
Host                          Loss%  Snt   Last   Avg  Best  Wrst StDev
1. _gateway                     0.0%   8     0.7   0.6   0.2   0.3   0.1
2. 192.168.1.254                  0.0%   8     0.7   0.6   0.2   0.3   0.1
3. dns.google                   0.0%   7     0.7   0.6   0.2   0.3   0.1
```

Dentro de una red interna se veria mejor el efecto ya que uno conoce aproximandamente que dispositivos existen dentro de la red.

Comando ifstat

Es una herramienta para informar la actividad de un interfaz.

- Ejemplo

```
[user@linux ~]$ ifstat
             #host          #tuordenador
#kernel        #EntradaPaq     #SalidaPaq     #EntradaData    #SalidaData
Interface       RX Pkts/Rate    TX Pkts/Rate    RX Data/Rate    TX Data/Rate
              RX Errs/Drop    TX Errs/Drop    RX Over/Rate    TX Coll/Rate
lo                 42 0           42 0         5034 0         5034 0
                   0 0            0 0            0 0            0 0
enp0s3            21374 0         9055 0       23389K 0        1831K 0
                   0 0            0 0            0 0            0 0
```

podemos ver que en paquetes enviados por nuesta interfaz en0s3(TX Pkts) no tuvo ningun paquete con error(TX errs) o caido(Drop) y sucede lo mismo con los paquetes que entraron(RX pkts) por la misma interfaz.

Comando tcpdump

Es una herramienta la cual analiza el trafico que circula por la red de todas las interfaz que cuenta su dispositivo.

- Ejemplo de salida de este comando:

```
[user@linux ~]$ sudo tcpdump

dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:39:01.575406 IP 8.2.110.21.https > localhost.51002: Flags [P.], seq 651654678:651654709, ack
503686153, win 65535, length 31
11:39:01.575625 IP localhost.51002 > 8.2.110.21.https: Flags [.], ack 31, win 62780, length 0
11:39:01.575687 IP 8.2.110.21.https > localhost.51002: Flags [F.], seq 31, ack 1, win 65535, length 0
11:39:01.582224 IP localhost.60581 > _gateway.domain: 31841+ [1au] PTR? 21.110.2.8.in-addr.arpa.
(52)
11:39:01.622870 IP localhost.51002 > 8.2.110.21.https: Flags [.], ack 32, win 62780, length 0
11:39:01.727822 IP _gateway.domain > localhost.60581: 31841 NXDomain 0/1/1 (120)
11:39:01.728820 IP localhost.60581 > _gateway.domain: 31841+ PTR? 21.110.2.8.in-addr.arpa. (41)
```

- Selecionar el trafico de red de una interfaz especifica

```
[user@linux ~]$ sudo tcpdump -i enp0s3

dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:49:42.388944 IP localhost.49154 > 143.244.35.229.https: Flags [.], ack 648537732, win 65535,
length 0
11:49:42.389131 IP localhost.37554 > 38.71.2.236.https: Flags [.], ack 649856621, win 64064, length 0
11:49:42.389522 IP localhost.traceroute > e2a.google.com.https: Flags [.], ack 656837815, win 62780,
length 0
11:49:42.389576 IP localhost.52408 > ext-189-247-217-56.uninet.net.mx.https: Flags [.], ack
644805732, win 63970, length 0
11:49:42.389602 IP localhost.53120 > ext-189-247-217-33.uninet.net.mx.https: Flags [.], ack
643410929, win 62780, length 0
11:49:42.389625 IP localhost.52396 > ext-189-247-217-56.uninet.net.mx.https: Flags [.], ack
644627159, win 62780, length 0
11:49:42.389735 IP 143.244.35.229.https > localhost.49154: Flags [.], ack 1, win 65535, length 0
```