ICMP
(Internet Control Message Protocol)

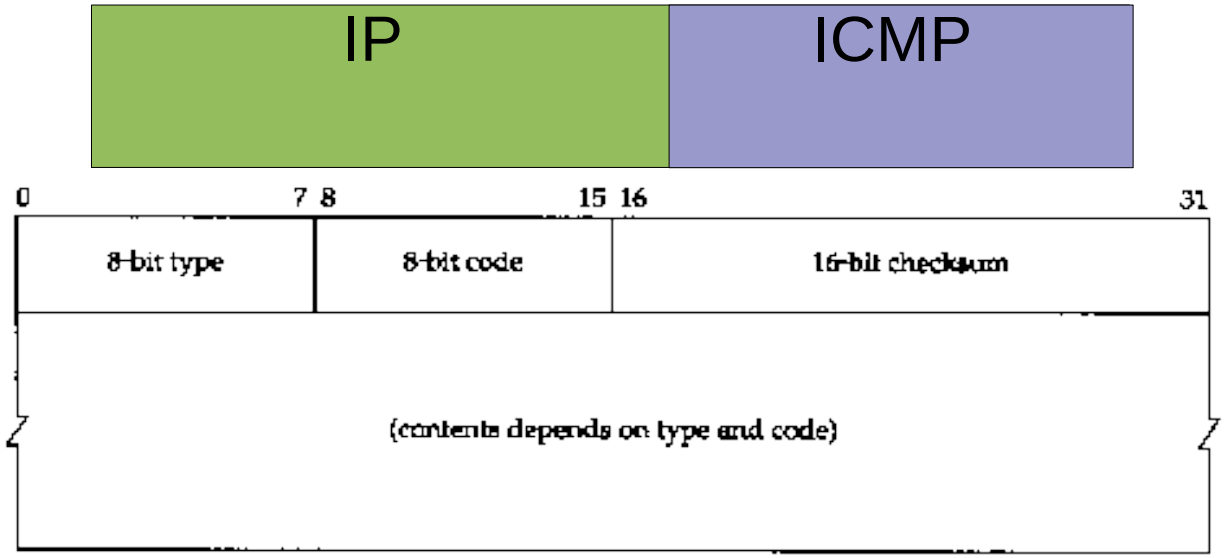
ICMP

(Internet Control Message Protocol)

- Protocolo de L3.
- Protocolo “Helper” de IP.
- IP carece de control, el mismo es dado por un protocolo auxiliar.
- ICMP no le agrega confiabilidad a IP, solo brinda un “feedback” para poder resolver problemas en la red.
- ICMP podría ser prescindible de en IPv4, aunque en la RFC se indica que se debe implementar en cada módulo IP.
- Definido en RFC-792.

ICMP (Cont.)

- ICMP se encapsula en IP.
- ICMP no es un protocolo de transporte, ya que no fue concebido para llevar datos de usuario.
- Formato de Mensaje:



Fuente: TCP/IP Illustrated, Vol. 1

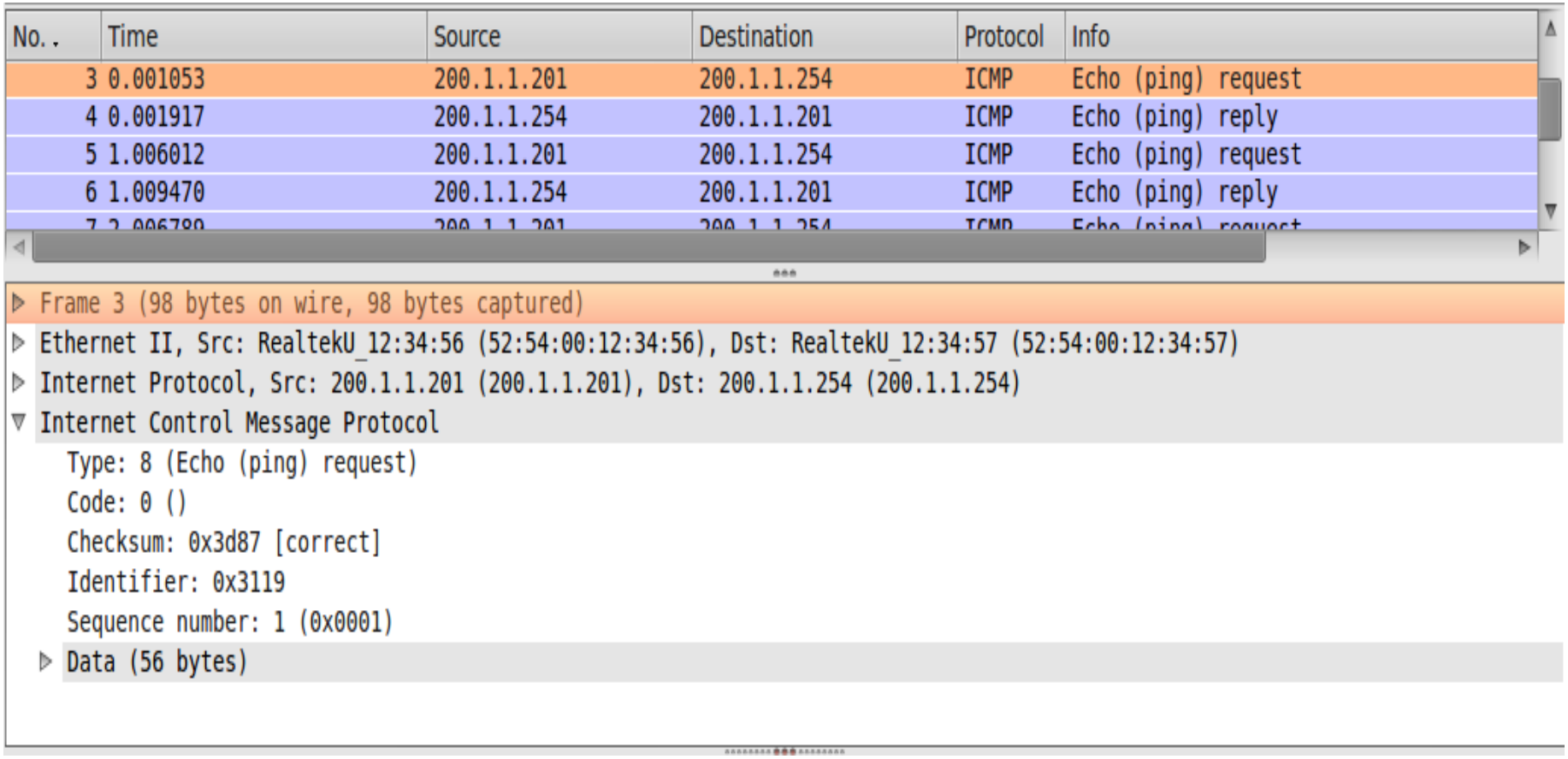
MENSAJES ICMP

- Algunos Tipos de Mensajes ICMP:
  - Echo Request/Echo Reply (PING).
  - Destino Inalcanzable.
  - TTL expirado.
  - Source Quench (Control de Congestión).
  - Redirección de Ruta.
  - Address Mask y Timestamp.

ICMP PING (Echo)

- Pensado para probar conectividad IP entre dos hosts.
- Sirve para medir el RTT min/avg/max/dev y loss, de esta forma poder diagnosticar problemas.
- Packet INternet Gopher, el nombre basado en el sonido de un sonar de un submarino al escanear.
- Si un nodo recibe un ICMP ***Echo Request***, debe responder copiando el contendio con un ***Echo Reply (PONG)***. RFC-1122.
- Actualmente, muy desprestigiado ;-) Se filtra.

ICMP PING (Echo) (Cont.)



No.	Time	Source	Destination	Protocol	Info
3	0.001053	200.1.1.201	200.1.1.254	ICMP	Echo (ping) request
4	0.001917	200.1.1.254	200.1.1.201	ICMP	Echo (ping) reply
5	1.006012	200.1.1.201	200.1.1.254	ICMP	Echo (ping) request
6	1.009470	200.1.1.254	200.1.1.201	ICMP	Echo (ping) reply

```
▷ Frame 3 (98 bytes on wire, 98 bytes captured)
▷ Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Dst: RealtekU_12:34:57 (52:54:00:12:34:57)
▷ Internet Protocol, Src: 200.1.1.201 (200.1.1.201), Dst: 200.1.1.254 (200.1.1.254)
▽ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0 ()
    Checksum: 0x3d87 [correct]
    Identifier: 0x3119
    Sequence number: 1 (0x0001)
  ▷ Data (56 bytes)
```

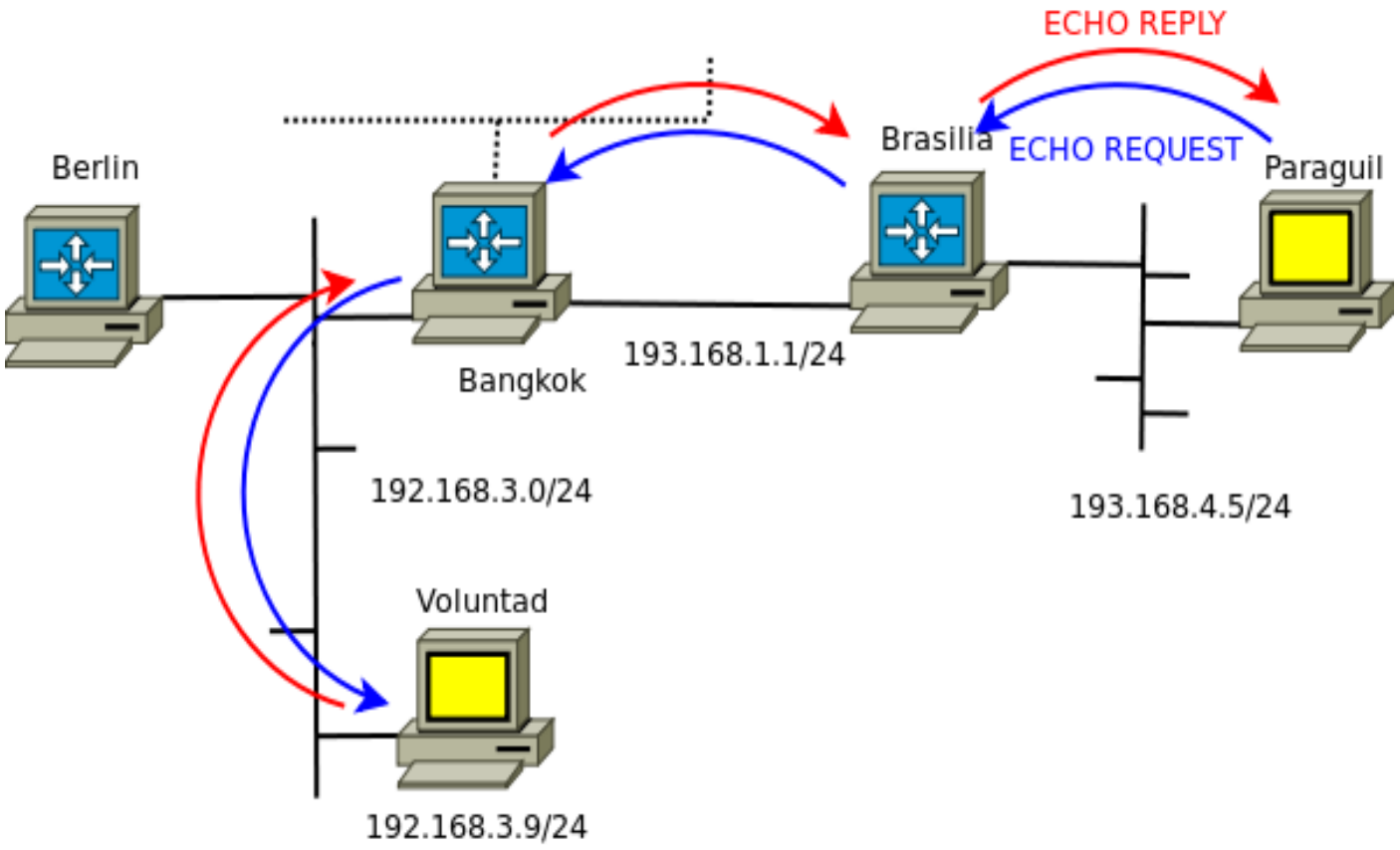
ICMP PING (Echo) (Cont.)

- ***Echo Request*** , ***Echo Reply***:

```
andres@h1(paraguil):~$ ping -c 3 193.168.3.9
PING 193.168.3.9 (193.168.3.9) 56(84) bytes of data.
64 bytes from 193.168.3.9: icmp_seq=1 ttl=53 time=149 ms
64 bytes from 193.168.3.9: icmp_seq=2 ttl=53 time=150 ms
64 bytes from 193.168.3.9: icmp_seq=3 ttl=53 time=147 ms


--- 193.168.3.9 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time
2002ms
rtt min/avg/max/mdev = 147.498/149.014/150.128/1.197 ms
```

ICMP PING (Echo) (Cont.)

- ***Echo Request*** , ***Echo Reply***:



ICMP Destino Inalcanzable

- Para indicar que una red, un host, un puerto es inalcanzable, diferentes causas.
  - Host Inalcanzable (Host Unreachable):
    - Posibles causas, no esta encendido el host, no responde ARP.
  - Red Inalcanzable (Network Unreachable):
    - No tiene el router una ruta en la tabla de ruteo a esta red.
  - Puerto Inalcanzable (Port Unreachable):
    - No hay un proceso UDP en el puerto.
  - Los mensajes requieren fragmentación.
  - El mensaje fue filtrado (admin).
  - Otros.

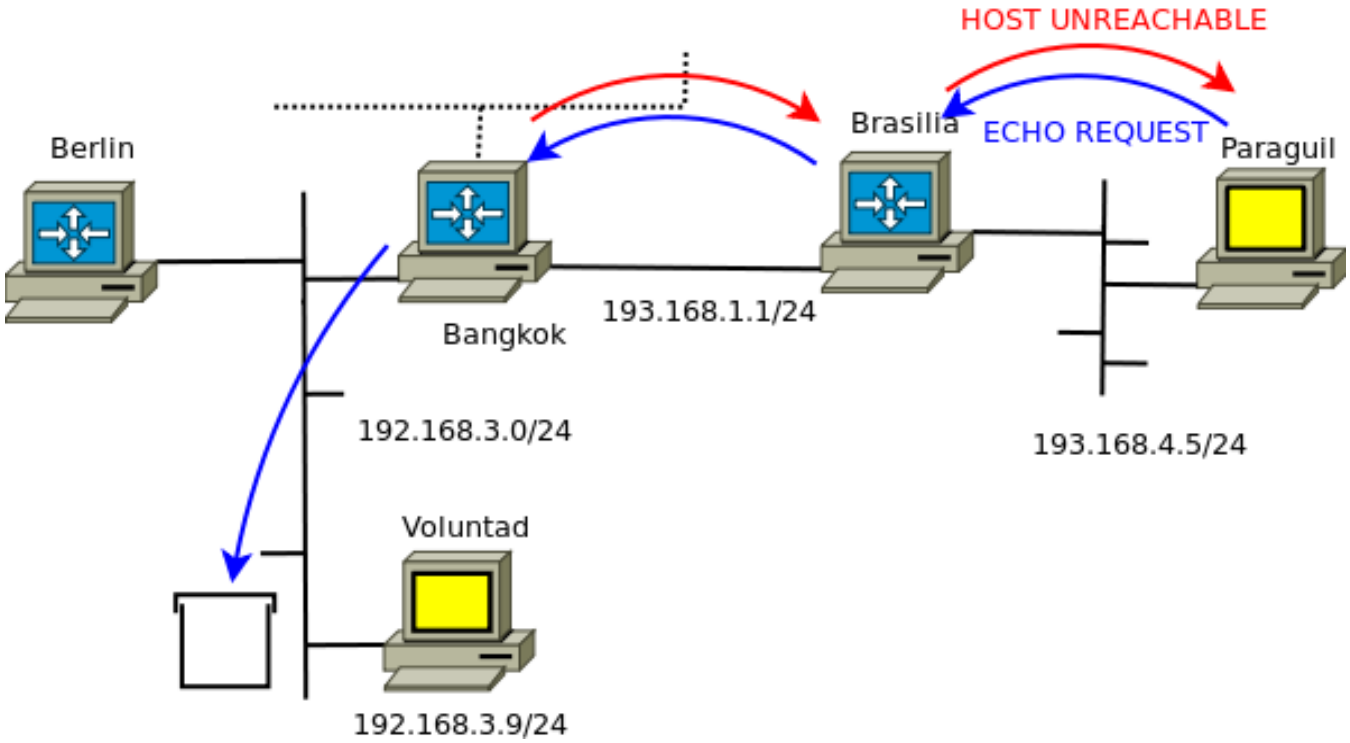
ICMP Destino Inalcanzable
(Cont.)

- ***Echo Request*** , ***Host Unreachable***:

```
andres@h1(paraguil):~$ ping -c 3 193.168.3.10
PING 193.168.3.10 (193.168.3.10) 56(84) bytes of data.
From 193.168.1.2 icmp_seq=1 Destination Host Unreachable
From 193.168.1.2 icmp_seq=2 Destination Host Unreachable
From 193.168.1.2 icmp_seq=3 Destination Host Unreachable


--- 193.168.3.10 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet
loss, time 2007ms
, pipe 3
```

ICMP Destino Inalcanzable
(Cont.)

- ***Echo Request*** , ***Host Unreachable***:



ICMP TTL Expirado

- El tiempo de vida ha expirado. En realidad es el hop count con el cual salió el mensaje ha expirado.
- Time Exceeded:
  - Tiempo Excedido en viaje.
  - Tiempo Excedido en re-ensamblado.
- TTL en IP, no solo ICMP.
- Valor máximo de TTL=255.
- Puede salir con otro valor.
- Si TTL == 0, pero ya llegó a la red destino debería enviarse.
- Utilizado por `traceroute(8)` con UDP o ICMP.

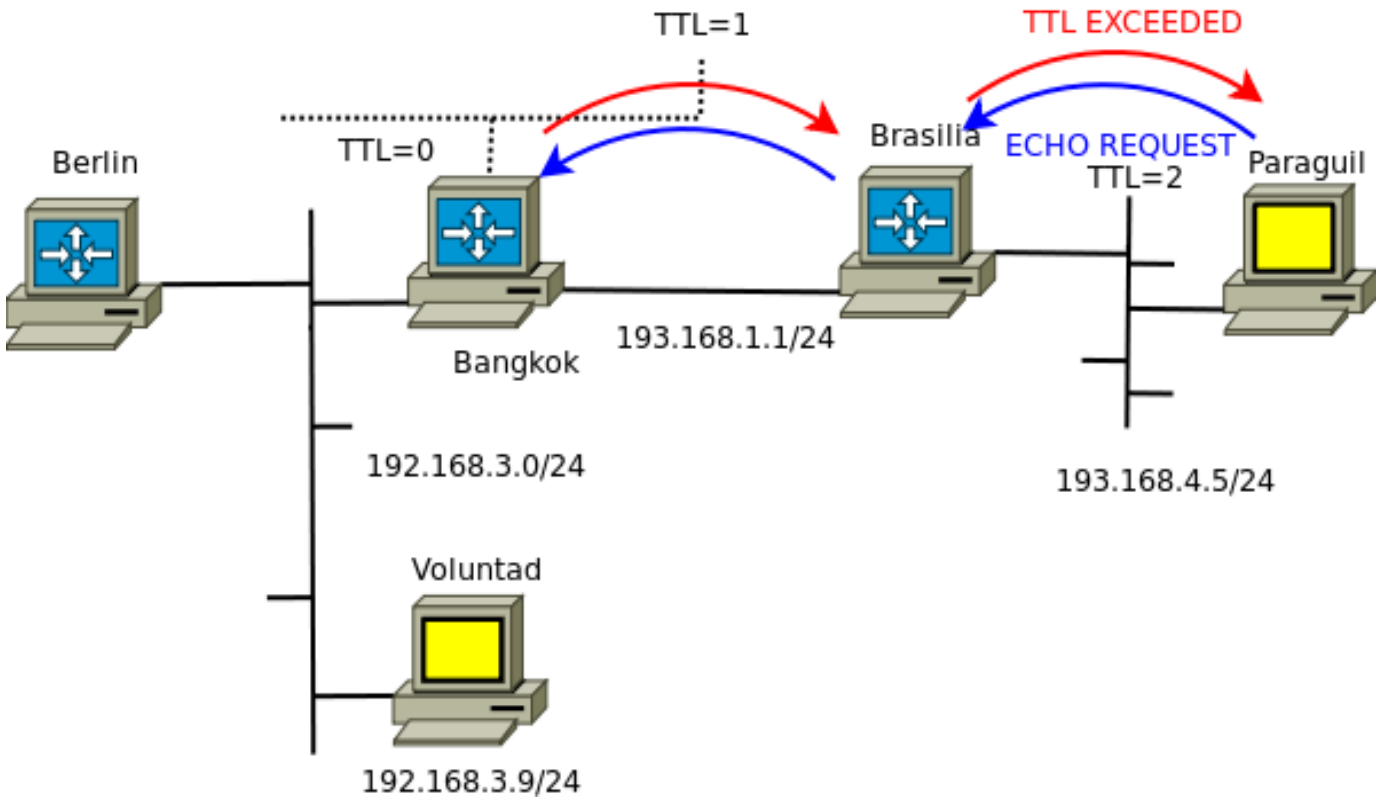
ICMP TTL Expirado (Cont.)

- ***Echo Request*** , ***TTL Exceeded***:

```
andres@h1(paraguil):~$ ping -c 2 -t 2 193.168.50.50
PING 193.168.50.50 (193.168.50.50) 56(84) bytes of
data.
From 193.168.1.2 icmp_seq=1 Time to live exceeded
From 193.168.1.2 icmp_seq=2 Time to live exceeded
From 193.168.1.2 icmp_seq=3 Time to live exceeded

--- 193.168.50.50 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100%
packet loss, time 2003ms
```

ICMP TTL Expirado (Cont.)

- ***Echo Request*** , ***TTL Exceeded***:



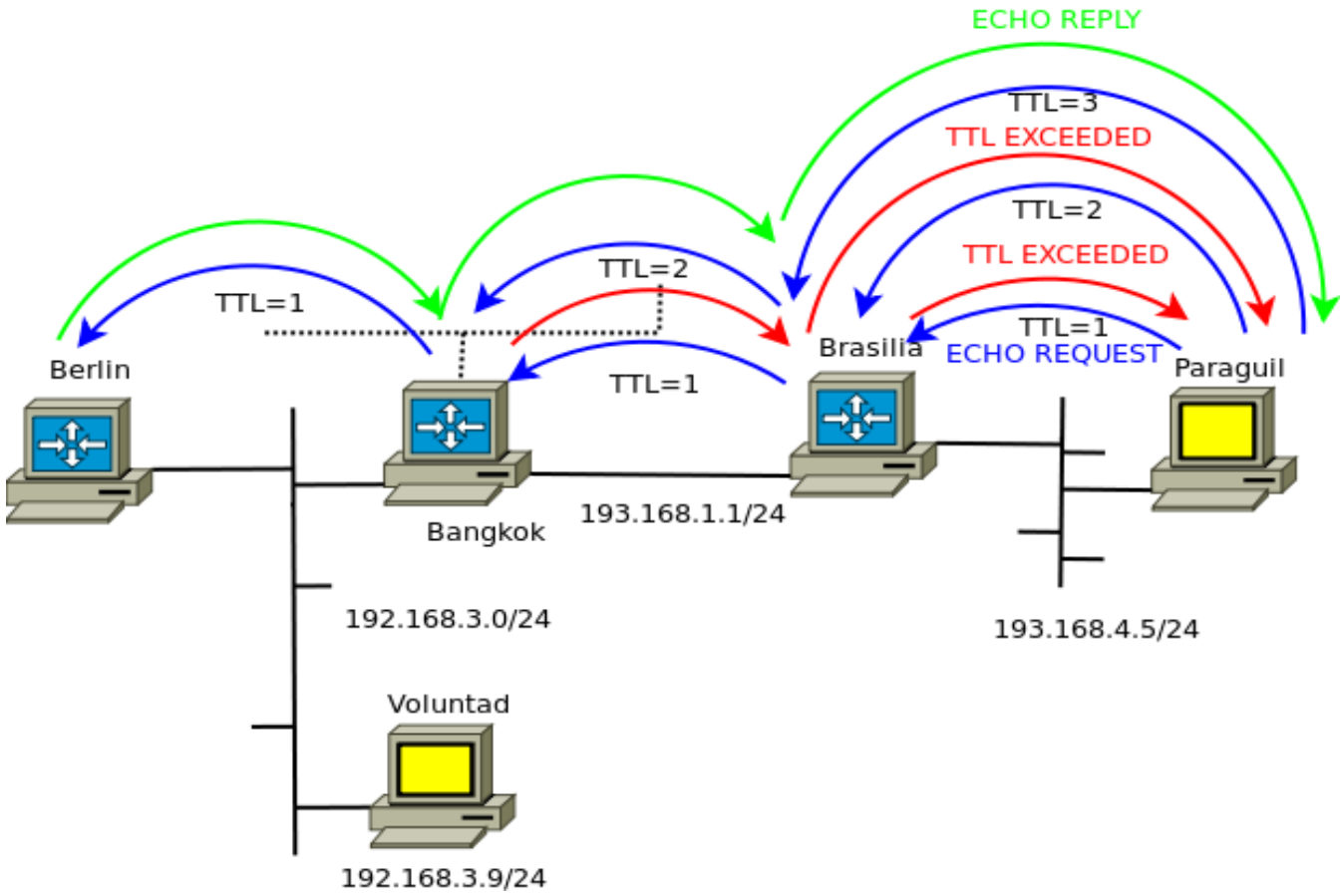
ICMP TTL Expirado (Cont.)

- ***Echo Request*** , ***TTL Exceeded*** , ***Echo Reply***:

```
root@h1(paraguil)~# traceroute -n -I 193.168.3.254
traceroute to 193.168.3.254 (193.168.3.254), 30 hops max,
60 byte packets

 1  193.168.4.65  3.698 ms  3.740 ms  4.405 ms
 2  193.168.1.2  9.185 ms  9.809 ms  14.130 ms
 3  193.168.3.254  14.973 ms  15.073 ms  17.312 ms
```

ICMP TTL Expirado (Cont.)

- ***Echo Request*** , ***TTL Exceeded*** , ***Echo Reply***:



ICMP Route Redirect

- ***Echo Request*** , ***Route Redirect*** , ***Echo Reply***:

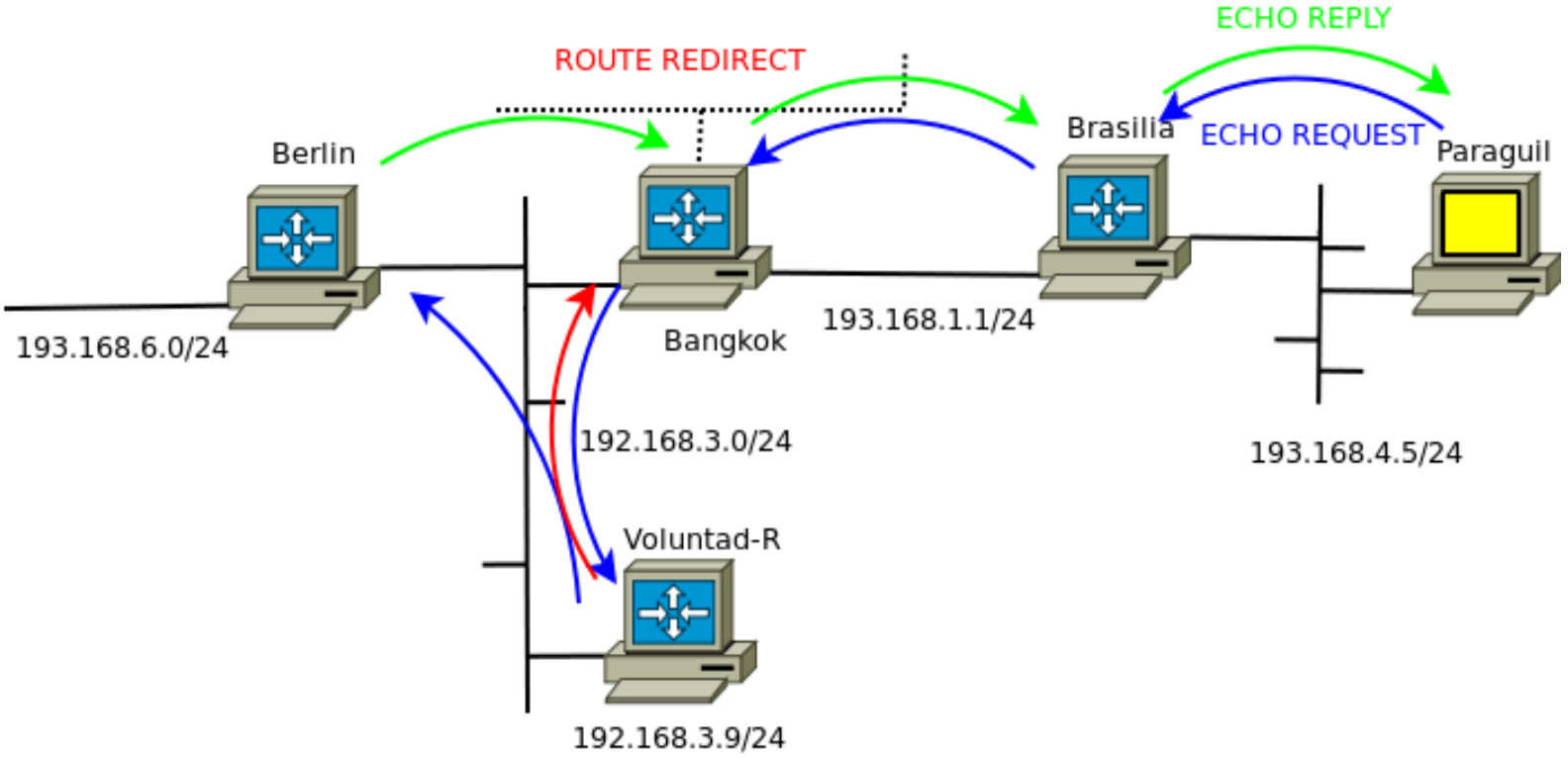
```
andres@h1(paraguil):~$ ping 193.168.6.1

andres@r2(bangkok):~$ netstat -nr
Destination     Gateway         Genmask           Flag Iface
...
193.168.6.0     193.168.3.9     255.255.255.0     G       e0
...
```

Luego del Redirect:

```
andres@r2(bangkok):~$ netstat -nr
Destination     Gateway         Genmask            Flag Iface
…
193.168.6.0     193.168.3.9     255.255.255.0      G      e0
193.168.6.1     193.168.3.254   255.255.255.255    DH     e0
...
```

ICMP Route Redirect (Cont.)

- ***Echo Request*** , ***Route Redirect*** , ***Echo Reply***:



Hoy desaconsejado y desactivado.

Referencias:

- Richard Stevens. TCP/IP Illustrated. Vol 1. The Protocols.

.

- Douglas Comer. Internetworking with TCP/IP. Vol 1.

- Data & Computer Communications (6th Edition), William Stallings.