Redes II

Eduardo Grosclaude

2014-08-13

[V0.1 - Material en preparación, se ruega no imprimir mientras aparezca esta nota]

Resumen

En este escrito se presenta la descripción y material inicial de la asignatura **Redes II**, para la carrera de Tecnicatura Universitaria en Administración de Sistemas y Software Libre, de la Universidad Nacional del Comahue.

La materia es electiva, cuatrimestral en modalidad presencial y las clases son de carácter teórico-práctico, desarrolladas en forma colaborativa. Está preparada con los objetivos generales de **actualizar y ampliar el instrumental de trabajo en ambientes de redes**.

Índice

Parte I
La asignatura

1. Objetivos

De la carrera

Según el documento fundamental de la Tecnicatura, el Técnico Superior en Administración de Sistemas y Software Libre estará capacitado para:

- Desarrollar actividades de administración de infraestructura. Comprendiendo la administración de sistemas, redes y los distintos componentes que forman la infraestructura de tecnología de una institución, ya sea pública o privada.
- Aportar criterios básicos para la toma de decisiones relativas a la adopción de nuevas tecnologías libres.
- Desempeñarse como soporte técnico, solucionando problemas afines por medio de la comunicación con comunidades de Software Libre, empresas y desarrolladores de software.
- Realizar tareas de trabajo en modo colaborativo, intrínseco al uso de tecnologías libres.
- Comprender y adoptar el estado del arte local, nacional y regional en lo referente a implementación de tecnologías libres. Tanto en los aspectos técnicos como legales.

De la asignatura

- Actualizar y ampliar el instrumental de trabajo en ambientes de redes.

2. Cursado

- Cuatrimestral de 16 semanas, 4 horas semanales, 64 horas totales
- Clases teórico-prácticas presenciales
- Promocionable con trabajos prácticos

3. Contenidos

Contenidos mínimos

- Switching.
- Redes Privadas Virtuales.
- Balance de carga y Alta Disponibilidad en redes.

Programa

1. Switching
   - Red Ethernet, dominio de colisión y dominio de Broadcast
   - Bridges, switches, arquitectura y funcionamiento.
   - VLANs, trunking
2. Redes Privadas Virtuales
   - Encapsulamiento
   - VPN de nivel 2 y de nivel 3
   - Configuración y administración de OpenVPN

- Configuración de ruteo y de firewalling en VPN

3. Alta Disponibilidad y Balance de carga en Redes
   - Arquitecturas de redundancia
   - Protocolo STP 802.1d
   - Ruteo, Ruteo por origen
   - Firewalls redundantes
   - Clustering de HA, herramientas heartbeat, HAproxy
   - Bonding y modos de configuración
   - Clustering de LB, herramientas LVS, Varnish

4. Bibliografía inicial

1 C., Zimmerman, Joann Spurgeon, Ethernet switches. Sebastopol, CA: O'Reilly Media, 2013.

Parte II
Switching

1. Ethernet

1. ¿Qué módulos del kernel Linux están controlando las interfaces de red de su equipo? ¿Cuáles comandos permiten conocer las marcas y modelos de las placas instaladas? ¿Qué diferencia hay entre placas y chipsets? ¿Cómo se puede investigar cuál módulo corresponde a cuál marca y modelo de placa de red?
2. ¿Qué es el bus PCI y qué son los números de dispositivos asignados? ¿Cuál es la relación entre el bus PCI y los nombres de dispositivos de red en Linux?
3. ¿Qué información aporta el comando ethtool? ¿Qué clases de placas de red soporta? ¿Qué significa *Link detected* en la salida de este comando?
4. ¿Qué información transporta un frame Ethernet? ¿Qué diferencias existen entre los frames que circulan por una Ethernet cableada y una inalámbrica?
5. ¿Qué diferencias existen entre el diseño de la red Ethernet original, implementada con coaxil, y la que está implementada con cableado en estrella, conectada mediante hubs? ¿Qué diferencias existen entre esta última y una implementada con switches?

2. Dominios de colisión y de broadcast

1. ¿Qué es un bridge, qué configuración lleva, qué función realiza sobre los frames que circulan por la red, y cómo aprende su información de trabajo?
2. ¿Existen bridges inalámbricos?
3. ¿A qué se llama segmentación?
4. ¿Un hub es equivalente a un bridge? ¿Un router es equivalente a un bridge? ¿Un switch es equivalente a un bridge?
5. ¿Qué es un frame de broadcast? ¿Qué es un frame unicast? ¿Cómo se distingue un frame de broadcast?
6. ¿Qué protocolos utilizan frames de broadcast? ¿Cómo es aprovechado el mecanismo de broadcast por el protocolo ARP? ¿Qué otros usos podría recibir el mecanismo de broadcast?
7. ¿Qué conducta observan los hosts de la red al recibir un frame de broadcast? ¿En qué casos puede resultar esto un problema y por qué? ¿Cuáles son las contramedidas?
8. ¿Qué es un dominio de colisión? ¿Qué es un dominio de broadcast? ¿Qué tipo de dispositivo es el que delimita la frontera entre dos dominios de colisión? ¿Qué tipo de dispositivo es el que delimita la frontera entre dos dominios de broadcast?
9. ¿Qué efecto tiene la introducción de un bridge en un dominio de colisión? El número de equipos en un mismo dominio de colisión ¿se incrementa o se reduce? ¿Qué efecto tiene esto sobre la probabilidad de colisión?
10. ¿Qué diferencia hay entre un paquete de broadcast y un frame de broadcast? Los routers, ¿repiten los frames de broadcasts?
11. En la figura 1, ¿cuáles son los dominios de colisión y de broadcast que pueden distinguirse? Si el host H1 emite un frame de broadcast, ¿qué otros hosts lo reciben? Si el host H4 emite un broadcast, ¿qué otros hosts lo reciben?
12. En la figura 3, ¿cuáles son los dominios de colisión y de broadcast que pueden distinguirse? Si el host H1 emite un frame de broadcast, ¿qué otros hosts lo reciben?
13. El concepto de dominio de colisión, ¿sigue siendo aplicable en la actualidad, cuando prácticamente la totalidad de las redes usan bridging en lugar de repetidores?
14. El uso de bridges, ¿limita el tráfico de broadcast sobre un segmento de red?

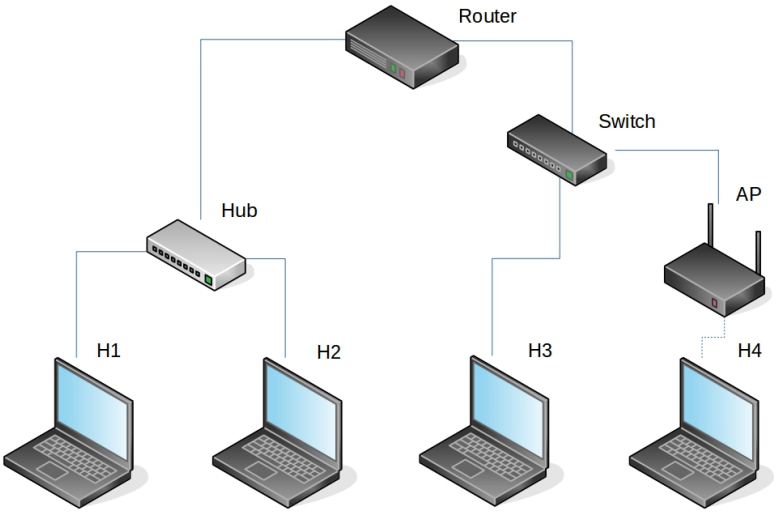

Figura 1: Colisiones y broadcasts

3. Switches

1. ¿Cuál es la función de un switch?
2. ¿Cuántos dominios de colisión hay en una red implementada sobre un switch? ¿Cuántos dominios de broadcast hay en una red implementada sobre un switch?
3. ¿En qué consiste el proceso de conmutación de un frame? ¿Qué modos de conmutación son los más usados?
4. ¿Cómo aprende su información de trabajo un switch? ¿Dónde almacena dicha información? ¿Cómo accede a esta información?
5. ¿Qué debe hacer un switch ante un frame dirigido a una estación ("unicast") cuya dirección destino figura en sus tablas?
6. ¿Qué debe hacer un switch ante un frame dirigido a una estación ("unicast") que no figura en ninguna de sus tablas? ¿Cómo se llama esta acción?
7. ¿Qué debe hacer un switch ante un frame cuya dirección origen no figura en sus tablas?
8. ¿Qué debe hacer un switch ante un frame de broadcast? ¿Cómo se llama esta acción?
9. En una topología compuesta por un árbol de tres switches como en la figura 3, ¿cómo aprenden los switches las direcciones de los equipos que no están directamente conectados? ¿Cuántos dominios de broadcast aparecen en dicha figura?
10. ¿En qué orden aparecen las direcciones destino y origen en el frame Ethernet? ¿En qué orden aparecen las direcciones destino y origen en los paquetes IP y en los segmentos TCP o UDP? ¿De qué forma aprovechan los switches la diferencia?
11. En la figura 4, si el host H1 establece conexión TCP con H3, ¿quiénes más pueden ver el tráfico entre H1 y H3? Si el host H1 establece conexión TCP con H4, ¿quiénes más pueden ver el tráfico entre H1 y H4?
12. ¿Cuántas redes aparecen, respectivamente, en las topologías de figuras 1, 3 y 4? ¿Cuántos espacios de direccionamiento IP diferentes habrá en cada topología?
13. ¿Existen switches inalámbricos? ¿En qué se parecen y en qué se diferencian un switch cableado y un punto de acceso inalámbrico?

14. ¿Qué diferencias existen entre las conexiones de switches en cascada y apiladas (*stacked*)?
15. ¿Qué velocidad suelen tener los ports de un switch? ¿Qué dicen las normas de cableado respecto de la calidad del cable, su longitud y su forma de instalación, para cada caso?
16. Si los ports de un switch tienen una velocidad determinada, ¿tiene sentido conectar a un port un conjunto de hosts capaces de transmitir, en forma agregada, mayor cantidad de bits por segundo que la velocidad admitida por el port? ¿Qué significa *oversubscription*?
17. En una red compartida implementada con hubs, ¿cuál es el ancho de banda obtenido por cada cliente? ¿Y en una red implementada con switches?
18. En la Fig. 2, supongamos que los hosts H1 y H3 mantienen tráfico entre sí al mismo tiempo que H2 y H4 lo hacen entre sí. ¿Cuál será la velocidad máxima de dicho tráfico si el dispositivo es un hub que funciona a 100Mbps? ¿Y si es un switch que funciona a 100Mbps?
19. En aquellos switches con ports de diferentes velocidades, ¿cuáles podrían ser los usos de los ports de mayor velocidad?
20. ¿Qué son los dispositivos de red administrables? ¿En qué consiste el protocolo SNMP? ¿Qué características operativas de un switch administrable pueden consultarse o modificarse mediante SNMP?
21. ¿Qué características administrables de un switch tienen que ver con la gestión de seguridad en redes?

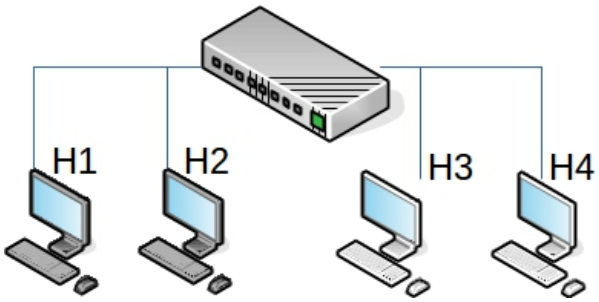

Figura 2: Competencia por el medio

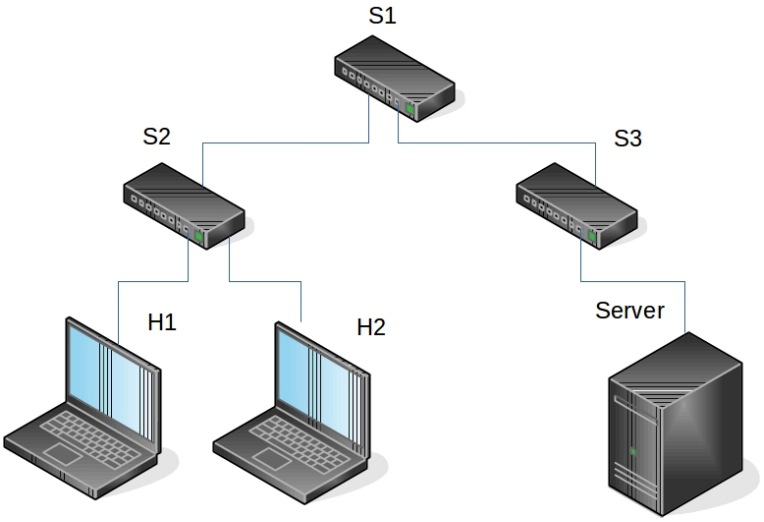

Figura 3: Jerarquía de switches

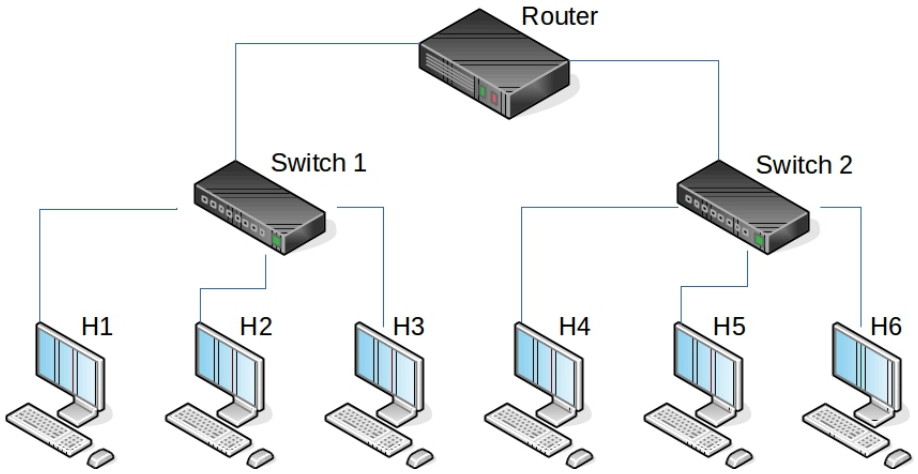

Figura 4: Dominios

4. Arquitecturas de redundancia

1. ¿Qué ventajas aporta la redundancia de enlaces en una red LAN? ¿Qué formas de redundancia se pueden implementar? ¿En qué consiste la tolerancia a fallos?
2. ¿Qué ocurre en una red Ethernet con múltiples caminos entre dos hosts? ¿Qué escenarios de fallo se pueden presentar?
3. ¿Cómo se puede detectar una tormenta de broadcasts?
4. ¿Qué ventaja ofrece el protocolo IEEE 802.1d (STP)? ¿Cómo es su modo de operación y qué intenta construir? ¿Qué dispositivos soportan 802.1d?
5. ¿Cómo se elige un dispositivo raíz del árbol STP? ¿Cómo se determinan los caminos al raíz? ¿Qué demora puede tener normalmente la convergencia de STP?
6. ¿Qué datos de configuración o estado, que sean relevantes para 802.1d, y cuya configuración por el administrador sea posible, admiten los bridges y switches? ¿En qué puede influir el administrador de redes sobre la elección del raíz? ¿Cómo se puede aprovechar este hecho?
7. ¿En qué consiste el protocolo RSTP?

5. VLANs

Un diseño clásico de redes de campus consiste en un router que proyecta segmentos de LAN como radios de una estrella (Fig. 5). La función de comunicar los radios, que anteriormente era cumplida por el backbone de la red, en este diseño se logra por la conmutación efectuada por el router, por lo cual suele llamarse de backbone colapsado.

Con este diseño, los dominios de broadcast, y por lo tanto los espacios IP definidos sobre ellos, quedan limitados geográficamente. Si en una zona del campus donde llega un radio de la estrella se necesita ubicar nodos sobre dos dominios de broadcast (porque se desea aislarlos por motivos de seguridad, porque se desea situar equipos sobre dos espacios IP diferentes, o porque se desea limitar la competencia de ambas clases de tráfico por el medio), debe haber dos cableados y deben ocuparse dos bocas del router central.

Con la funcionalidad avanzada de VLANs provista por algunos switches (y definida en el estándar IEEE 802.1Q), el mismo cableado, y el sistema de switches de llegada, puede usarse para conducir dos o más dominios de broadcast.

- ¿En qué consiste el diseño de red de campus de backbone colapsado? ¿Qué impacto tiene este diseño sobre la posibilidad de distribuir equipos de diferentes clases sobre una misma región de la red?

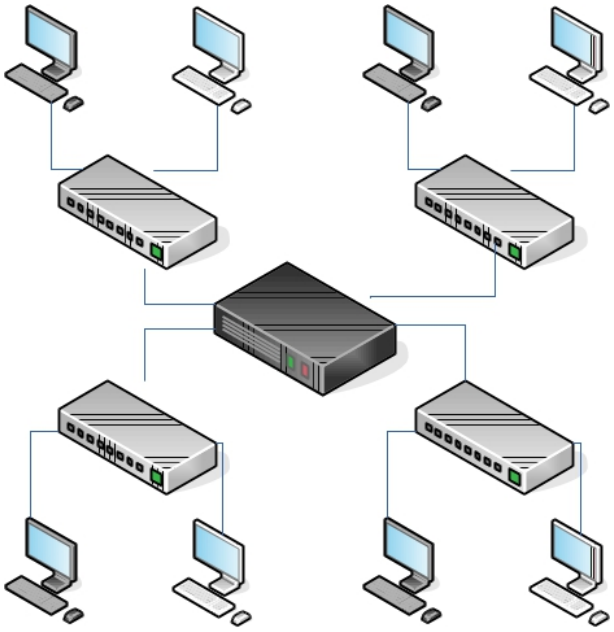

Figura 5: Backbone colapsado

- ¿Cuál es la finalidad de definir VLANs en un switch?
- ¿Cómo se modifica el formato de frame Ethernet para lograr la capacidad de separar los dominios de broadcast al definir VLANs?
- ¿Qué debe hacer un switch con VLANs definidas al recibir un frame de broadcast sobre una de sus interfaces? ¿Qué debe hacer con un frame unicast?
- En la topología de la figura 6, los tres switches tienen definidas dos VLANs. Los hosts H1, H2 y H4 pertenecen a la VLAN 1, y los hosts H3, H5 y H6 a la VLAN 2.
  - ¿Qué deben hacer los switches con un frame de broadcast recibido desde el host H2?
  - ¿Qué deben hacer los switches con un frame unicast recibido desde el host H5 y dirigido a H6? ¿Lo mismo, pero desde H5 a H3? ¿Qué diferencia en el formato de los frames existe entre un caso y otro, en cada punto del camino?
  - ¿Qué condición deben cumplir los ports que interconectan los switches entre sí para poder distribuir las VLANs por toda la topología?
  - ¿Es posible que una aplicación en el host H5 inicie conexión TCP/IP con una aplicación servidora situada en H2?
- ¿Qué elemento externo es necesario para conectar diferentes VLANs en una misma jerarquía de switches?
- ¿Qué son los switches multicapa o *multilayer*?

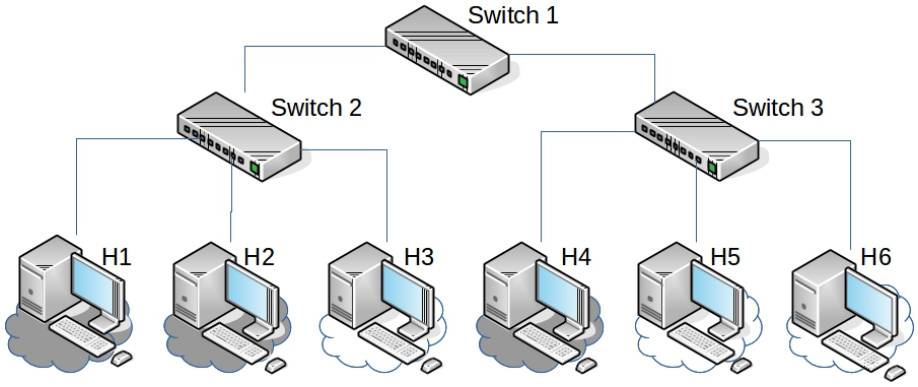

Figura 6: VLANs

Parte III

Redes Privadas Virtuales

Parte IV

Balance de carga y Alta Disponibilidad en redes

Parte V
Anexos

iptables.log

```
Logged 539 packets on interface eth1
  From 0000:0000:1011:1213:0100:0000:0000:0000 - 3 packets to icmpv6(130)
  From 0000:0000:0000:859e:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0000:0023:ff53:4d42:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0000:0000:0000:3433:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0000:0000:0000:3132:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0000:0000:0000:7d3a:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0000:0000:0000:6e63:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0000:0000:0000:937f:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0000:0000:0000:0000:0000:0000:0000:0000 - 2 packets to icmpv6(130)
  From 0000:0000:0000:0000:0100:0000:0000:0000 - 40 packets to icmpv6(130)
  From 0000:0000:0000:6569:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 000e:175f:531c:580e:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0011:11db:a2d4:0a00:0100:0000:0000:0000 - 2 packets to icmpv6(130)
  From 002c:799a:0694:8c26:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0100:0000:0600:0000:0100:0000:0000:0000 - 2 packets to icmpv6(130)
  From 0101:080a:00c6:0621:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:00c6:f565:0007:994d:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:00c7:39ad:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:00c7:3e49:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:00c7:5bd1:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:1551:7183:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:1a9a:1543:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:4553:94db:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:4557:126c:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:4559:6ffd:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:4559:e9ac:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:455a:3fd8:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:455a:cc78:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:455c:c658:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:455d:4147:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:455d:bbfc:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:455e:3351:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:4567:104c:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:4575:8fa3:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:4575:fcd3:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:4584:d388:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:458c:f368:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0101:080a:4594:8809:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0102:0417:0000:0000:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0102:a16d:0a00:00c8:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 0204:05b4:0402:080a:0100:0000:0000:0000 - 2 packets to icmpv6(130)
  From 0300:0000:0400:0000:0100:0000:0000:0000 - 3 packets to icmpv6(130)
  From 036b:696d:0675:6e63:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 10d4:d5cb:f80c:14d5:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 1400:0300:9709:0000:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 2269:6422:3a20:2232:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3037:3337:3431:3832:0100:0000:0000:0000 - 1 packet to icmpv6(130)
```

```
  From 3135:3332:3a38:3439:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3234:3238:323a:3834:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3333:3238:323a:3834:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3335:3839:323a:3834:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3336:3532:323a:3834:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3336:3837:3039:3132:0100:0000:0000:0000 - 8 packets to icmpv6(130)
  From 3430:3734:3330:3532:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3432:3230:3239:3a33:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3432:3635:3239:3a33:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3433:3230:3332:3a38:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3433:3534:3039:3a33:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3734:3237:3339:313a:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3734:3330:3238:313a:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3734:3330:3636:313a:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3734:3330:3930:323a:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3734:3334:3533:313a:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 3734:3334:3736:393a:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 616a:6f72:223a:2031:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 6d65:6e74:7322:3a7b:0100:0000:0000:0000 - 9 packets to icmpv6(130)
  From 6f20:3134:3037:3433:0100:0000:0000:0000 - 2 packets to icmpv6(130)
  From 7473:223a:7b7d:7d00:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 7473:223a:7b7d:7d32:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From 7473:223a:7b7d:7d3a:0100:0000:0000:0000 - 4 packets to icmpv6(130)
  From 7473:223a:7b7d:7d7b:0100:0000:0000:0000 - 3 packets to icmpv6(130)
  From 756e:6e69:6e67:223a:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From bf1d:f661:984e:fcb0:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From c011:fdda:43fe:4d59:65fe:e1aa:c7d5:683a - 1 packet to icmpv6(130)
  From c012:aa5c:173c:261c:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From c012:cfa3:e641:3b5f:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From c013:4b15:1c15:3311:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From c013:9389:bcf8:f7d4:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From c014:ff7d:0000:0000:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From e063:837f:0000:0000:0100:0000:0000:0000 - 3 packets to icmpv6(130)
  From e063:837f:2077:937f:0100:0000:0000:0000 - 1 packet to icmpv6(130)
  From e063:837f:301f:937f:0100:0000:0000:0000 - 3 packets to icmpv6(130)
  From 0.0.0.0 - 154 packets to igmp(0)
  From 10.0.3.4 - 154 packets to igmp(0)
  From 10.0.3.21 - 75 packets to igmp(0)
  From 10.0.3.209 - 2 packets to igmp(0)

Listed by source hosts:
Logged 18 packets on interface virbr0
  From fe80:0000:0000:0000:5054:00ff:feed:8246 - 18 packets to udp(5353)

Listed by source hosts:
Logged 50 packets on interface wlan0
  From 10.0.4.1 - 2 packets to udp(68)
  From 64.233.186.188 - 15 packets to tcp(44421,53418)
  From 64.235.151.8 - 5 packets to tcp(56214)
  From 173.194.42.0 - 1 packet to tcp(56677)
  From 173.194.42.21 - 3 packets to tcp(58597)
  From 173.194.42.22 - 7 packets to tcp(35536)
  From 173.194.42.75 - 3 packets to tcp(48585)
  From 173.194.42.85 - 4 packets to tcp(44550)
  From 173.194.42.86 - 1 packet to tcp(51940)
```

```
From 192.168.1.1 - 2 packets to udp(68)
From 192.168.2.1 - 2 packets to udp(68)
From 195.135.221.134 - 1 packet to tcp(51756)
From 195.154.174.66 - 1 packet to tcp(58047)
From 200.42.136.212 - 3 packets to tcp(59351,59361)
```