Ministerio de Educación
Gobierno de Chile

UNIVERSIDAD CATÓLICA DE TEMUCO

Identificación, análisis y filtrado de datos en una red local

Módulo 5: **Configuración de la seguridad en redes de área local.**

Conectividad y Redes

Objetivos de Aprendizaje de la Especialidad

Módulo 1	**OA1** Leer y utilizar técnicamente proyectos de conectividad y redes, considerando planos o diagramas de una red de área local (red LAN), basándose en los modelos TCP/IP y OSI. **OA3** Instalar y mantener cableados estructurados, incluyendo fibra óptica, utilizados en la construcción de redes, basándose en las especificaciones técnicas correspondientes. **OA7** Instalar y configurar una red inalámbrica según tecnologías y protocolos establecidos.
Módulo 2	**OA2** Instalar y configurar sistemas operativos en computadores personales con el fin de incorporarlos a una red LAN, cumpliendo con los estándares de calidad y seguridad establecidos. **OA11** Armar y configurar un equipo personal, basándose en manuales de instalación, utilizando las herramientas apropiadas y respetando las normas de seguridad establecidos.
Módulo 3	**OA8** Aplicar herramientas de software que permitan obtener servicios de intranet e internet de manera eficiente.
Módulo 4	**OA4** Realizar pruebas de conexión y señales en equipos y redes, optimizando el rendimiento de la red y utilizando instrumentos de medición y certificación de calidad de la señal, considerando las especificaciones técnicas.
Módulo 5	OA5 Aplicar métodos de seguridad informática para mitigar amenazas en una red LAN, aplicando técnicas como filtrado de tráfico, listas de control de acceso u otras.
Módulo 6	**OA9** Mantener y actualizar el hardware de los computadores personales y de comunicación, basándose en un cronograma de trabajo, de adcuerdo a las especificaciones técnicas del equipo.
Módulo 7	**OA10** Mantener actualizado el software de productividad y programas utilitarios en un equipo personal, de acuerdo a los requerimientos de los usuarios.
Módulo 8	**OA6** Aplicar procedimientos de recuperación de fallas y realizar copias de respaldo de los servidores, manteniendo la integridad de la información.
Módulo 9	No esta asociado a Objetivos de Aprendizaje de la Especialidad (OAE), sino a Genéricos. No obstante, puede asociarse a un OAE como estrategia didáctica.

Perfil de Egreso – Objetivos de Aprendizaje Genéricos

A- Comunicarse oralmente y por escrito con claridad, utilizando registros de habla y de escritura pertinentes a la situación laboral y a la relación con los interlocutores.	**B-** Leer y utilizar distintos tipos de textos relacionados con el trabajo, tales como especificaciones técnicas, normativas diversas, legislación laboral, así como noticias y artículos que enriquezcan su experiencia laboral.	**C-** Realizar las tareas de manera prolija, cumpliendo plazos establecidos y estándares de calidad, y buscando alternativas y soluciones cuando se presentan problemas pertinentes a las funciones desempeñadas.
D- Trabajar eficazmente en equipo, coordinando acciones con otros in situ o a distancia, solicitando y prestando cooperación para el buen cumplimiento de sus tareas habituales o emergentes.	**E-** Tratar con respeto a subordinados, superiores, colegas, clientes, personas con discapacidades, sin hacer distinciones de género, de clase social, de etnias u otras.	**F-** Respetar y solicitar respeto de deberes y derechos laborales establecidos, así como de aquellas normas culturales internas de la organización que influyen positivamente en el sentido de pertenencia y en la motivación laboral.
G- Participar en diversas situaciones de aprendizaje, formales e informales, y calificarse para desarrollar mejor su trabajo actual o bien para asumir nuevas tareas o puestos de trabajo, en una perspectiva de formación permanente.	**H-** Manejar tecnologías de la información y comunicación para obtener y procesar información pertinente al trabajo, así como para comunicar resultados, instrucciones e ideas.	**I-** Utilizar eficientemente los insumos para los procesos productivos y disponer cuidadosamente los desechos, en una perspectiva de eficiencia energética y cuidado ambiental.
J- Emprender iniciativas útiles en los lugares de trabajo y/o proyectos propios, aplicando principios básicos de gestión financiera y administración para generarles viabilidad.	**K-** Prevenir situaciones de riesgo y enfermedades ocupasionales, evaluando las condiciones del entorno del trabajo y utilizando los elementos de protección personal según la normativa correspondiente.	**L-** Tomar decisiones financieras bien informadas, con proyección a mediano y largo plazo, respecto del ahorro, especialmente del ahorro previsional, de los seguros, y de los riesgos y oportunidades del endeudamiento crediticio así como de la inversión.

Marco de Cualificaciones Técnico Profesional (MCTP) Nivel 3 y su relación con los OAG

HABILIDADES

1. Información
1. Analiza y utiliza información de acuerdo a parámetros establecidos para responder a las necesidades propias de sus actividades y funciones.
2. Identifica y analiza información para fundamentar y responder a las necesidades propias de sus actividades.

2. Resolución de problemas
1. Reconoce y previene problemas de acuerdo a parámetros establecidos en contextos conocidos propios de su actividad o funcion.
2. Detecta las causas que originan problemas en contextos conocidos de acuerdo a parámetros establecidos.
3. Aplica soluciones a problemas de acuerdo a parámetros establecidos en contextos conocidos propios de una función.

3. Uso de recursos
1. Selecciona y utiliza materiales, herramientas y equipamiento para responder a una necesidad propia de una actividad o función especializada en contextos conocidos.
2. Organiza y comprueba la disponibilidad de los materiales, herramientas y equipamiento.
3. Identifica y aplica procedimientos y técnicas específicas de una función de acuedo a parámetros establecidos.

4. Comunicación
4. Comunica y recibe información relacionada a su actividad o función, a través de medios y soportes adecuados en contextos conocidos.

APLICACIÓN EN CONTEXTO

5. Trabajo con otros
1. Trabaja colaborativamente en actividades y funciones coordinándose con otros en diversos contextos.

6. Autonomía
1. Se desempeña con autonomía en actividades y funciones especializadas en diversos contextos con supervisión directa.
2. Toma decisiones en actividades propias y en aquellas que inciden en el quehacer de otros en contextos conocidos.
3. Evalua el proceso y el resultado de sus actividades y funciones de acuerdo a parámetros establecidos para mejorar sus prácticas.
4. Busca oportunidades y redes para el desarrollo de sus capacidades

7. Ética y responsabilidad
1. Actúa de acuerdo a las normas y protocolos que guían su desempeño y reconoce el impacto que la calidad de su trabajo tiene sobre el proceso productivo o la entrega de servicios.
2. Responde por cumplimiento de los procedimientos y resultados de sus actividades.
3. Comprende y valora los efectos de sus acciones sobre la salud y la vida, la organización, la sociedad y el medio ambiente.
4. Actúa acorde al marco de sus conocimientos. experiencias y alcance de sus actividades y funciones

CONOCIMIENTO

8. Conocimientos
1. Demuestra conocimientos especificos de su área y de las tendencias de desarrollo para el desempeño de sus actividades y funciones.

Metodología seleccionada

Demostración guiada

- Esta presentación te servirá para avanzar paso a paso en el desarrollo de la actividad propuesta.

Aprendizaje Esperado

- **5.2** Supervisa una red de área local a través de técnicas de análisis y filtrado de tráfico(protocolos), listas de control de acceso, monitoreo de red u otras, respetando la normativa legal vigente.

¿Qué vamos a lograr con esta actividad para llegar al Aprendizaje Esperado (AE)?

1. Conocer las características del análisis de tráfico en una red de área local.
2. Conocer los software o herramientas para realizar el proceso de análisis de tráfico.
3. Analizar proceso de filtrado tráfico.
4. Configurar una lista de control de acceso.

Cuando escuchas la expresión *“análisis de tráfico en red”* ¿Qué te imaginas?

¿Qué información debería entregar un software que analice el tráfico de red?

Rendimiento, seguridad y desempeño de una red local

¿Qué es el rendimiento y seguridad de red de área local?

En términos generales, el rendimiento de una red es la calidad del servicio que esta ofrece y permite la disponibilidad de los recursos, por ejemplo, si la red se ve en un horario punta estresada por la gran cantidad de tráfico, ésta debería ser capaz de soportar y mantener el rendimiento estable de la red.

La seguridad de una red busca resguardar la información y para eso hay tres requisitos principales:

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

Imagen: https://cambiodigital-ol.com/2020/03/la-triada-cia-definicion-componentes-y-ejemplos/

¿Cómo se clasifica el rendimiento y seguridad de red de área local?

Para determinar el rendimiento, hay una serie de parámetros que podemos utilizar para clasificarlas, como por ejemplo:

A. • **Ancho de banda:** Mientras tenga una mejor velocidad en mi red, tendré un mejor rendimiento.

B. • **Latencia:** Se refiere a el tiempo de demora entre enviar información entre un emisor y receptor, o acceder a un servicio. La relación con el ancho de banda es que, si ttengo mayores velocidades, esta latencia debería ser menor.

C. • **Tasa de errores:** La cantidad de errores que se registran en un periodo determinado, ya sea para enviar información o acceder a un servicio.

¿Cómo se clasifica el rendimiento y seguridad de red de área local?

01

- Con todos estos datos podemos establecer,dependiendo de los resultados de cada uno de ellos, un rendimiento alto, medio o bajo.

02

- Es importante hacer estas mediciones en horario de poco tráfico y de mucho tráfico para así probar el rendimiento de la red en distintas situaciones.

¿Cómo se clasifica el rendimiento y seguridad de red de área local?

- Desde el punto de vista de la seguridad podemos clasificarla en:

  - **Seguridad Restrictiva:** Se deniega todo y se permite sólo aquello que se va utilizar.

  - **Seguridad Permisiva:** Se permite todo y se deniega lo que puede causar una vulnerabilidad.

La recomendación siempre es tener una política de seguridad restrictiva.

Pregunta de reflexión

¿Que tipo de seguridad crees que tiene en su computador personal?

¿Cómo crees que los constantes ataques a entidades financieras han afectado el rendimiento de su red?

Tipos de datos y protocolos

¿Qué características tienen los distintos tipos de tráfico de una red local?

Los distintos tipos de tráfico de una red de área local tienen la característica que se clasifican de la siguiente manera:

- **VOZ**
- **DATOS**
- **VIDEO**

Imagen: Cisco Systems, Inc.

¿Cuál es la estructura de los protocolos de estos tráficos?

La estructura de un protocolo

01

- **Encabezado:** Información de control por ejemplo, dirección MAC, dirección IP, Protocolo, etc.

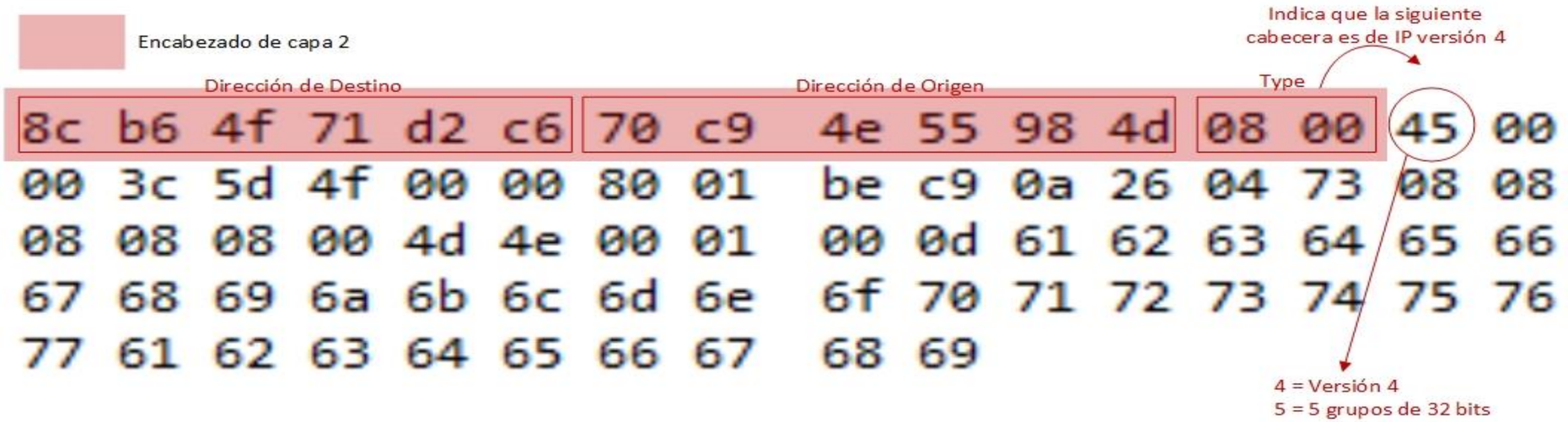
02

- **Datos:** Los datos que se envían.

03

- **Trailer:** Información de control para la detección de errores.

¿Cuál es la estructura de los protocolos de estos tráficos?



La estructura de un protocolo:

Imagen: https://lesand.cl/foro/cabecera-ethernet-e-ip

01

- **Encabezado:** Información de control, por ejemplo dirección MAC, dirección IP, Protocolo, etc.

02

- **Datos:** Los datos que se envían.

03

- **Trailer:** Información de control para la detección de errores.

¿Cuál es la estructura de los protocolos de estos tráficos?

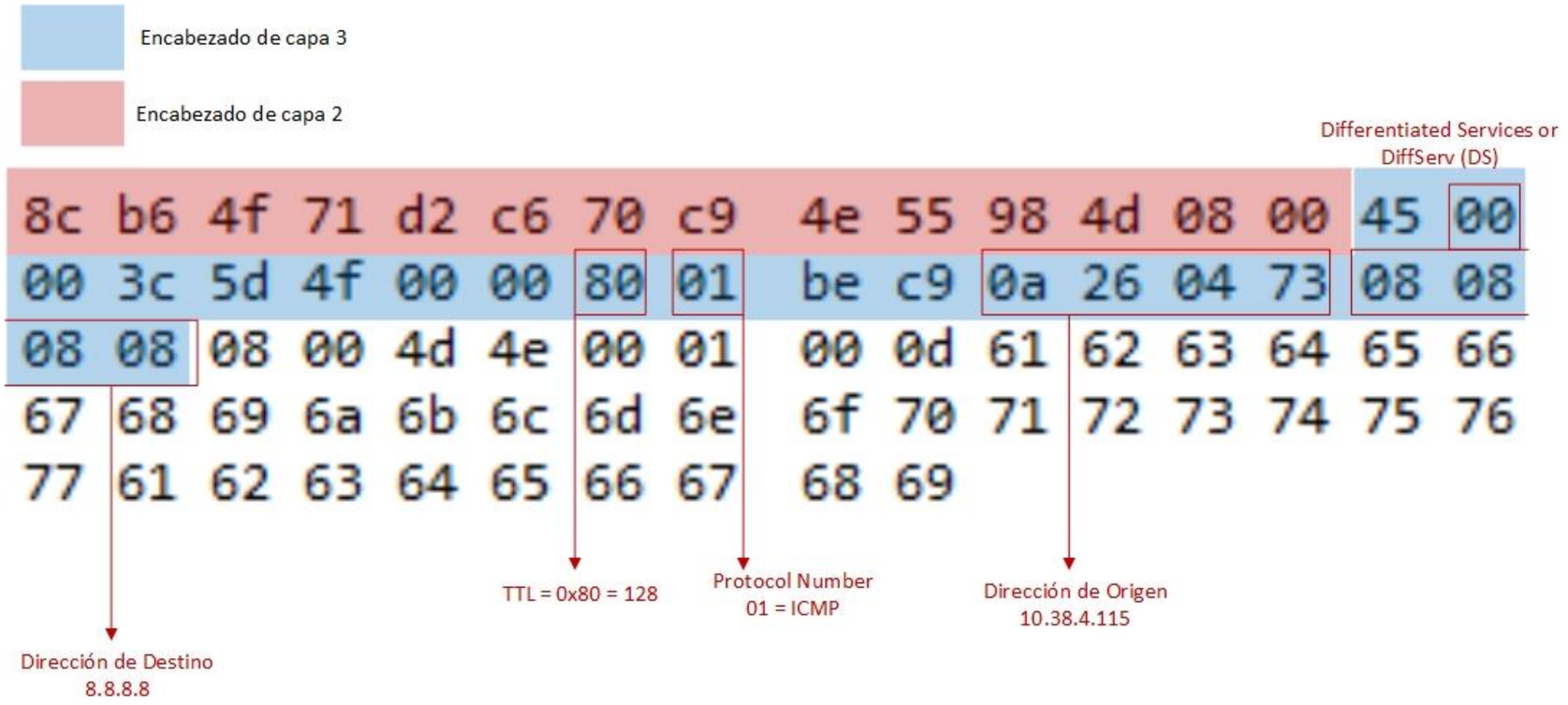


Imagen: https://lesand.cl/foro/cabecera-ethernet-e-ip

¿Cuál es la estructura de los protocolos de estos tráficos?

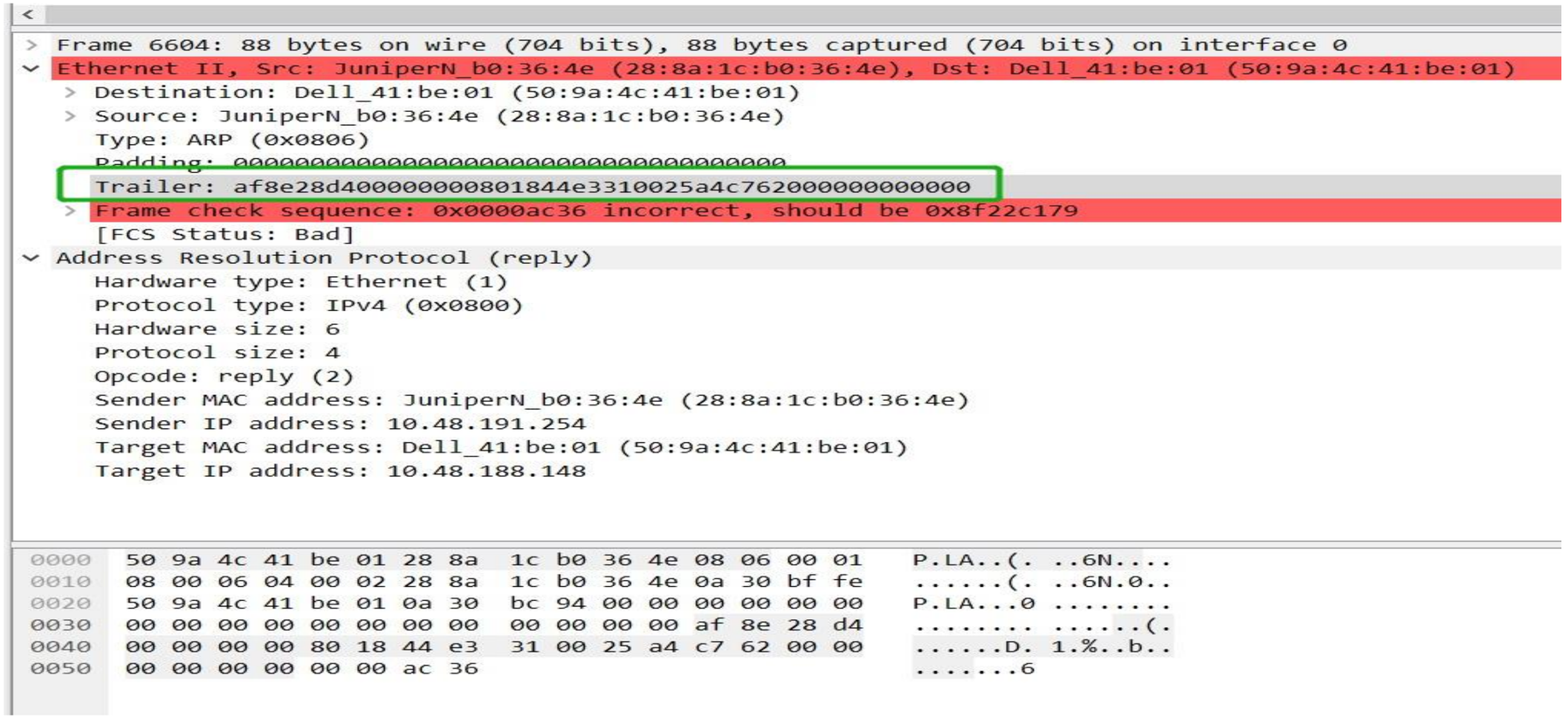


Imagen: https://i.loli.net/2019/04/29/5cc6540a25470.jpg

Configuración de listas de acceso en una red de área local y filtrado de tráfico

Elementos a configurar en el control de acceso en una red de área local

Para realizar la configuración de una lista de control de acceso es necesario considerar los siguientes elementos:

A.

- Tipo de lista de acceso:

  Estándar: Se identifica con el número 1-99 y solo permite o deniega un origen.
  Extendida: Se identifica con el número 100-199 solo permite o deniega un origen y destino.
  Nombrada: Se identifica con un nombre y puede ser estándar o extendida .

B.

- Establecer si voy a permitir o denegar tráfico.

C.

- Establecer aquellas redes que voy a permitir o denegar tráfico.

Pasos para la configuración de control de acceso en una red de área local

- Para configurar una lista de control de acceso se siguen los siguientes pasos:

- Establecer el tipo de lista de acceso, en este caso se muestra una lista de control de acceso estándar, que permite el tráfico de la red 192.168.0.0 a cualquier destino. Por defecto, cuando hay un “permit,” todo lo demás está denegado.

```
R1(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

Imagen: fuente propia.

Pasos para la configuración de control de acceso en una red de área local

- Luego, se ingresa en una interfaz y se agrega la lista de control de acceso de entrada o salida.

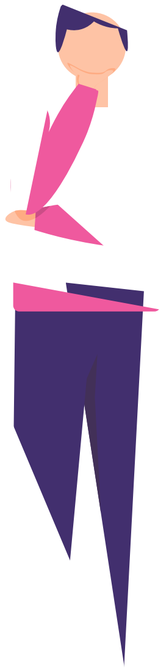
- En este caso se ingresó a la interface fastEthernet 0/0 y se aplicó la lista de acceso de entrada.

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip access-group 1 in
```

Imagen: fuente propia.

Pregunta de reflexión

¿Por qué debería implementar listas de control de acceso en una empresa?



Filtrado de red

- El filtrado de red es una técnica que sirve para permitir o denegar cierto tráfico en una red. Existen diversas razones para utilizarlo, ya sea para hacer más eficiente la red, políticas de seguridad, definir el tráfico que puede tener salida hacia internet dentro de una LAN , etc.

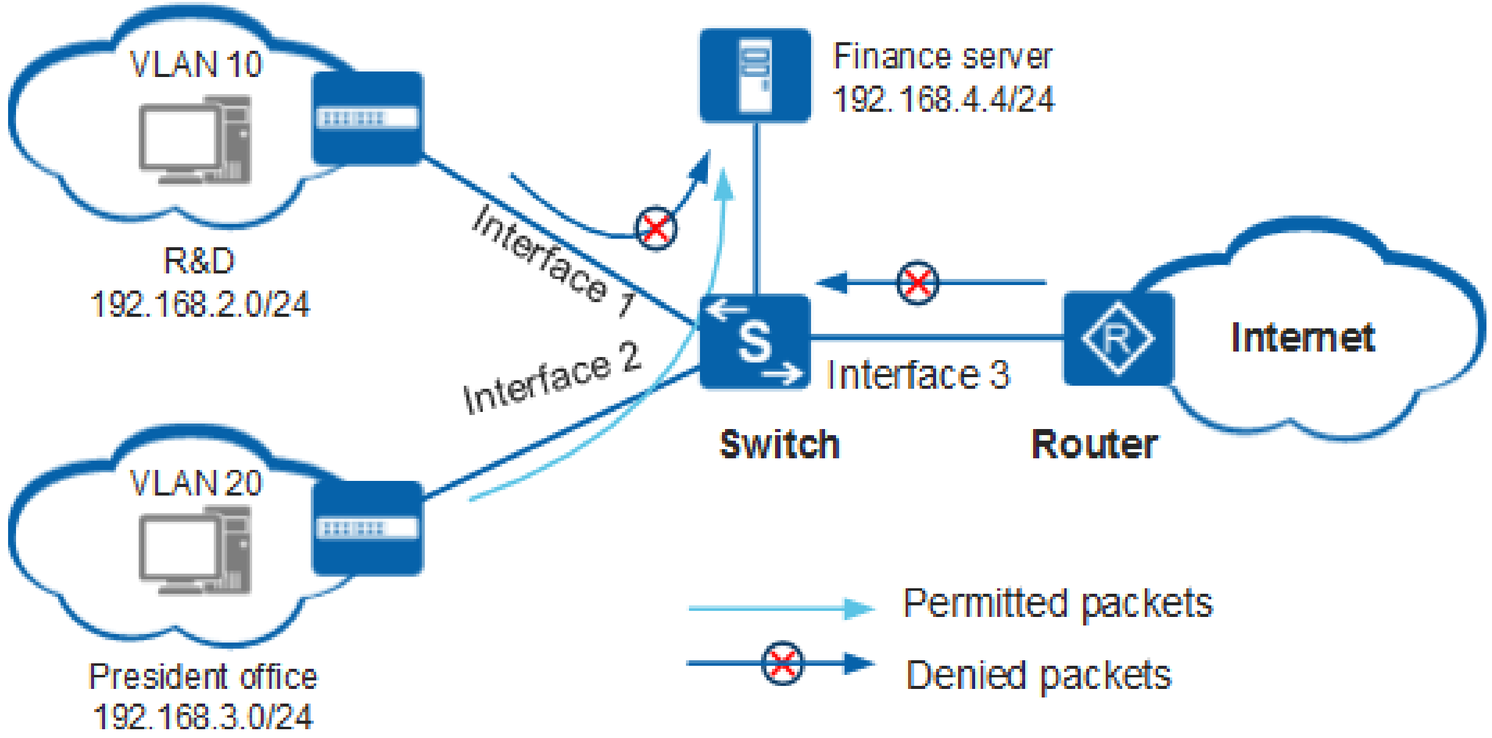


Imagen: https://forum.huawei.com/enterprise/es/data/attachment/forum/202002/13/123439gyaffy9a5c039czr.png?acl1.png

Análisis de tráfico de red

- El propósito del análisis de tráfico de red es capturar paquetes dentro de una red y ofrecer la información detallada de ésta.

- Para lograr este análisis se dispone de una serie de herramientas o software como: wireshark y tcpdum, por ejemplo.

Ejemplo Práctico: Análisis de tráfico con Software Wireshark

Wireshark es un analizador de protocolos de software o una aplicación que se utiliza para el diagnóstico de problemas de red, verificación, desarrollo de protocolo y software y educación.

Es una herramienta útil para cualquiera que trabaje con redes y se puede utilizar para el análisis de datos y la solución de problemas.

- Esta herramienta está disponible para Windows, Mac y Linux de manera gratuita, y ha sido pensada para profesionales de las TI.
- Otra herramienta similar a Wireshark es TCPDUM.

Análisis de tráfico de red

- Un ejemplo de la información que podemos recopilar en la captura de tráfico es :
  - **IP origen.**
  - **IP destino.**
  - **MAC origen.**
  - **MAC destino.**
  - **Protocolo.**
  - **Versión IPv4/IPv6.**
  - **Etc.**

28023	1580.626300	209.197.3.15	192.168.1.86	TLSv1.3	93 Application Data
28024	1580.626595	209.197.3.15	192.168.1.86	TLSv1.3	78 Application Data
28025	1580.626715	192.168.1.86	209.197.3.15	TCP	54 54903 → 443 [ACK] Seq=582 Ack=4737 Win=131584 Len=0
28026	1580.627521	192.168.1.86	209.197.3.15	TCP	54 54903 → 443 [ACK] Seq=582 Ack=4738 Win=131584 Len=0
28027	1581.799854	IntelCor_d8:ab:08	Broadcast	ARP	60 Who has 192.168.1.89? Tell 192.168.1.93
28028	1582.798281	IntelCor_d8:ab:08	Broadcast	ARP	60 Who has 192.168.1.89? Tell 192.168.1.93
28029	1583.544223	192.168.1.86	142.250.0.95	TCP	55 [TCP Keep-Alive] 54790 → 443 [ACK] Seq=1242 Ack=5417 Win=131328 Len=1
28030	1583.547785	142.250.0.95	192.168.1.86	TCP	66 [TCP Keep-Alive ACK] 443 → 54790 [ACK] Seq=5417 Ack=1243 Win=67840 Len=0 SLE=1242 SRE=1243
28031	1583.797983	IntelCor_d8:ab:08	Broadcast	ARP	60 Who has 192.168.1.89? Tell 192.168.1.93
28032	1584.131173	AskeyCom_24:d6:12	Broadcast	ARP	60 Who has 192.168.1.98? Tell 192.168.1.1
28033	1584.630203	192.168.1.86	64.233.190.95	TCP	55 [TCP Keep-Alive] 54794 → 443 [ACK] Seq=1283 Ack=4093 Win=131328 Len=1
28034	1584.636226	64.233.190.95	192.168.1.86	TCP	66 [TCP Keep-Alive ACK] 443 → 54794 [ACK] Seq=4093 Ack=1284 Win=67840 Len=0 SLE=1283 SRE=1284
28035	1584.780229	35.186.165.146	192.168.1.86	TLSv1.2	100 Application Data
28036	1584.780230	35.186.165.146	192.168.1.86	TLSv1.2	85 Encrypted Alert
28037	1584.780231	35.186.165.146	192.168.1.86	TCP	54 443 → 54784 [FIN, ACK] Seq=590370 Ack=2419 Win=32768 Len=0
28038	1584.780535	192.168.1.86	35.186.165.146	TCP	54 54784 → 443 [ACK] Seq=2419 Ack=590370 Win=749568 Len=0
28039	1584.781363	192.168.1.86	35.186.165.146	TCP	54 54784 → 443 [RST, ACK] Seq=2419 Ack=590370 Win=0 Len=0
28040	1585.133897	AskeyCom_24:d6:12	Broadcast	ARP	60 Who has 192.168.1.98? Tell 192.168.1.1
28041	1585.171784	AskeyCom_24:d6:12	Broadcast	ARP	60 Who has 192.168.1.106? Tell 192.168.1.1
28042	1585.307158	192.168.1.86	172.217.192.136	TCP	55 [TCP Keep-Alive] 54822 → 443 [ACK] Seq=8158 Ack=42441 Win=130560 Len=1
28043	1585.311395	172.217.192.136	192.168.1.86	TCP	66 [TCP Keep-Alive ACK] 443 → 54822 [ACK] Seq=42441 Ack=8159 Win=80896 Len=0 SLE=8158 SRE=8159
28044	1585.332601	IntelCor_d8:ab:08	Broadcast	ARP	60 Who has 192.168.1.1? Tell 192.168.1.93
28045	1586.125612	IntelCor_d8:ab:08	Broadcast	ARP	60 Who has 192.168.1.1? Tell 192.168.1.93
28046	1586.135579	AskeyCom_24:d6:12	Broadcast	ARP	60 Who has 192.168.1.98? Tell 192.168.1.1
28047	1586.175448	AskeyCom_24:d6:12	Broadcast	ARP	60 Who has 192.168.1.106? Tell 192.168.1.1
28048	1587.175418	AskeyCom_24:d6:12	Broadcast	ARP	60 Who has 192.168.1.106? Tell 192.168.1.1
28049	1588.954793	192.168.1.86	13.227.200.102	TCP	55 [TCP Keep-Alive] 54823 → 443 [ACK] Seq=1162 Ack=9697 Win=131584 Len=1
28050	1588.957967	13.227.200.102	192.168.1.86	TCP	66 [TCP Keep-Alive ACK] 443 → 54823 [ACK] Seq=9697 Ack=1163 Win=31488 Len=0 SLE=1162 SRE=1163
28051	1589.268435	192.168.1.86	172.217.192.149	TCP	55 [TCP Keep-Alive] 54824 → 443 [ACK] Seq=1335 Ack=3743 Win=130560 Len=1

> Frame 1: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits) on interface \Device\NPF_{7742F7A1-FA2B-47AB-9B73-DDC17E7DB182}, id 0

```
0000  94 b8 6d 91 20 ad 7c db  98 24 d6 12 08 00 45 00   ··m· ·|· ·$····E·
0010  00 e0 00 00 40 00 31 06  13 88 42 6e 31 24 c0 a8   ····@·1· ··Bn1$··
0020  01 56 01 bb d5 06 a6 a3  71 3a 7a 32 85 92 50 18   ·V····· q:z2··P·
0030  04 05 7c e5 00 00 4b 45  00 00 5c ba 00 00 00 00   ··|···KE ··\·····
0040  ad 01 00 00 00 8b c5 b9  c4 78 81 21 01 68 c0 39   ········ ·x·!·h·9
0050  f7 6f 02 1b 9b 6e 53 13  7a af dc 3b 4a 3f ad 36   ·o···nS· z··;J?·6
0060  01 60 2d 0a 73 b6 80 f7  1c d2 8b 73 95 c5 a7 10   ·`-·s··· ···s····
0070  aa 9d c6 51 a3 0c 84 e8  f9 45 d0 74 10 8b 06 6c   ···Q···· ·E·t···l
0080  6d 7f 8a b6 ed 29 b3 5e  4b 1a ab 63 94 dd 76 22   m····)·^ K··c··v"
0090  6a d5 78 55 c4 80 54 33  ee 86 c0 4c 5a f9 c9 cd   j·xU··T3 ···LZ···
00a0  55 97 fc f5 b0 8e 4f 73  e1 6c 80 f7 3a 5e 20 c0   U·····Os ·l··:^ ·
00b0  18 e3 5f 61 45 67 57 f3  24 02 8e d3 21 ca d5 43   ··_aEgW· $···!··C
00c0  e7 20 bc fc 0b 9a fe 7f  c3 77 1b aa d7 6e fa 7a   · ····· ·w···n·z
00d0  c9 48 df 22 dc a4 2f 52  83 17 c4 2a 37 26 33 3d   ·H·"··/R ···*7&3=
00e0  0d 80 03 af 5e 5f 3f 7c  d6 63 b4 73 f7 00         ····^_?| ·c·s··
```

Análisis de trafico de red

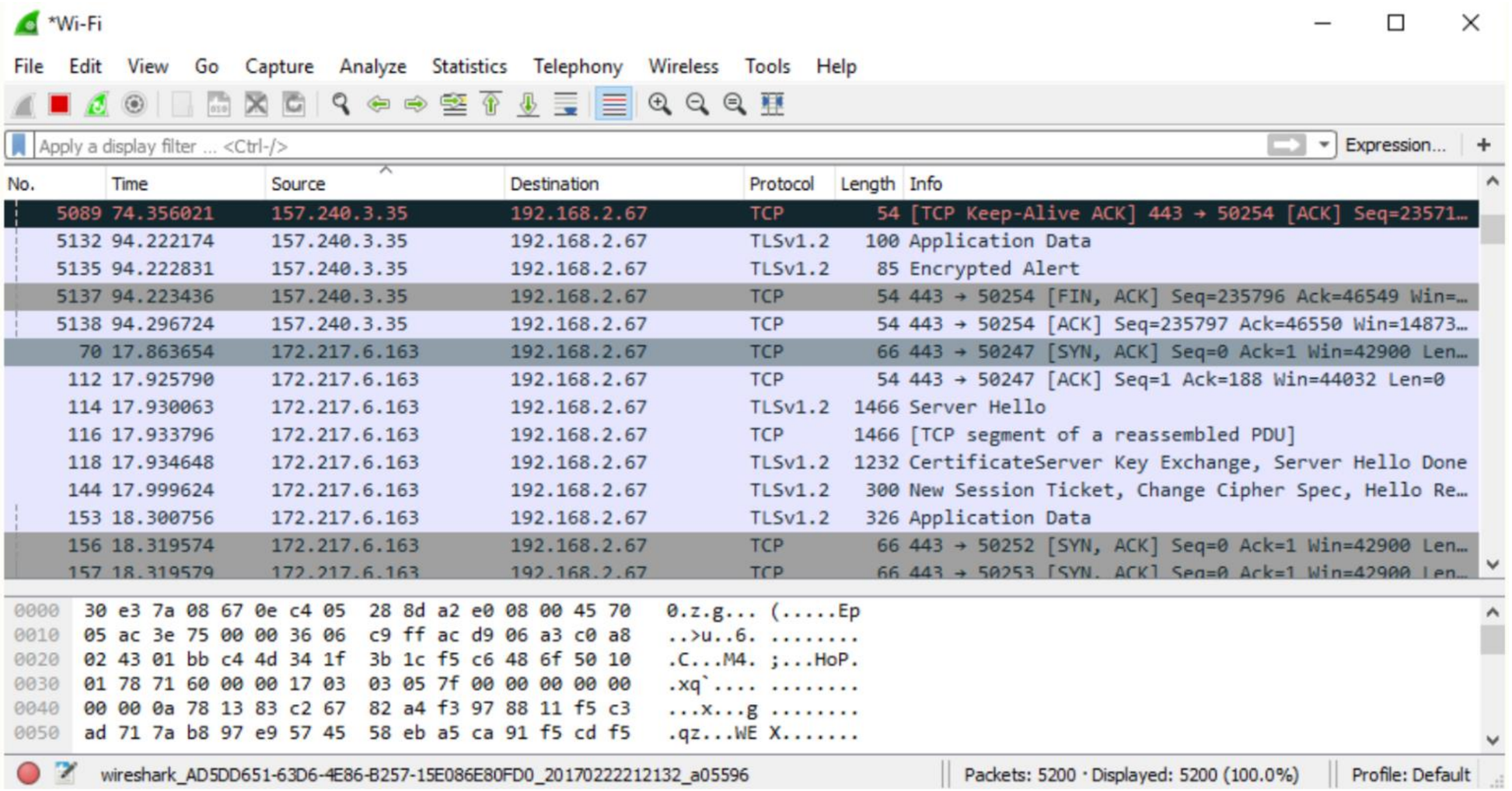
Adicionalmente, al revisar las capturas de tráfico podemos entregar la siguiente información:

A. • Revisar si se están utilizando protocolos de comunicación seguros o inseguros.

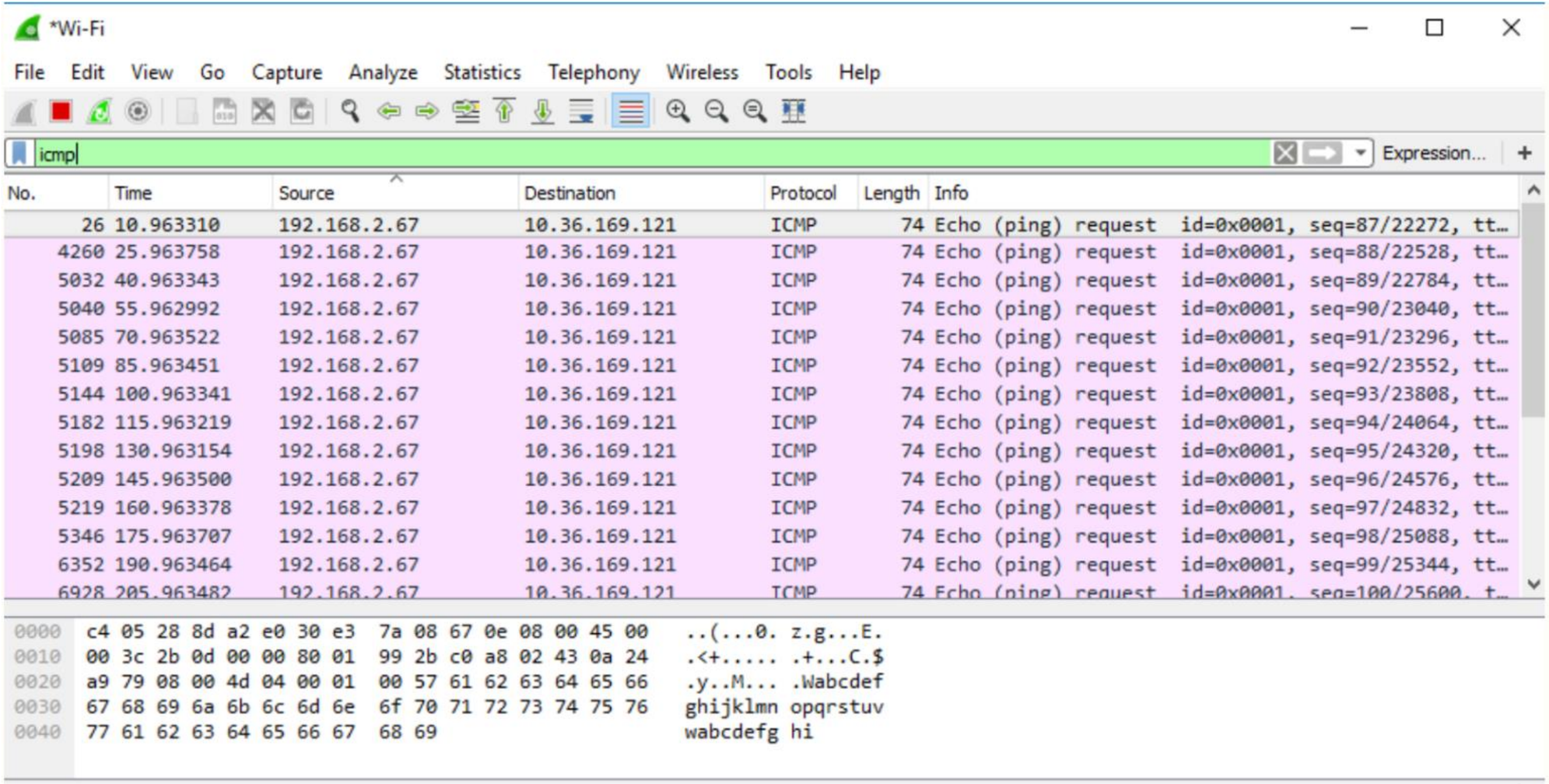
B. • Verificar si estoy recibiendo algún tipo de ataque en mi red.

C. • Generar un documento, indicando aquellas recomendaciones de seguridad en base a todas las capturas realizadas, por ejemplo: autenticar ciertos protocolos, utilizar protocolos de comunicación segura, etc.

La información comienza a desplazar hacia abajo la sección superior de Wireshark.
Las líneas de datos aparecen en diferentes colores según el protocolo.



Ejemplo captura de tráfico de un PING.



Tcpdum

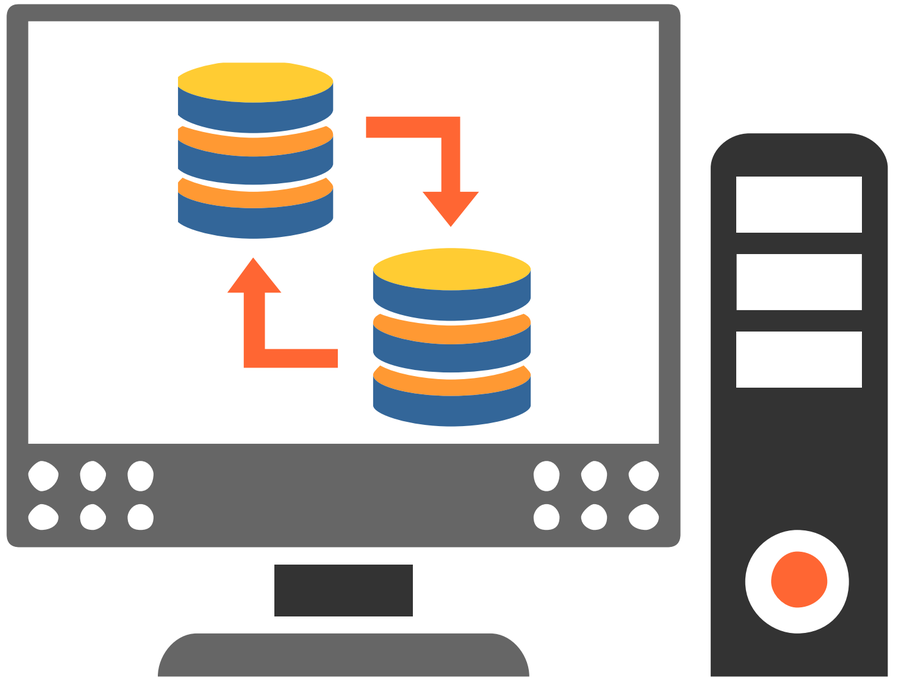
01

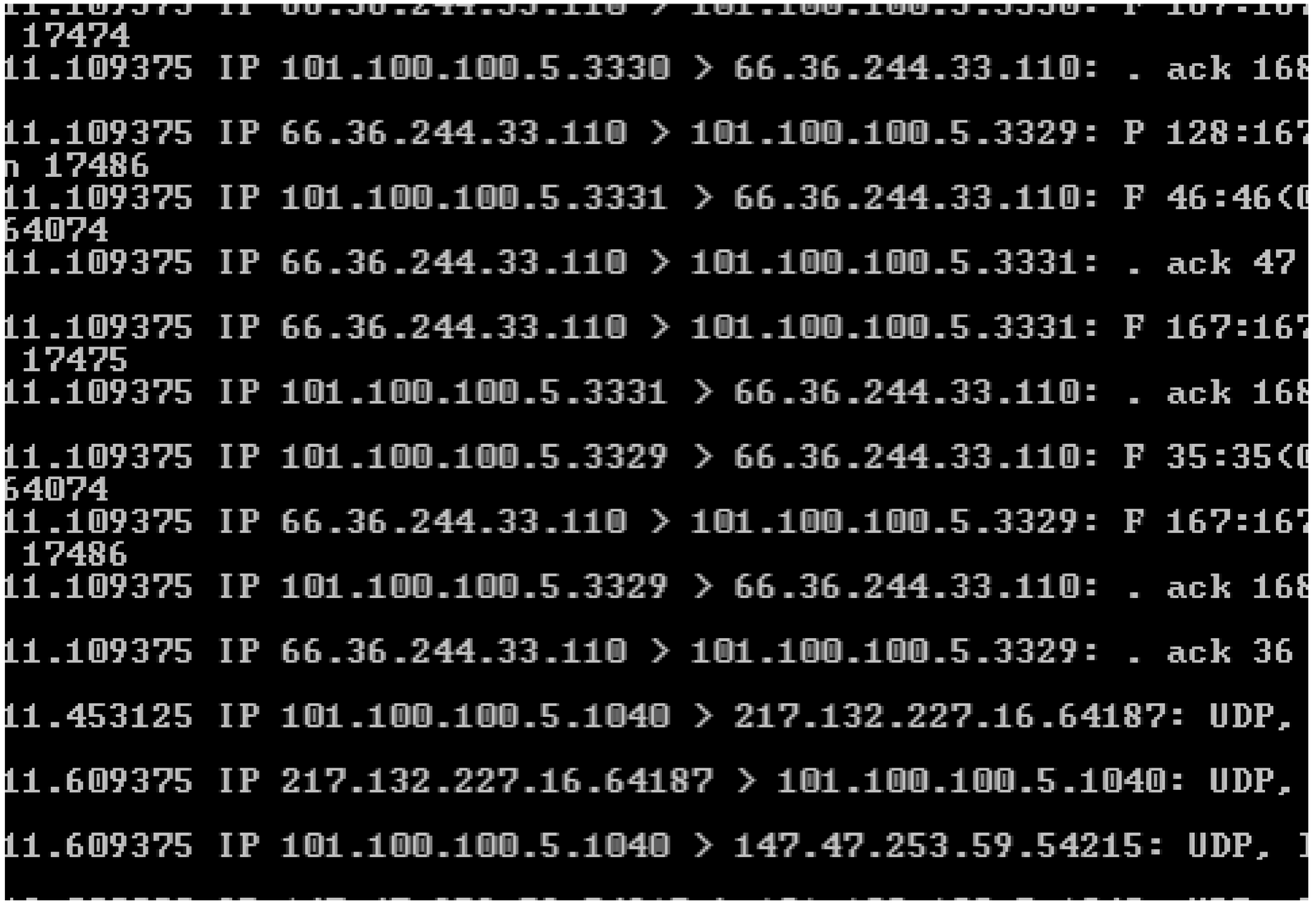
- Tcpdum es una herramienta de Linux para el análisis de tráfico de red por línea de comandos.

02

- La forma de capturar en una terminal de Linux es la siguiente:

  tcpdum -i eth0 (eth0 corresponde a la interfaz por la cual quiero capturar).

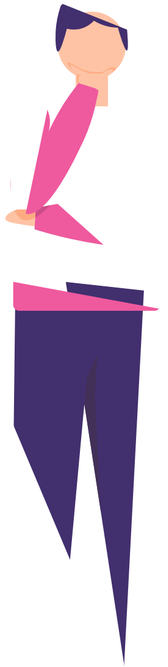



17474
11.109375 IP 101.100.100.5.3330 > 66.36.244.33.110: . ack 168
11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: P 128:167
n 17486
11.109375 IP 101.100.100.5.3331 > 66.36.244.33.110: F 46:46(0
64074
11.109375 IP 66.36.244.33.110 > 101.100.100.5.3331: . ack 47
11.109375 IP 66.36.244.33.110 > 101.100.100.5.3331: F 167:167
17475
11.109375 IP 101.100.100.5.3331 > 66.36.244.33.110: . ack 168
11.109375 IP 101.100.100.5.3329 > 66.36.244.33.110: F 35:35(0
64074
11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: F 167:167
17486
11.109375 IP 101.100.100.5.3329 > 66.36.244.33.110: . ack 168
11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: . ack 36
11.453125 IP 101.100.100.5.1040 > 217.132.227.16.64187: UDP,
11.609375 IP 217.132.227.16.64187 > 101.100.100.5.1040: UDP,
11.609375 IP 101.100.100.5.1040 > 147.47.253.59.54215: UDP,

Tcpdump

Pregunta de reflexión

¿De qué manera estas herramientas de análisis de tráfico creen que ayudan en el proceso de solución de problemas en una empresa?



Ticket de salida

01

Realiza un esquema gráfico que muestre los pasos a seguir para monitorear la red con Wireshark.

02

¿Qué dudas tuviste al analizar el tráfico de red? ¿Cómo las resolviste?

03

¿Qué tipos de problemas pueden identificarse al hacer un monitoreo de red?

Referencias

https://www.ciscopress.com/store/ccna-200-301-official-cert-guide-volume-1-9780135792735

https://www.ciscopress.com/store/ccna-200-301-official-cert-guide-volume-2-9781587147135

https://www.wireshark.org/docs/

https://packetlife.net/captures/

Preguntas