Universidad Tecnológica Nacional
Facultad Regional Avellaneda

Carrera:

Técnico Universitario en Programación

Materia:

Arquitectura y sistemas operativos

Identificación, análisis y filtrado de datos en una red local

Configuración de la seguridad en redes de área local.

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, 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**

¿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 tengo 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:

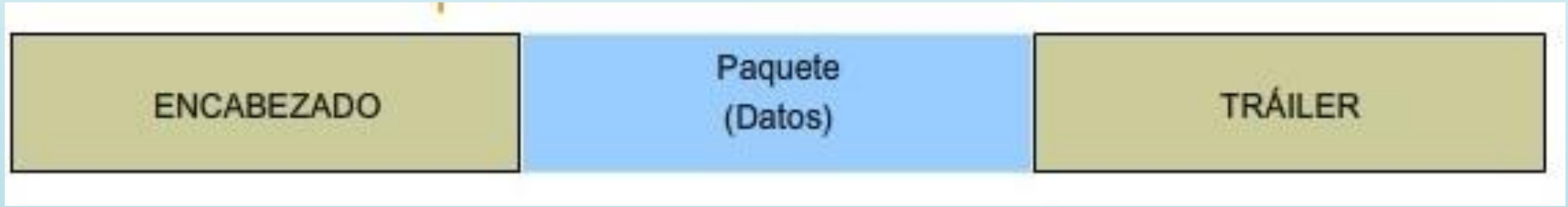
- **VOZ**
- **DATOS**
- **VIDEO**

Imagen: Cisco Systems, Inc.

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

En las redes de computadoras, la dirección MAC es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red. Se la conoce también como dirección física, y es única para cada dispositivo

- **La estructura de un protocolo**



01
- **Encabezado:** Información de control por ejemplo, dirección MAC, dirección IP, Protocolo, etc.

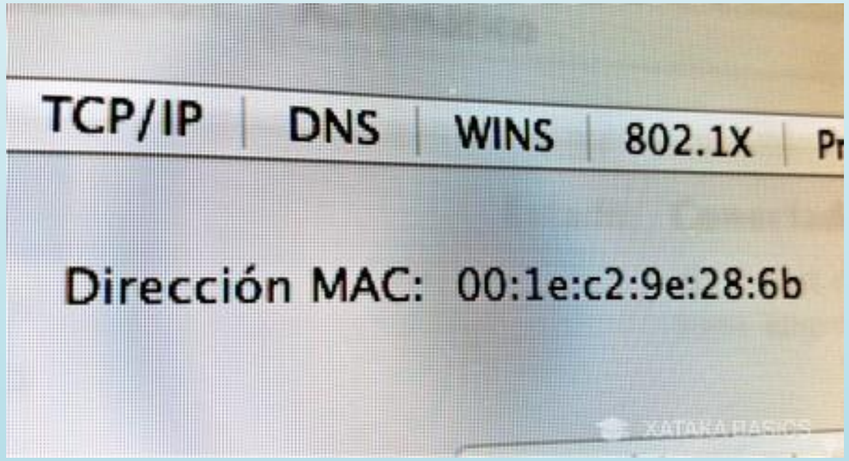
02
- **Datos:** Los datos que se envían.

03
- **Trailer:** Información de control para la detección de errores.

¿Qué es la dirección Mac de un dispositivo?

La dirección MAC es un identificador único que **cada fabricante le asigna a la tarjeta de red** de sus dispositivos conectados, desde un ordenador o móvil hasta routers, impresoras u otros dispositivos como tu Chromecast. Sus siglas vienen del inglés, y significan **Media Access Control**. Como hay dispositivos con diferentes tarjetas de red, como una para WiFi y otra para Ethernet, algunos pueden tener diferentes direcciones MAC dependiendo de por dónde se conecten.

Las direcciones MAC están formadas por 48 bits representados generalmente por dígitos hexadecimales. Como cada hexadecimal equivale a cuatro binarios (48:4=12), la dirección acaba siendo formada por 12 dígitos agrupados en seis parejas separadas generalmente por dos puntos, aunque también puede haber un guión o nada en absoluto. De esta manera, un ejemplo de dirección MAC podría ser 00:1e:c2:9e:28:6b.



La mitad de los bits de una dirección MAC, tres de las seis parejas, identifican al fabricante, y la otra mitad al modelo.

¿Cómo puedo obtener el MAC de mi dispositivo?

Obtener el MAC en Windows

- Pulsa las teclas *Windows + R* para abrir Ejecutar.
- Escribe *cmd* y presiona *Enter* para ir al *Símbolo de sistema*
- Escribe *ipconfig /all*.
- En la entrada *Dirección física* te dirá la dirección MAC de tu ordenador.

Obtener el MAC en macOS

- Abre las *Preferencias del Sistema*.
- Haz click en *Red*, y en el panel de la izquierda selecciona en la que estás conectado.
- Pulsa sobre el botón *Avanzado* en la parte inferior de la ventana.
- Elige la pestaña *Hardware*, y en ella tienes tu MAC.

Obtener el MAC en GNU/Linux

- Ve a la consola del sistema.
- Escribe *ifconfig*.
- El MAC es la dirección del campo HWaddr.

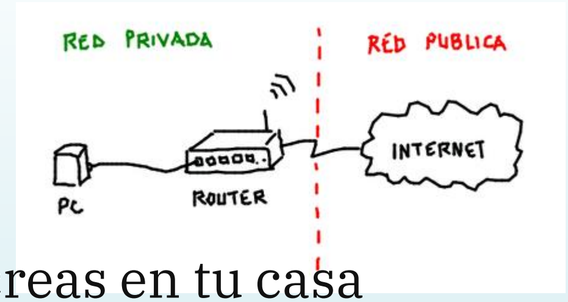
¿Qué son las direcciones IP?

IP significa “Internet Protocol“ o "**Protocolo de Internet**”. Se trata de un protocolo de comunicaciones a través de la red. Por otro lado están las **direcciones IP**, que es el número que escoges o se te asigna dentro de la red, y que es la manera que tiene Internet de saber quién es quién.
Se utiliza para identificarte cuando estás conectado. **Hay dos tipos de direcciones IP.**

IP Pública

Es la dirección que asignan las empresas que dan acceso a Internet y sirve para **identificarte dentro de Internet** cuando te conectas.
Nadie puede navegar por la red sin una IP, y ninguna página web puede estar online si no tiene una IP asociada. Cuando se escribes una dirección como 'www.google.es', lo que hace el navegador es **traducir ese texto a una dirección IP** para poder conectarse a la página de Google y acceder a su contenido.
Estas direcciones IP públicas son como la matrícula que se te asigna cuando te conectas. Es una manera de identificarte como usuario en la inmensidad de la red, ya que **ninguna IP se puede repetir.**

¿Qué es y para qué sirve una IP privada?



Las **IP Privadas**, que son las que se utilizan en redes privadas como la que creas en tu casa conectando varios dispositivos a través de tu WiFi. Cuando lo haces, cada dispositivo como tu impresora, tu router o tu smartphone tiene una IP propia, y para que no haya conflictos cada uno de ellos tendrá una IP diferente.
Las direcciones IP están formadas por **cuatro números de hasta tres cifras separados por tres puntos**. Los valores de cada número pueden variar entre 0 y 255
Hay tres rangos que **se reservan exclusivamente para las IPs privadas**, y que son los siguientes:
•**Clase A**: 10.0.0.0 a 10.255.255.255. Para las redes más grandes, como las de las compañías internacionales
•**Clase B**: 172.16.0.0 a 172.31.255.255. Para redes de tamaño mediano, como las redes de una universidad
•**Clase C**: 192.168.0.0 a 192.168.255.255. **Para las redes más pequeñas y domésticas**

Las IPs privadas **no se repiten dentro de una misma red.**
La **IP privada de tu ordenador no es la misma que la pública**. Dentro de tu red tu ordenador se identificará entre el resto de aparatos con su IP privada, pero cuando salgas a Internet lo harás mediante una IP pública que será diferente.

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.

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.

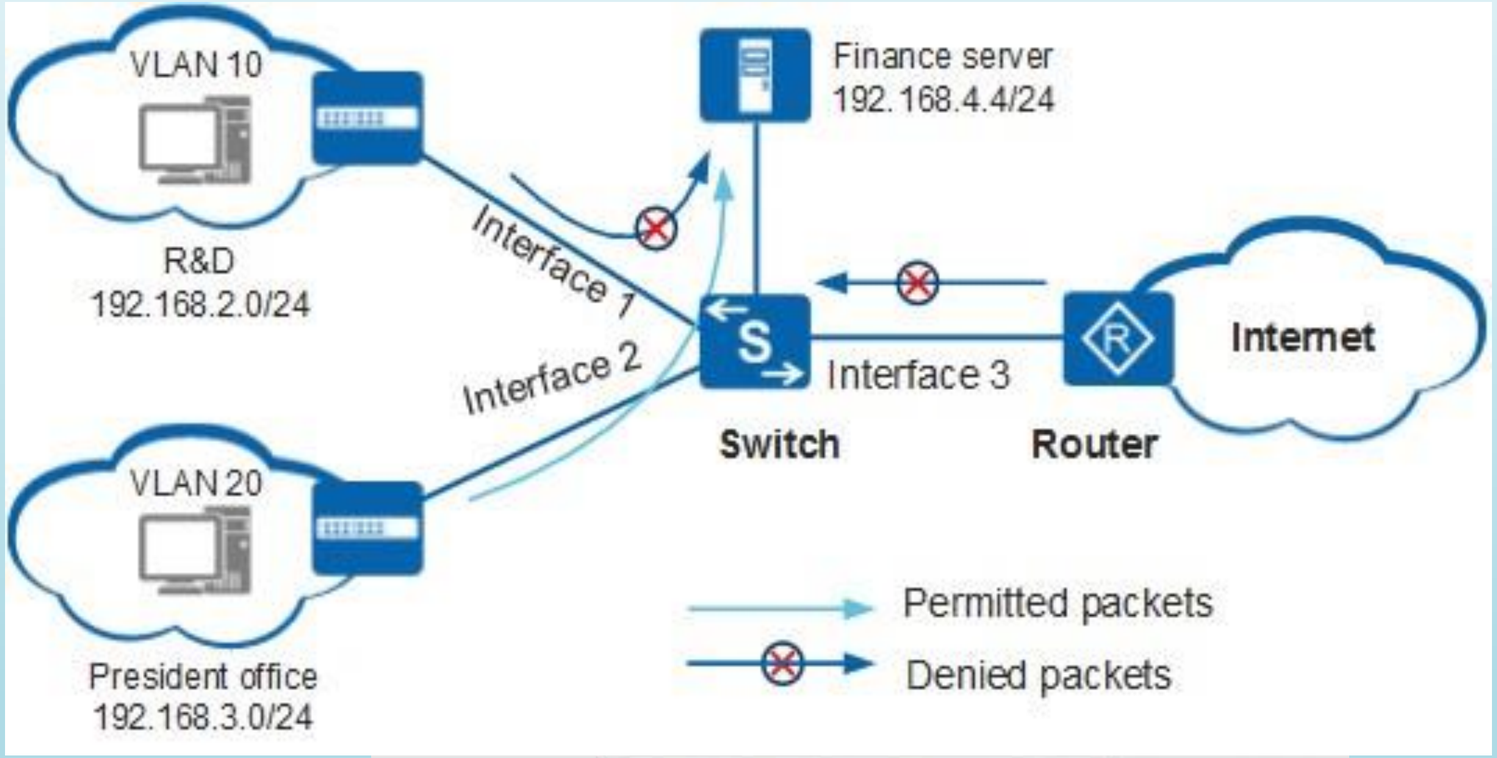


Imagen: https://forum.huawei.com/enterprise/es/data/attachment/forum/202002/13/123439gyaffy9a5c039czr.png?acl1.png

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.
  Wireshark es una herramienta para capturar y analizar paquetes en una red. Puedes usarlo para solucionar problemas de red, analizar la seguridad de esta última, aprender diferentes protocolos de red y probar implementaciones de protocolos.

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.**

IPv4 utiliza una dirección de 32 bits, mientras que **IPv6** utiliza una de 128 bits. Esto significa que IPv6 ofrece 1.028 veces más direcciones que IPv4, lo que básicamente resuelve el problema de «quedarse sin direcciones» (al menos en un futuro previsible).

IPv4: 192.168.10.150
IPv6: 3002:0bd6:0000:0000:0000:ee00:0033:6778

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.