MÓDULO 1 MF0490_3: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

5 Monitorización de sistemas y comunicaciones

core networks

5 Monitorización de sistemas y comunicaciones

5.1 Dispositivos de comunicaciones

core networks

Tarjeta de Red

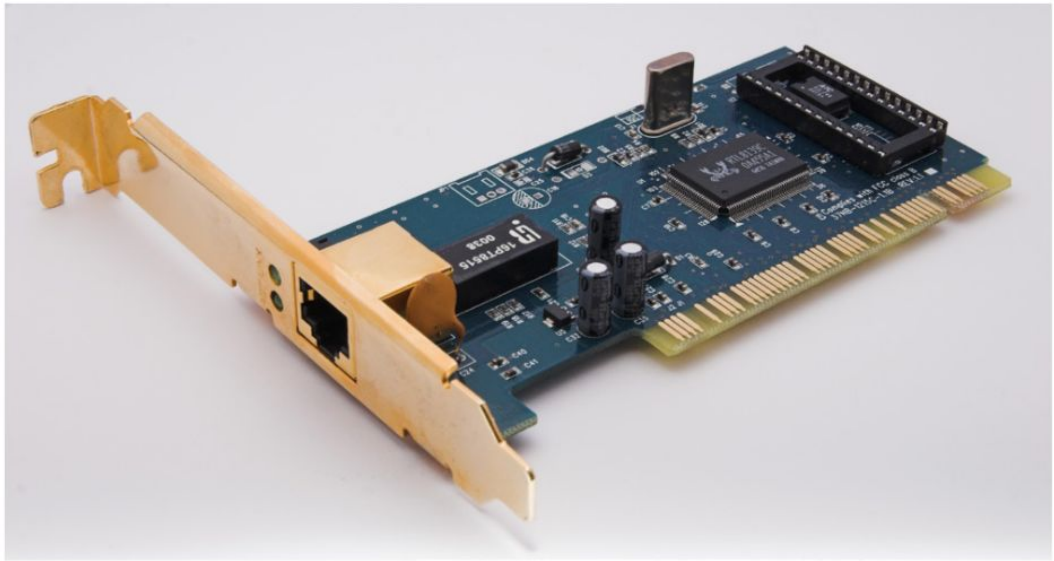


Figura 5.2. *Tarjeta de red PCI. Fuente: Commons Wikimedia*

Switch

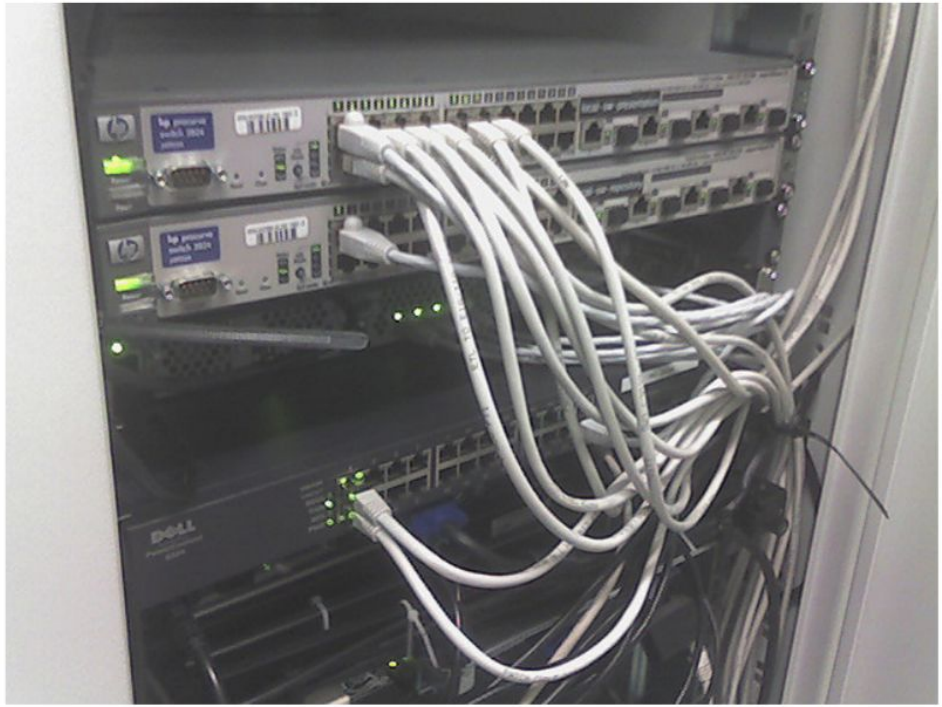


Figura 5.4. *Switch de HP. Cortesía de Tony Birrer*

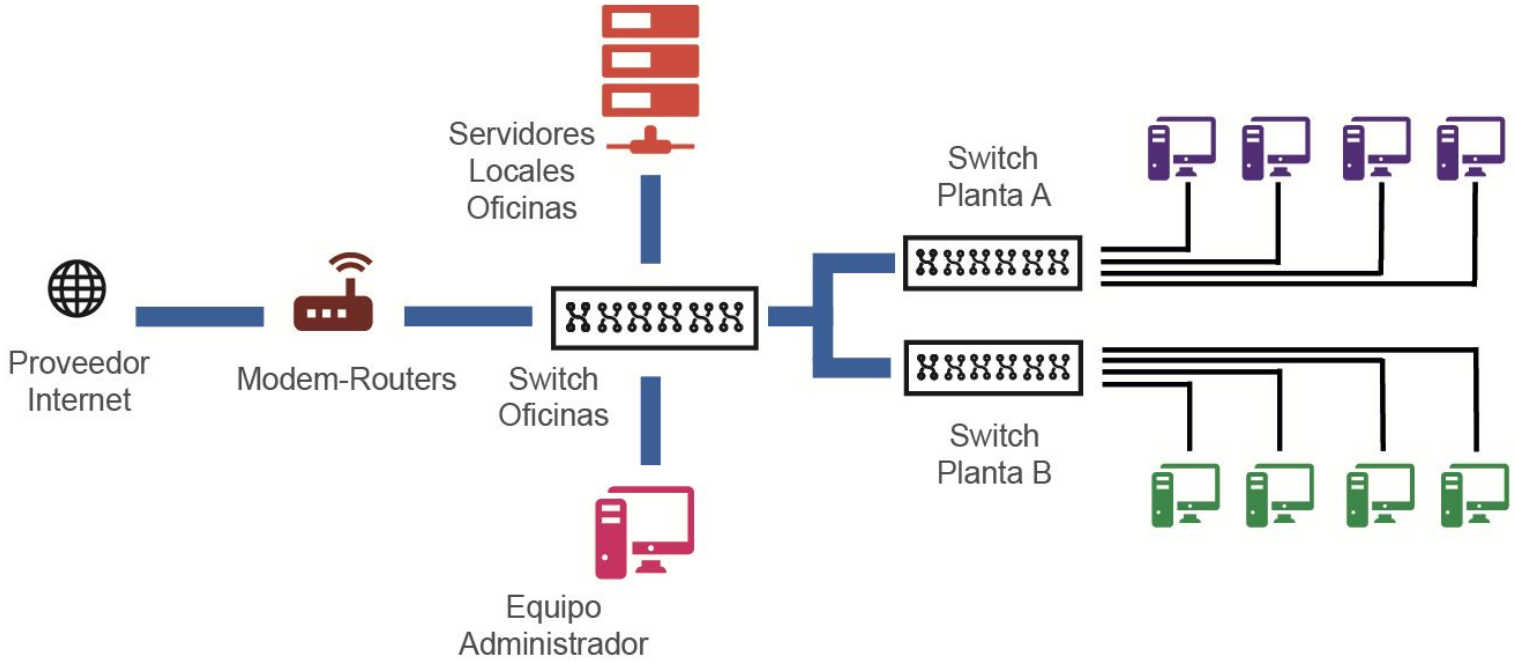
Punto inalámbrico

Figura 5.5. *Cisco Access Point. Cortesía de Per Olof Forsberg*

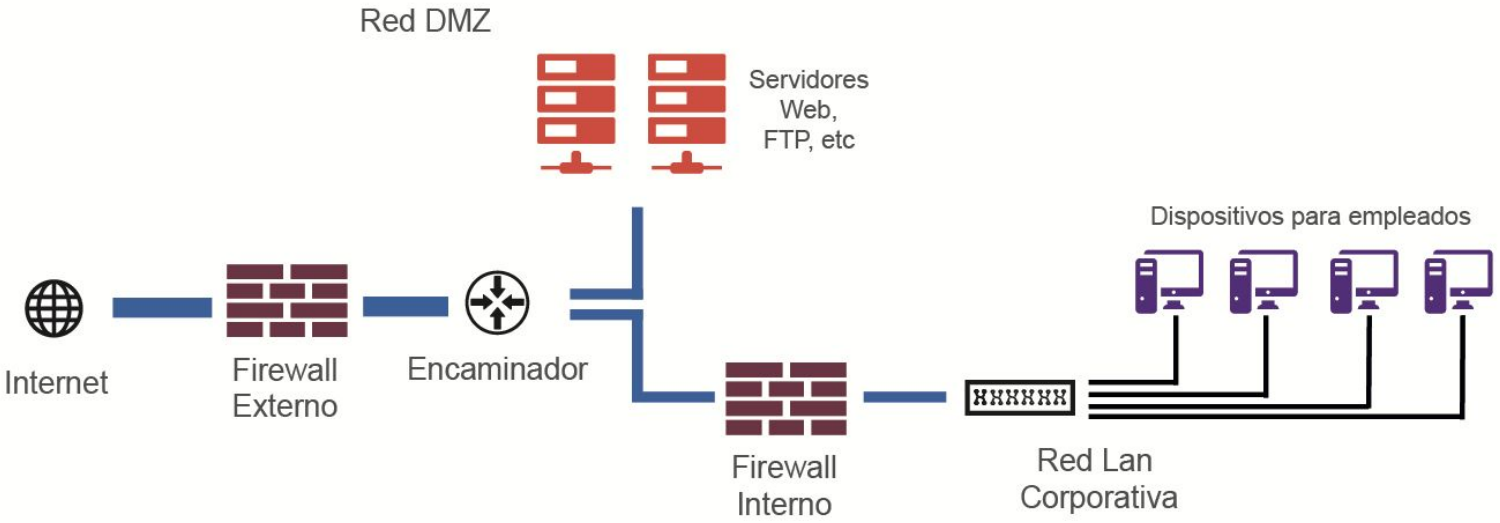
Router

Figura 5.6. *Router Asus WL-520GU. Cortesía de Jeff Keyzer*

Esquema


Servidores
Locales
Oficinas
Switch
Planta A
Proveedor
Internet
Modem-Routers
Switch
Oficinas
Switch
Planta B
Equipo
Administrador

Esquema


Red DMZ
Servidores
Web,
FTP, etc
Dispositivos para empleados
Internet
Firewall
Externo
Encaminador
Firewall
Interno
Red Lan
Corporativa

5 Monitorización de sistemas y comunicaciones

5.2 Protocolos y servicios de comunicaciones

core networks

Protocolos de comunicaciones

En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física.

core networks

HTTP

El protocolo de transferencia de hipertexto, por sus siglas en inglés, es utilizado por los navegadores web para realizar peticiones a los servidores web y recibir las respuestas de estos. Los mensajes empleados son de texto plano y su principal característica es que emplea una serie de métodos para la gestión de estos, así como una serie de códigos para representar los estados de conexión.

HTTPS

Es la versión segura del protocolo HTTP, asegurada por el cifrado entre el cliente y el servidor SSL/TLS.

SMTP

El protocolo simple de transferencia de correo electrónico, por sus siglas en inglés, es el estándar de envío de mensajes por los clientes de correo electrónico en el formato exacto de los archivos. Está compuesto de tres secuencias de comando, MAIL, RCTP y DATA, para establecer la dirección de retorno, la de destino y el contenido del mensaje respectivamente.

FTP

El protocolo de transferencia de archivos, por sus siglas en inglés, es utilizado para transferir archivos entre dos máquinas conectadas en red mediante internet, pudiendo realizar las transferencias de dos tipos ASCII o binaria.

DNS

El protocolo sistema de dominio de nombres, por sus siglas en inglés, es un sistema para resolver en una red de servidores distribuidos, redes IP, los nombres de host IP de cada uno de ellos. Su función más importante es la asignación de nombres a una IP.

5 Monitorización de sistemas y comunicaciones

5.3 Parámetros de configuración y funcionamiento de los equipos de comunicaciones

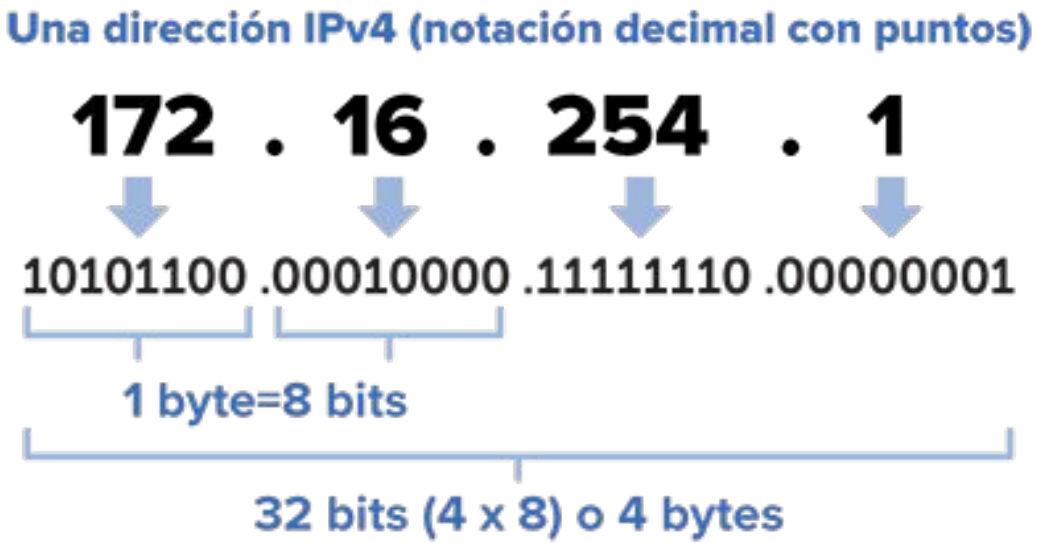
core networks

Dirección IP

La dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, teléfono inteligente) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits expresado en código hexadecimal, para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado en la red.

Dirección IP



Máscara de subred

La máscara de subred o subneting señala qué bytes (o qué porción) de su dirección es el identificador de la red.

Mediante la máscara de red o subred, un sistema (ordenador, puerta de enlace, router, etc.) podrá saber si debe enviar un paquete dentro o fuera de la subred en la que está conectado. Por ejemplo, si el router tiene la dirección IP 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una dirección IP con formato 192.168.1.X, se envía hacia la red local, mientras que direcciones con distinto formato de dirección IP serán enviadas hacia afuera (internet, otra red local mayor, entre otros).

De manera práctica, 255 identifica el octeto como parte del identificador de red y 0 identifica el octeto de subred.

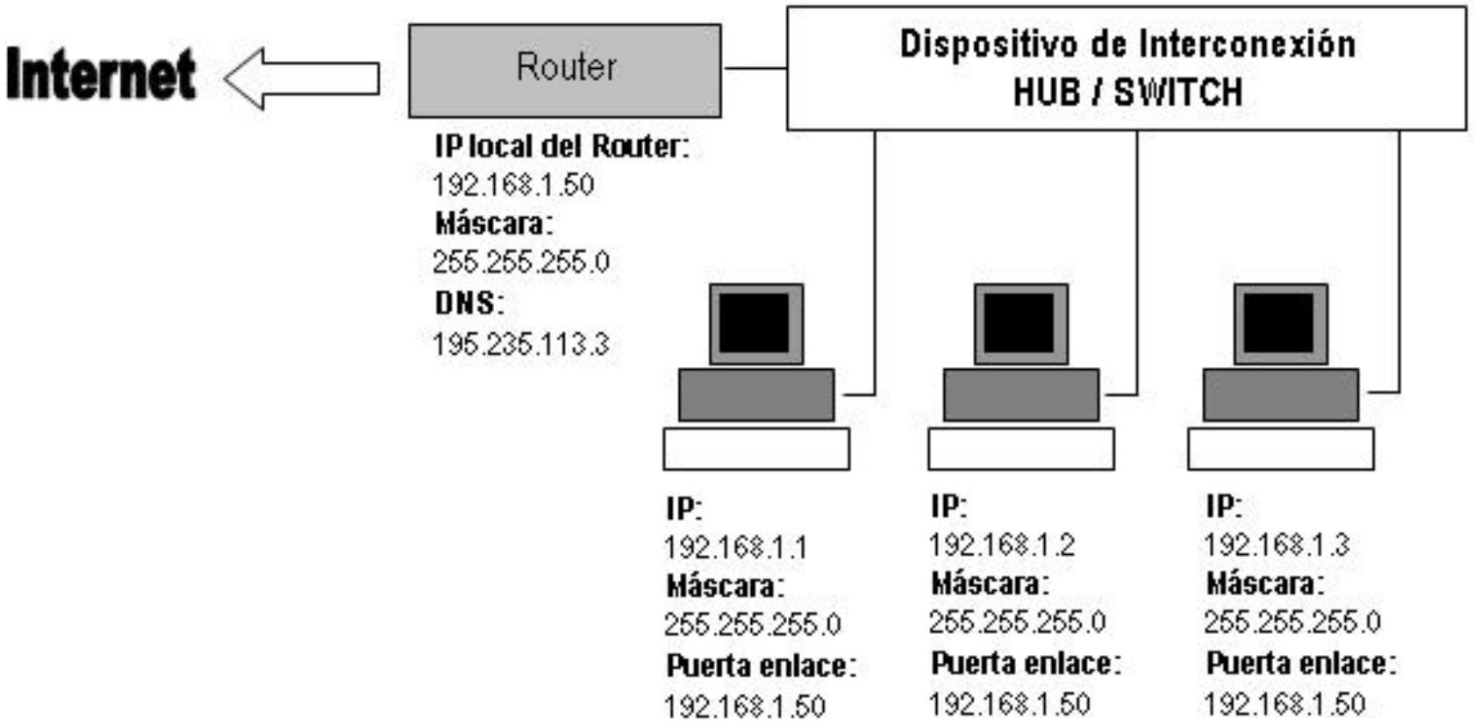
Puerta de enlace

La pasarela (en inglés gateway) o puerta de enlace es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más ordenadores.

Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

En las redes domésticas corresponde con el router de conexión al proveedor de servicios de internet y por tanto para su configuración, puerta de enlace predeterminada, se usa la IP interna de éste.

Esquema básico



Servidores DNS

El sistema de nombres de dominio (Domain Name System o DNS, por sus siglas en inglés) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes.

Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

Servicio DHCP

El protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP) es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

Este servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente.

core networks

Firewall

Un cortafuegos o firewall es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Todos los mensajes que entren o salgan de la red pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar el cortafuegos a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

core networks

5 Monitorización de sistemas y comunicaciones

5.4 Procesos de monitorización y respuesta

core networks

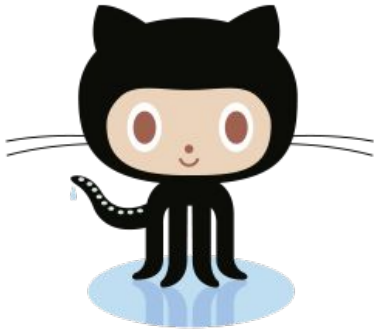
Ciclo de vida de gestión de incidencias

- Detección y registro
- Clasificación y soporte inicial
- Investigación y diagnóstico
- Resolución y recuperación
- Cierre de la incidencia
- Seguimiento de la incidencia

core networks

Herramientas de gestión de incidencias

Herramientas de control de versiones



GitHub

5 Monitorización de sistemas y comunicaciones

5.5 Herramientas de monitorización de puertos y servicios

core networks

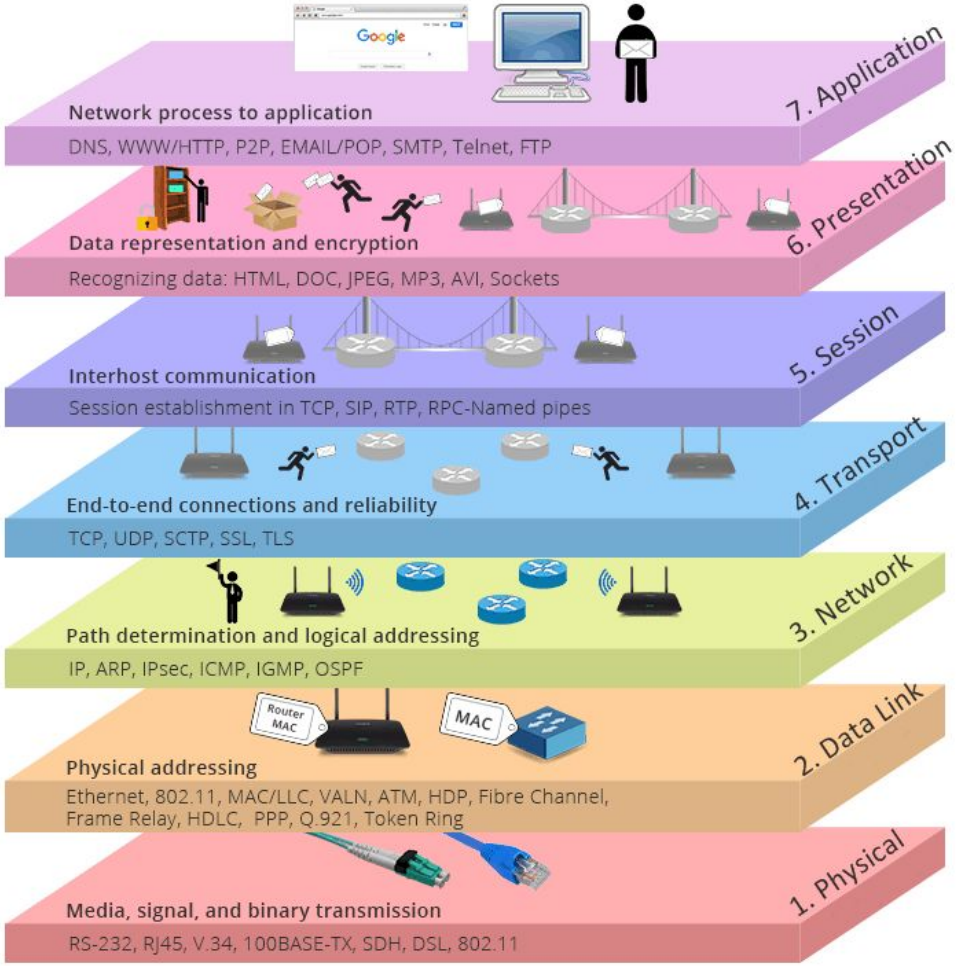
Modelo TCP/IP

El modelo TCP/IP es una descripción de protocolos de red desarrollado por Vinton Cerf y Robert E. Kahn, en la década de 1970. Fue implantado en la red ARPANET, la primera red de área amplia (WAN), desarrollada por encargo de DARPA, una agencia del Departamento de Defensa de los Estados Unidos, y predecesora de Internet. A veces se denomina como «modelo DoD» o «modelo DARPA».

El modelo TCP/IP es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

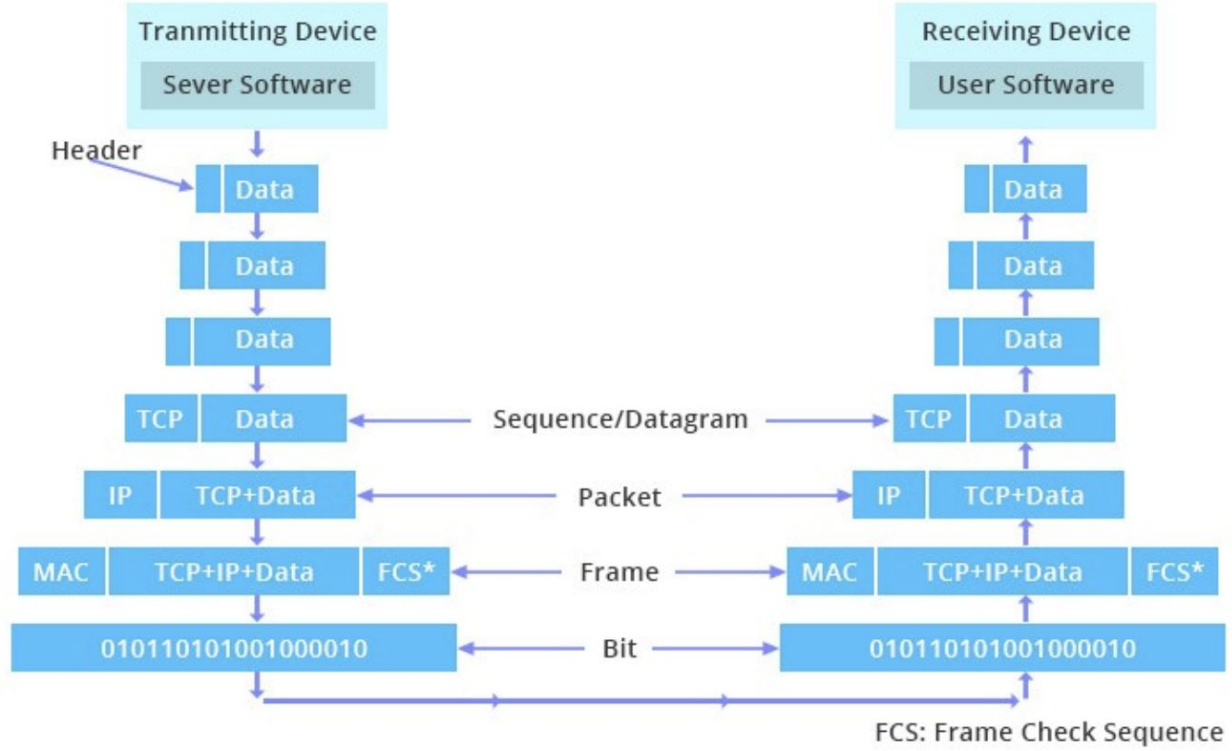
core networks

Capas

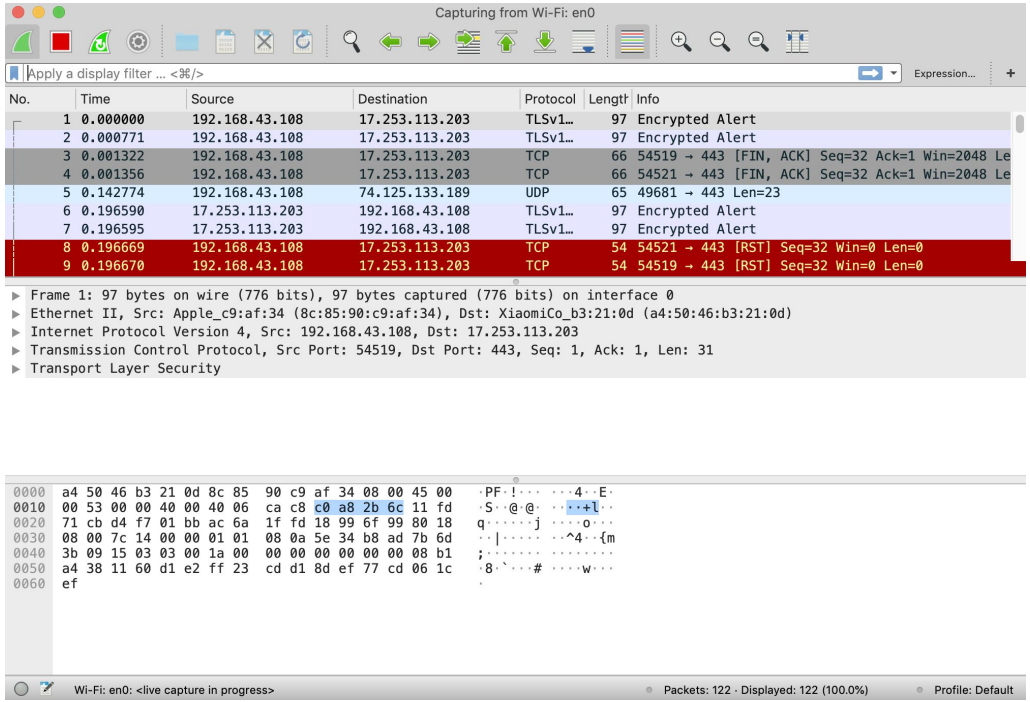


core networks

Transporte


Tranmitting Device
Sever Software
Receiving Device
User Software
Header
Data
Data
Data
TCP
Data
Sequence/Datagram
TCP
Data
IP
TCP+Data
Packet
IP
TCP+Data
MAC
TCP+IP+Data
FCS*
Frame
MAC
TCP+IP+Data
FCS*
0101101010010000 10
Bit
0101101010010000 10
FCS: Frame Check Sequence

Whireshark


Capturing from Wi-Fi: en0
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.43.108 17.253.113.203 TLSv1… 97 Encrypted Alert
2 0.000771 192.168.43.108 17.253.113.203 TLSv1… 97 Encrypted Alert
3 0.001322 192.168.43.108 17.253.113.203 TCP 66 54519 → 443 [FIN, ACK] Seq=32 Ack=1 Win=2048 Le
4 0.001356 192.168.43.108 17.253.113.203 TCP 66 54521 → 443 [FIN, ACK] Seq=32 Ack=1 Win=2048 Le
5 0.142774 192.168.43.108 74.125.133.189 UDP 65 49681 → 443 Len=23
6 0.196590 17.253.113.203 192.168.43.108 TLSv1… 97 Encrypted Alert
7 0.196595 17.253.113.203 192.168.43.108 TLSv1… 97 Encrypted Alert
8 0.196669 192.168.43.108 17.253.113.203 TCP 54 54521 → 443 [RST] Seq=32 Win=0 Len=0
9 0.196670 192.168.43.108 17.253.113.203 TCP 54 54519 → 443 [RST] Seq=32 Win=0 Len=0
Frame 1: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0
Ethernet II, Src: Apple_c9:af:34 (8c:85:90:c9:af:34), Dst: XiaomiCo_b3:21:0d (a4:50:46:b3:21:0d)
Internet Protocol Version 4, Src: 192.168.43.108, Dst: 17.253.113.203
Transmission Control Protocol, Src Port: 54519, Dst Port: 443, Seq: 1, Ack: 1, Len: 31
Transport Layer Security
0000 a4 50 46 b3 21 0d 8c 85 90 c9 af 34 08 00 45 00
0010 00 53 00 00 40 00 40 06 ca c8 c0 a8 2b 6c 11 fd
0020 71 cb d4 f7 01 bb ac 6a 1f fd 18 99 6f 99 80 18
0030 08 00 7c 14 00 00 01 01 08 0a 5e 34 b8 ad 7b 6d
0040 3b 09 15 03 03 00 1a 00 00 00 00 00 00 00 08 b1
0050 a4 38 11 60 d1 e2 ff 23 cd d1 8d ef 77 cd 06 1c
0060 ef
Wi-Fi: en0: <live capture in progress>
Packets: 122 · Displayed: 122 (100.0%)
Profile: Default

5 Monitorización de sistemas y comunicaciones

5.6 Herramientas de monitorización de sistemas y servicios

core networks

Nagios

Recurso

https://www.howtoforge.com/tutorial/ubuntu-nagios/

core networks

5 Monitorización de sistemas y comunicaciones

5.7 Sistemas de gestión de información y eventos de seguridad

core networks

SIEM

SIEM (información de seguridad y gestión de eventos), es una tecnología capaz de detectar rápidamente, responder y neutralizar las amenazas informáticas. Su objetivo principal es el de proporcionar una visión global de la seguridad de la tecnología de la información.

Un sistema SIEM permite tener control absoluto sobre la seguridad informática de la empresa. Al tener información y administración total sobre todos los eventos que suceden segundo a segundo, resulta más fácil detectar tendencias y centrarse en patrones fuera de lo común.

core networks

SIEM (II)

La tecnología SIEM nace de la combinación de las funciones de dos categorías de productos: SEM (gestión de eventos de seguridad) y SIM (gestión de información de seguridad).

- SEM centraliza el almacenamiento y permite un análisis casi en tiempo real de lo que está sucediendo en la gestión de la seguridad, detectando patrones anormales de accesibilidad y dando mayor visibilidad a los sistemas de seguridad.
- Mientas que SIM recopila los datos a largo plazo en un repositorio central para luego analizarlo, proporcionando informes automatizados al personal de seguridad informática.

5 Monitorización de sistemas y comunicaciones

5.8 Gestión de registros de elementos de red y filtrado

core networks

Características de gestión de logs

- **Colección de datos de logs**: Esto cubre poder recoger todos los registros utilizando métodos basados en agentes o sin agentes, o una combinación de los dos.
- **Retención eficiente**: Si bien la recolección y almacenamiento de datos de registro no suena como un gran reto de ingeniería, ser capaz de recoger gigabytes e incluso terabytes de datos de registro eficientemente y retenerlos mientras se provee búsquedas y acceso rápido no es trivial. Dado que muchas regulaciones indican términos específicos para la retención de datos de registro (durante muchos años), esta función es crítica para un sistema de administración de logs.

Características de gestión de logs(II)

- **Búsquedas**: La búsqueda es la principal forma de acceso a la información en todos los logs, incluyendo los logs de aplicaciones personalizadas. Buscar es indispensable para la investigación de registros, análisis forense de registros y la búsqueda de fallos durante el uso de logs de aplicación para la solución de problemas.
- **Indexación**: La indexación de logs es un componente clave de un sistema de gestión de registros. La tecnología de indexación crea una estructura de datos llamada índice, que permite búsqueda rápida de tipo palabra clave o tipo booleano a través de todo el almacenamiento de logs.

Características de gestión de logs(III)

- **Reportes**: Los reportes y reportes programados cubren todos los datos recolectados por el producto de gestión de logs y es similar a los reportes del SIEM. La fortaleza de los reportes sea para razones de seguridad, regulaciones u operación puede hacer o deshacer la solución de gestión de logs. La presentación de reportes debe ser rápida, personalizable y fácil de usar para una amplia gama de propósitos.