SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

1.7.0. Capítulo 7

Identificación de servicios

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Una extensa área de la seguridad de la información es la seguridad lógica, abordando la problemática del acceso lógico.

El perímetro de los activos se extiende con el uso de las redes.

Complementando los mecanismos de acceso lógico internos (identificación, autenticación y autorización), procede dar un paso más allá de este dominio lógico, para enfrentar otra área crucial de la seguridad lógica, como es la seguridad de redes, analizando posibles vulnerabilidades.

2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS

1968 ARPA (Agencia de Investigación de Proyectos Avanzados dependiente del Departamento de Defensa de EEUU) aprueba un plan de comunicaciones que permitieran conectar redes con sistemas de transmisión diferentes, que tuvieran tolerancia a fallos, en caso de que una parte de la red no estuviera disponible, y que permitieran la ejecución de diversas aplicaciones (ARPANET).

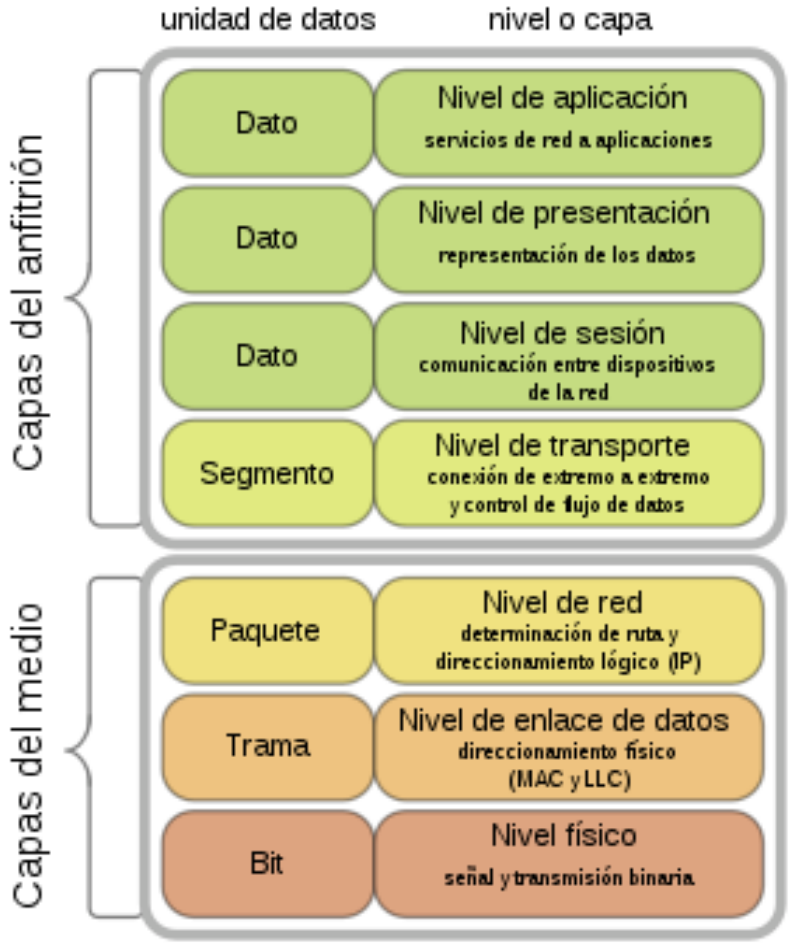
El primer enlace de ARPANET se estableció el 21 de noviembre de 1969 entre UCLA y Stanford.

1983 Se inicia la transición al modelo de protocolos TCP/IP.

2.1. ARQUITECTURA TCP/IP

Modelo OSI (Open System Interconnection):

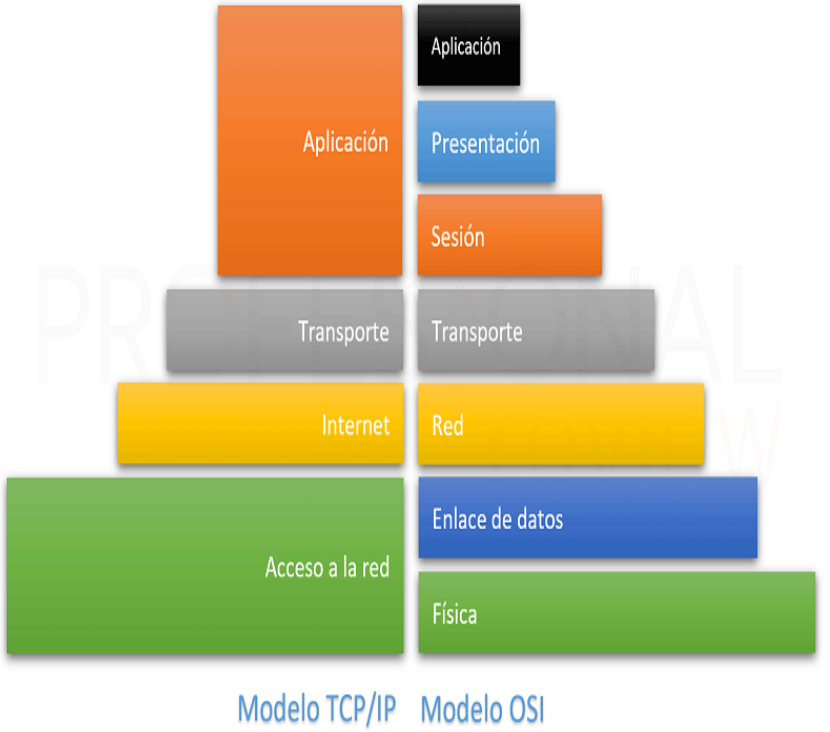
- **Nivel 1: capa física**, debe proporcionar conexiones (fiables o no) punto a punto.
- **Nivel 2: capa de enlace**, debe proporcionar una conexión fiable, punto a punto.
- **Nivel 3: capa de red**, debe proporcionar direccionamiento y enrutamiento para la entrega, fiable o no, de datagramas entre puntos de la red.
- **Nivel 4: capa de transporte**, debe proporcionar entrega fiable de paquetes entre puntos de la red.
- **Nivel 5: capa de sesión**, debe manejar las sesiones entre aplicaciones internas al nodo.
- **Nivel 6: capa de presentación**, debe presentar la información con independencia del nodo.
- **Nivel 7: capa de aplicación**, protocolos, funciones o servicios que usan la red.



2.1. ARQUITECTURA TCP/IP

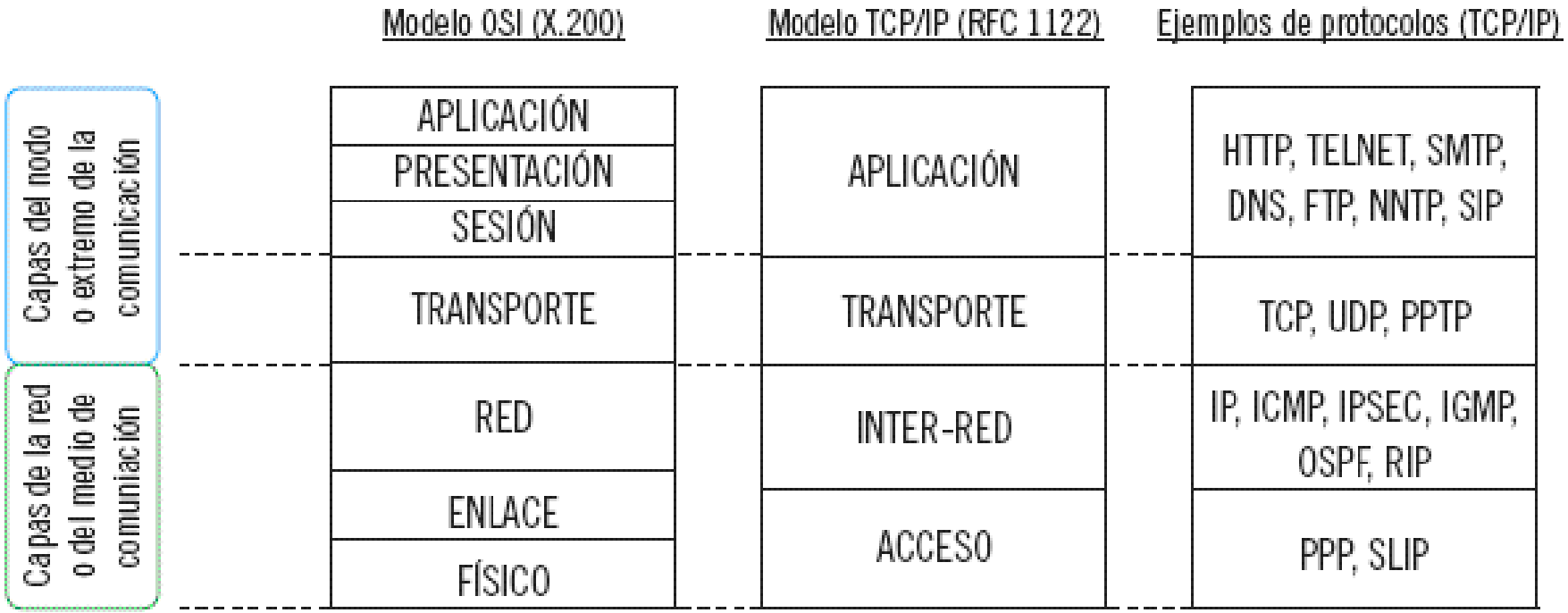
Modelo TCP/IP:

- Capa 1, o **capa de acceso** al medio o de enlace, que dicta que debe existir un protocolo para conectar el nodo a la red.
- Capa 2, o **capa inter-redes**, que permite que los nodos envíen paquetes a la red, y que estos lleguen (ordenados o no, con errores o no) a su destino, quizá por diferentes caminos. El protocolo más importante es el IP.
- Capa 3, o **capa de transporte**, que permite que los nodos establezcan una conversación (resolución de los errores y ordenación de los paquetes). Los protocolos más importantes son TCP (orientado a establecer o mantener la conversación mediante una conexión fiable nodo a nodo), y UDP (que no está orientado al establecimiento de una conexión nodo a nodo, y que no es fiable).
- Capa 4, o **capa de aplicación**, que entrega unos protocolos de red disponibles para las aplicaciones del usuario. El más conocido es el protocolo HTTP, que emplean las aplicaciones de navegación web.



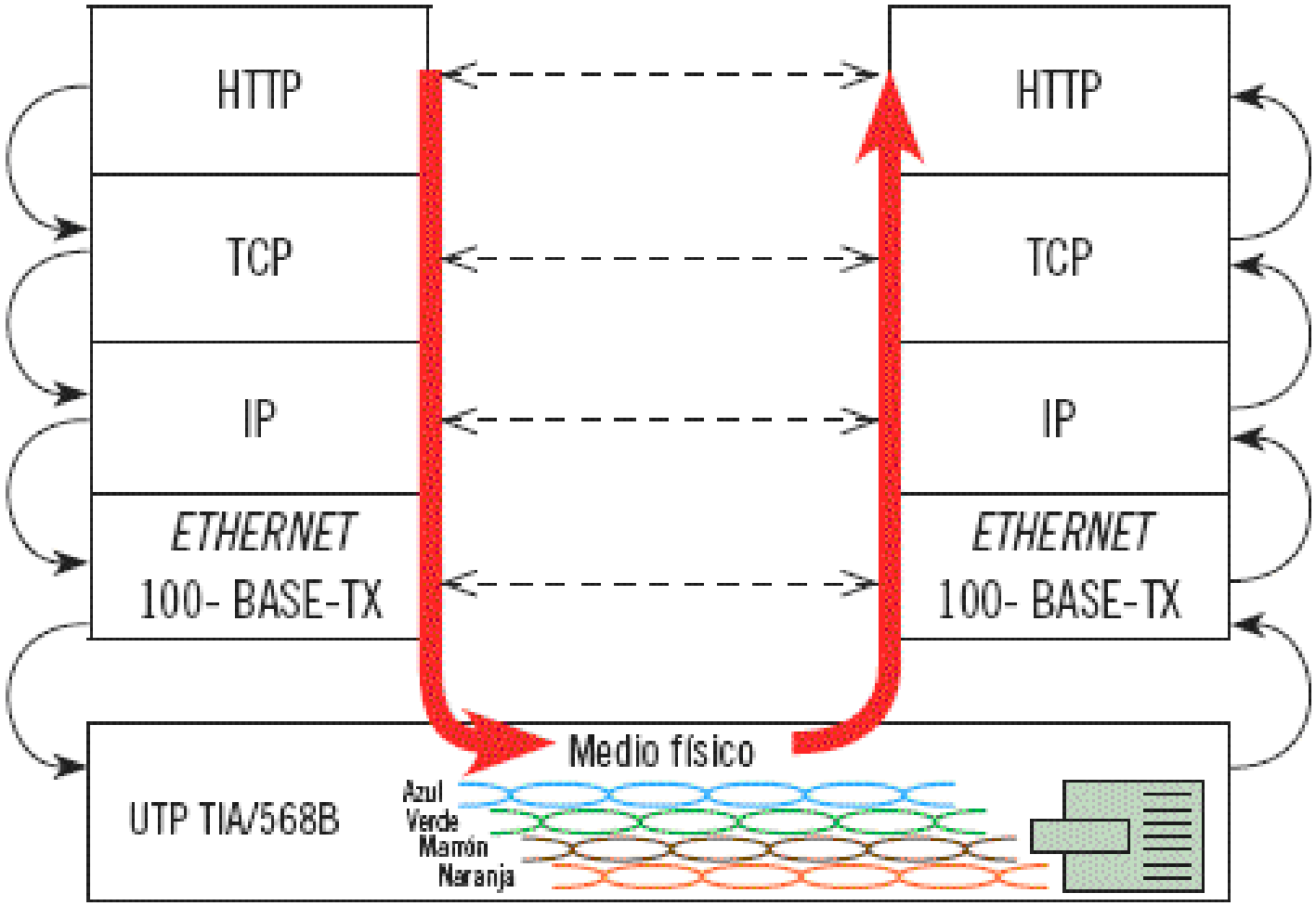
2.1. ARQUITECTURA TCP/IP

Modelo de comunicación OSI TCP/IP. Protocolos de ejemplo, representación gráfica del flujo de datos en una consulta web y encapsulación de la información

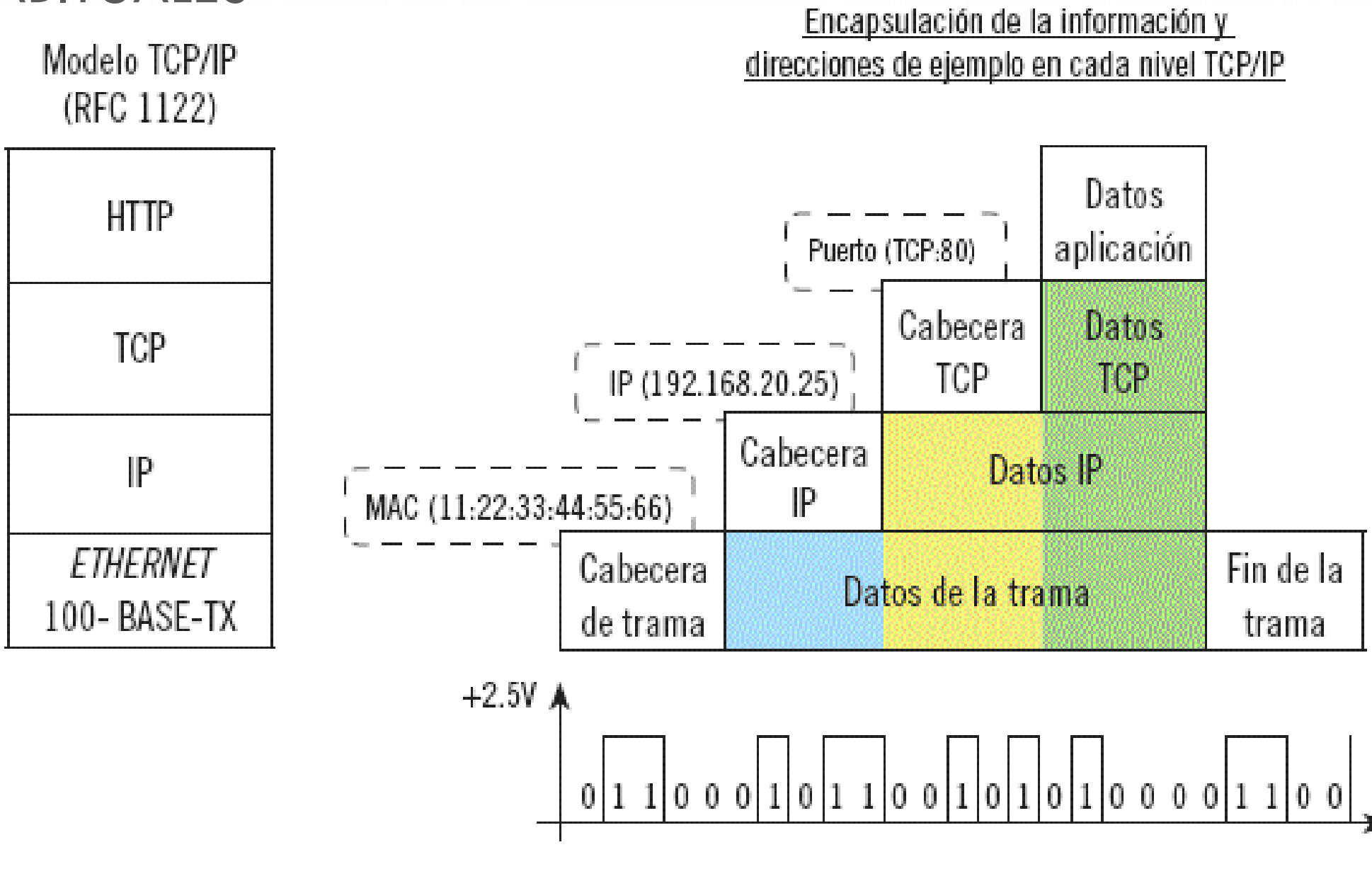


2.1. ARQUITECTURA TCP/IP

Ejemplo sencillo de comunicación web en LAN *Ethernet* 100Mbps con cable de 4 pares



2.2. PROTOCOLOS, SERVICIOS Y PUERTOS MÁS HABITUALES

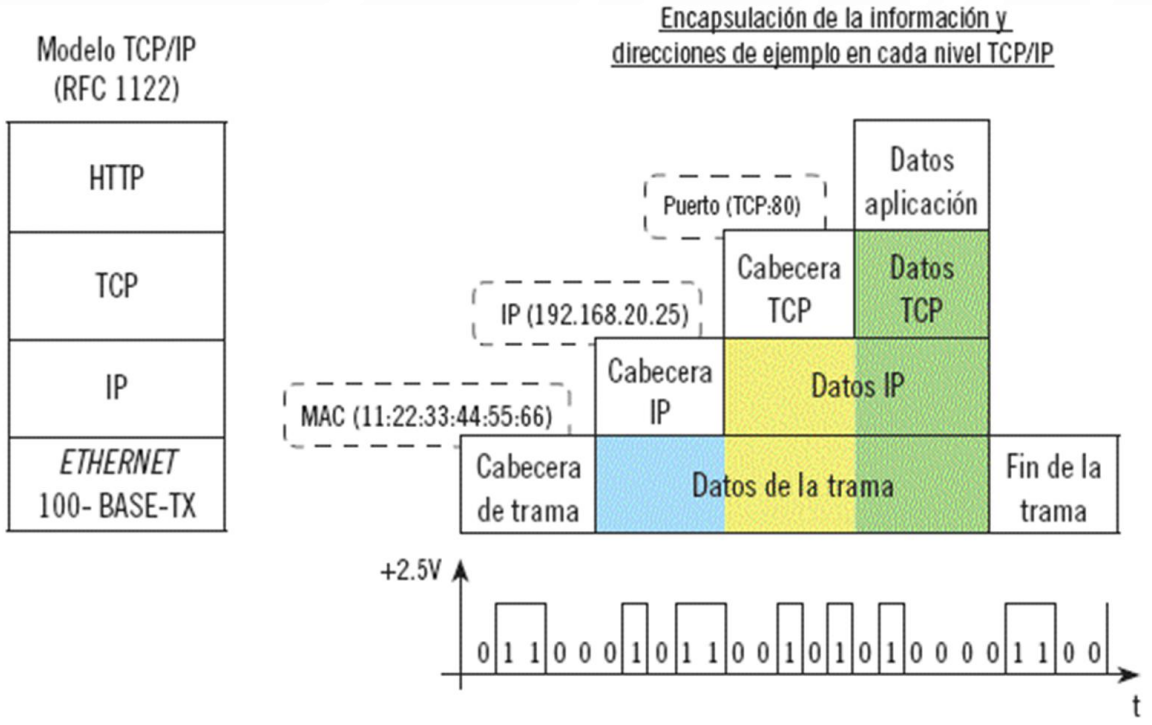


2.2. PROTOCOLOS, SERVICIOS Y PUERTOS MÁS HABITUALES

Cada nodo de la red dispone de una dirección.

En la capa de acceso se usa la dirección MAC (o Medium Access Control), del adaptador de red que conecta el nodo al medio físico.

En la capa de inter-red se usa la dirección IP (o Internet Protocol), que se configura para cada conexión de red.



2.2. PROTOCOLOS, SERVICIOS Y PUERTOS MÁS HABITUALES

Existen 65536 puertos disponibles para el protocolo TCP, y también hay 65535 puertos definibles para el protocolo UDP, siendo la entidad IANA el órgano responsable de mantener la definición de las asignaciones estándar, dividiendo los puertos en tres rangos (RFC 6335):

- Puertos de sistema o puertos bien conocidos: 0-1023 .
- Puertos de usuario o puertos registrados: 1024-49151.
- Puertos dinámicos o privados o efímeros: 49152-65535.

Estos puertos se pueden cambiar, pero no se pueden solapar.

https://es.wikipedia.org/wiki/Anexo:Puertos_de_red

Actividades

SE HA AVERIADO UN SERVIDOR DE LA EMPRESA, Y DE MANERA TEMPORAL, SE PIENSA ATAJAR EL PROBLEMA EMPLEANDO OTRO EQUIPO ANTIGUO, QUE SE GUARDABA PARA CASOS DE EMERGENCIA. LA ÚLTIMA COPIA DE SEGURIDAD QUE SE TIENE ES ANTIGUA, Y TRAS RESTAURARLA, SOLO SE ENCUENTRAN ACCESIBLES LOS PUERTOS TCP/ 25, UDP/ 68, TCP/ 80, TCP/ 115, TCP-UDP/ 123, Y TCP/ 465. SE ESPERA QUE EL SERVIDOR DE LA EMPRESA PROPORCIONE LOS SIGUIENTES SERVICIOS: (1) ACCESO HTTP Y HTTPS A LA WEB CORPORATIVA, (2) SERVICIO FTP DE TRANSFERENCIA DE FICHEROS, (3) SERVICIO SMTP DE ENVÍO DE CORREO ELECTRÓNICO, (4) SERVICIO NTP DE SINCRONIZACIÓN HORARIA, (5) SERVICIO DE NOMBRES DNS, Y (6) SERVICIO DE CONFIGURACIÓN DINÁMICA DE RED DHCP. ¿QUÉ SERVICIOS DE LOS ESPERADOS NO ESTÁN DISPONIBLES A PARTIR DE LA COPIA DE SEGURIDAD RESTAURADA?

2.2. PROTOCOLOS, SERVICIOS Y PUERTOS MÁS HABITUALES

Debe valorarse cerrar los puertos que no sean estrictamente necesarios.

Debe valorarse la conveniencia de aplicar la contramedida de cambiar la prestación de los servicios desde sus puertos por defecto (esperados o bien conocidos) a puertos diferentes, bien de usuario o bien dinámicos (no recomendables).

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS

Las aplicaciones, protocolos y servicios, ofrecen intrínsecamente vulnerabilidades.

Es crucial reducir al mínimo las vías de acceso lógico a las potenciales vulnerabilidades, es decir, minimizar los puertos de acceso a la red:

- **Eliminando todos los servicios que no se necesiten.**
- **prohibiendo el acceso por defecto a todos los puertos (tanto en los equipos de seguridad perimetral como en los propios servidores).**
- **Habilitando solo los servicios y su acceso a través de puertos de comunicaciones cuando realmente se necesite.**

3.1. HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

Todos los sistemas, Windows y Linux, incorporan herramientas de red:

PING

No emplea ningún protocolo de transporte (es decir, no usa ningún puerto TCP o UDP), sino que funciona directamente en la capa de red, empleando el protocolo de mensajes de control ICMP (Internet Control Message Protocol), que es parte del protocolo IP.

3.1. HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

Todos los sistemas, Windows y Linux, incorporan herramientas de red:

TRACEROUTE

Orientada al diagnóstico de la ruta de conexión.

Empleando el campo TTL (Time To Live) de los paquetes o datagramas del protocolo de red IP, permite averiguar qué ruta sigue un paquete hasta alcanzar su destino.

El campo TTL permite que un paquete no perdure eternamente en la red si no alcanza su destino, para lo que cada equipo que procesa el paquete le resta una unidad, y cuando alcanza el valor 0, el equipo desecha el paquete informando al remitente.

3.1. HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

Todos los sistemas, Windows y Linux, incorporan herramientas de red:

NSLOOKUP

Orientada a obtener información de un dominio o de una dirección IP, este comando realiza consultas a un servidor de nombre (DNS), para averiguar la traducción de un nombre de internet o dominio, a su dirección IP; o viceversa.

En Linux, el comando empleado es dig.

Por ejemplo, si se trata de un servicio de correo electrónico, se puede averiguar la dirección IP para acceder al servicio, realizando la siguiente consulta:

nslookup –type = MX nombre_de_dominio_de_interes

3.1. HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

Todos los sistemas, Windows y Linux, incorporan herramientas de red:

WHOIS

Orientada a obtener información de un dominio, o de una dirección IP, esta aplicación permite averiguar quién es el propietario de un nombre de dominio o de una dirección IP, dirigiendo la consulta a un servidor whois (por ejemplo a whois.nic.es, responsable de los dominios “. es”).

3.1. HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

Todos los sistemas, Windows y Linux, incorporan herramientas de red:

TELNET

Orientado al establecimiento de una conexión, esta aplicación permite iniciar una sesión remota en un nodo remoto, siempre en modo carácter o modo terminal, para gestionar el equipo remoto mediante comandos.

También existe la aplicación SSH, de uso muy extendido y recomendado por emplear conexiones cifradas.

3.2. HERRAMIENTAS DE ANÁLISIS DE PUERTOS

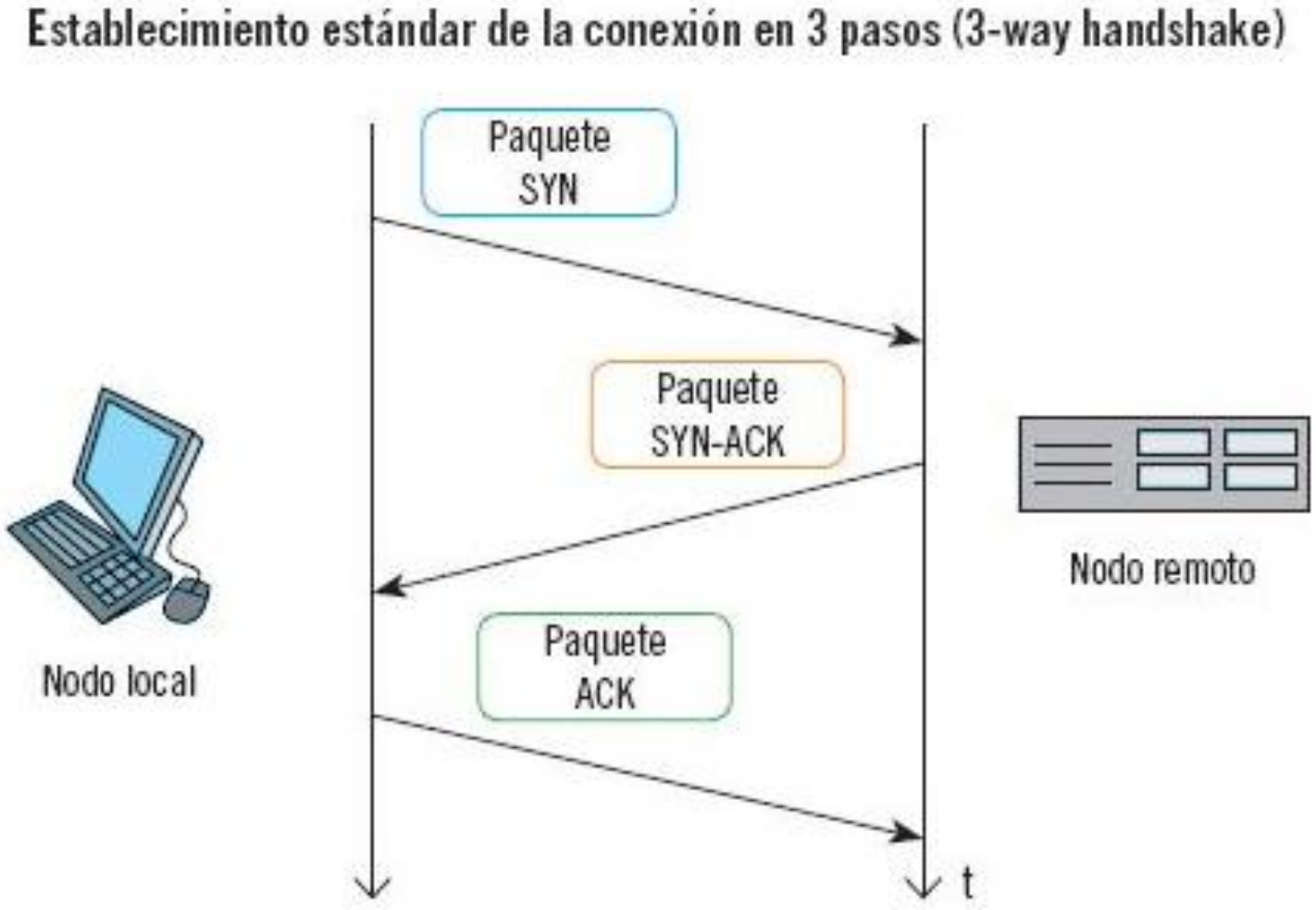
Son herramientas de análisis de nodos remotos:

SUPERSCAN (McAfee)

NMAP

3.2. HERRAMIENTAS DE ANÁLISIS DE PUERTOS

Procedimiento de conexión de tres pasos estándar de TCP:



4. HERRAMINETAS DE ANÁLISIS DE TRÁFICO

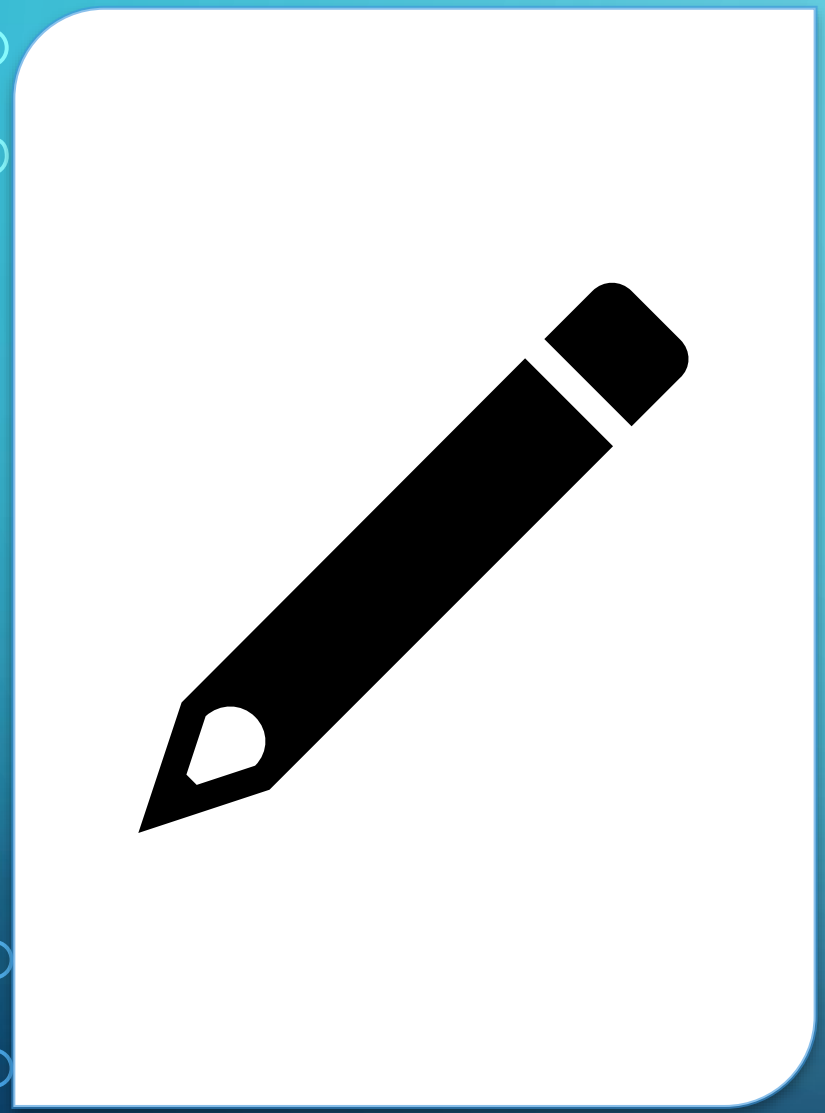
Herramientas de captura de tráfico (sniffers):

MICROSOFT NETWORK MONITOR

TCPDUMP

WIRESHARK

Actividades



1.7.100.1.EJERCICIOSCAPITULO_7.DOCX