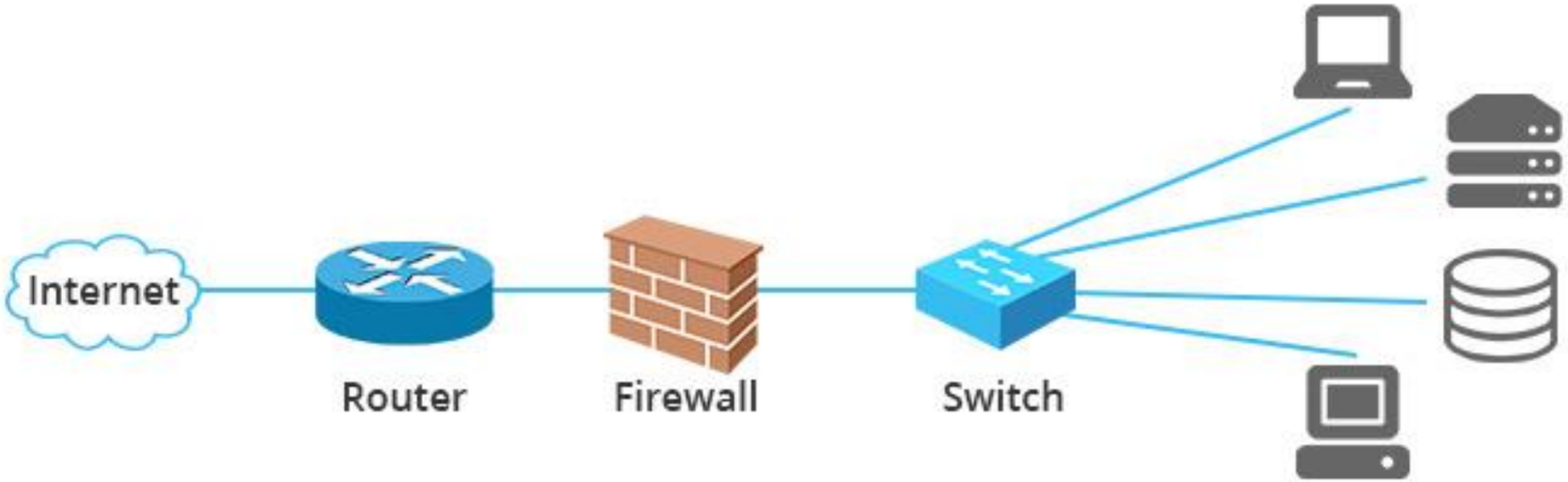
UNIVERSIDAD ADOLFO IBÁÑEZ

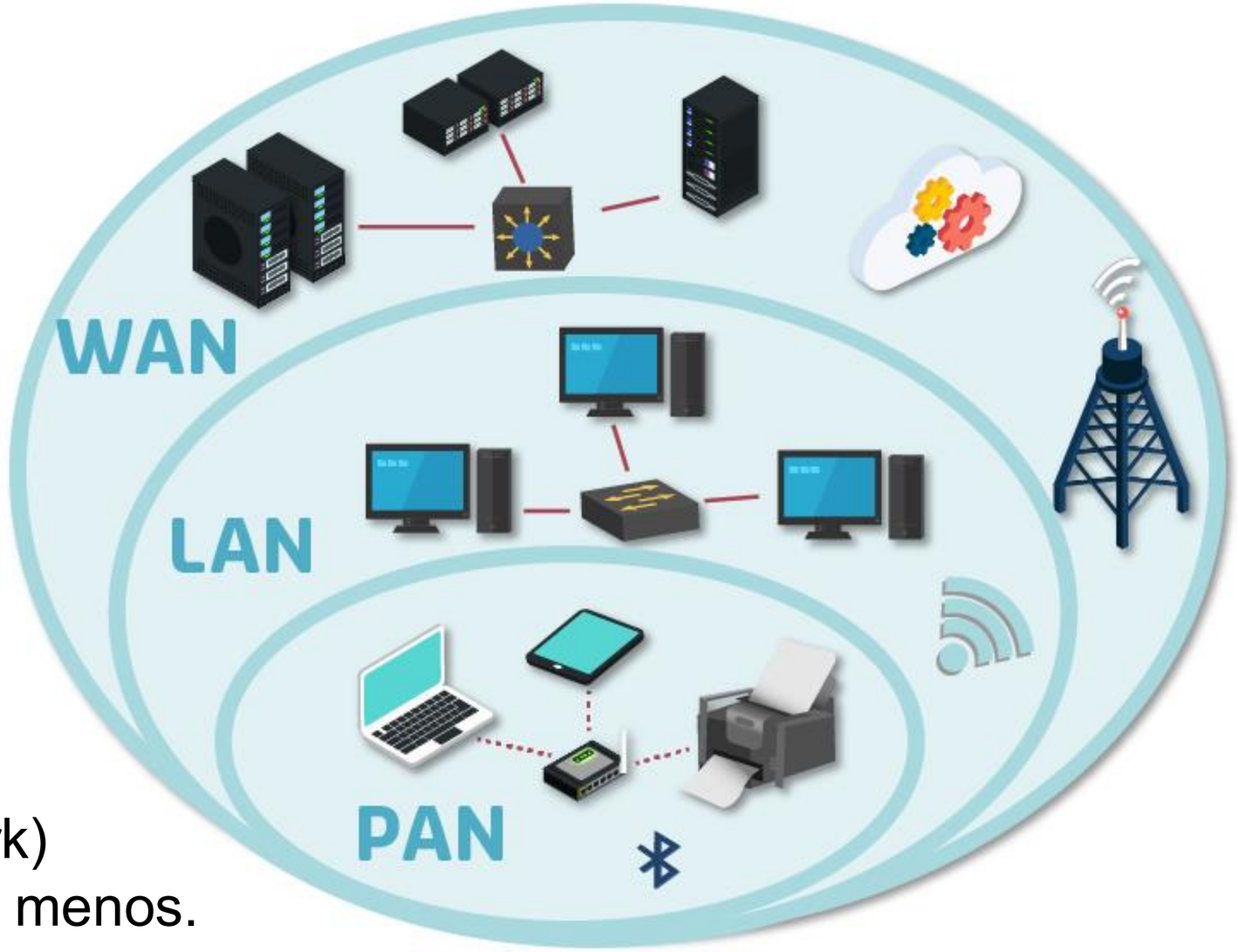
TICS413: SEGURIDAD TI

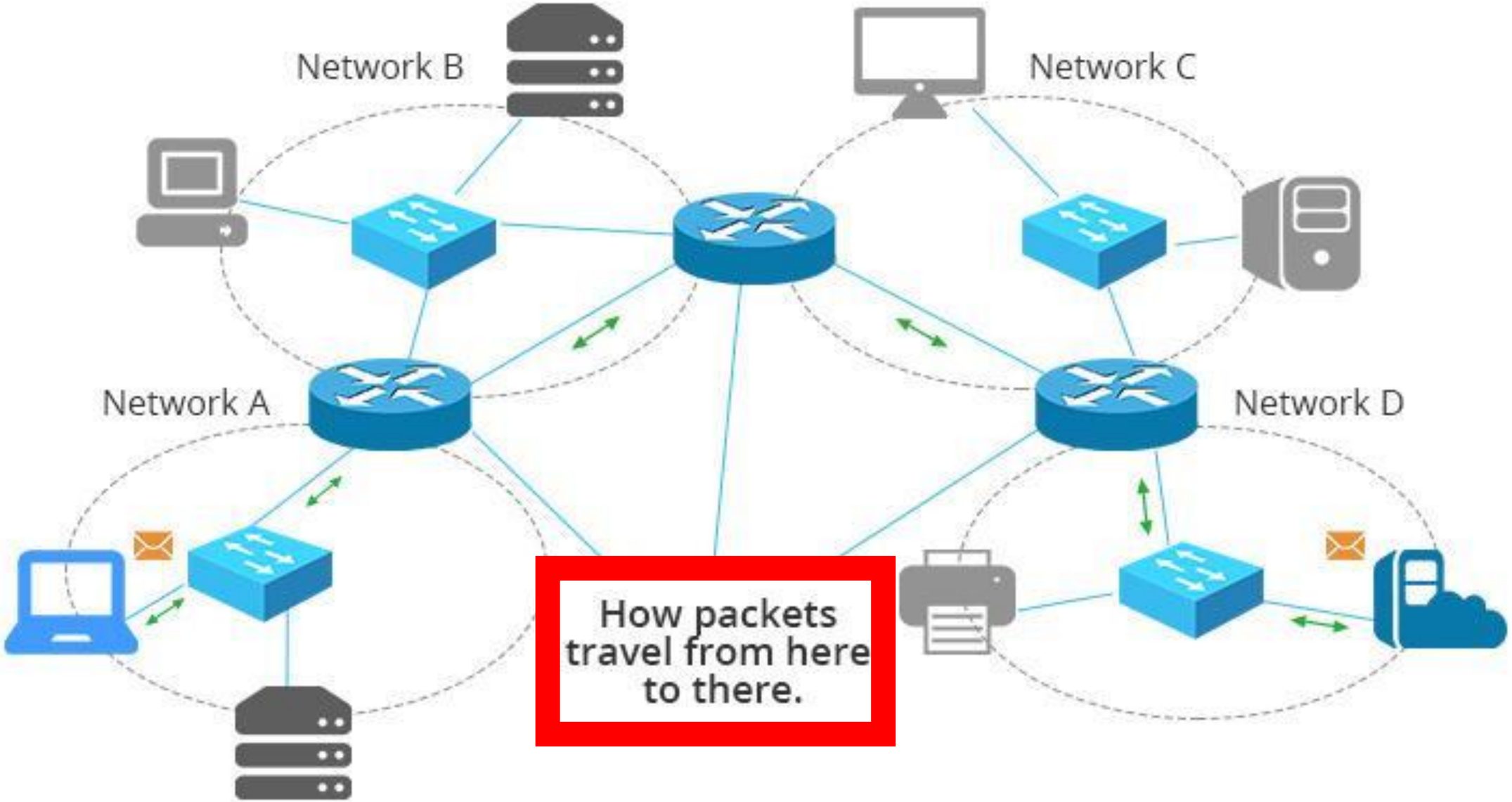
PRINCIPIOS Y SEGURIDAD EN REDES

ELEMENTOS

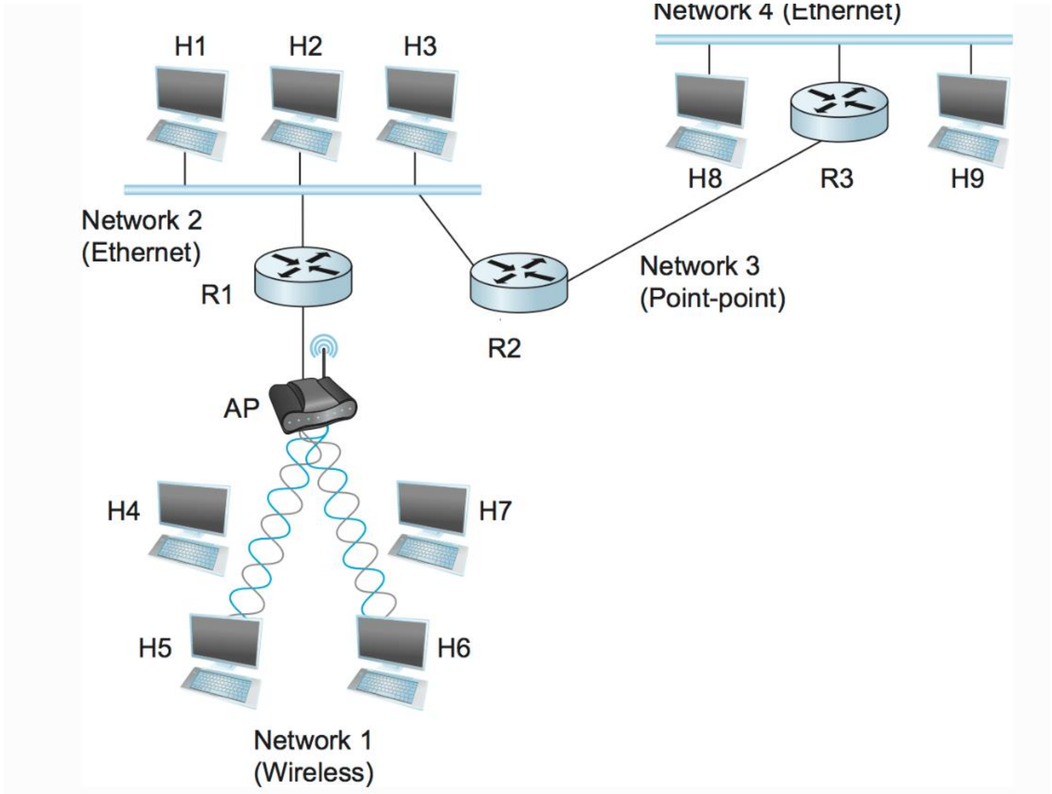


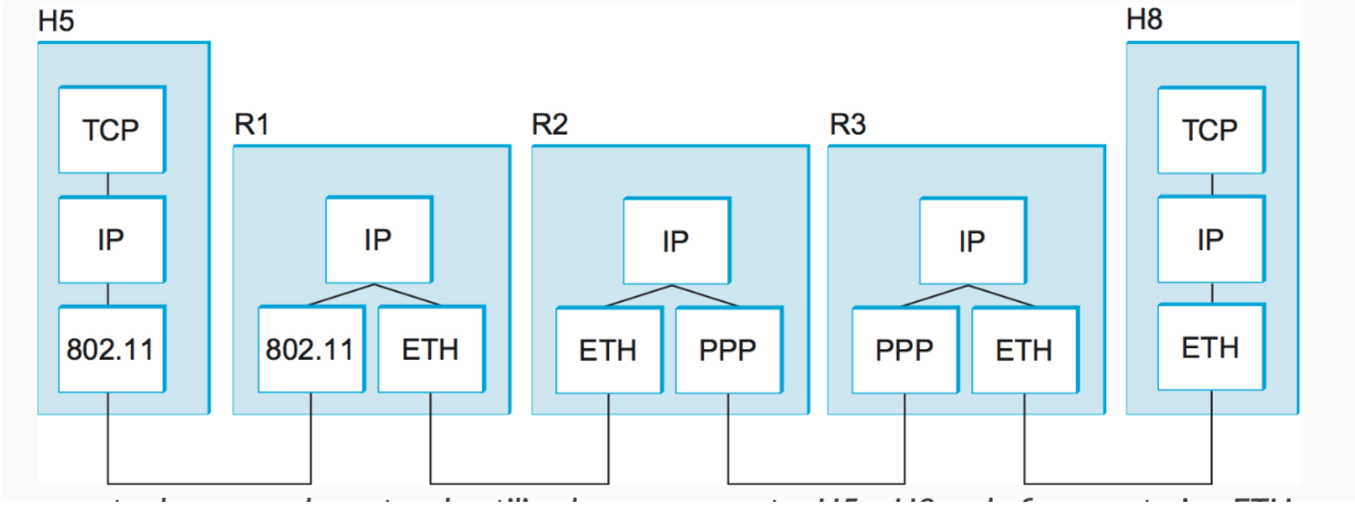
- WAN más de 10 km
- LAN menos de 10 km
- PAN (Personal Area Network)
  Distancias cortas 10-20 m o menos.



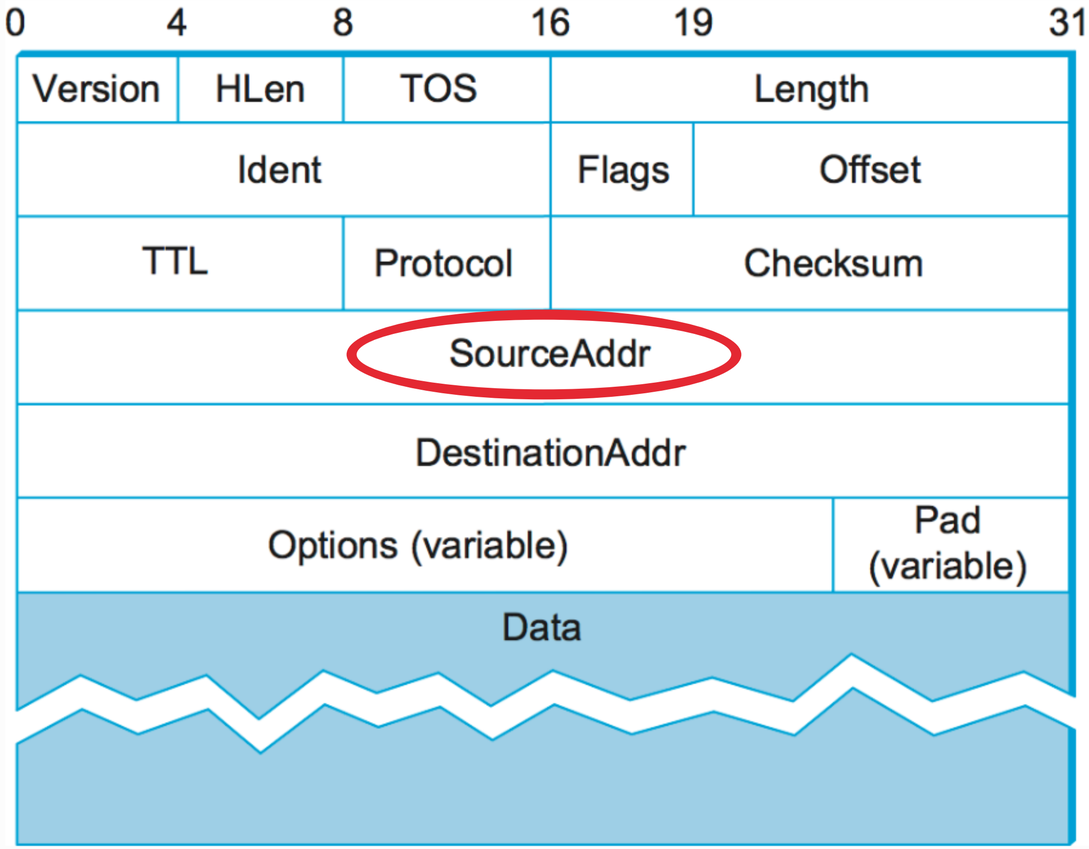

Network B
Network C
Network A
Network D
How packets travel from here to there.

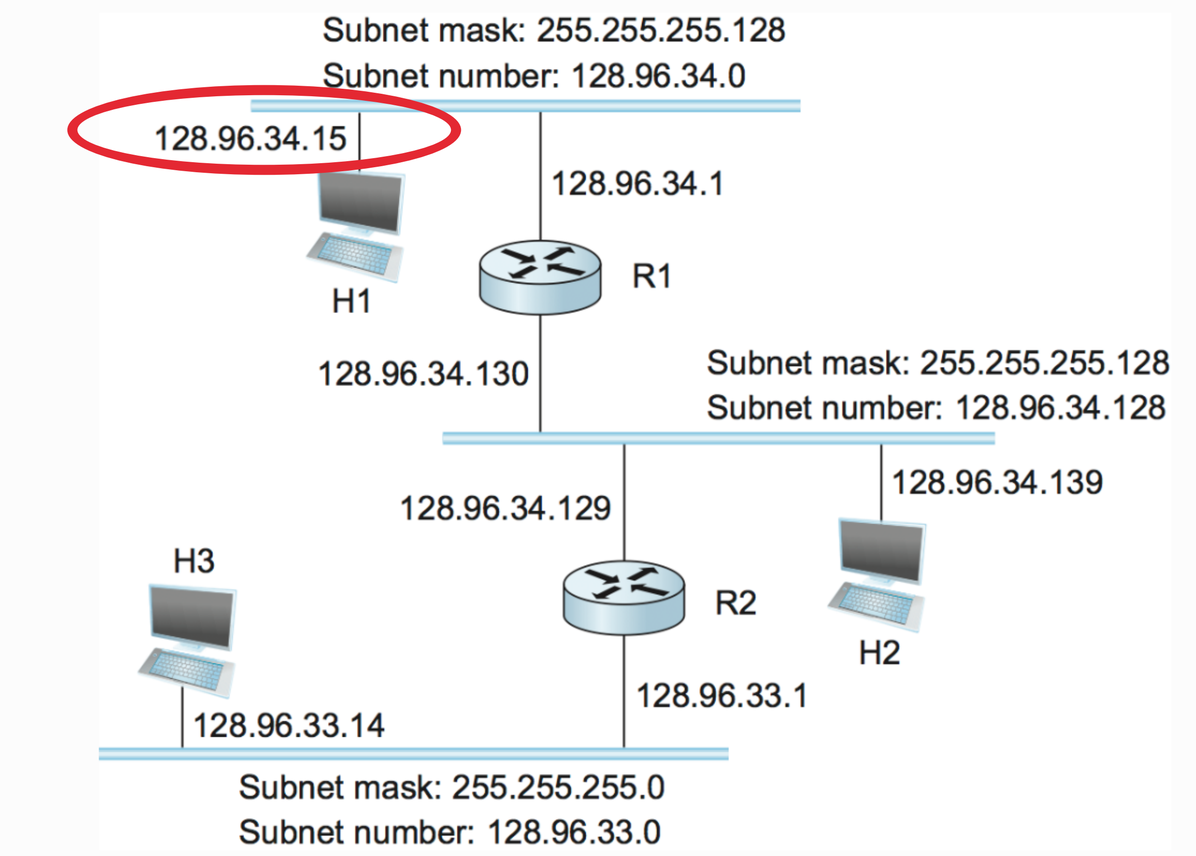
ENRUTAMIENTO/TRANSFORMACIONES



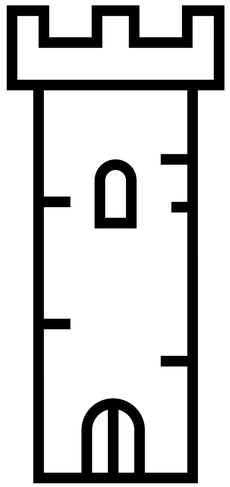


PAQUETE


0
4
8
16
19
31
Version
HLen
TOS
Length
Ident
Flags
Offset
TTL
Protocol
Checksum
SourceAddr
DestinationAddr
Options (variable)
Pad
(variable)
Data


Subnet mask: 255.255.255.128
Subnet number: 128.96.34.0
128.96.34.15
128.96.34.1
H1
R1
128.96.34.130
Subnet mask: 255.255.255.128
Subnet number: 128.96.34.128
128.96.34.129
128.96.34.139
H3
R2
H2
128.96.33.1
128.96.33.14
Subnet mask: 255.255.255.0
Subnet number: 128.96.33.0

PROTOCOLOS

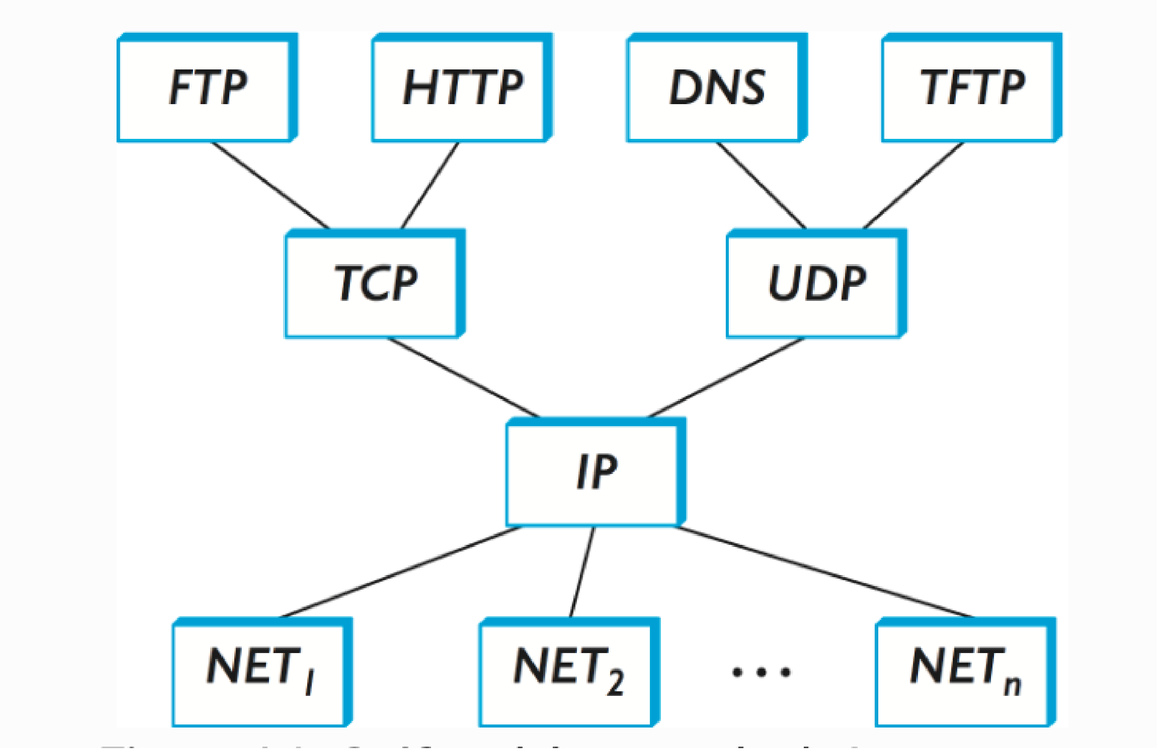


protocolos

- Computadores necesitan lenguaje común para comunicarse
- Hoy la mayoría habla al menos uno estándar
  - TCP – Protocolo de control de transmisión
  - IP – Protocolo de Internet
- Protocolo: conjunto de reglas que gobiernan el formato de mensajes que los computadores intercambian
  - Gobierna como el equipamiento de red interactúa para entregar la data cruzando la red

TCP/IP

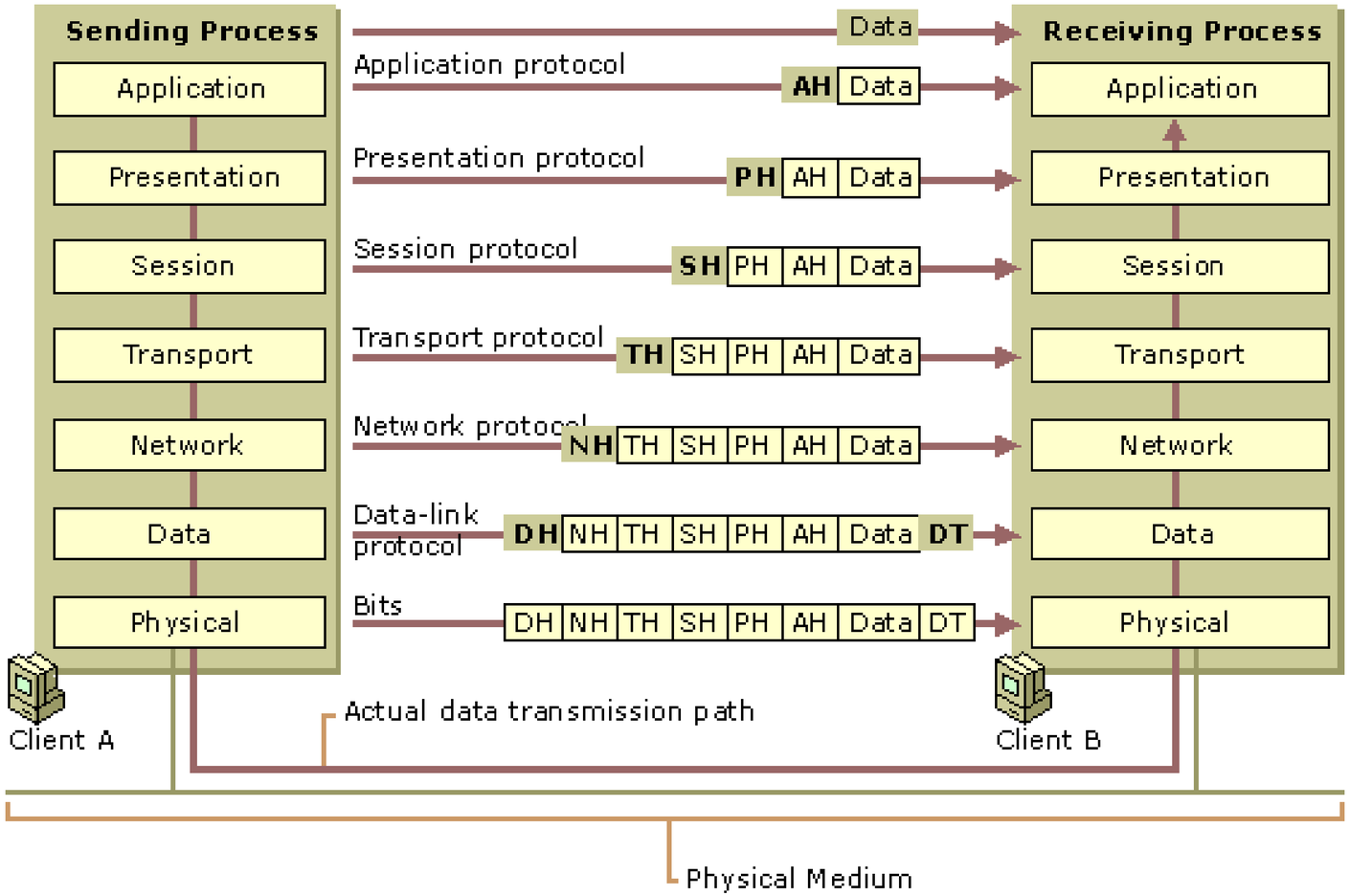
- No es solo un protocolo sino un conjunto de protocolos



UNIVERSIDAD ADOLFO IBÁÑEZ

MODELO OSI

Comunicación entre 2 equipos



Microsoft TechNet, “Data flow in the OSI Model”

EL MODELO OSI

- Es el modelo conceptual que permite caracterizar y estandarizar las funciones de un sistema de comunicaciones en cascada o tasas para construir una red y usar sus recursos conectados
  - particionándolo en 7 capas de abstracción
- Permite el desarrollo de tecnologías que actúen por cada capa independiente de las contiguas
- Cada capa funciona como un servicio usualmente para la capa subyacente
- Cada capa usualmente agrega datos de encabezado → por tanto avanzar en capas hacia abajo se denomina encapsulación y en reversa desencapsulación

ENCAPSULACIÓN

OSI

Capa de Aplicación	Datos
Capa de Presentación	Encabezado + Datos
Capa de Sesión	Encabezado + Encabezado + Datos
Capa de Transporte	Encabezado + Encabezado + Encabezado + Datos
Capa de Red	Encabezado + Encabezado + Encabezado + Encabezado + Datos
Capa de enlace de datos	Encabezado + Encabezado + Encabezado + Encabezado + Encabezado + Datos + Pie
Capa Física	Encabezado + Encabezado + Encabezado + Encabezado+Encabezado + Encabezado + Datos + Pie +Pie

EXISTEN OTROS MODELOS

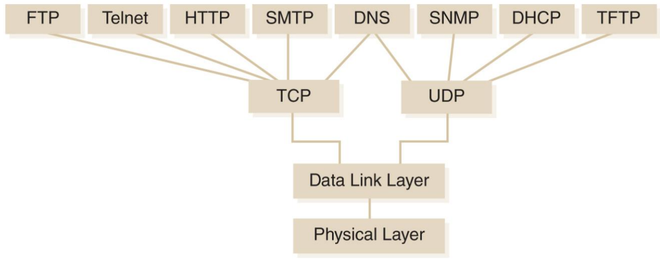
OSI	TCP/IP
Capa de Aplicación	Capa de Aplicación (protocolos capa transporte)
Capa de Presentación	
Capa de Sesión	
Capa de Transporte	Capa de Transporte Permite que datos se transporten entre dispositivos
Capa de Red	Capa de red o internet Crea o inserta paquetes
Capa de enlace de datos	Capa de acceso de red Mover datos a través de la red
Capa Física	

UNIVERSIDAD ADOLFO IBÁÑEZ

CAPA 7

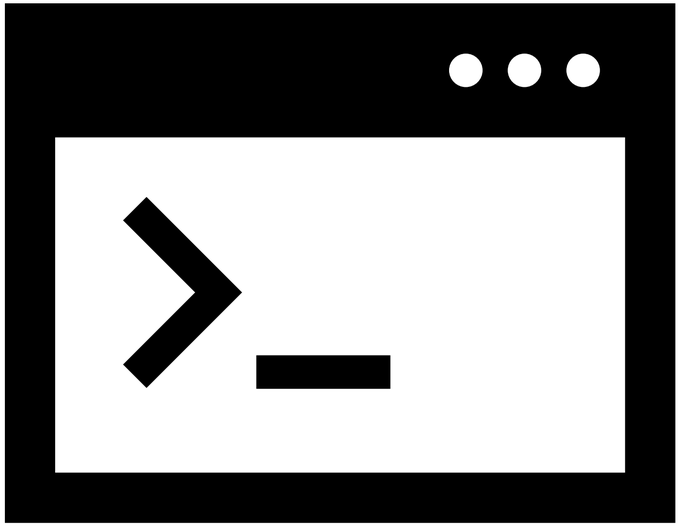
CAPA 7: APLICACIÓN

- Esta capa es responsable para interactuar con los usuarios finales mediante software de aplicación y esto incluye todos los programas en un computador que permite a los usuarios interactuar con la red.
- Define los protocolos estandarizados de interacción entre equipos
- Protocolos:
  - Traspaso de archivos: FTP, SFTP, NFS
  - E-Mail: POP3/IMAP, SMTP → Ejemplo: software de email pues transmite y recibe mensaje sobre la red.
  - Soporte de redes: DNS
  - Administración remota: TELNET, SSH
  - Web: HTTP



TELNET

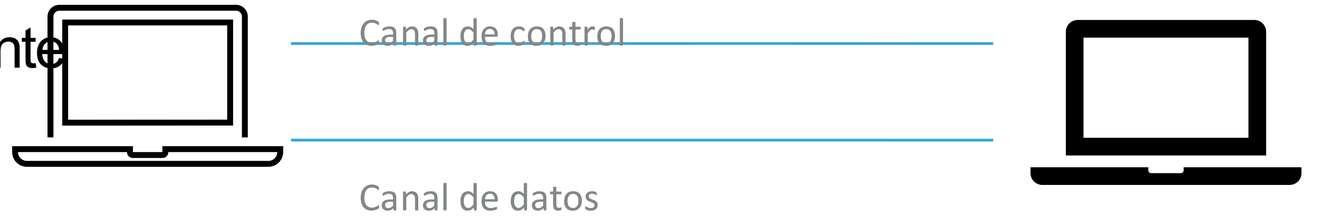
- Protocolo de interacción con terminales vía texto
- Crea una conexión de terminal virtual
- Permite acceder a los usuarios acceder a las aplicaciones de otro equipo de manera remota
- Desarrollado inicialmente en 1969
- Sin encriptación
- Sin autentificación



FILE TRANSFER PROTOCOL (FTP)

- Transferencia de archivos a través de redes/internet
  - Protocolo específicamente diseñado para tal tarea
- Utiliza conexiones separadas para el control y transferencia de datos
- Modelo cliente servidor
- Algunas aplicaciones cliente tienen interfaz gráfica para mostrar los archivos de cada lado y facilitar el traspaso
- Activo vs pasivo donde en pasivo el cliente da a conocer el puerto por el cual puede recibir datos sin bloqueo de cortafuegos

DEBE LIMITARSE



SECURE SHELL (SSH)

- Protocolo encriptado para comunicación segura:
  - Interacción con terminales
  - Transferencia de archivos
  - Replicación de puertos (túneles)
  - Creación y administración de VPN’s
  - Información cifrada – técnicas de cifrado lo que lo diferencia de telnet
  - Múltiples formas de autentificación (user/pass, llave pública...)
  - Puerto asignado 22

CAPA 7: VULNERABILIDADES

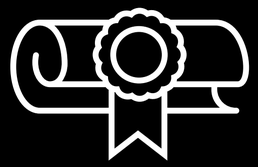
- Problemas de diseño permiten el uso de recursos de la aplicación por parte de usuarios no autentificados
- Puertas traseras y defectos de diseño de aplicaciones que permiten evadir controles de seguridad
- Controles inadecuados de seguridad estilo “todo o nada”, lo que resulta en derechos de acceso excesivos o insuficientes.
- Fallos de programación aprovechables para botar programas o causar comportamiento no deseado
- Ejemplo SSH Vulnerables a ataques de replay: información maliciosa es retransmitida – se relaciona con suplantación de identidad y denegación de servicio

CAPA 7: CONTROLES

- Controles a nivel de aplicación para definir y hacer cumplir políticas de acceso a recursos de la aplicación
- Estándares, testing y compliance de código y funcionalidad de aplicaciones en términos de seguridad
- Algunos firewalls permiten detectar y prevenir ataques a este nivel
- Cifrado -> confidencialidad e integridad de datos
- Firmas digitales -> autenticación – no rechazo e integridad de datos

SEGURIDAD EN EMAIL Y MENSAJERIA

- Emails son enviados usando el protocolo simple mail transfer (SMPT)
- Mecanismos para alcanzar seguridad punto a punto
  - Ejemplo: Asigna pares llaves privada pública
    - Confidencial – **encripta** mensaje con llave pública del destinatario
    - Integridad – firma el mensaje con su llave privada



https://learn.microsoft.com/es-es/security-updates/security/cmoprotegerlaconfidencialidaddelcorreoelectronicoenmicrosoftesregulados

SMTPS PERMITE CIFRAR EL CONTENIDO EN CASO DE QUE SE FILTRARA

CAPA 6

CAPA 6: PRESENTACIÓN

PRÓXIMA UNIDAD

- Recepciona lo enviado por la capa de aplicación
- Ésta capa se encarga de métodos de codificación, **cifrado** y compresión para los hosts que realizan la comunicación:
  - Organizar los datos enviados
  - Homogeneizar las comunicaciones entre diferentes dispositivos, sistemas de codificación, etc.
    - Ej, ASCII, UTF-8, etc.
- Deja todo preparado para la capa de sesión

CAPA 6: VULNERABILIDADES

- En general tácticas de ingeniería social para engañar a los usuarios para que proporcionen información personal y confidencial o hagan clic en un enlace malicioso
  - ¿Cómo usted cree que se realiza esto?
  - ¿Qué objetivo tiene el atacante?
    - Ejemplos: robo de credenciales de inicio de sesión e información de tarjetas de crédito
    - Instalación de malware en el sistema de victima
- Ataques a codificación y descodificación de datos – inyección de código malicioso

CAPA 6: VULNERABILIDADES Y CONTROLES

- Vulnerabilidades
  - Mal manejo de entradas inesperadas, lo que podría llevar a fallos o toma de control de sistemas
  - Vulnerabilidades en SSL/TLS
- Controles
  - Chequeo de entradas
  - Revisión de sistemas criptográficos (SSL/TLS)

CAPA 5

CAPA 5: SESIÓN

- Ésta capa se encarga de:
  - Apertura, cierre y manejo de sesiones abiertas de comunicación
  - Interrupciones en la comunicación
- Protocolos
  - Remote Procedure Call (RPC)
  - otros

CAPA 5: VULNERABILIDADES

- Interceptación de información sensible (passwords, identificadores de sesión)
- Spoofing de identificadores de sesión
- Filtración de información mediante intentos fallidos de autentificación
- Fuerza bruta sobre credenciales de autentificación

SESIÓN
RIESGOS: ACCESO A RECURSOS NO AUTORIZADOS ACCESO A INFO

ACTIVA: ALTERA TRÁFICO EN TIEMPO REAL
PASIVO: MONITOREAN EL TRÁFICO – TOMAN SESIÓN

CAPA 5: CONTROLES

- SSL/TLS
  - Se inicia en capa 5 y funciona en capa 6
  - Secure Sockets Layer desarrollado originalmente por Netscape en la década de 1990 como un protocolo de seguridad para cifrar las comunicaciones entre un cliente (como un navegador web) y un servidor.
  - SSL brinda confidencialidad, autenticación e integridad a través del cifrado de datos transmitidos.
  - TLS fue diseñado para abordar las limitaciones y vulnerabilidades de las versiones más antiguas de SSL.
- Tiempo de expiración de sesiones
- Nivel de corte
  - Cantidad de intentos de autentificación antes de “cortar” al usuario (indefinidamente o por un rato)

CAPA 4

CAPA 4: TRANSPORTE

- Responsable de romper datos en paquetes y transmitirlos por la red (control de flujo y error)
- Esta capa se encarga de:
  - Reordenamiento de paquetes
  - Confiabilidad: Que la información llegue sin errores. Lidia con paquetes perdidos
  - Multiplexación: Uso de múltiples servicios (puertos)
- Protocolos
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)

CAPA 4: VULNERABILIDADES Y CONTROLES

- Vulnerabilidades:
  - Diferencias en la implementación de protocolos pueden llevar a riesgo de fingerprinting
    - como el comportamiento específico de un sistema operativo o la puesta en práctica de ciertas características de un protocolo, pueden ser utilizadas para identificar un sistema en particular.
    - Los atacantes pueden analizar las respuestas de los sistemas objetivo a ciertas peticiones o mensajes de protocolo para determinar detalles sobre el sistema, como su sistema operativo, versión de software, configuración de red, etc.
  - Denial-Of-Service
  - Amplificación en respuestas de servidores
  - Escaneo de puertos
- Controles:
  - Firewalls + IPS/IDS
    - bloquear o alertar sobre patrones de tráfico sospechosos asociados con fingerprinting.
    - Mantener sistemas actualizados con los últimos parches de seguridad y configuraciones

CAPA 3

CAPA 3: RED

- Ésta capa se encarga principalmente del enrutamiento de paquetes
- Misión: Que el paquete llegue a su destino **aunque no haya una conexión directa**
- Protocolos:
  - Internet Protocol: IPv4, IPv6
  - Internet Group Management Protocol (IGMP)
    - Ej. multicasting
  - Internet Control Message Protocol (ICMP)
    - Ej. ping

CAPA 3: VULNERABILIDADES Y CONTROLES

- Vulnerabilidades
  - Man-in-the-middle (MITM) (suplantación de identidad de ARP)
  - Spoofing de direcciones IP
  - Flooding de paquetes ICMP (ping de la muerte)
- Controles
  - Minimización de abuso de ICMP/IGMP
  - Firewalls
  - sistemas de detección y prevención de intrusiones (IDS/IPS)
  - servicios de mitigación de DDoS (Ataque de Denegación de Servicio Distribuido).

CAPA 2

CAPA 2: ENLACE DE DATOS

- En esta capa los datos se preparan para su uso en la capa física
- Su objetivo es conseguir que la información fluya libre de errores entre 2 equipos
- Finaliza la comunicación entre los nodos de red
- Divide paquetes en tramas y los transmite de origen a destino

CAPA 2: VULNERABILIDADES Y CONTROLES

- Vulnerabilidades
  - Spoofing de direcciones MAC: cuando altera la dirección de control de acceso a medios en un dispositivo para hacerse pasar por otro dispositivo en la red
    - Suplantaciones de DHCP/de ARP (protocolo para resolver direcciones)

- otras

CAPA 1

CAPA 1: FÍSICA

- Encargada de conectar adecuadamente los nodos de la red mediante medios cableados o inalámbricos
- Describe el hardware usado, ej:
  - Interfaces de red
  - Caracteríscas físicas y mecanicas de la conexión
- Describe también la forma de transmitir bits y bytes de datos
  - Pulsos eléctricos para cables de red
  - Ondas de radio
  - Luz para fibra óptica

CAPA 1: VULNERABILIDADES

- Robo físico
- Pérdida de energía eléctrica o control ambiental
- Desconexión de enlaces físicos de datos
- Interceptación de datos
- Keylogging

ATAQUES DE OLFATEO/RASTREO : ATACANTE CAPTURA Y ANALIZA EL TRÁFICO DE LA RED PARA RECOPILAR INFORMACIÓN CONFIDENCIAL

CAPA 1: CONTROLES

- Seguridad física
  - Vigilancia vía CCTV
  - Control de acceso a sistemas
- Blindaje
  - Cables blindados electromagnéticamente
  - Jaulas de Faraday
  - Bloqueadores de señal GSM