UNIVERSIDAD ADOLFO IBÁÑEZ

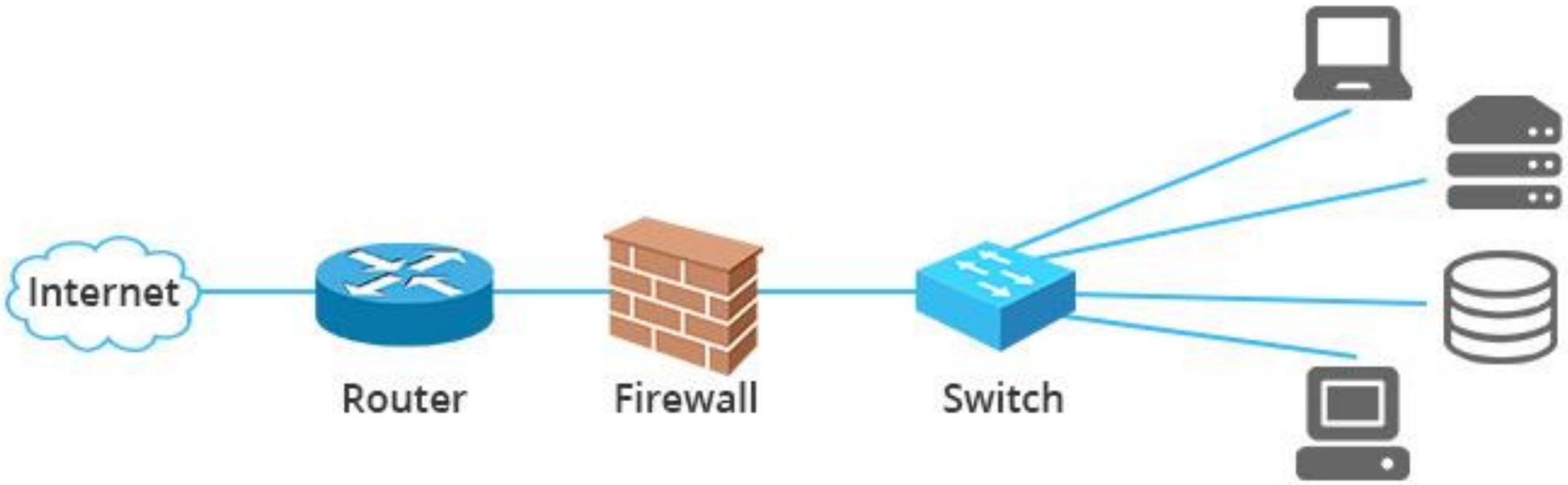
Semana 10

TICS413: SEGURIDAD TI

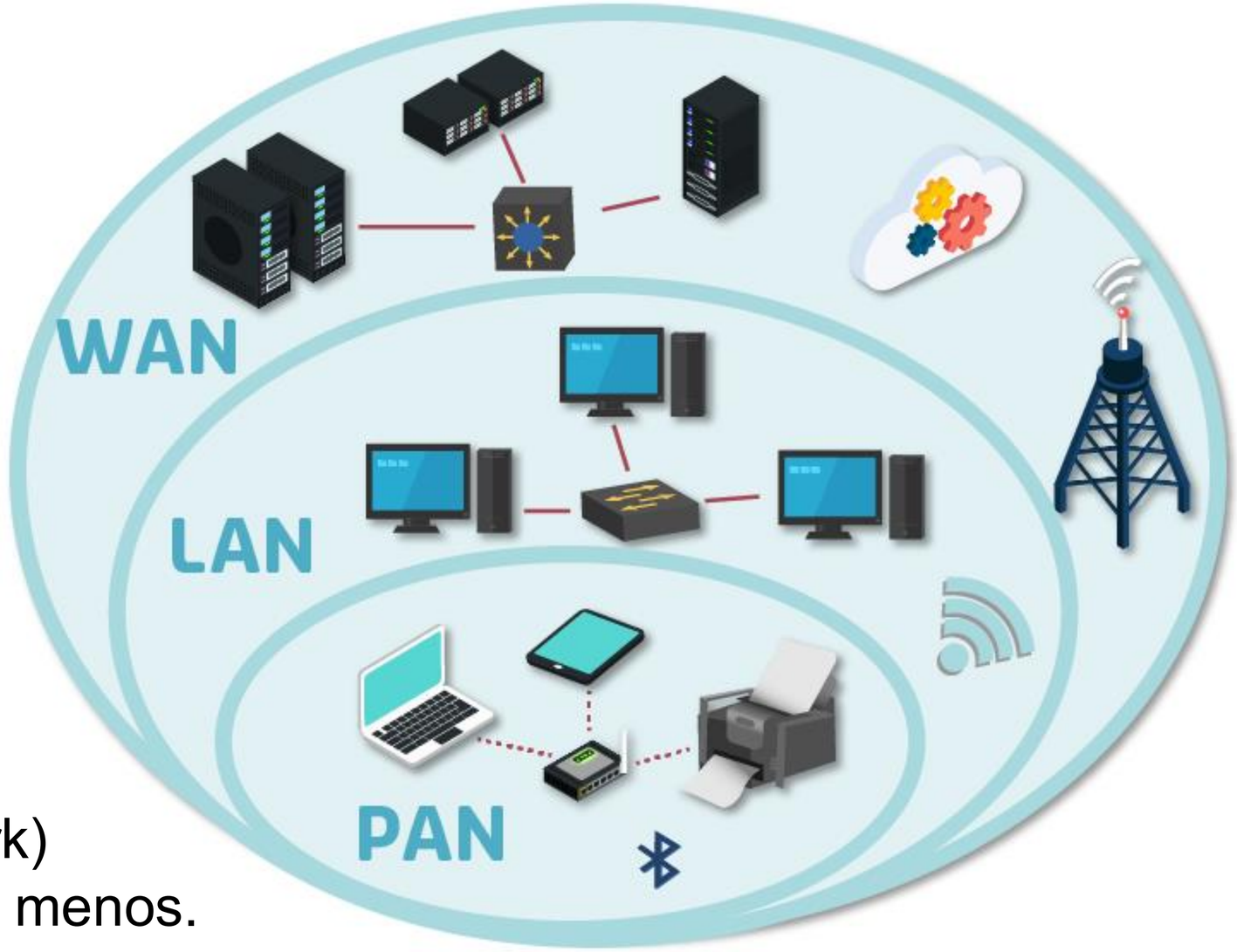
Unidad Seguridad en redes y comunicaciones

PAQUETES REDES

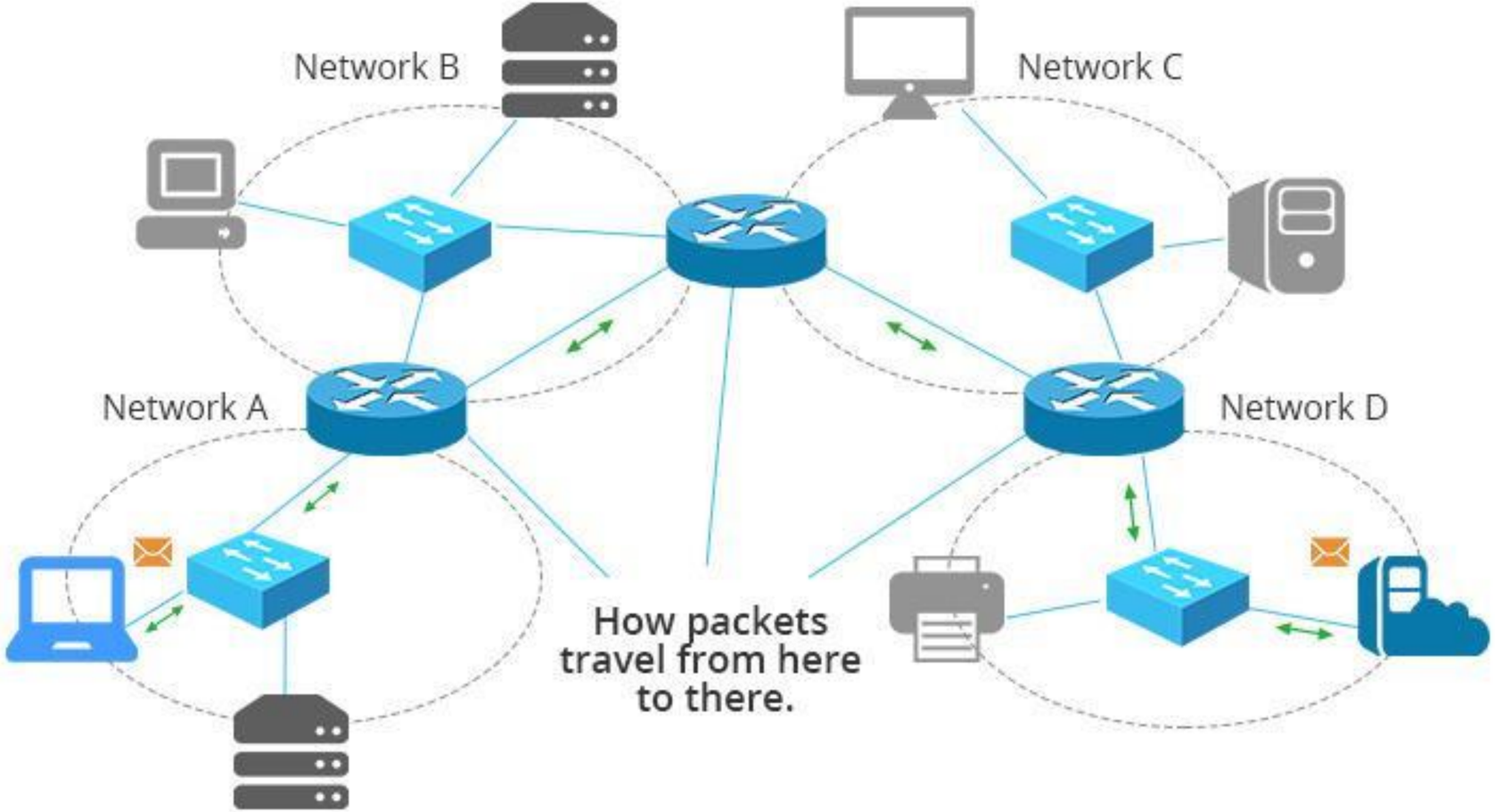
ELEMENTOS



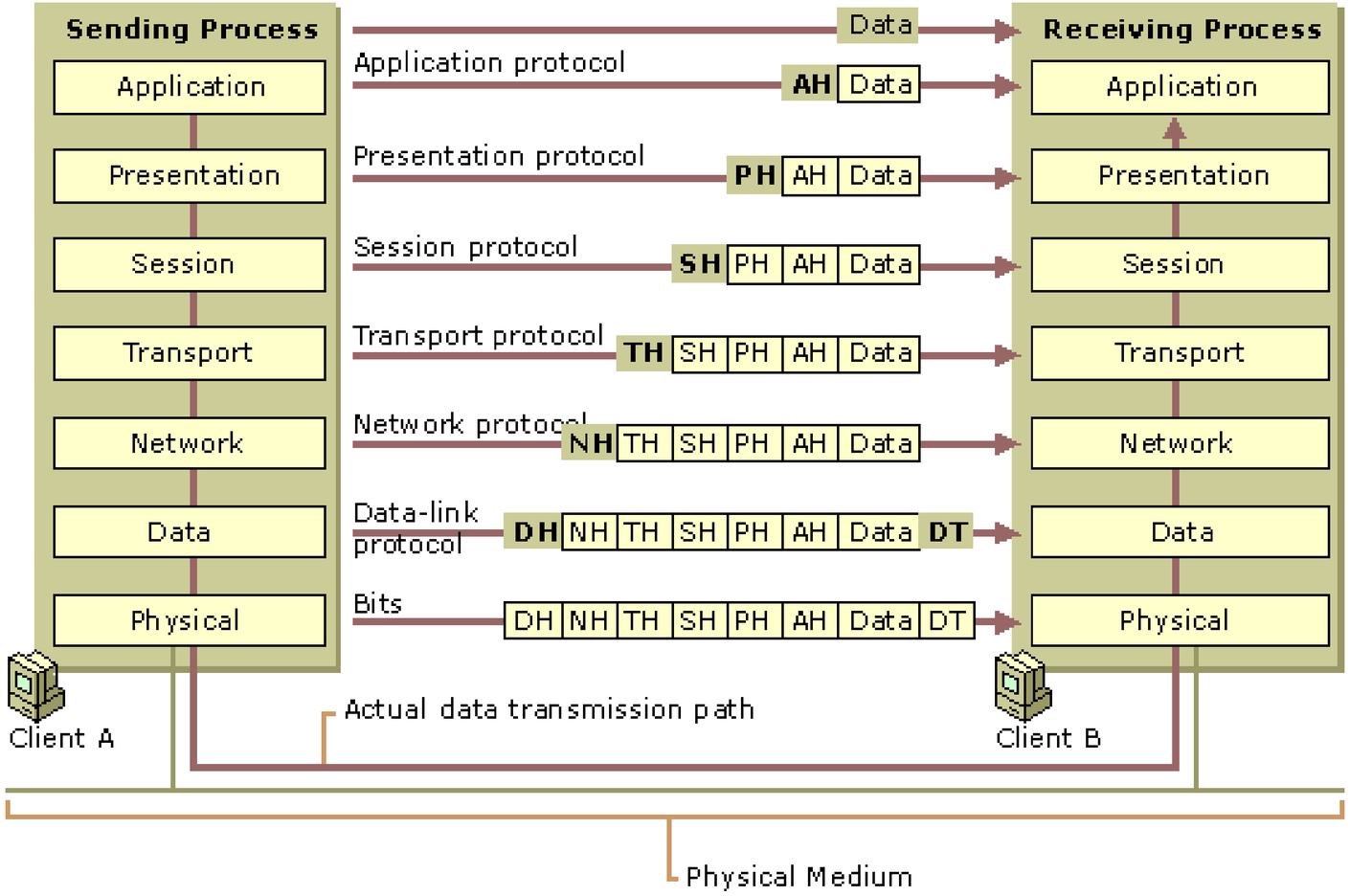
- WAN más de 10 km
- LAN menos de 10 km
- PAN (Personal Area Network)
  Distancias cortas 10-20 m o menos.



Ejemplo redes combinadas - ¿dónde podría ser?

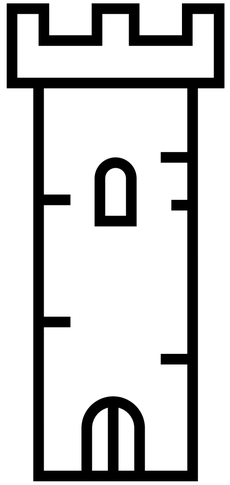


Comunicación entre 2 equipos



Microsoft TechNet, “Data flow in the OSI Model”

PROTOCOLOS

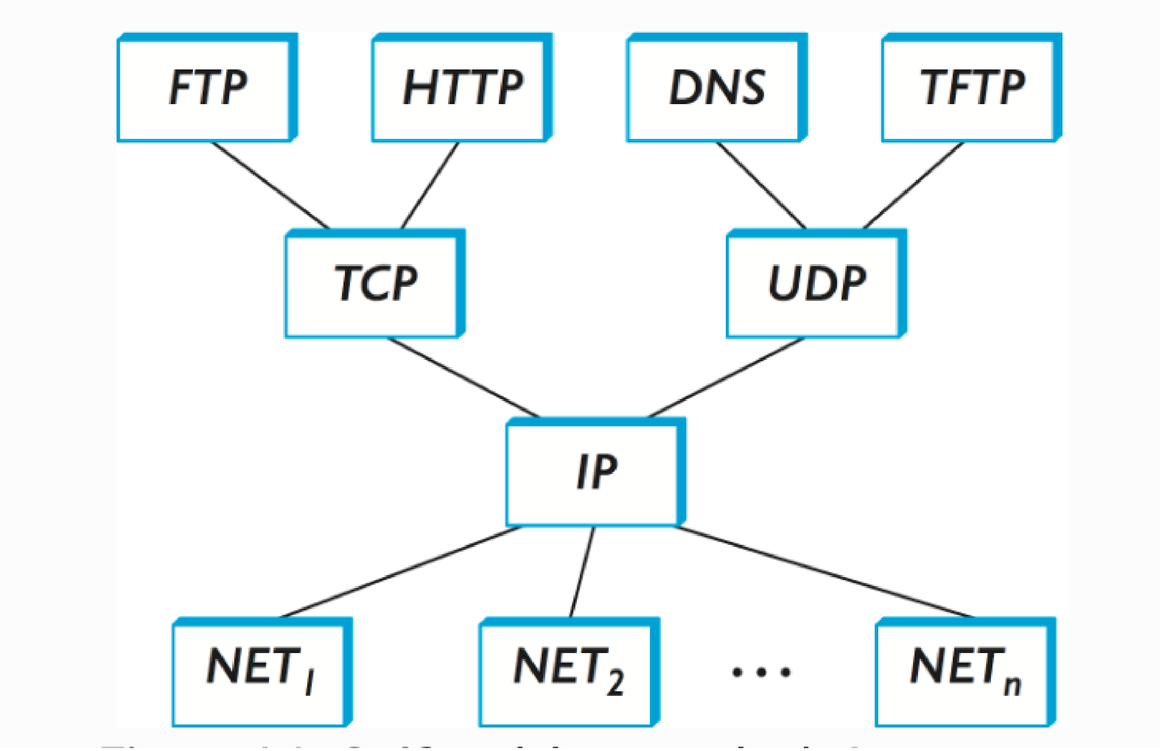


protocolos

- 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

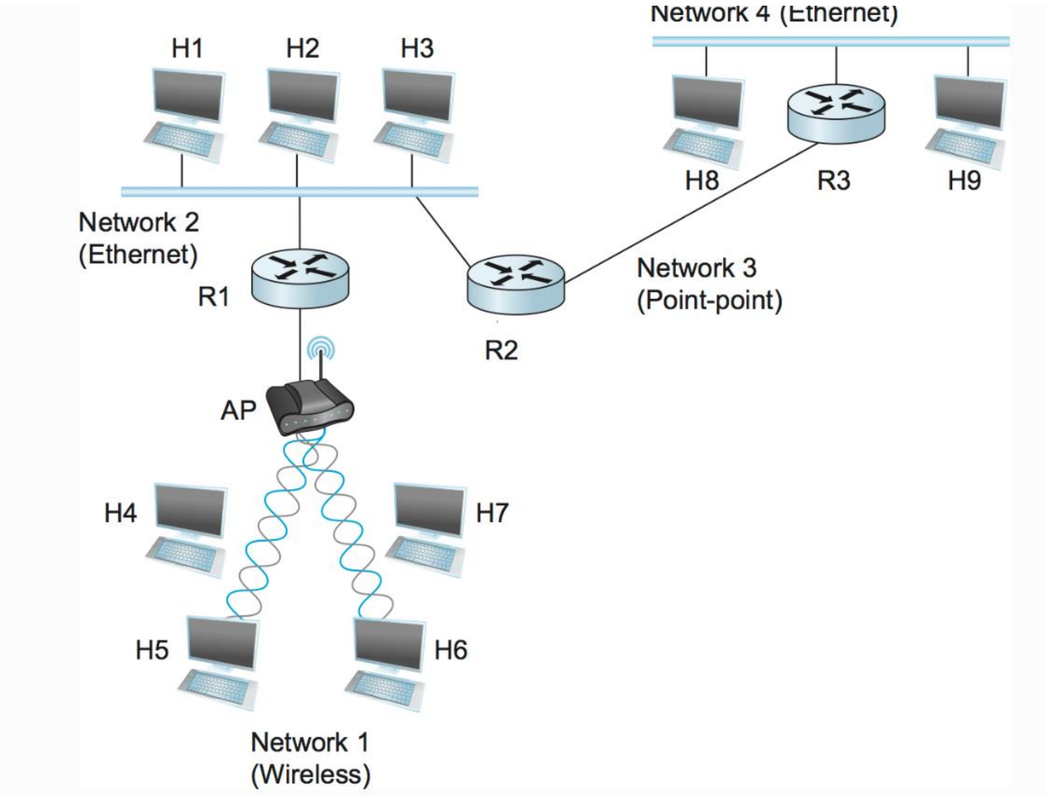
- No es solo un protocolo sino un conjunto de protocolos

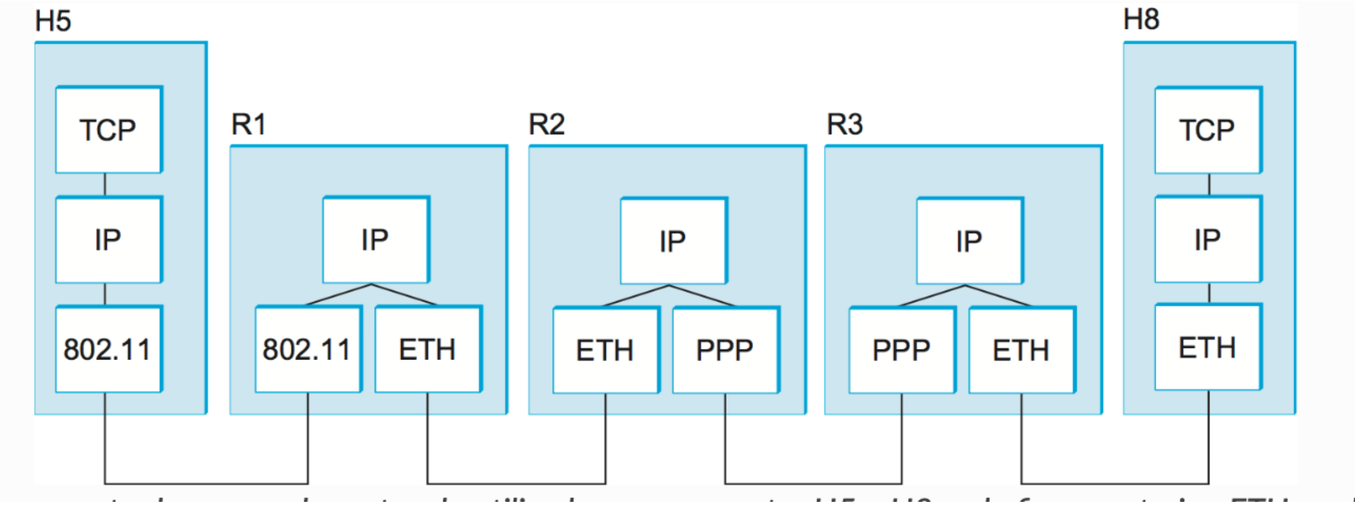


PUERTOS COMUNES

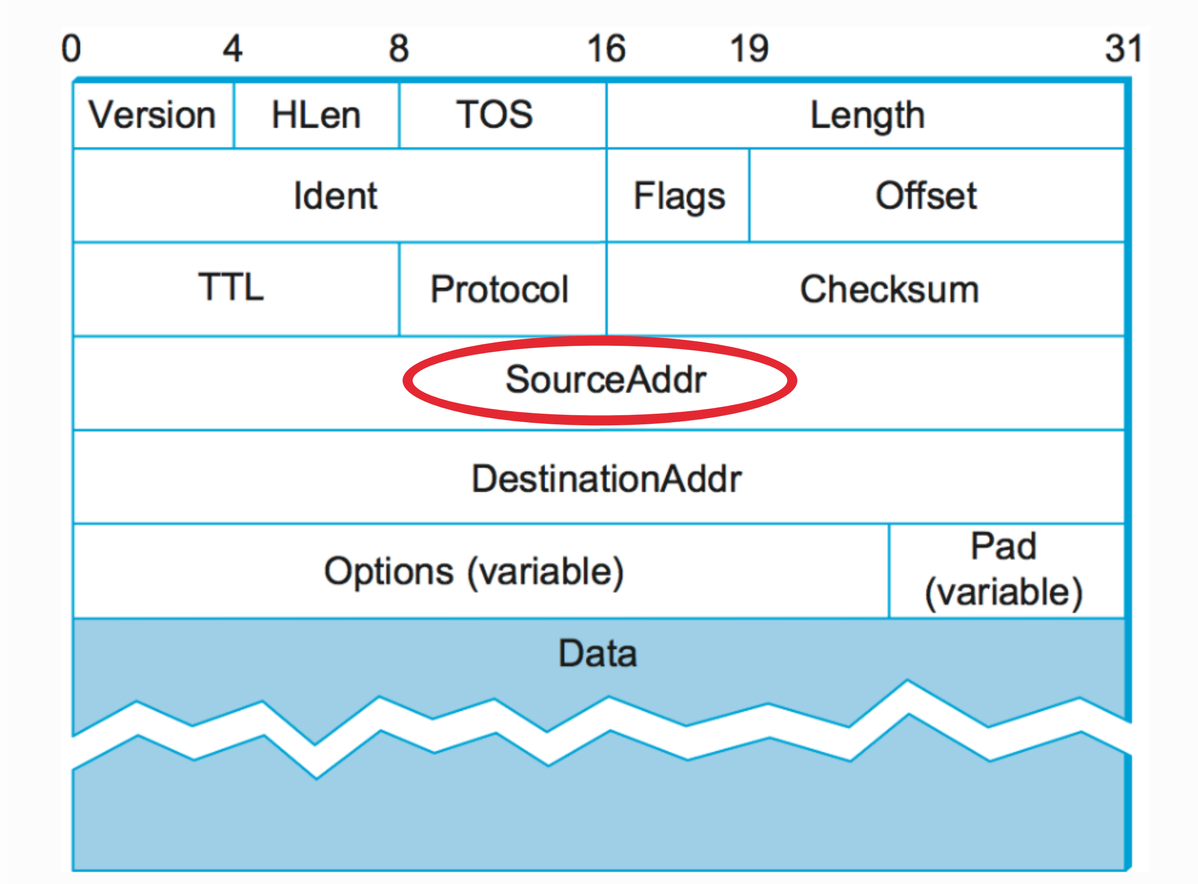
PORT	SERVICE/USE
20	FTP data transfer
21	FTP control
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67/68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP)
88	Kerberos
110	Post Office Protocol v3 (POP3)
139	Network Basic Input/Output System (NetBIOS) Session Service
143	Internet Message Access Protocol (IMAP)
161	Simple Network Management Protocol (SNMP)
162	SNMP Trap
443	HTTP over Secure Sockets Layer/Transport Layer Security (SSL/TLS)
445	Simple Message Block (SMB) over IP
3389	Terminal Server

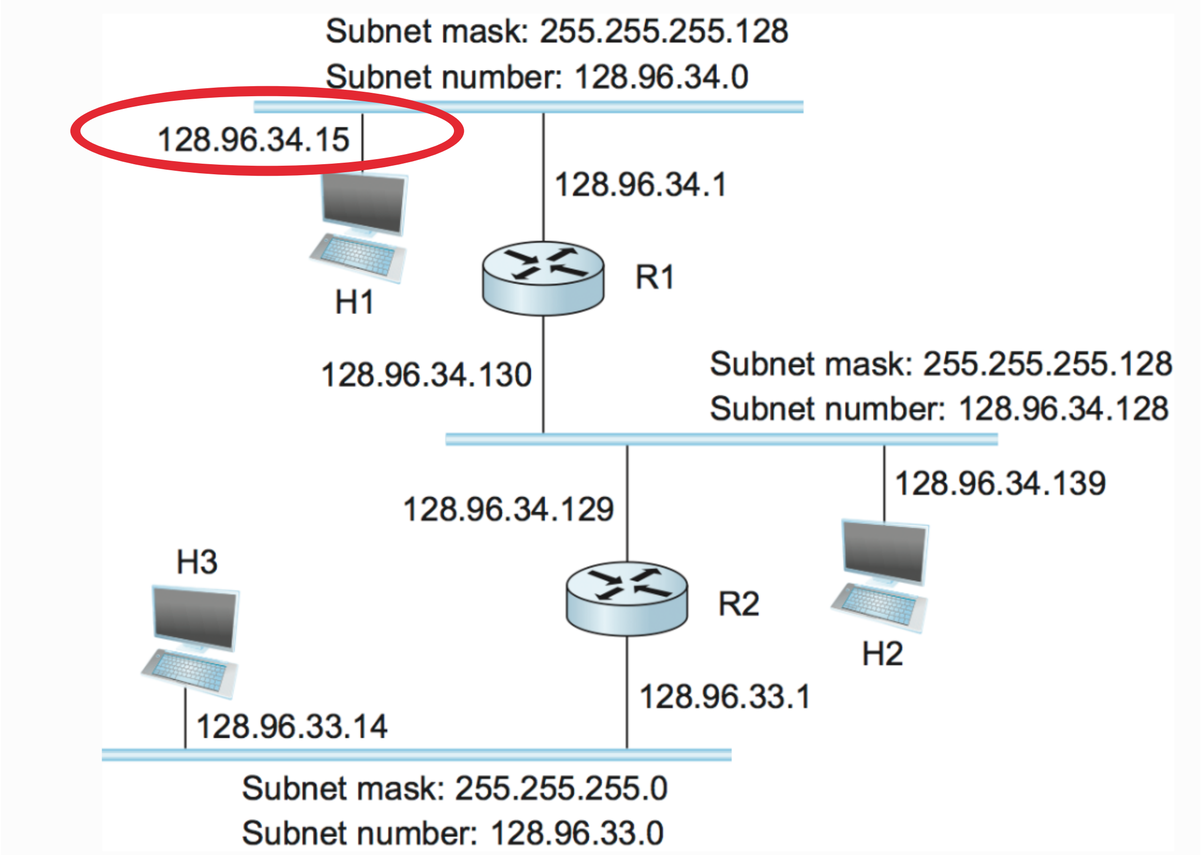
ENRUTAMIENTO/TRANSFORMACIONES



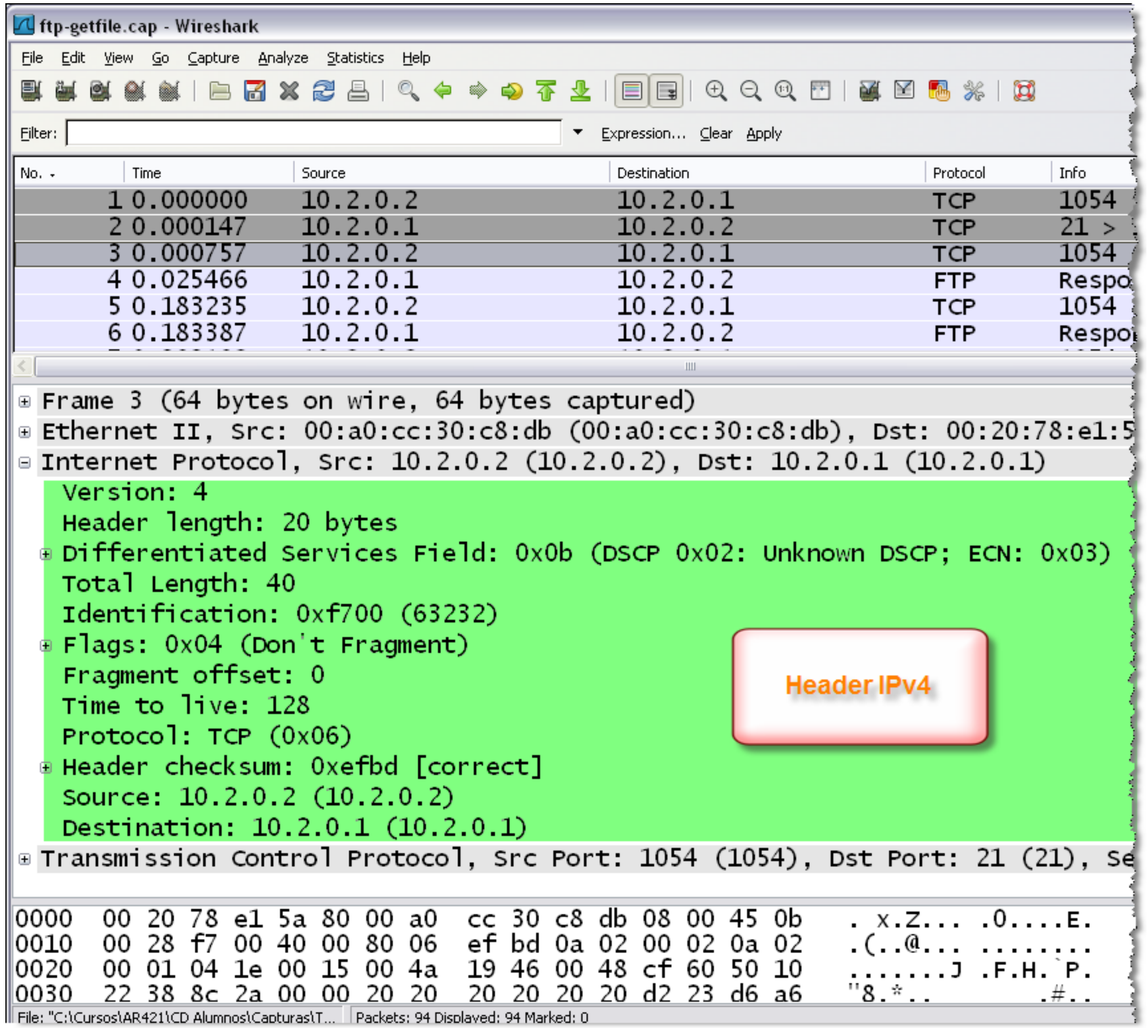


PAQUETE


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

IPV4 HEADER, WIRESHARK VIEW



Caso

- Trabaja como analista de seguridad para una agencia de seguros.
- Los empleados de la empresa acceden periódicamente a la página web de ventas de la empresa para buscar seguros que pueden gustar a sus clientes.
- Una tarde, recibe una alerta automática de su sistema de monitoreo que indica un problema con el servidor web.
- Intenta visitar el sitio web de la empresa, pero recibe un mensaje de error de tiempo de espera de conexión en su navegador.

Sección 1: Identifique el tipo de ataque que pudo haber causado esto interrupción de la red
Una posible explicación para el mensaje de error de tiempo de espera de conexión del sitio web es: Los registros muestran que: Este evento podría ser:

NECESITA MÁS INFORMACIÓN ¿DE DONDE O CÓMO PODEMOS OBTENERLA?

¿Cómo obtener más información?

- Utilice un rastreador de paquetes para capturar paquetes de datos en tránsito hacia y desde el servidor web.
  -

HIPÓTESIS: SI OBSERVA UNA GRAN CANTIDAD DE SOLICITUDES TCP SYN PROVENIENTES DE UNA DIRECCIÓN IP DESCONOCIDA - EL SERVIDOR WEB PODRÍA ESTAR ABRUMADO POR EL VOLUMEN DE TRÁFICO ENTRANTE Y ESTAR PERDIENDO SU CAPACIDAD DE RESPONDER A LA CANTIDAD ANORMALMENTE GRANDE DE SOLICITUDES SYN.

Una transacción normal entre un visitante de un sitio web y el servidor web sería como

No.	Tiempo	Fuente	Destino	Protocolo	Información
47	3.144521	198.51.100.23	192.0.2.1	tcp	42584->443 [SYN] Sec=0 Win=5792 Len=120...
48	3.195755	192.0.2.1	198.51.100.23	tcp	443->42584 [SYN, ACK] Sec=0 Win-5792 Len=120...
49	3.246989	198.51.100.23	192.0.2.1	tcp	42584->443 [ACK] Sec=1 Win-5792 Len=120...
50	3.298223	198.51.100.23	192.0.2.1	HTTP	OBTENER /sales.html HTTP/1.1
51	3.349457	192.0.2.1	198.51.100.23	HTTP	HTTP/1.1 200 OK (texto/html)

Los actores maliciosos pueden aprovechar el protocolo TCP inundando un servidor con solicitudes de paquetes SYN

UNIVERSIDAD ADOLFO IBÁÑEZ

SERVIDOR WEB 192.0.2.1

Fuente	Destino
198.51.100.23	192.0.2.1
192.0.2.1	198.51.100.23
198.51.100.23	192.0.2.1

Protocolo	Información
tcp	42584->443 [SYN] Sec=0 Win-5792 Len=120...
tcp	443->42584 [SYN, ACK] Sec=0 Win-5792 Len=120...
tcp	42584->443 [ACK] Sec=1 Win-5792 Len=120...

Caso – Identificación

rojo	52	3.390692	203.0.113.0	192.0.2.1	tcp	54770->443 [SYN] Sec=0 Win=5792 Len=0...
rojo	53	3.441926	192.0.2.1	203.0.113.0	tcp	443->54770 [SYN, ACK] Sec=0 Win-5792 Len=120...
rojo	54	3.493160	203.0.113.0	192.0.2.1	tcp	54770->443 [ACK Seq=1 Win=5792 Len=0...
verde	55	3.544394	198.51.100.14	192.0.2.1	tcp	14785->443 [SYN] Sec=0 Win-5792 Len=120...
verde	56	3.599628	192.0.2.1	198.51.100.14	tcp	443->14785 [SYN, ACI Win-5792 Len=120...
rojo	57	3.664863	203.0.113.0	192.0.2.1	tcp	54770->443 [SYN] Se Win=5792 Len=0...
verde	58	3.730097	198.51.100.14	192.0.2.1	tcp	14785->443 [ACK] Se Win-5792 Len=120...
rojo	59	3.795332	203.0.113.0	192.0.2.1	tcp	54770->443 [SYN] Se Win-5792 Len=120...
verde	60	3.860567	198.51.100.14	192.0.2.1	HTTP	OBTENER /sales.html
rojo	61	3.939499	203.0.113.0	192.0.2.1	tcp	54770->443 [SYN] Se Win-5792 Len=120...
verde	62	4.018431	192.0.2.1	198.51.100.14	HTTP	HTTP/1.1 200 OK (text

El atacante sigue enviando más solicitudes SYN, lo cual es anormal.

verde	71	6.228728	198.51.100.5	192.0.2.1	HTTP	OBTENER /sales.html HTTP/1.1
rojo	72	6.229638	203.0.113.0	192.0.2.1	tcp	54770->443 [SYN] Sec=0 Win=5792 Len=0...
amarillo	73	6.230548	192.0.2.1	198.51.100.16	tcp	443->32641 [RST, ACK] Sec=0 Win-5792 Len=120...
rojo	74	6.330539	203.0.113.0	192.0.2.1	tcp	54770->443 [SYN] Sec=0 Win-5792 Len=0
verde	75	6.330885	198.51.100.7	192.0.2.1	tcp	42584->443 [SYN] Sec=0 Win=5792 Len=0...
rojo	76	6.331231	203.0.113.0	192.0.2.1	tcp	54770->443 [SYN] Sec=0 Win=5792 Len=0...
amarillo	77	7.330577	192.0.2.1	198.51.100.5	tcp	HTTP/1.1 504 Tiempo de espera de puerta de enlace (texto/html)
rojo	78	7.331323	203.0.113.0	192.0.2.1	tcp	54770->443 [SYN] Sec=0 Win=5792 Len=0...

Sección 1: Identifique el tipo de ataque que pudo haber causado esto interrupción de la red	
Una posible explicación para el mensaje de error de tiempo de espera de conexión del sitio web es:	
Los registros muestran que:	Ataque de denegación de servicio (DoS) a nivel de red, denominado ataque de inundación SYN, que tiene como objetivo el ancho de banda de la red para realentizar el tráfico.
Este evento podría ser:	

UNIVERSIDAD ADOLFO IBÁÑEZ

¿Qué hacer por mientras?

- Desconecta el servidor temporalmente para que la máquina pueda recuperarse y volver a un estado operativo normal.

¿BUENA IDEA?

- También configura el firewall de la empresa para bloquear la dirección IP que estaba enviando la cantidad anormal de solicitudes SYN.
- Usted sabe que su solución de bloqueo de IP no durará mucho, ya que un atacante puede falsificar otras direcciones IP para sortear este bloqueo (spoofing).
- Debe alertar a su equipo sobre este problema rápidamente y discutir los próximos pasos para detener a este atacante y evitar que este problema vuelva a ocurrir.

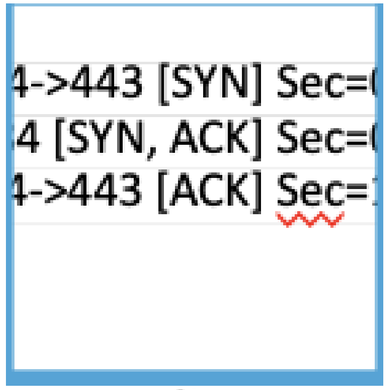
Sección 2: Explique cómo el ataque está provocando el mal funcionamiento del sitio web.

Cuando los visitantes del sitio web intentan establecer una conexión con el servidor web, se produce un protocolo de enlace de tres vías utilizando el protocolo TCP. Explique los tres pasos del apretón de manos:

1.

2.

3.



Explique qué sucede cuando un actor malintencionado envía una gran cantidad de paquetes SYN a la vez: **Como solo hay una dirección IP que ataca el servidor web, puede asumir que se trata de un ataque directo de inundación DoS SYN.**

Explique qué indican los registros y cómo afecta eso al servidor:

[redacted]

Sección 1: Identifique el tipo de ataque que pudo haber causado esto interrupción de la red
ataque DoS es Una posible explicación para la caída del sitio web dado el error de tiempo de espera de conexión. Los registros muestran que el servidor web deja de responder después de sobrecargarse con solicitudes de paquetes SYN. Este evento podría ser un tipo de ataque DoS llamado inundación SYN.

Sección 2: Explique cómo el ataque está provocando el mal funcionamiento del sitio web.
Cuando los visitantes del sitio web intentan establecer una conexión con el servidor web, se produce un protocolo de enlace de tres vías utilizando el protocolo TCP. El apretón de manos consta de tres pasos: 1. Se envía un paquete SYN desde el origen al destino, solicitando conectarse. 2. El destino responde al origen con un paquete SYN-ACK para aceptar la solicitud de conexión.El destino reservará recursos para que la fuente se conecte. 3. Se envía un paquete ACK final desde el origen al destino reconociendo el permiso para conectarse. En el caso de un ataque de inundación SYN, un actor malintencionado enviará una gran cantidad de paquetes SYN a la vez, lo que abruma los recursos disponibles del servidor para reservar para la conexión. Cuando esto sucede, no quedan recursos del servidor para solicitudes de conexión TCP legítimas. Los registros indican que el servidor web se ha visto abrumado y no puede procesar las solicitudes SYN de los visitantes. El servidor no puede abrir una nueva conexión para nuevos visitantes que reciben una mensaje de error de tiempo de espera.

PREGUNTAS