Laboratorio 1

Nota: Wireshark no incluye ni el preámbulo, ni el FCS (SVT, Secuencia de la verificación de la trama)

1. Analizar la siguiente captura de Wireshark de tráfico TCP

¿Qué capas aparecen en cada paquete?

¿En qué paquetes aparece la capa de aplicación?

¿Qué IP inicia la conversación?

¿Cuál es el puerto de origen y destino?

¿Qué IP finaliza la conversación?

```
No.     Time           Source          Destination     Protocol Length Info
      1 0.000000000    192.168.11.10   201.235.253.60  TCP      62     14327→80  [SYN] Seq=0 Win=16384
Len=0 MSS=1460 SACK_PERM=1

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: Tp-LinkT_d9:ee:ee (00:25:86:d9:ee:ee), Dst: Cisco-Li_3d:8f:d1 (00:25:9c:3d:8f:d1)
Internet Protocol Version 4, Src: 192.168.11.10 (192.168.11.10), Dst: 201.235.253.60 (201.235.253.60)
Transmission Control Protocol, Src Port: 14327 (14327), Dst Port: 80 (80), Seq: 0, Len: 0

No.     Time           Source          Destination     Protocol Length Info
      2 0.012220000    201.235.253.60  192.168.11.10   TCP      62     80→14327  [SYN, ACK] Seq=0 Ack=1
Win=14600 Len=0 MSS=1460 SACK_PERM=1

Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: Cisco-Li_3d:8f:d1 (00:25:9c:3d:8f:d1), Dst: Tp-LinkT_d9:ee:ee (00:25:86:d9:ee:ee)
Internet Protocol Version 4, Src: 201.235.253.60 (201.235.253.60), Dst: 192.168.11.10 (192.168.11.10)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 14327 (14327), Seq: 0, Ack: 1, Len: 0

No.     Time           Source          Destination     Protocol Length Info
      3 0.012262000    192.168.11.10   201.235.253.60  TCP      54     14327→80  [ACK] Seq=1 Ack=1
Win=17520 Len=0

Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Tp-LinkT_d9:ee:ee (00:25:86:d9:ee:ee), Dst: Cisco-Li_3d:8f:d1 (00:25:9c:3d:8f:d1)
Internet Protocol Version 4, Src: 192.168.11.10 (192.168.11.10), Dst: 201.235.253.60 (201.235.253.60)
Transmission Control Protocol, Src Port: 14327 (14327), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 0

No.     Time           Source          Destination     Protocol Length Info
      4 0.012721000    192.168.11.10   201.235.253.60  HTTP     402    GET / HTTP/1.1

Frame 4: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits) on interface 0
```

Ethernet II, Src: Tp-LinkT_d9:ee:ee (00:25:86:d9:ee:ee), Dst: Cisco-Li_3d:8f:d1 (00:25:9c:3d:8f:d1)
Internet Protocol Version 4, Src: 192.168.11.10 (192.168.11.10), Dst: 201.235.253.60 (201.235.253.60)
Transmission Control Protocol, Src Port: 14327 (14327), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 348
Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
5	0.028278000	201.235.253.60	192.168.11.10	TCP	54	80→14327 [ACK] Seq=1 Ack=349 Win=15544 Len=0

Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Cisco-Li_3d:8f:d1 (00:25:9c:3d:8f:d1), Dst: Tp-LinkT_d9:ee:ee (00:25:86:d9:ee:ee)
Internet Protocol Version 4, Src: 201.235.253.60 (201.235.253.60), Dst: 192.168.11.10 (192.168.11.10)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 14327 (14327), Seq: 1, Ack: 349, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
6	0.066790000	201.235.253.60	192.168.11.10	HTTP	1451	HTTP/1.1 200 OK (text/html)

Frame 6: 1451 bytes on wire (11608 bits), 1451 bytes captured (11608 bits) on interface 0
Ethernet II, Src: Cisco-Li_3d:8f:d1 (00:25:9c:3d:8f:d1), Dst: Tp-LinkT_d9:ee:ee (00:25:86:d9:ee:ee)
Internet Protocol Version 4, Src: 201.235.253.60 (201.235.253.60), Dst: 192.168.11.10 (192.168.11.10)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 14327 (14327), Seq: 1, Ack: 349, Len: 1397
Hypertext Transfer Protocol
Line-based text data: text/html

No.	Time	Source	Destination	Protocol	Length	Info
7	0.200444000	192.168.11.10	201.235.253.60	TCP	54	14327→80 [ACK] Seq=349 Ack=1398 Win=16123 Len=0

Frame 7: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Tp-LinkT_d9:ee:ee (00:25:86:d9:ee:ee), Dst: Cisco-Li_3d:8f:d1 (00:25:9c:3d:8f:d1)
Internet Protocol Version 4, Src: 192.168.11.10 (192.168.11.10), Dst: 201.235.253.60 (201.235.253.60)
Transmission Control Protocol, Src Port: 14327 (14327), Dst Port: 80 (80), Seq: 349, Ack: 1398, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
8	5.053898000	201.235.253.60	192.168.11.10	TCP	54	80→14327 [FIN, ACK] Seq=1398 Ack=349 Win=15544 Len=0

Frame 8: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Cisco-Li_3d:8f:d1 (00:25:9c:3d:8f:d1), Dst: Tp-LinkT_d9:ee:ee (00:25:86:d9:ee:ee)
Internet Protocol Version 4, Src: 201.235.253.60 (201.235.253.60), Dst: 192.168.11.10 (192.168.11.10)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 14327 (14327), Seq: 1398, Ack: 349, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
9	5.053929000	192.168.11.10	201.235.253.60	TCP	54	14327→80 [ACK] Seq=349 Ack=1399 Win=16123 Len=0

Frame 9: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Tp-LinkT_d9:ee:ee (00:25:86:d9:ee:ee), Dst: Cisco-Li_3d:8f:d1 (00:25:9c:3d:8f:d1)
Internet Protocol Version 4, Src: 192.168.11.10 (192.168.11.10), Dst: 201.235.253.60 (201.235.253.60)
Transmission Control Protocol, Src Port: 14327 (14327), Dst Port: 80 (80), Seq: 349, Ack: 1399, Len: 0

1. **¿Qué capas aparecen en cada paquete?**

En cada paquete de la captura, aparecen las siguientes capas:

Capa 2 (Enlace de datos): Ethernet II (con las direcciones MAC de origen y destino).

Capa 3 (Red): IP (protocolo IP, con las direcciones IP de origen y destino).

Capa 4 (Transporte): TCP (protocolo TCP, con los puertos de origen y destino, y la secuencia y acuse de recibo).

Capa 7 (Aplicación): HTTP (solo en los paquetes que corresponden a la comunicación HTTP, como el paquete 4 y el paquete 6).

¿En qué paquetes aparece la capa de aplicación?

La capa de aplicación aparece en los siguientes paquetes:

Paquete 4: HTTP (GET / HTTP/1.1)

Paquete 6: HTTP (HTTP/1.1 200 OK)

¿Qué IP inicia la conversación?

La IP que inicia la conversación es **192.168.11.10** (en el paquete 1, el primer SYN enviado).

¿Cuál es el puerto de origen y destino?

En el paquete 1 (SYN), el puerto de origen es **14327** y el puerto de destino es **80**.

Este mismo puerto de origen y destino se mantiene en toda la conversación.

¿Qué IP finaliza la conversación?

La IP que finaliza la conversación es **201.235.253.60** (en el paquete 8, con un FIN, ACK enviado desde esa IP).

2. Analizar la siguiente captura de Wireshark de tráfico UDP

Identificar la dirección IP del cliente y la del servidor.

Identificar los puertos involucrados indicando a qué tipo pertenecen.

¿Cuál es el tamaño de datos correspondiente a la capa de aplicación del cliente?

¿Cuál es el tamaño de datos correspondiente a la capa de aplicación en el servidor?

No.	Time	Source	Destination	Protocol	Length	Info
17	3.275669207	192.168.80.250	192.168.80.11	DNS	70	Standard query 0x4b86 MX kernel.org

Frame 17: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
Interface id: 0 (wlp7s0)
Encapsulation type: Ethernet (1)
Arrival Time: Aug 16, 2016 15:40:25.708641616 ART
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1471372825.708641616 seconds
[Time delta from previous captured frame: 1.057071971 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 3.275669207 seconds]
Frame Number: 17
Frame Length: 70 bytes (560 bits)
Capture Length: 70 bytes (560 bits)
[Frame is marked: False]
[Frame is ignored: False]
File Offset: 2544 (0x9f0)
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HonHaiPr_02:4d:3f (0c:84:dc:02:4d:3f), Dst: Tp-LinkT_37:2d:34 (10:fe:ed:37:2d:34)
Destination: Tp-LinkT_37:2d:34 (10:fe:ed:37:2d:34)
Address: Tp-LinkT_37:2d:34 (10:fe:ed:37:2d:34)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: HonHaiPr_02:4d:3f (0c:84:dc:02:4d:3f)
Address: HonHaiPr_02:4d:3f (0c:84:dc:02:4d:3f)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.80.250, Dst: 192.168.80.11
0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 56

Identification: 0xa63f (42559)

Flags: 0x00

0... .... = Reserved bit: Not set

.0.. .... = Don't fragment: Not set

..0. .... = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: UDP (17)

Header checksum: 0xb21f [validation disabled]

[Good: False]

[Bad: False]

Source: 192.168.80.250

Destination: 192.168.80.11

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

User Datagram Protocol, Src Port: 59024, Dst Port: 53

Source Port: 59024

Destination Port: 53

Length: 36

Checksum: 0x8d39 [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

[Stream index: 0]

Domain Name System (query)

[Response In: 24]

Transaction ID: 0x4b86

Flags: 0x0100 Standard query

0... .... = Response: Message is a query

.000 0... .... = Opcode: Standard query (0)

.... ..0. .... = Truncated: Message is not truncated

....1 .... = Recursion desired: Do query recursively

.... .0.. .... = Z: reserved (0)

....0 .... = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

kernel.org: type MX, class IN

Name: kernel.org
[Name Length: 10]
[Label Count: 2]
Type: MX (Mail eXchange) (15)
Class: IN (0x0001)

No.	Time	Source	Destination	Protocol	Length	Info
24	3.493657338	192.168.80.11	192.168.80.250	DNS	157	Standard query response 0x4b86 MX kernel.org

MX 30 ns2.kernel.org MX 30 ns4.kernel.org MX 999 bl-ckh-le.kernel.org MX 10 mail.kernel.org

Frame 24: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface 0
Interface id: 0 (wlp7s0)
Encapsulation type: Ethernet (1)
Arrival Time: Aug 16, 2016 15:40:25.926629747 ART
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1471372825.926629747 seconds
[Time delta from previous captured frame: 0.095370934 seconds]
[Time delta from previous displayed frame: 0.217988131 seconds]
[Time since reference or first frame: 3.493657338 seconds]
Frame Number: 24
Frame Length: 157 bytes (1256 bits)
Capture Length: 157 bytes (1256 bits)
[Frame is marked: False]
[Frame is ignored: False]
File Offset: 3772 (0xebc)
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: Tp-LinkT_37:2d:34 (10:fe:ed:37:2d:34), Dst: HonHaiPr_02:4d:3f (0c:84:dc:02:4d:3f)
Destination: HonHaiPr_02:4d:3f (0c:84:dc:02:4d:3f)
Address: HonHaiPr_02:4d:3f (0c:84:dc:02:4d:3f)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Tp-LinkT_37:2d:34 (10:fe:ed:37:2d:34)
Address: Tp-LinkT_37:2d:34 (10:fe:ed:37:2d:34)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.80.11, Dst: 192.168.80.250
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 143

Identification: 0xe5a6 (58790)

Flags: 0x02 (Don't Fragment)

0... .... = Reserved bit: Not set

.1.. .... = Don't fragment: Set

..0. .... = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: UDP (17)

Header checksum: 0x3261 [validation disabled]

[Good: False]

[Bad: False]

Source: 192.168.80.11

Destination: 192.168.80.250

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

User Datagram Protocol, Src Port: 53, Dst Port: 59024

Source Port: 53

Destination Port: 59024

Length: 123

Checksum: 0x4456 [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

[Stream index: 0]

Domain Name System (response)

[Request In: 17]

[Time: 0.217988131 seconds]

Transaction ID: 0x4b86

Flags: 0x8180 Standard query response, No error

1... .... = Response: Message is a response

.000 0... .... = Opcode: Standard query (0)

.... .0.. .... = Authoritative: Server is not an authority for domain

.... ..0. .... = Truncated: Message is not truncated

....1 .... = Recursion desired: Do query recursively

.... 1... .... = Recursion available: Server can do recursive queries

.... .0.. .... = Z: reserved (0)

....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server

....0 .... = Non-authenticated data: Unacceptable

.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 4

Authority RRs: 0

Additional RRs: 0

Queries

kernel.org: type MX, class IN
Name: kernel.org
[Name Length: 10]
[Label Count: 2]
Type: MX (Mail eXchange) (15)
Class: IN (0x0001)
Answers
kernel.org: type MX, class IN, preference 30, mx ns2.kernel.org
Name: kernel.org
Type: MX (Mail eXchange) (15)
Class: IN (0x0001)
Time to live: 599
Data length: 8
Preference: 30
Mail Exchange: ns2.kernel.org
kernel.org: type MX, class IN, preference 30, mx ns4.kernel.org
Name: kernel.org
Type: MX (Mail eXchange) (15)
Class: IN (0x0001)
Time to live: 599
Data length: 8
Preference: 30
Mail Exchange: ns4.kernel.org
kernel.org: type MX, class IN, preference 999, mx bl-ckh-le.kernel.org
Name: kernel.org
Type: MX (Mail eXchange) (15)
Class: IN (0x0001)
Time to live: 599

Data length: 14
Preference: 999
Mail Exchange: bl-ckh-le.kernel.org
kernel.org: type MX, class IN, preference 10, mx mail.kernel.org
Name: kernel.org
Type: MX (Mail eXchange) (15)
Class: IN (0x0001)
Time to live: 599
Data length: 9
Preference: 10
Mail Exchange: mail.kernel.org

2. Identificación de **direcciones IP**:

Cliente: La dirección IP del cliente es 192.168.80.250 (origen en el paquete)**.**

Servidor: La dirección IP del servidor es 192.168.80.11 (destino en el paquete)**.**

Puertos involucrados:

Cliente: El puerto de origen del cliente es 59024, que es un puerto dinámico o efímero, usado para la comunicación temporal y sin un tipo específico asignado.

Servidor: El puerto de destino del servidor es 53, que es el puerto estándar utilizado para el protocolo DNS**.**

Tamaño de datos en la capa de aplicación (cliente):

En el primer paquete (Frame 17), que es una consulta DNS desde el cliente, el tamaño de datos correspondiente a la capa de aplicación es de 36 bytes, que es el tamaño de los datos del protocolo UDP en este paquete (Longitud total: 56 bytes - Encabezado IP: 20 bytes - Encabezado UDP: 8 bytes).

Tamaño de datos en la capa de aplicación (servidor):

En el segundo paquete (Frame 24), que es la respuesta DNS desde el servidor, el tamaño de datos correspondiente a la capa de aplicación es de 123 bytes, que es el tamaño de los datos del protocolo UDP en este paquete (Longitud total: 143 bytes - Encabezado IP: 20 bytes - Encabezado UDP: 20 bytes).

3. Dibujar un diagrama con los siguientes componentes:

CPE (Customer Premises Equipment) [Equipo Local del Cliente)

Dp (Demarcation point) [Punto de demarcación]

Ll (Local loop) [Bucle local]

CO (Central Office) [Oficina Central]

Tn (Toll network) [La línea troncal dentro de la red del proveedor de la WAN]

CSU/DSU (channel service unit/data service unit)

CPE [Router/PC] -----> Dp [Cloud] -----> Ll [Serial DCE/DTE Cable] -----> CO [Router] -----> Tn [Cloud]

| | |

+--- CSU/DSU [Nota] --+

4. Hacer un esquema de la conexión serial WAN, con los distintos tipos de dispositivos. Indicando:

Equipo que hace la transmisión de datos por la interfaz serie.

Dibujar la conexión para tener acceso a la consola del modem.

Indicar los tipos de cables utilizados

Para describir la conexión serial WAN y sus dispositivos, aquí un esquema simplificado

Transmisión de datos:

El **Router o Switch** es el equipo encargado de transmitir los datos a través de la interfaz serial. Conecta a los dispositivos que forman parte de la red WAN.

Acceso a la consola del módem:

Para acceder a la consola del módem, se debe utilizar una conexión **serial (RS-232)**, generalmente a través de un puerto **RJ-45 a DB-9** o un **cable de consola** (dependiendo del modelo del módem).

Tipos de cables utilizados:

Cable de consola (RJ-45 a DB-9 o RJ-45 a DB-25): Este cable se utiliza para conectar un **PC** o **terminal de acceso** al módem o router a través de la consola.

Cable serial (DB-9 a DB-9): Usado para la conexión entre el router y el módem si ambos dispositivos tienen puertos seriales.

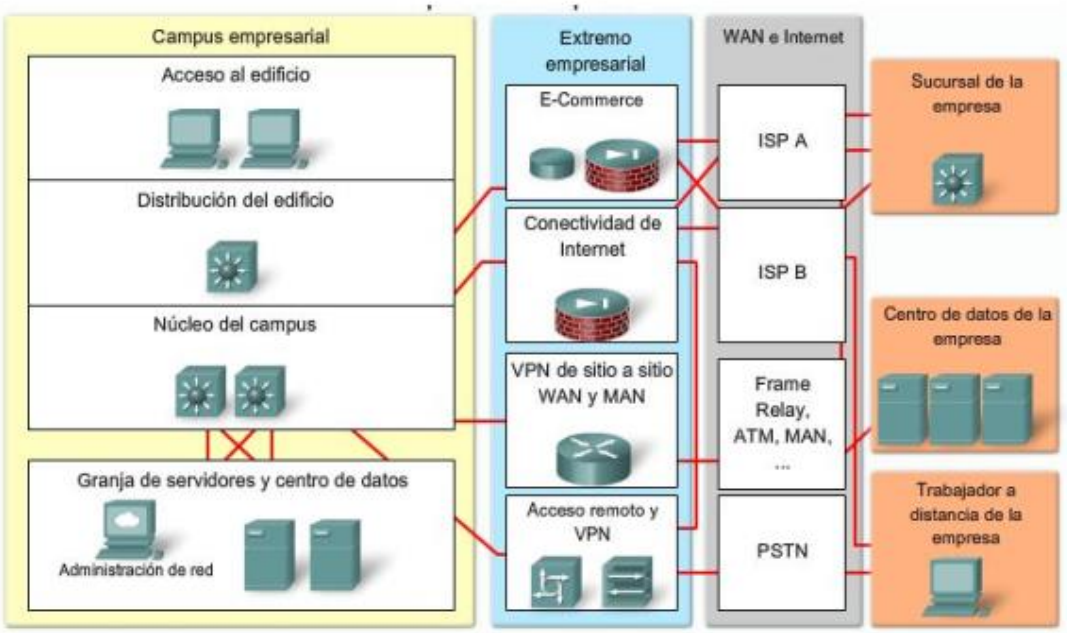
Diagrama de conexión:

[PC/Terminal de Acceso] --(Cable de consola RJ-45 a DB-9)--> [Módem/Router] --(Cable Serial DB-9 a DB-9)--> [Equipo de transmisión WAN]

5. Dibujar el modelo jerárquico distribuido:

indicando los tipos de dispositivos en cada capa.

Las palabras: Velocidad, Conmutación, filtrado, tienen que ver cada una con una capa en particular, escribirla en el esquema.



6. Hacer un esquema de una conexión VPN de acceso remoto.

Usuario remoto (PC/Laptop)

| |---- Conexión a Internet (Red Pública)

| |---- VPN Client (Cliente VPN instalado en el dispositivo)

| |---- Túnel VPN Encriptado

| |---- Firewall/VPN Gateway (Puerta de enlace VPN en la red corporativa)

| |---- LAN Corporativa (Red privada interna)

Descripción del flujo:

Usuario remoto:

Un empleado accede desde una computadora o laptop fuera de la oficina.

Conexión a Internet:

Se utiliza la red pública (por ejemplo, Wi-Fi en casa o datos móviles) para establecer la conexión inicial.

Cliente VPN:

El software cliente crea un túnel cifrado para proteger los datos enviados entre el usuario y la red corporativa.

Túnel VPN encriptado:

Proporciona seguridad y privacidad durante la transmisión de datos.

Firewall/VPN Gateway:

Verifica credenciales, aplica políticas de acceso y permite el tráfico seguro hacia la red interna.

LAN corporativa:

Acceso autorizado a recursos internos como servidores, archivos compartidos e impresoras.

Este esquema muestra cómo funciona una conexión VPN para permitir el acceso seguro a recursos corporativos desde ubicaciones remotas.

7. Hacer un esquema de una conexión VPN site-to-site.

Esquema en texto de una conexión VPN Site-to-Site:

Sede 1 (LAN 1)

|

|---- Router/Firewall con VPN Gateway (Sede 1)

|

|---- Túnel VPN Encriptado

|

|---- Router/Firewall con VPN Gateway (Sede 2)

|

Sede 2 (LAN 2)

Descripción del flujo:

LAN 1 (Red local de la sede 1):

Dispositivos y servidores locales acceden a la red.

Router/Firewall con VPN Gateway (Sede 1):

Establece un túnel VPN cifrado hacia la otra sede.

Túnel VPN encriptado:

Protege los datos durante la transmisión entre las dos redes locales a través de Internet.

Router/Firewall con VPN Gateway (Sede 2):

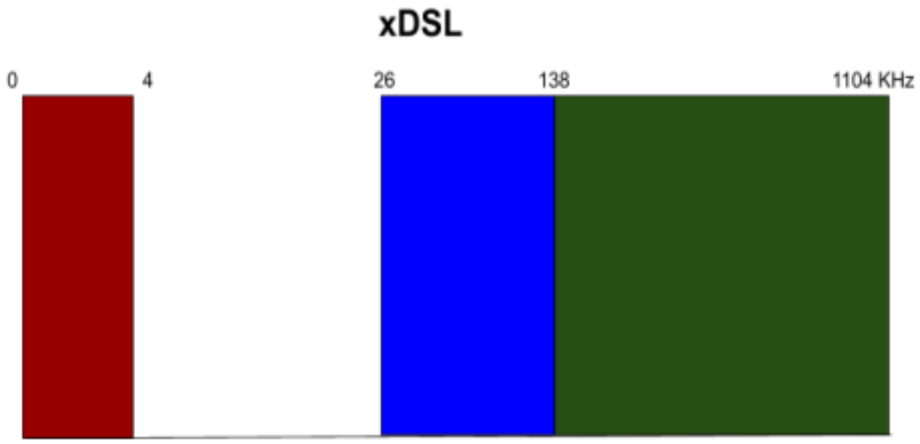
Recibe los datos cifrados, los desencripta y los dirige a la red local de la sede 2.

LAN 2 (Red local de la sede 2):

Dispositivos y servidores acceden a los datos compartidos desde la sede 1.

Aplicación:
Este esquema permite la comunicación segura entre dos oficinas remotas como si estuvieran en la misma red física, ideal para compartir recursos corporativos entre sedes.

8. De acuerdo con el siguiente gráfico explicar:



¿A qué tipo de tecnología xDSL corresponde?

¿Qué representa el la banda roja?

¿Qué representa la banda azul?

¿Qué representa la banda verde?

¿Qué implicancias prácticas conlleva la distribución de las bandas?

El gráfico parece representar la distribución de bandas de frecuencias en una tecnología xDSL. Respondiendo a las preguntas:

¿A qué tipo de tecnología xDSL corresponde?
Este gráfico probablemente representa **ADSL (Asymmetric Digital Subscriber Line)**, dado que esta tecnología usa bandas separadas para upstream (subida), downstream (bajada) y voz, con mayor ancho de banda dedicado al downstream.

¿Qué representa la banda roja?
La banda roja (0-4 kHz) generalmente corresponde al canal de **telefonía de voz (POTS)**. Este es el rango dedicado para servicios de voz tradicionales.

¿Qué representa la banda azul?
La banda azul (26-138 kHz) representa el canal de **upstream (subida)**. Aquí se asigna el espectro para enviar datos desde el usuario hacia la red.

¿Qué representa la banda verde?
La banda verde (138-1104 kHz) corresponde al canal de **downstream (bajada)**. Este es el rango asignado para recibir datos desde la red hacia el usuario, típicamente mayor que el upstream.

¿Qué implicancias prácticas conlleva la distribución de las bandas?

Asimetría en el ancho de banda: Al asignar un espectro mayor al downstream, ADSL se adapta bien a los patrones de uso típicos de internet, donde los usuarios descargan más información (navegación, streaming) de la que suben.

Separación del servicio de voz y datos: La banda dedicada a POTS asegura que las llamadas telefónicas no interfieran con la transmisión de datos.

Limitación del alcance y la velocidad: La calidad y velocidad de ADSL dependen de la distancia entre el usuario y la central telefónica, debido a la atenuación de las señales de alta frecuencia.

9. Se transmite un archivo de 15 MB entre 2 sucursales de una empresa mediante un enlace Wi-Fi que usa 802.11a. ¿Cuál es el tiempo mínimo que tardará en llegar? ¿Cuánto tardará (como mínimo) en copiarse dentro de una sucursal de una notebook a otra que se conectan a un Access Point mediante 802.11b? ¿Podrías proponer alguna mejora para que los archivos se transmitan más rápido? Si es así ¿Qué propondrías?

Para calcular el tiempo mínimo que tardará en llegar un archivo en ambos casos, primero necesitamos conocer la velocidad de transmisión de los dos estándares Wi-Fi mencionados.

Enlace Wi-Fi 802.11a (Para transmitir entre las sucursales)

Velocidad de 802.11a: Hasta 54 Mbps (en condiciones ideales).

Tamaño del archivo: 15 MB = 15 * 8 = 120 Mb.

La fórmula para calcular el tiempo de transmisión es:

Tiempo = Tamaño del archivo / velocidad de transmisión

Entonces, el tiempo mínimo será:

Tiempo = 120Mb/54 Mbps = 2.22 segundos

Enlace Wi-Fi 802.11b (Para copiar entre notebooks dentro de una sucursal)

Velocidad de 802.11b: Hasta 11 Mbps.

Tamaño del archivo: 15 MB = 120 Mb.

Aplicamos la misma fórmula:

Tiempo = 120Mb/11Mbps = 10.91 segundos

Mejoras propuestas para mejorar la velocidad de transmisión:

Cambiar a un estándar más rápido:

Si es posible, cambiar de 802.11a a 802.11n o 802.11ac podría mejorar significativamente la velocidad de transmisión. Estos estándares alcanzan velocidades mucho mayores, como 150 Mbps (802.11n) o 1 Gbps (802.11ac) bajo condiciones ideales.

Optimizar la configuración de la red Wi-Fi:

Asegúrese de que las sucursales o notebooks estén utilizando canales menos congestionados en el espectro Wi-Fi, para evitar interferencias y mejorar el rendimiento.

Usar una banda de 5 GHz (si es posible) en lugar de 2.4 GHz puede reducir la interferencia y ofrecer mayor ancho de banda.

Usar cables de red para la transferencia entre dispositivos:

Si es posible, una solución más rápida y fiable sería conectar las notebooks a través de cables Ethernet, evitando las limitaciones de Wi-Fi y proporcionando una conexión más estable y rápida.

Actualizar equipos y routers:

Utilizar routers modernos que soporten las últimas versiones de Wi-Fi (como 802.11ac o 802.11ax) puede proporcionar mayores velocidades de transmisión y mejorar la cobertura.

Mejorar el entorno de la red:

Asegurarse de que no haya obstáculos o interferencias (como microondas, paredes gruesas o múltiples dispositivos conectados) que puedan afectar la señal Wi-Fi.

Si se implementan algunas de estas mejoras, se puede reducir considerablemente el tiempo de transmisión de archivos.

10. Dibujar un esquema en el cual el Bucle local es totalmente Wireless, especificar qué medidas de seguridad tomaría.

Esquema en texto de un bucle local totalmente inalámbrico:

Usuario Final (PC/Laptop/Smartphone)

|

|---- Conexión Wi-Fi (Enlace Inalámbrico)

|

|---- Punto de Acceso Inalámbrico (AP)

|

|---- Enlace Wireless (Antenas Punto a Punto o Multipunto)

|

|---- Estación Base (Proveedora del Servicio)

|

|---- Red de Proveedor (WAN/Internet)

Medidas de seguridad recomendadas:

Cifrado WPA3:

Usar WPA3 para cifrar las comunicaciones inalámbricas y proteger los datos transmitidos.

Autenticación 802.1X con RADIUS:

Implementar autenticación basada en RADIUS para validar usuarios y dispositivos autorizados.

VPN para tráfico de datos:

Configurar conexiones VPN para cifrar datos entre el usuario final y la red corporativa o el proveedor.

Filtrado de MAC Address:

Permitir acceso solo a dispositivos con direcciones MAC específicas.

Firewall en el punto de acceso y estación base:

Configurar reglas para controlar el tráfico entrante y saliente.

Segmentación de redes (VLANs):

Crear VLANs para separar tráfico interno, invitados y usuarios remotos.

Actualizaciones de firmware:

Mantener actualizados los puntos de acceso y routers para corregir vulnerabilidades.

Desactivar SSID Broadcasting:

Ocultar el nombre de la red para evitar su detección fácil.

Implementar IDS/IPS:

Utilizar sistemas de detección y prevención de intrusos para monitorear actividad sospechosa.

Control de acceso físico:

Proteger los dispositivos inalámbricos contra manipulaciones físicas.