UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

Department of Computer Sciences

Computer Networks

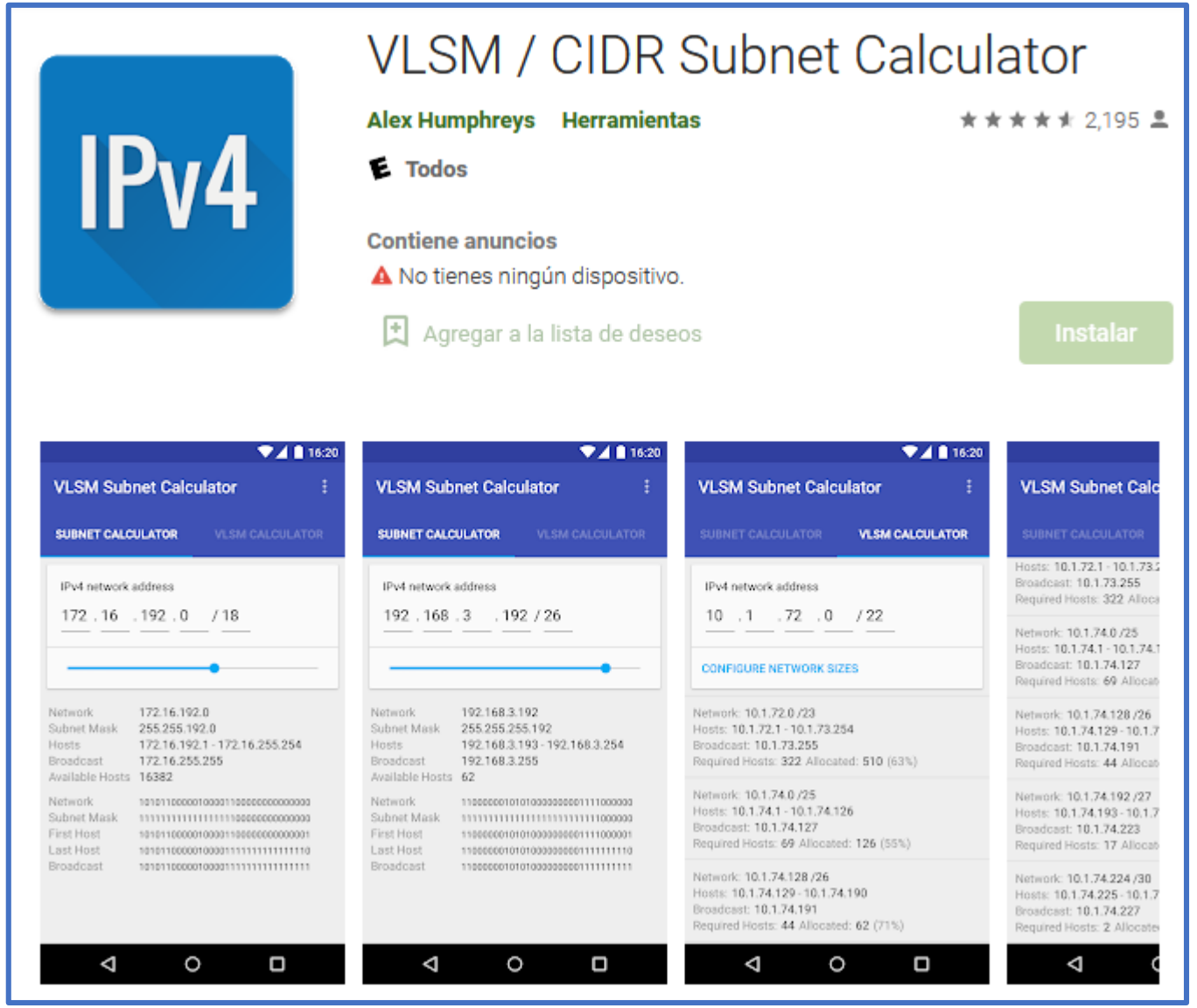
NCR: 14575

Profesor: Walter Fuertes Díaz, PhD.

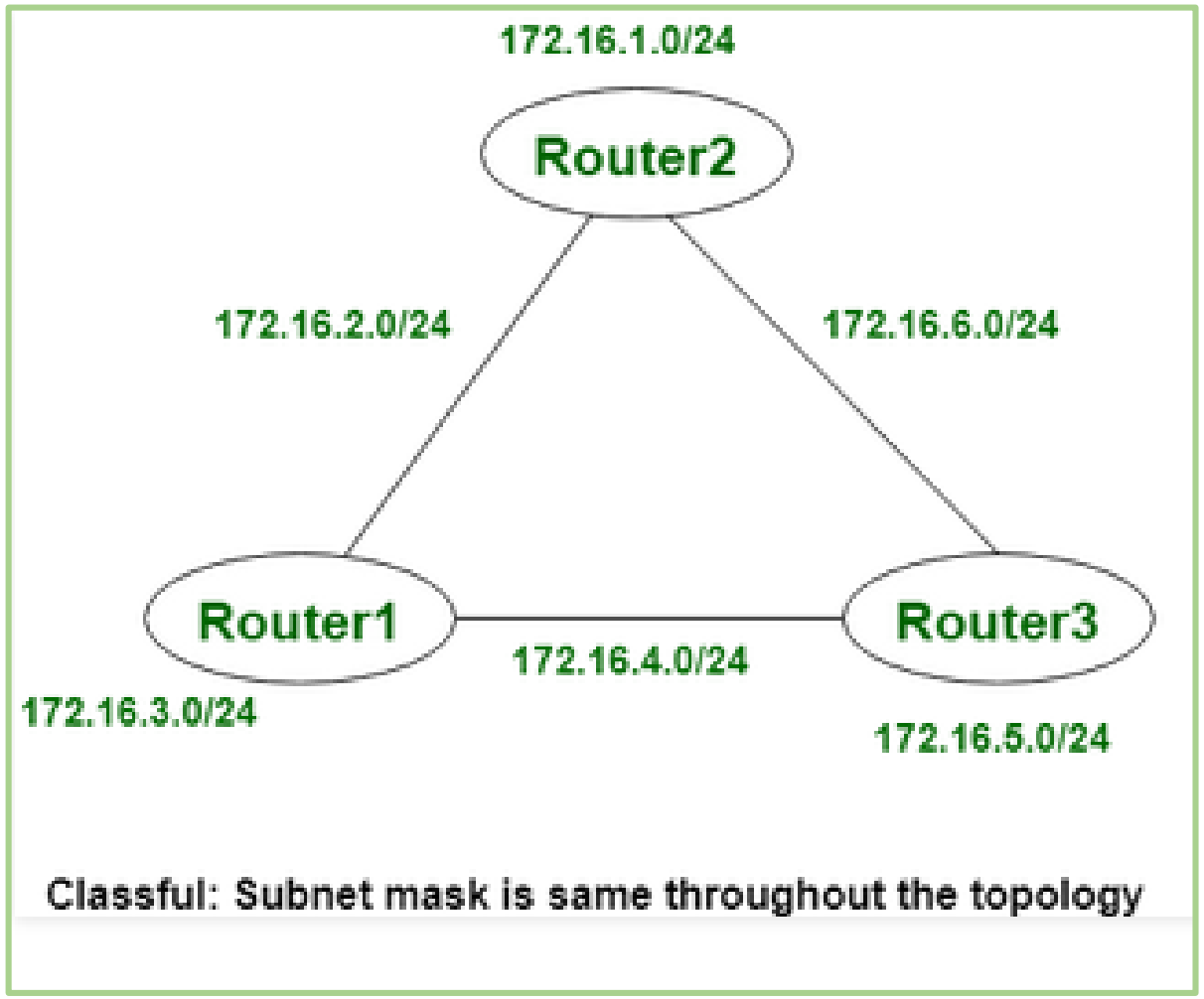
Second Unit.

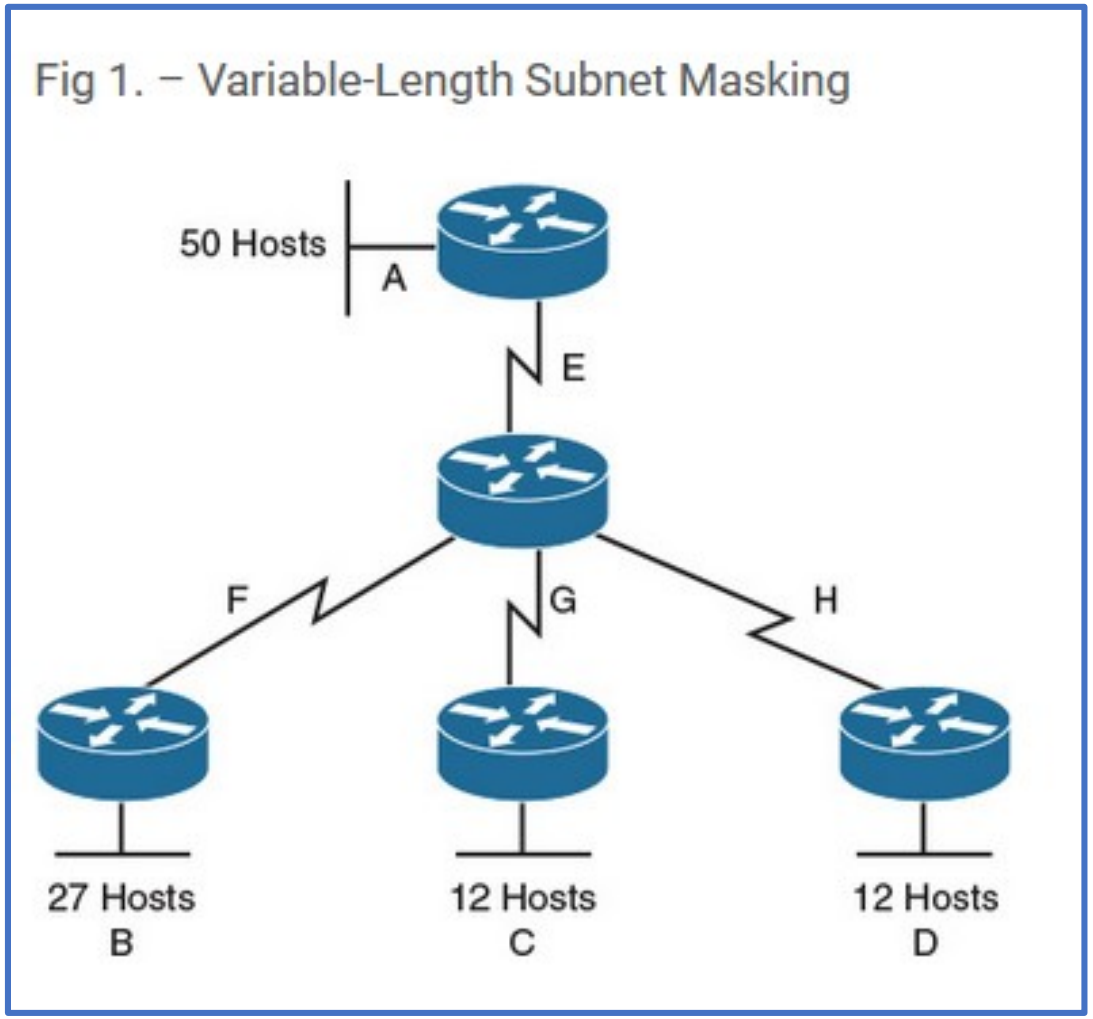
VLSM (Variable-Length Subnet Mask)

Google Play Store



Classful vs Classless





Fuente: Geeksforgeeks, “Classful Routing Vs Classless Routing” , URL: https://www.geeksforgeeks.org/difference-between-classful-routing-and-classless-routing/

Classful vs Classless

Differences between FLSM Subnetting and VLSM Subnetting

FLSM (Fixed Length Subnet Masks) Subnetting	VLSM (Variable Length Subnet Masks) Subnetting
All subnets are equal in size.	Subnets are variable in size.
All subnets have equal number of hosts.	Subnets have variable number of hosts.
All subnets use same subnet mask.	Subnets use different subnet masks.
It is easy in configuration and administration.	It is complex in configuration and administration.
It wastes a lot of IP addresses.	It wastes minimum IP addresses.
It is also known as classfull Subnetting.	It is also known as classless Subnetting.
It supports both classfull and classless routing protocols.	It supports only classless routing protocols.

Fuente: Geeksforgeeks, “Classful Routing Vs Classless Routing” , URL: https://www.geeksforgeeks.org/difference-between-classful-routing-and-classless-routing/

VLSM (Variable-Length Subnet Mask)

FLSM (Fixed Length Subnet Mask) (ClassFul)

It is the traditional Method if a fixed size subnet mask is used; that is, the same mask for all the subnets, all the subnets will have the same size;

So, for example, if the largest subnet needs 200 computers, all the subnets will have a size of 254 IP addresses (using 8 bits for 8 also assigns a subnet address with 254 IP addresses;

The remaining 252 addresses are being wasted;

This waste is extreme in the links between nodes of the wide network (WAN), which only need two IP addresses.

VLSM (Variable Length Subnet Mask, ClassLess)

Intending to alleviate this problem, in 1987, the VLSM standard emerged, Variable Length Subnet Mask (subnet mask with variable length):

It is defined in RFC 1009 as supporting subnets with different lengths of masks. This standard allows for more flexible IP addressing.

By using multiple masks, the subnets that are created do not have the same number of computers, allowing for an organization of the address space that is more in line with actual needs without wasting IP addresses.

In the same local network, there will be subnets with few computers with few IP addresses and subnets with many computers with a greater range of IP addresses.

It works based on the host number that is being requested.

Fuente: Redes Locales y Globales, “VLSM”, Disponible en: URL: https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/2-escasez-de-direcciones-ip-soluciones/2-vlsm

Classless Subnetting

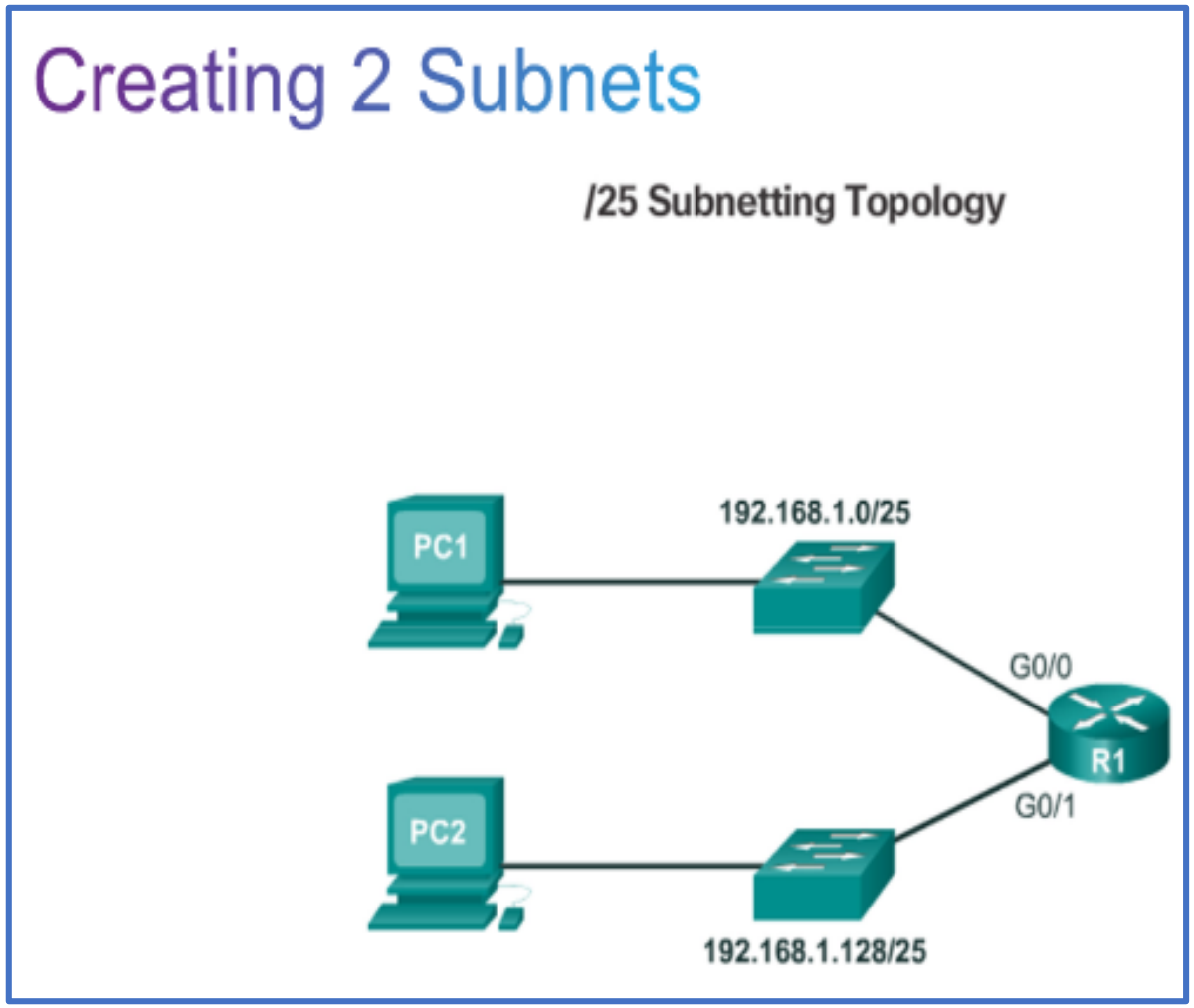
- /25 – Borrowing 1 bit from the fourth octet creates 2 subnets supporting 126 hosts each.
- /26 – Borrowing 2 bits creates 4 subnets supporting 62 hosts each.
- /27– Borrowing 3 bits creates 8 subnets supporting 30 hosts each.
- /28 – Borrowing 4 bits creates 16 subnets supporting 14 hosts each.
- /29 – Borrowing 5 bits creates 32 subnets supporting 6 hosts each.
- /30– Borrowing 6 bits creates 64 subnets supporting 2 hosts each.

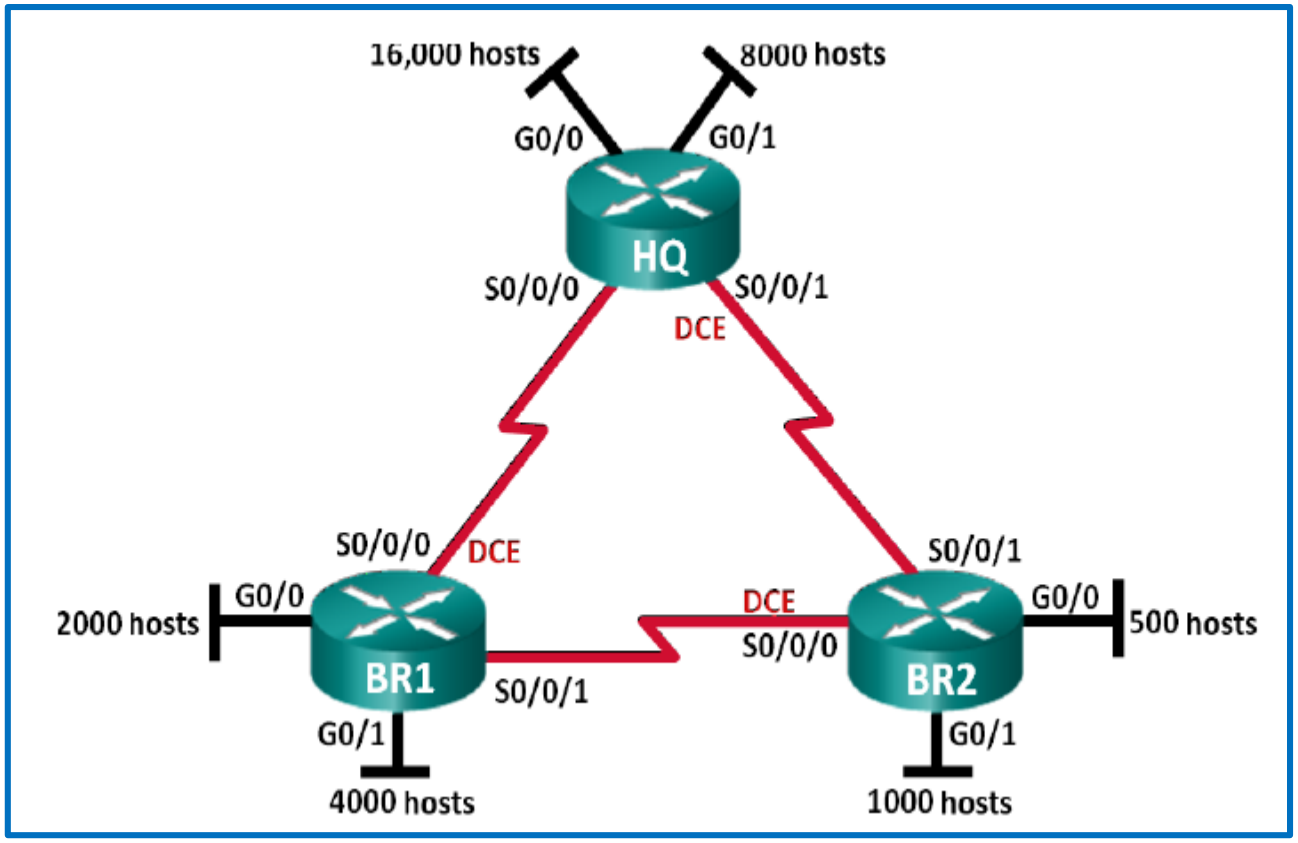
Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

VLSM

- Dada la red 192.168.1.0/24 verifique el prefijo (VLSM)
- 192.168.1.00000000
- 192.168.1.10000000, 255.255.255.128, 192.168.1.0/25, #Hosts=2^n-2; 2^7-2=126
- 192.168.1.11000000, 255.255.255.192, 192.168.1.0/26, #Hosts=2^n-2; 2^6-2=62.
- 192.168.1.11100000, 255.255.255.224, 192.168.1.0/27, #Hosts=2^n-2; 2^5-2=30.
- 192.168.1.11110000, 255.255.255.240, 192.168.1.0/28, #Hosts=2^n-2; 2^4-2=14.

VLSM (Variable-Length Subnet Mask)





VLSM (Variable-Length Subnet Mask)

Subnetting Formulas

To calculate the number of subnets.

2^n

n= bits borrowed

192 . 168 . 1 . 0

nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

Borrowing 1 bit:	2^1 = 2
Borrowing 2 bits:	2^2 = 4
Borrowing 3 bits:	2^3 = 8
Borrowing 4 bits:	2^4 = 16
Borrowing 5 bits:	2^5 = 32
Borrowing 6 bits:	2^6 = 64

Subnetting Formulas (cont.)

To calculate the number of hosts.

2^n-2

n= the number of bits remaining in the host field

192. 168. 1. 0 000 0000

7 bits remain in host field

2^7 = 128 hosts per subnet
2^7 - 2 = 126 valid hosts per subnet

Creating Subnets with a /16 prefix

Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000	2	32564
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.nnhhhhhh.hhhhhhhh 11111111.11111111.11000000.00000000	4	16282
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.nnnhhhhh.hhhhhhhh 11111111.11111111.11100000.00000000	8	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.nnnnhhhh.hhhhhhhh 11111111.11111111.11110000.00000000	16	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.nnnnnhhh.hhhhhhhh 11111111.11111111.11111000.00000000	32	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.nnnnnnhh.hhhhhhhh 11111111.11111111.11111100.00000000	64	1022
/23	255.255.254.0	nnnnnnnn.nnnnnnnn.nnnnnnnh.hhhhhhhh 11111111.11111111.11111110.00000000	128	510
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	256	254
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	512	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	1024	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	2048	30

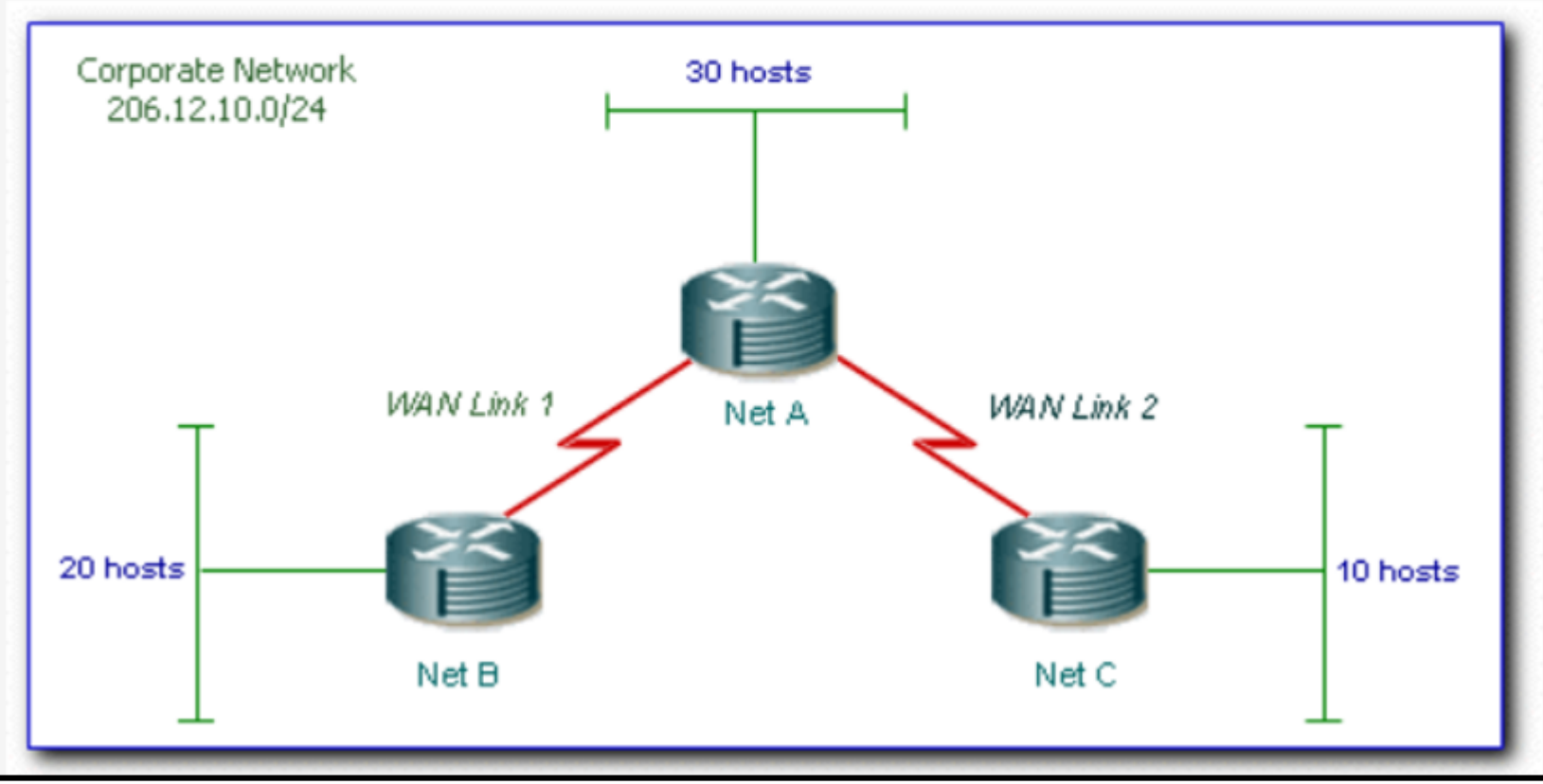
Cálculo de VLSM

Pasos:

1. Ordenar de mayor a menor
2. Determinar la máscara actual
3. Aplicar la Formula 2^n-2
4. Obtener la nueva mascara
5. Calcular el salto de red
6. Rellenar la tabla
7. Probar en el IP-Subnet Calc.
8. Simular en Packet Tracert

A corporate network with the network address of **206.12.10.0/24** is shown below. The network administrators plan to create separate 5 subnets. The requirements of each subnet are as follows:-

- Net A requires 30 hosts
- Net B requires 20 hosts
- Net C requires 10 hosts
- Each WAN connection requires 2 IP addresses on separate subnets



VLSM-Exercise 1

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Dada la red **172.16.0.0/24** se pide dividirla en Subredes con 40 hosts, 120 hosts, 12 hosts.

Máscara de Red actual:

255	255	255	0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0

Para **120** hosts. **Fórmula: 2^n-2>=N° de hosts**: 2^7-2=126; 126>=120

Nueva máscara de subred

255	255	255	128
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 0 0 0 0 0 0 0

Saltos de Red: **256 – 128 = 128**

Para **40** hosts. **Fórmula: 2^n-2>=N° de hosts**: 2^6-2>=40; 62>=40.

Nueva máscara de subred

255	255	255	192
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 0 0 0 0 0 0

Saltos de Red: **256 – 192 =64**

Nro. De Subred	Host solicitados	Host Encontrados	Prefijo de Mask	Máscara decimal punteada de subred	Dirección de Subred	Primera IP útil	Última IP útil	Dirección de Broadcast
1	120	126	/25	255.255.255.128	172.16.0.0	172.16.0.1	172.16.0.126	172.16.0.127
2	40	62	/26	255.255.255.192	172.16.0.128	172.16.0.129	172.16.0.190	172.16.0.191
3	12							

VLSM-Exercise 1

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Dada la red **172.16.0.0/24** se pide dividirla en Subredes con 40 hosts, 120 hosts, 12 hosts.

Máscara de Red actual:

255	255	255	0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0

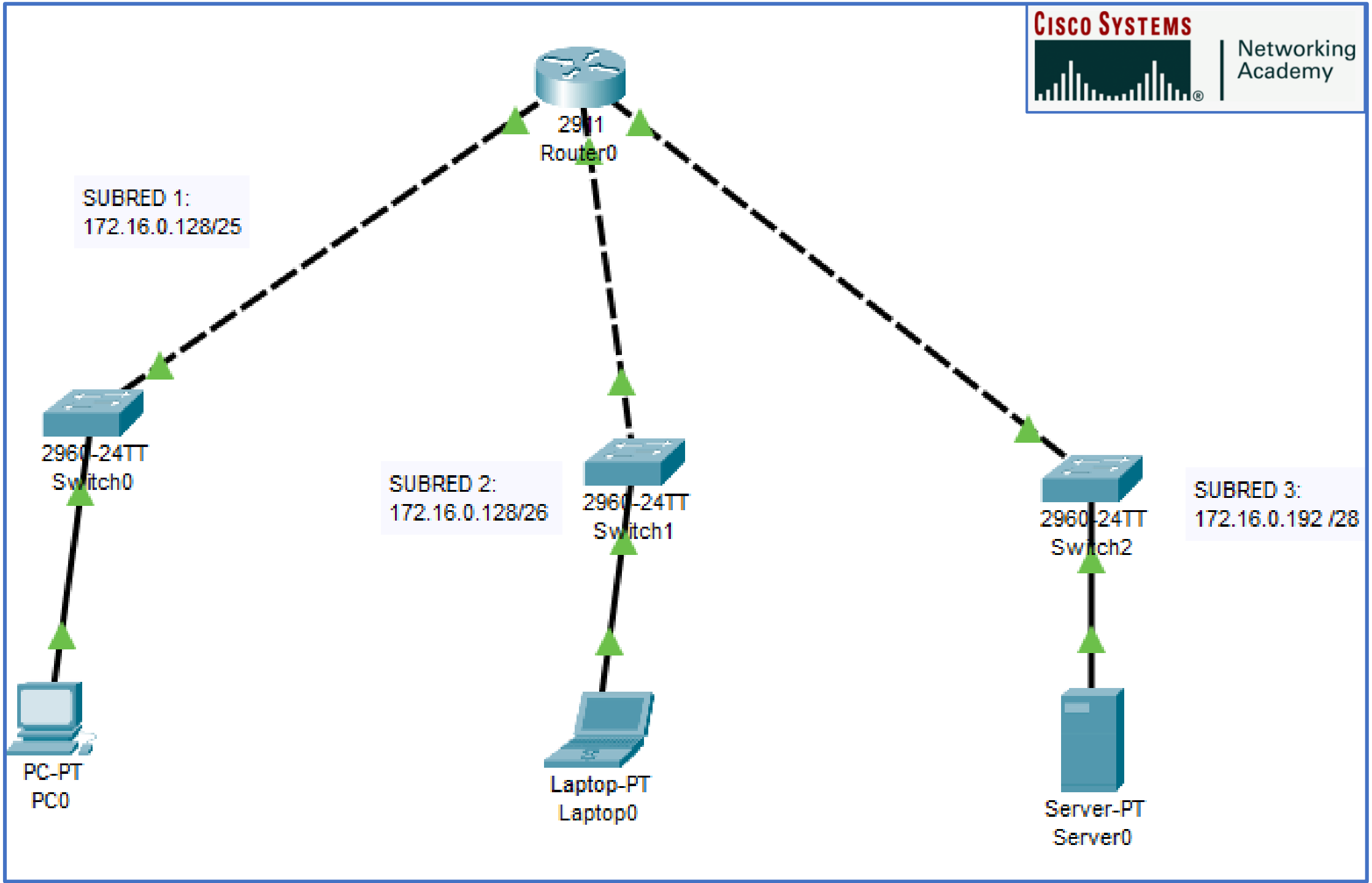
Para **12** hosts. **Fórmula: $2^n-2>=N°$ de hosts**: $2^4-2=14$; $14>=12$

Nueva máscara de subred

255	255	255	240
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 0 0 0 0

Saltos de Red: **256 – 240 = 16**

Nro. De Subred	Host solicitados	Host Encontrados	Prefijo de Mask	Máscara decimal punteada de subred	Dirección de Subred	Primera IP útil	Última IP útil	Dirección de Broadcast
1	120	126	/25	255.255.255.128	172.16.0.0	172.16.0.1	172.16.0.126	172.16.0.127
2	40	62	/26	255.255.255.192	172.16.0.128	172.16.0.129	172.16.0.190	172.16.0.191
3	12	14	/28	255.255.255.240	172.16.0.192	172.16.0.193	172.16.0.206	172.16.0.207

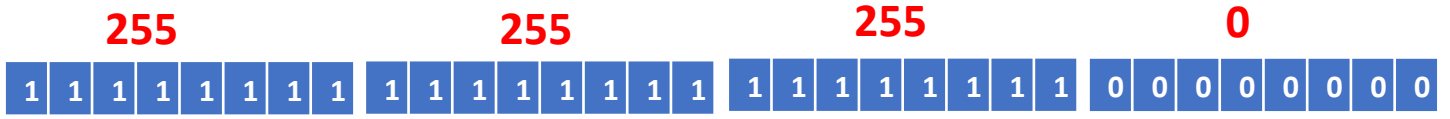

Cisco Systems
Networking Academy
2911
Router0
SUBRED 1:
172.16.0.128/25
2960-24TT
Switch0
SUBRED 2:
172.16.0.128/26
2960-24TT
Switch1
2960-24TT
Switch2
SUBRED 3:
172.16.0.192 /28
PC-PT
PC0
Laptop-PT
Laptop0
Server-PT
Server0

VLSM-Exercise 2

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Dada la red **192.168.1.0/24** se pide subredes con 60, 120, 10 y 24 hosts.

Máscara de Red actual:



Para **120** hosts. **Fórmula: 2^n-2>=N° de hosts**: 2^7-2=126; 126>=120

Nueva máscara de subred

Saltos de Red: **256 – 128 = 128**

Para **60** hosts. **Fórmula: 2^n-2>=N° de hosts**: 2^6-2=64; 62>=60

Nueva máscara de subred

Saltos de Red: **256 – 192 = 64**

Nro. De Subred	Host solicitados	Host Encontrados	Prefijo de Mask	Máscara decimal punteada de subred	Dirección de Subred	Primera IP útil	Última IP útil	Dirección de Broadcast
1	120	126	/25	255.255.255.128	192.168.1.0	192.168.1.1	192.168.1.126	192.168.1.127
2	60	62	/26	255.255.255.192	192.168.1.128	192.168.1.129	192.168.1.190	172.16.0.191
3	24							

VLSM-Exercise 2

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Dada la red 192.168.1.0/24 se pide subredes con 60, 120, 10 y 24 hosts.

Máscara de Red actual:

255	255	255	0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0

Para **24** hosts. **Fórmula: 2^n-2>=N° de hosts**: 2^5-2=24; 30>=24

Nueva máscara de subred

255	255	255	224
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 0 0 0 0 0

Saltos de Red: **256 – 224 = 32**

Para **10** hosts. **Fórmula: 2^n-2>=N° de hosts**: 2^4-2=10; 14>=10

Nueva máscara de subred

255	255	255	240
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 0 0 0 0

Saltos de Red: **256 – 240 = 16**

Nro. De SubR	Host solicitados	Host Encontrados	Prefijo de Mask	Máscara decimal punteada de subred	Dirección de Subred	Primera IP útil	Última IP útil	Dirección de Broadcast
1	120	126	/25	255.255.255.128	192.168.1.0	192.168.1.1	192.168.1.126	192.168.1.127
2	60	62	/26	255.255.255.192	192.168.1.128	192.168.1.129	192.168.1.190	172.16.0.191
3	24	30	/27	255.255.255.224	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223
4	10	14	/28	255.255.255.240	192.168.1.224	192.168.1.225	192.168.1.238	192.168.1.239

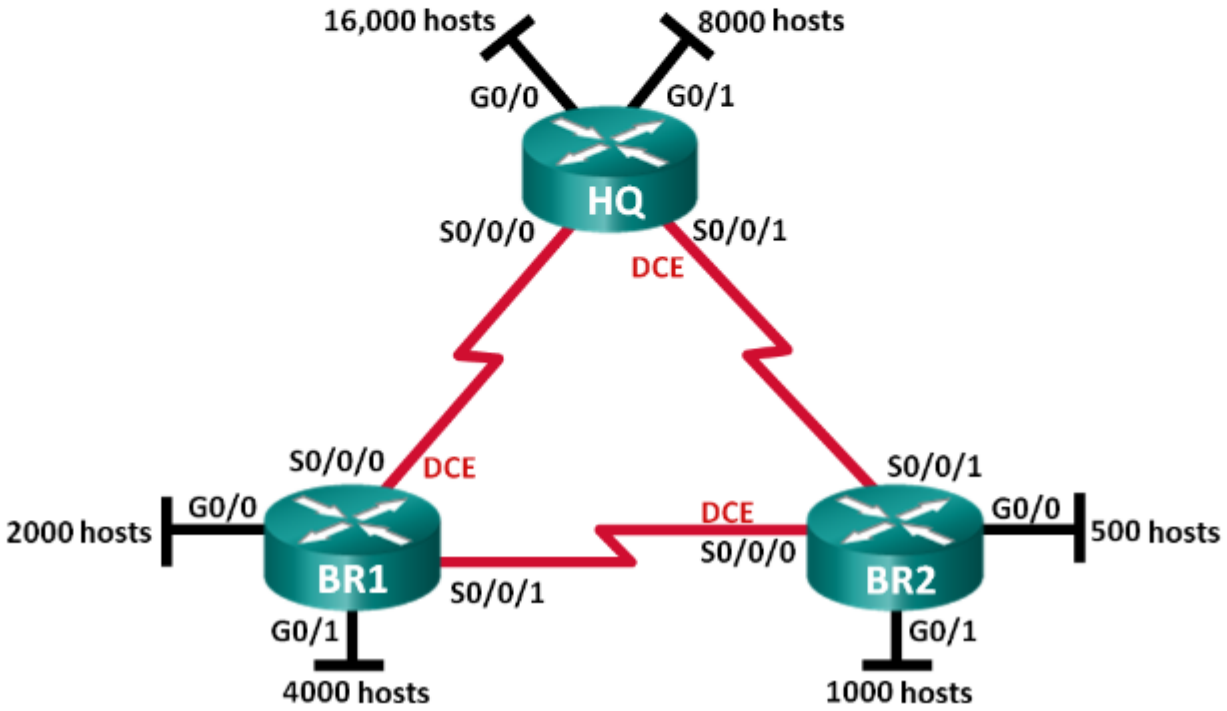
CISCO-NetAcad- Lab. 6.3.3.7

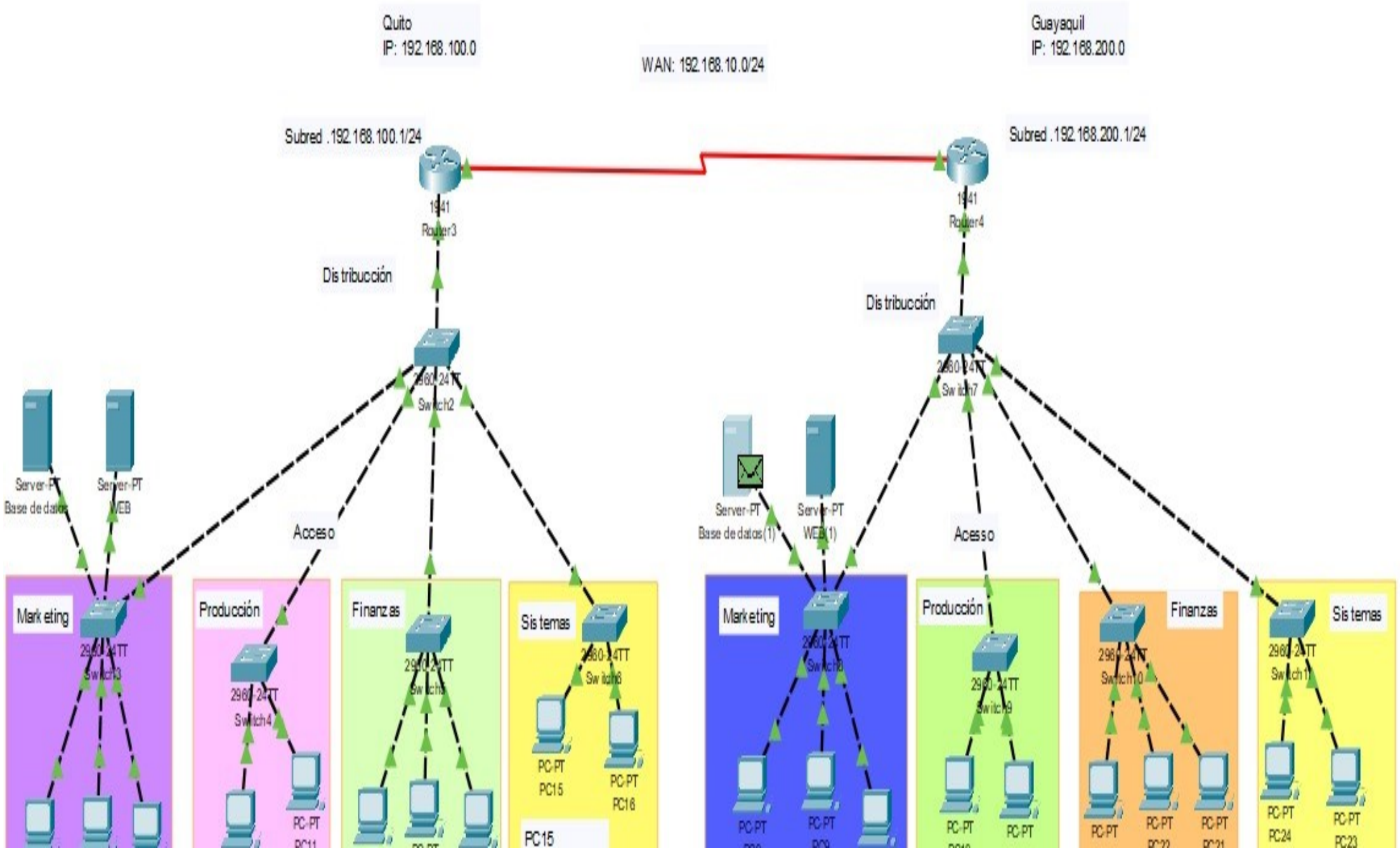
Práctica de Laboratorio

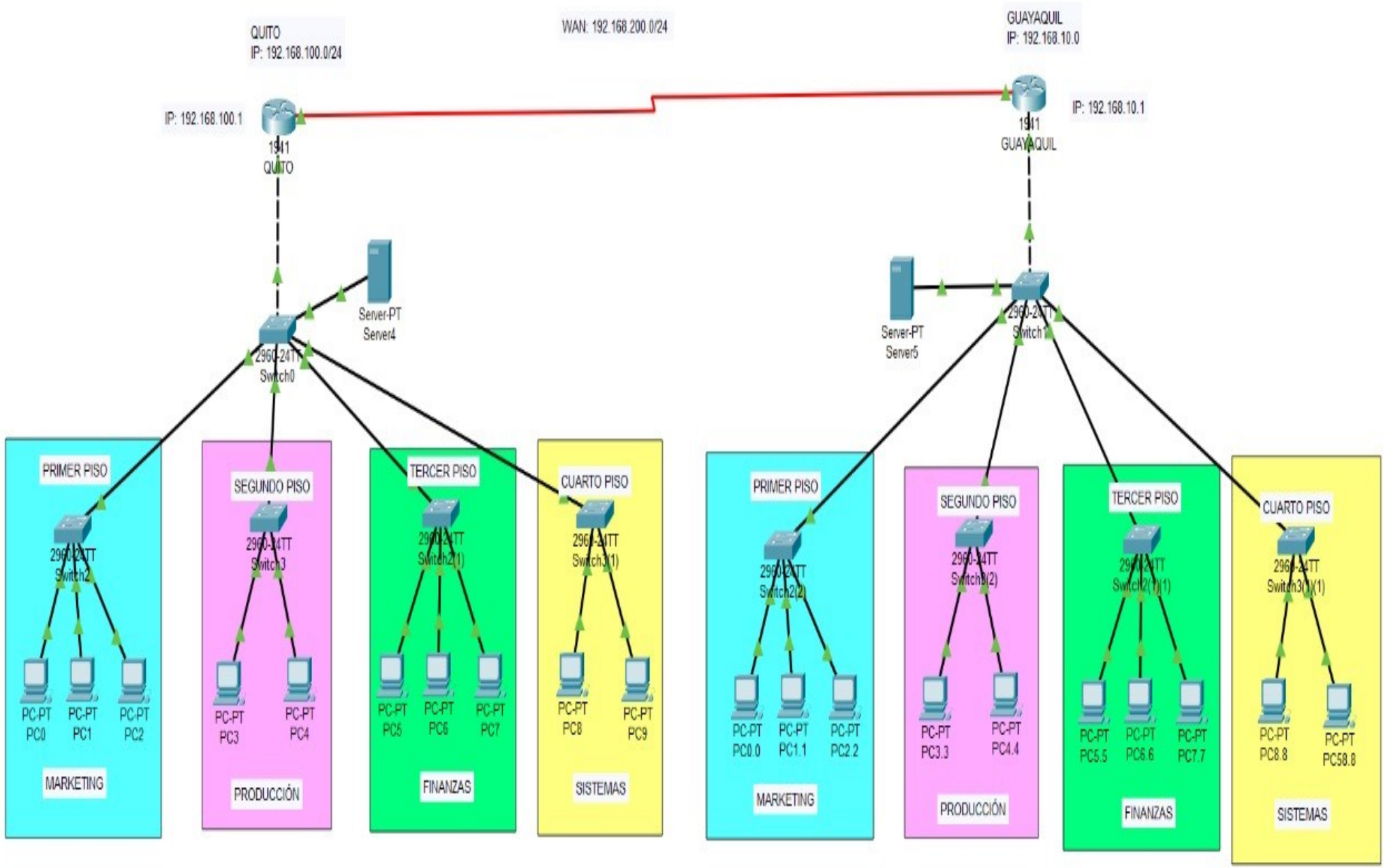
Cisco Networking Academy® Mind Wide Open™

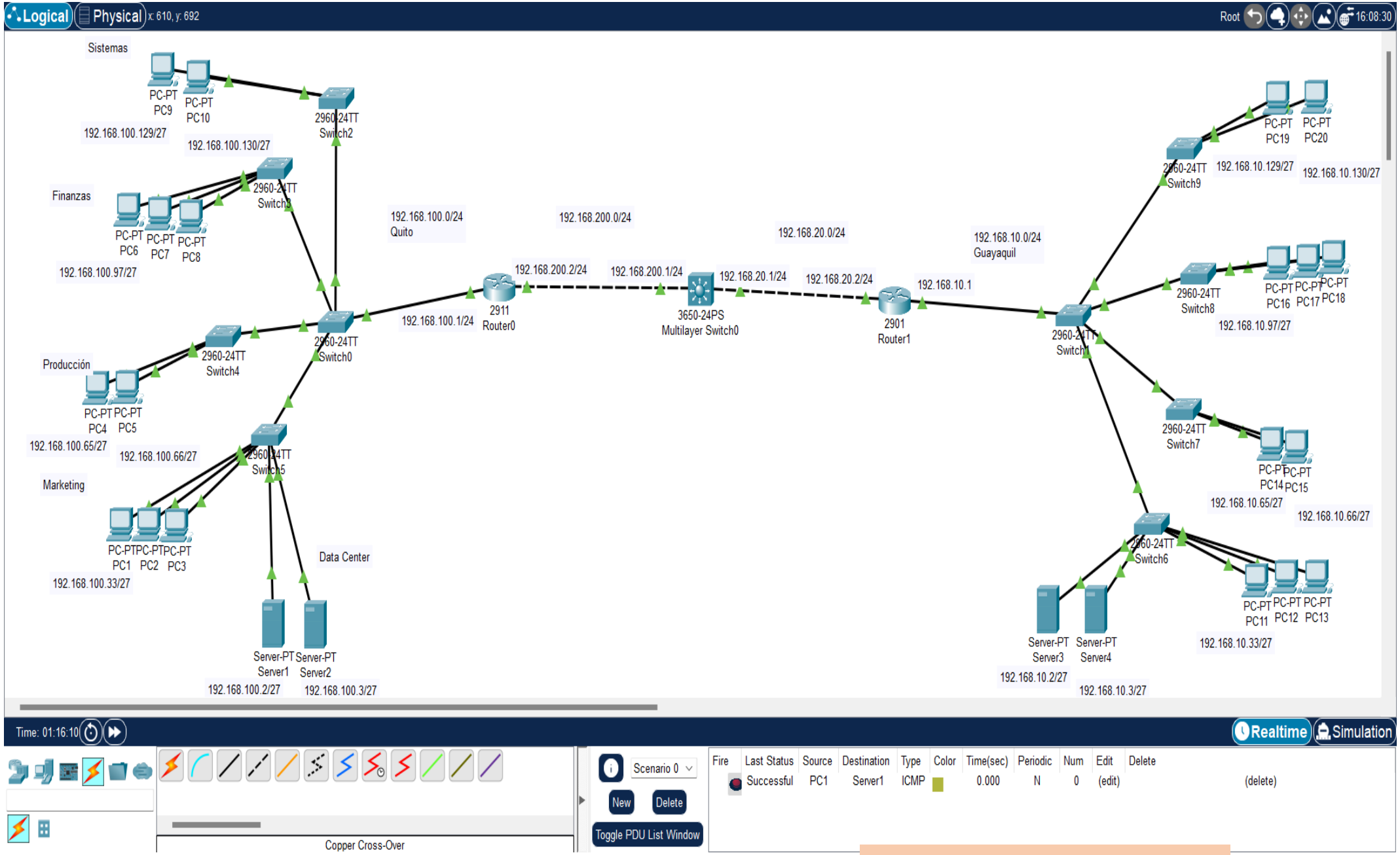
Práctica de laboratorio: diseño e implementación de direccionamiento IPv4 con VLSM

Topología

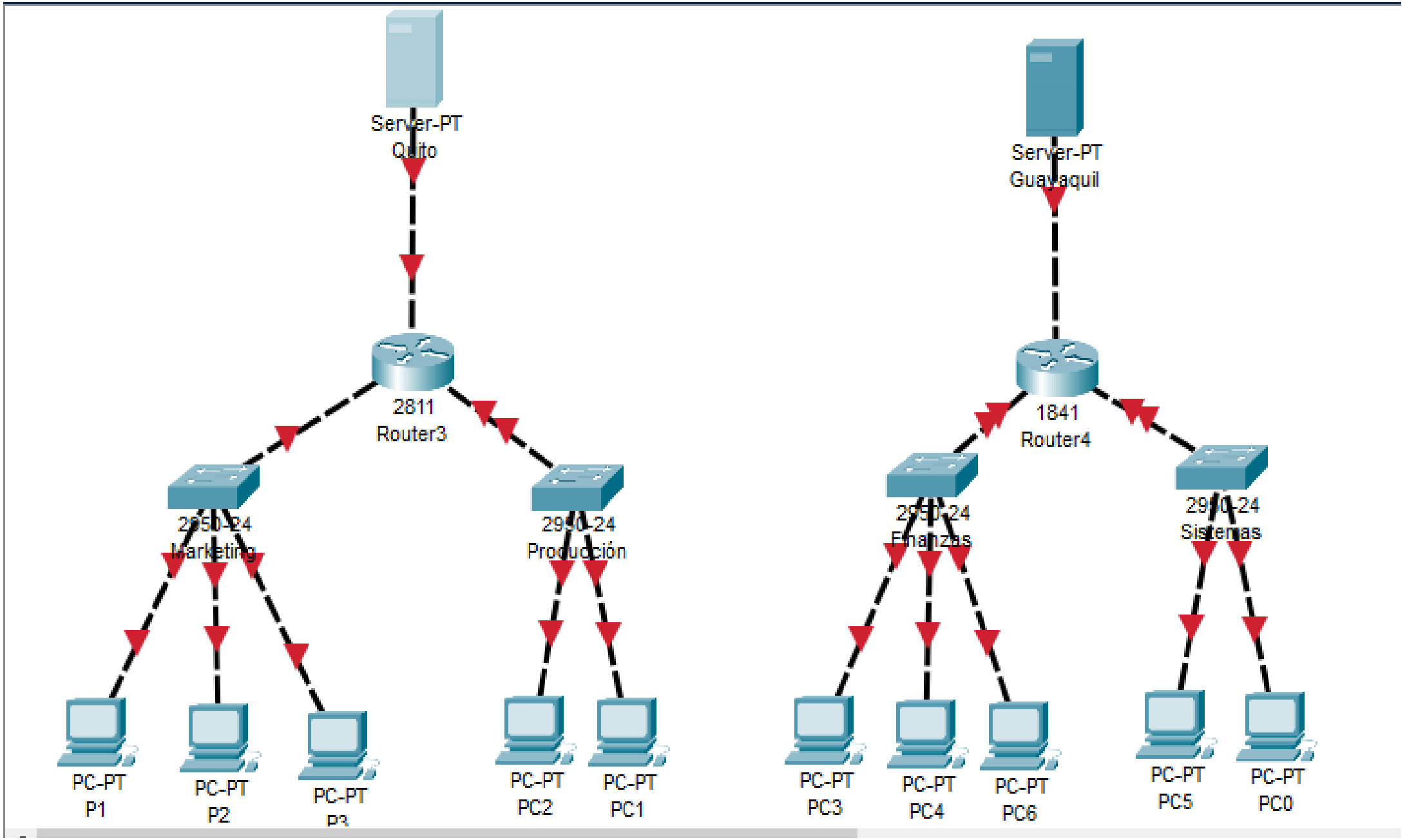


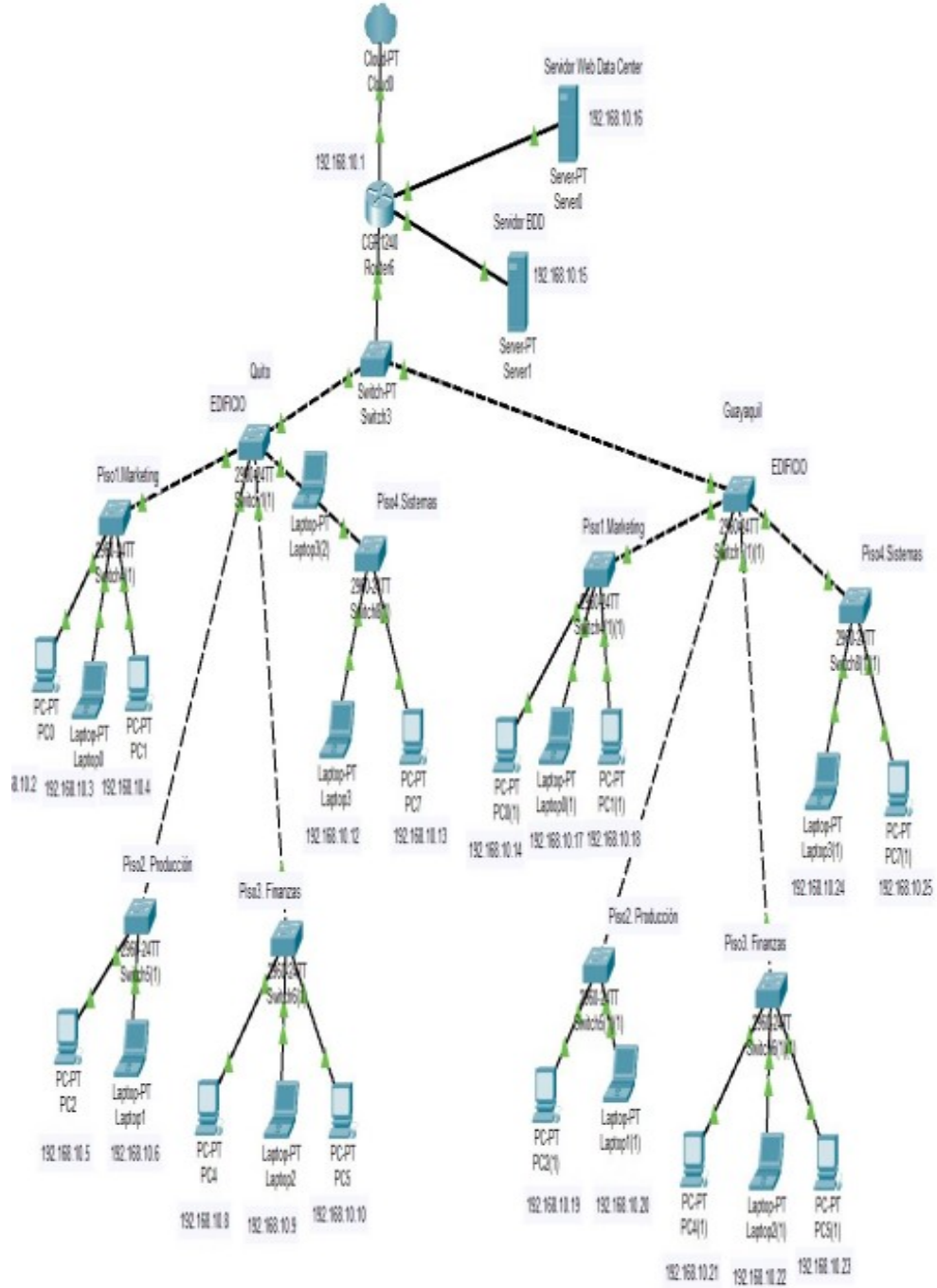

Quito
IP: 192.168.100.0
WAN: 192.168.10.0/24
Guayaquil
IP: 192.168.200.0
Subred .192.168.100.1/24
Subred .192.168.200.1/24
1941
Router3
1941
Router4
Distribucción
Distribucción
Acceso
Acceso
Server-PT
Base de datos
Server-PT
WEB
Server-PT
Base de datos(1)
Server-PT
WEB(1)
Marketing
Producción
Finanzas
Sistemas
Marketing
Producción
Finanzas
Sistemas
PC-PT
PC15
PC-PT
PC16
PC15
PC-PT
PC24
PC-PT
PC23

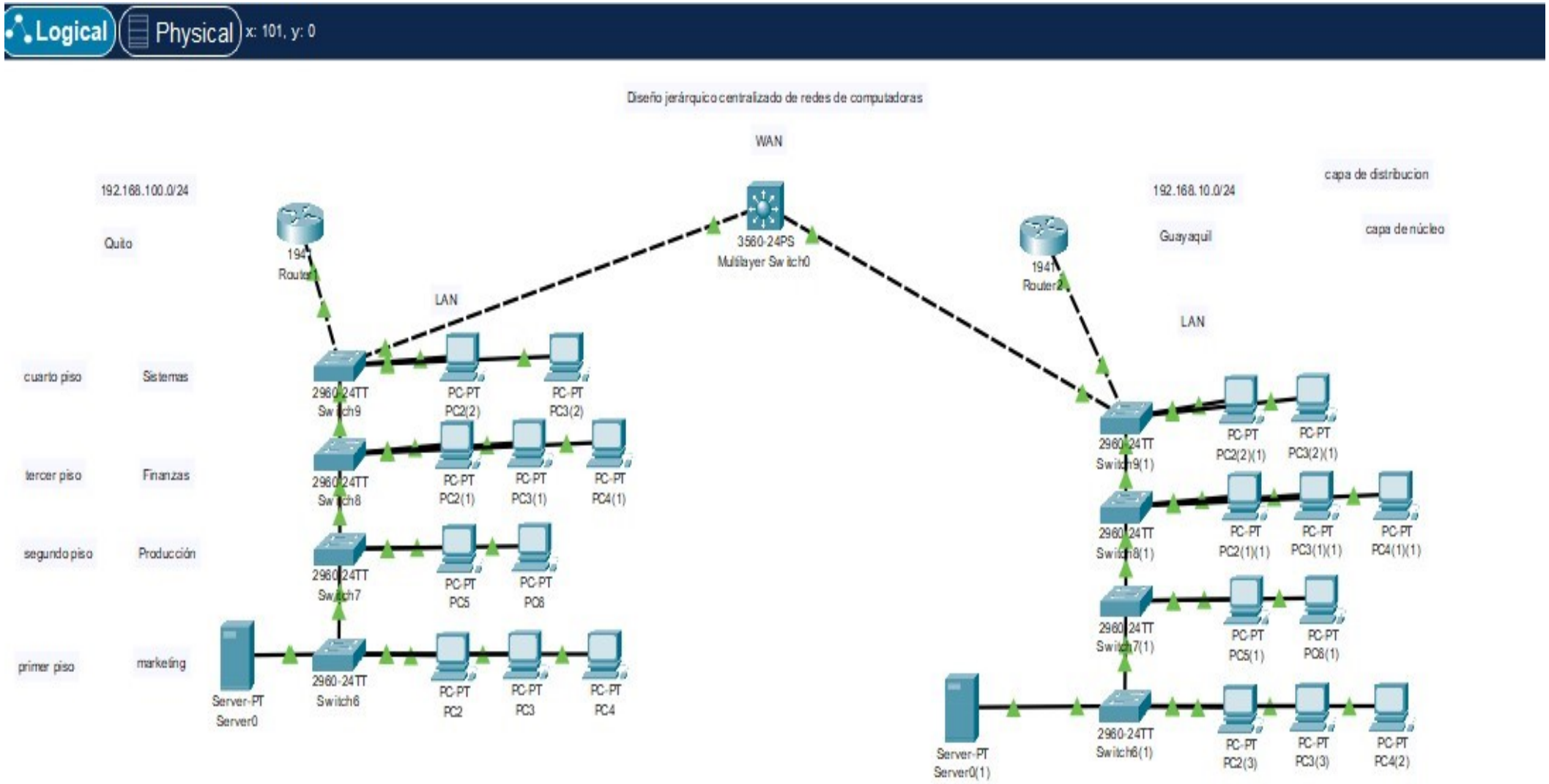

QUITO
IP: 192.168.100.0/24
WAN: 192.168.200.0/24
GUAYAQUIL
IP: 192.168.10.0
IP: 192.168.100.1
1941
QUITO
IP: 192.168.10.1
1941
GUAYAQUIL
Server-PT
Server4
2960-24TT
Switch0
Server-PT
Server5
2960-24TT
Switch1
PRIMER PISO
SEGUNDO PISO
TERCER PISO
CUARTO PISO
2960-24TT
Switch2
2960-24TT
Switch3
2960-24TT
Switch2(1)
2960-24TT
Switch3(1)
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
PC-PT
PC6
PC-PT
PC7
PC-PT
PC8
PC-PT
PC9
MARKETING
PRODUCCIÓN
FINANZAS
SISTEMAS
PRIMER PISO
SEGUNDO PISO
TERCER PISO
CUARTO PISO
2960-24TT
Switch2(2)
2960-24TT
Switch3(2)
2960-24TT
Switch2(1)(1)
2960-24TT
Switch3(1)(1)
PC-PT
PC0.0
PC-PT
PC1.1
PC-PT
PC2.2
PC-PT
PC3.3
PC-PT
PC4.4
PC-PT
PC5.5
PC-PT
PC6.6
PC-PT
PC7.7
PC-PT
PC8.8
PC-PT
PC58.8
MARKETING
PRODUCCIÓN
FINANZAS
SISTEMAS

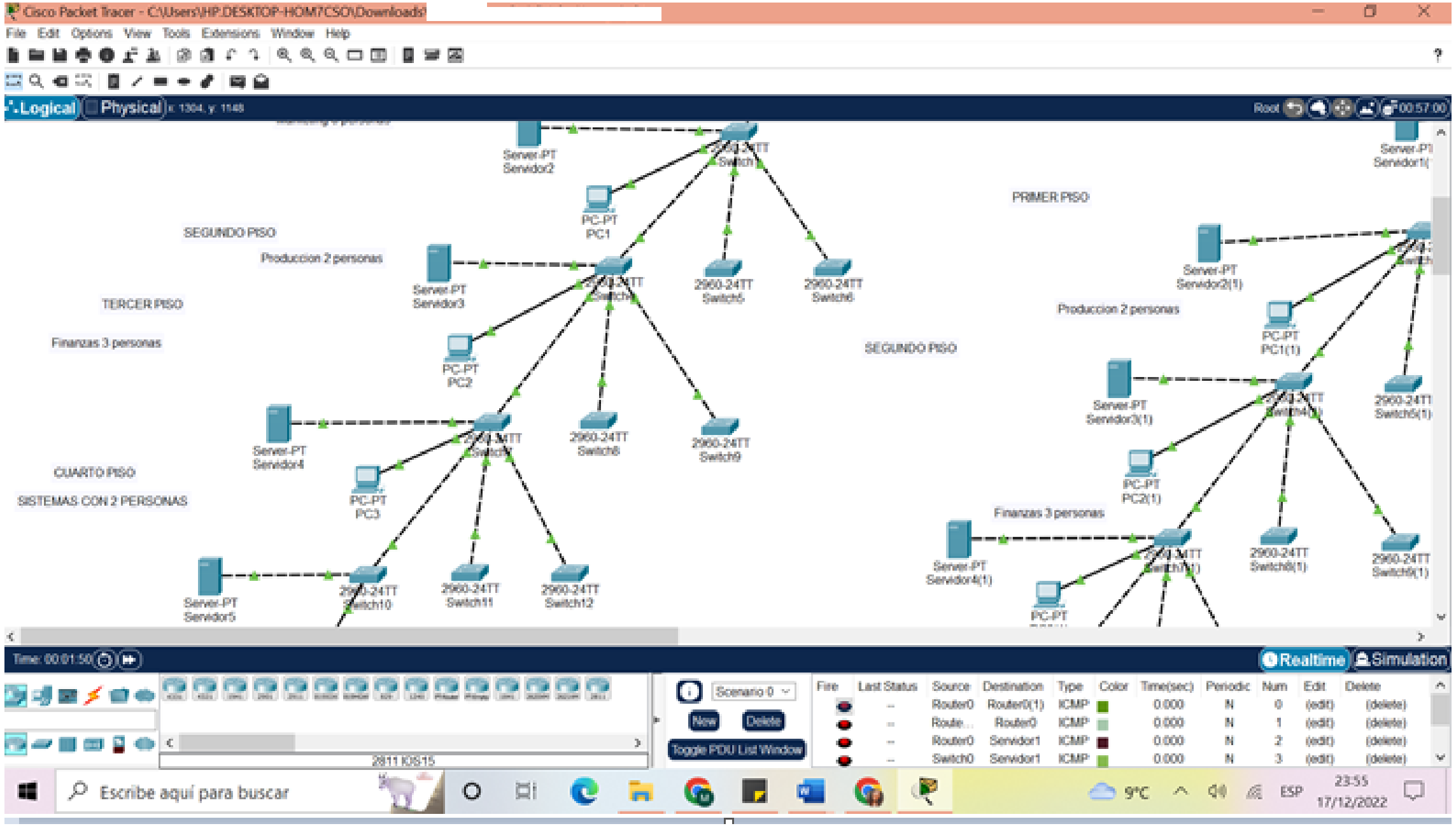


DISEÑO INCORRECTO


Server-PT
Quito
2811
Router3
2950-24
Marketing
2950-24
Producción
PC-PT
P1
PC-PT
P2
PC-PT
P3
PC-PT
PC2
PC-PT
PC1
Server-PT
Guayaquil
1841
Router4
2950-24
Finanzas
2950-24
Sistemas
PC-PT
PC3
PC-PT
PC4
PC-PT
PC6
PC-PT
PC5
PC-PT
PC0


Cloud-PT
Cloud0
192.168.10.1
Servidor Web Data Center
192.168.10.16
Server-PT
Server0
Servidor EDD
192.168.10.15
Server-PT
Server1
Router6
Switch-PT
Switch3
Quito
EDIFICIO
Piso1 Marketing
Piso4 Sistemas
Piso2 Producción
Piso3 Finanzas
Guayaquil
EDIFICIO
Piso1 Marketing
Piso4 Sistemas
Piso2 Producción
Piso3 Finanzas
PC-PT
PC0
Laptop-PT
Laptop0
PC-PT
PC1
192.168.10.4
Laptop-PT
Laptop3(2)
Laptop-PT
Laptop3
192.168.10.12
PC-PT
PC7
192.168.10.13
PC-PT
PC3(1)
192.168.10.14
Laptop-PT
Laptop0(1)
192.168.10.17
PC-PT
PC1(1)
192.168.10.18
Laptop-PT
Laptop3(1)
192.168.10.24
PC-PT
PC7(1)
192.168.10.25
PC-PT
PC2
192.168.10.5
Laptop-PT
Laptop1
192.168.10.6
PC-PT
PC4
192.168.10.9
Laptop-PT
Laptop2
192.168.10.5
PC-PT
PC5
192.168.10.10
PC-PT
PC2(1)
192.168.10.19
Laptop-PT
Laptop1(1)
192.168.10.20
PC-PT
PC4(1)
192.168.10.21
Laptop-PT
Laptop2(1)
192.168.10.22
PC-PT
PC5(1)
192.168.10.23


Logical
Physical
x: 101, y: 0
Diseño jerárquico centralizado de redes de computadoras
WAN
3560-24PS
Multilayer Switch0
192.168.100.0/24
Quito
LAN
cuarto piso
Sistemas
tercer piso
Finanzas
segundo piso
Producción
primer piso
marketing
2960-24TT
Switch9
PC-PT
PC2(2)
PC3(2)
2960-24TT
Switch8
PC-PT
PC2(1)
PC3(1)
PC4(1)
2960-24TT
Switch7
PC5
PC6
Server-PT
Server0
2960-24TT
Switch6
PC2
PC3
PC4
192.168.10.0/24
Guayaquil
capa de distribucion
capa de núcleo
LAN
2960-24TT
Switch9(1)
PC-PT
PC2(2)(1)
PC3(2)(1)
2960-24TT
Switch8(1)
PC-PT
PC2(1)(1)
PC3(1)(1)
PC4(1)(1)
2960-24TT
Switch7(1)
PC5(1)
PC6(1)
Server-PT
Server0(1)
2960-24TT
Switch6(1)
PC-PT
PC2(3)
PC3(3)
PC4(2)


Cisco Packet Tracer - C:\Users\HP.DESKTOP-HOM7CSO\Downloads\
File Edit Options View Tools Extensions Window Help
Logical
Physical
Root
00:57:00
Server-PT Servidor2
2960-24TT Switch
PC-PT PC1
SEGUNDO PISO
Produccion 2 personas
Server-PT Servidor3
2960-24TT Switch5
2960-24TT Switch6
TERCER PISO
Finanzas 3 personas
PC-PT PC2
Server-PT Servidor4
2960-24TT Switch7
2960-24TT Switch8
2960-24TT Switch9
PC-PT PC3
CUARTO PISO
SISTEMAS CON 2 PERSONAS
Server-PT Servidor5
2960-24TT Switch10
2960-24TT Switch11
2960-24TT Switch12
PRIMER PISO
Server-PT Servidor1(
Server-PT Servidor2(1)
Produccion 2 personas
PC-PT PC1(1)
Server-PT Servidor3(1)
2960-24TT Switch5(1)
PC-PT PC2(1)
SEGUNDO PISO
Finanzas 3 personas
Server-PT Servidor4(1)
2960-24TT Switch8(1)
2960-24TT Switch9(1)
PC-PT
Time: 00:01:50
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
2811 IOS15
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Router0
Router0(1)
ICMP
0.000
N
0
(edit)
(delete)
Router0
Servidor1
1
Switch0
2
3
Escribe aquí para buscar
9°C
ESP
23:55
17/12/2022

Protocolos de Redes Ethernet.

Funcionamiento de Ethernet

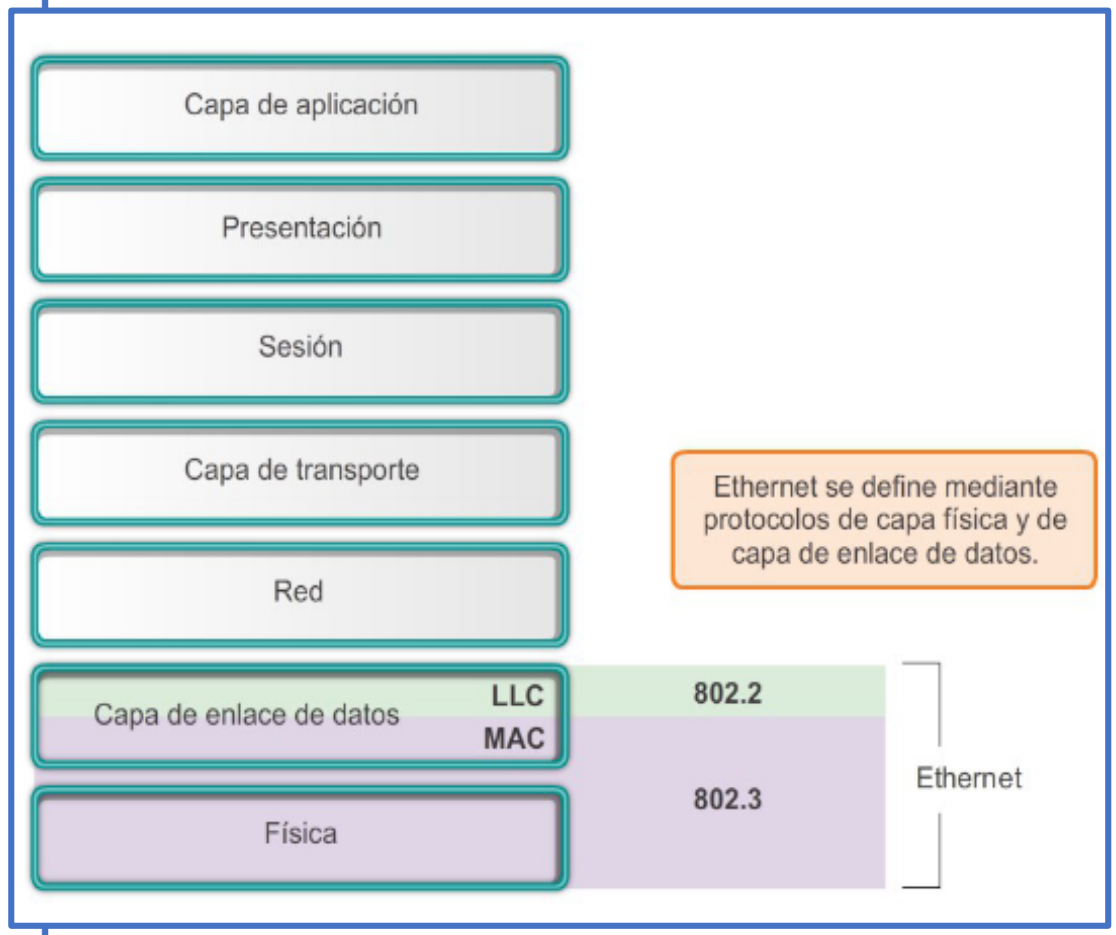
Subcapas LLC y MAC

Ethernet:

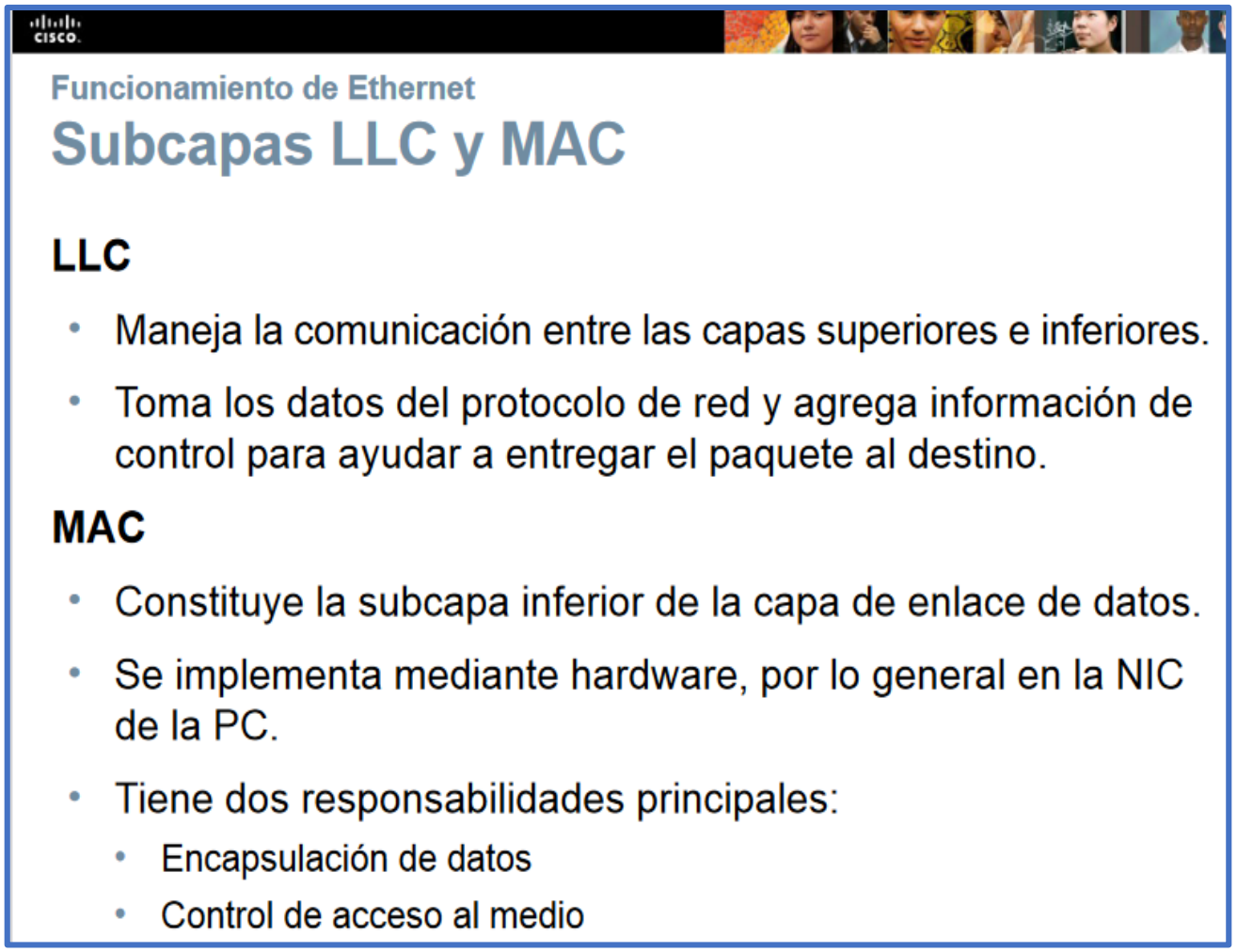
- Tecnología LAN más utilizada.
- Opera en la capa de enlace de datos y en la capa física.
- Familia de tecnologías de redes que se define en los estándares IEEE 802.2 y 802.3.
- Admite anchos de banda de datos de 10, 100, 1000, 10 000, 40 000 y 100 000 Mbps (100 Gbps).

Estándares de Ethernet:

- Definen los protocolos de capa 2 y las tecnologías de capa 1.
- Operan en dos subcapas separadas de la capa de enlace de datos: la de control de enlace lógico (LLC) y la MAC.



Protocolos de Redes Ethernet.



Funcionamiento de Ethernet

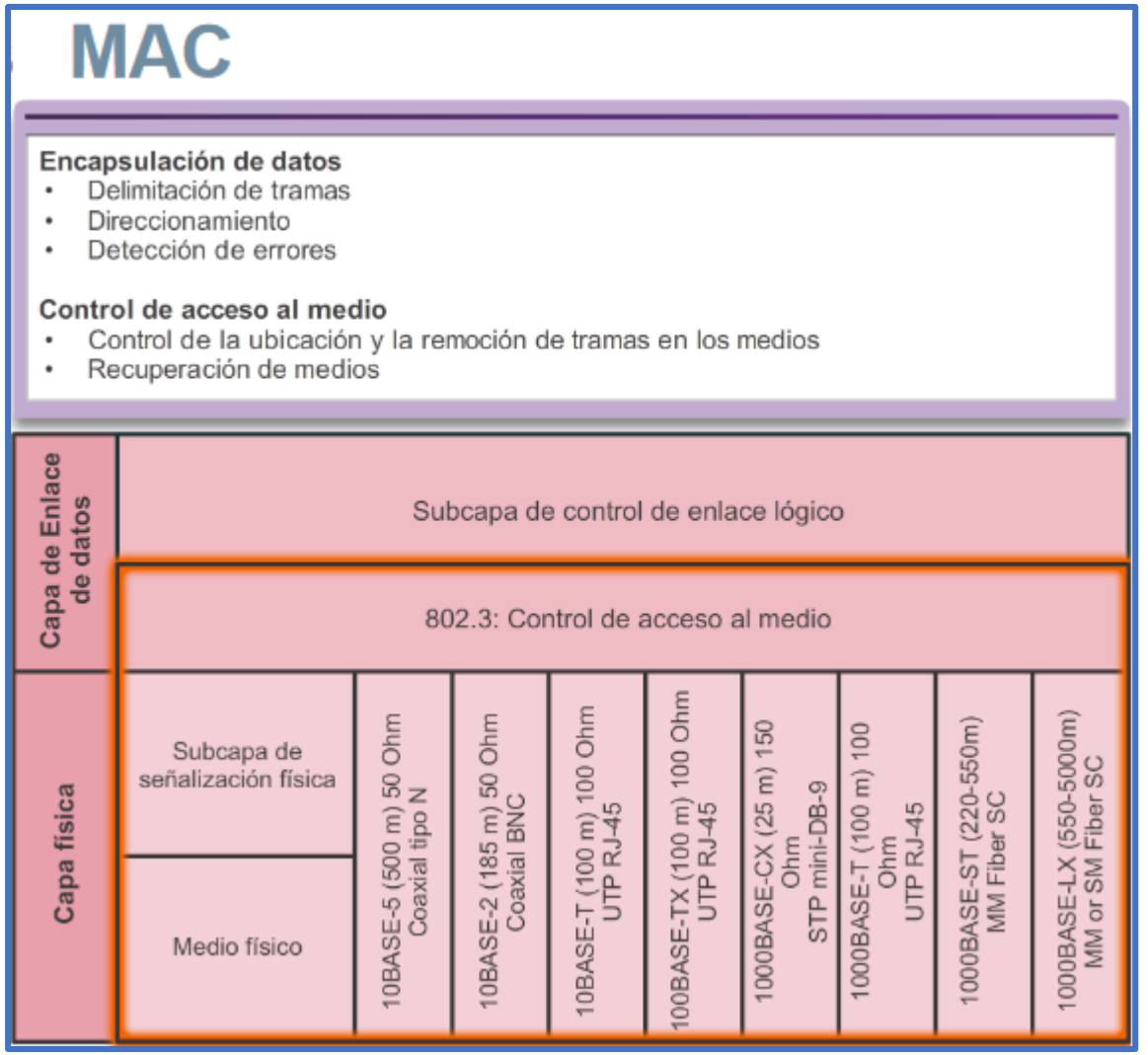
Subcapas LLC y MAC

LLC

- Maneja la comunicación entre las capas superiores e inferiores.
- Toma los datos del protocolo de red y agrega información de control para ayudar a entregar el paquete al destino.

MAC

- Constituye la subcapa inferior de la capa de enlace de datos.
- Se implementa mediante hardware, por lo general en la NIC de la PC.
- Tiene dos responsabilidades principales:
  - Encapsulación de datos
  - Control de acceso al medio



Protocolos de Redes Ethernet

Funcionamiento de Ethernet

Subcapa MAC

Encapsulación de datos

- Armado de la trama antes de la transmisión y desarmado de la trama en el momento en que se la recibe.
- La capa MAC agrega un encabezado y un tráiler a la PDU de la capa de red.

Proporciona tres funciones principales:

- Delimitación de tramas: identifica un grupo de bits que componen una trama; sincronización entre los nodos emisor y receptor.
- Direccionamiento: cada encabezado Ethernet que se agrega a la trama contiene la dirección física (dirección MAC) que permite que la trama se entregue a un nodo de destino.
- Detección de errores: cada trama de Ethernet contiene un tráiler con una comprobación de redundancia cíclica (CRC) del contenido de la trama.

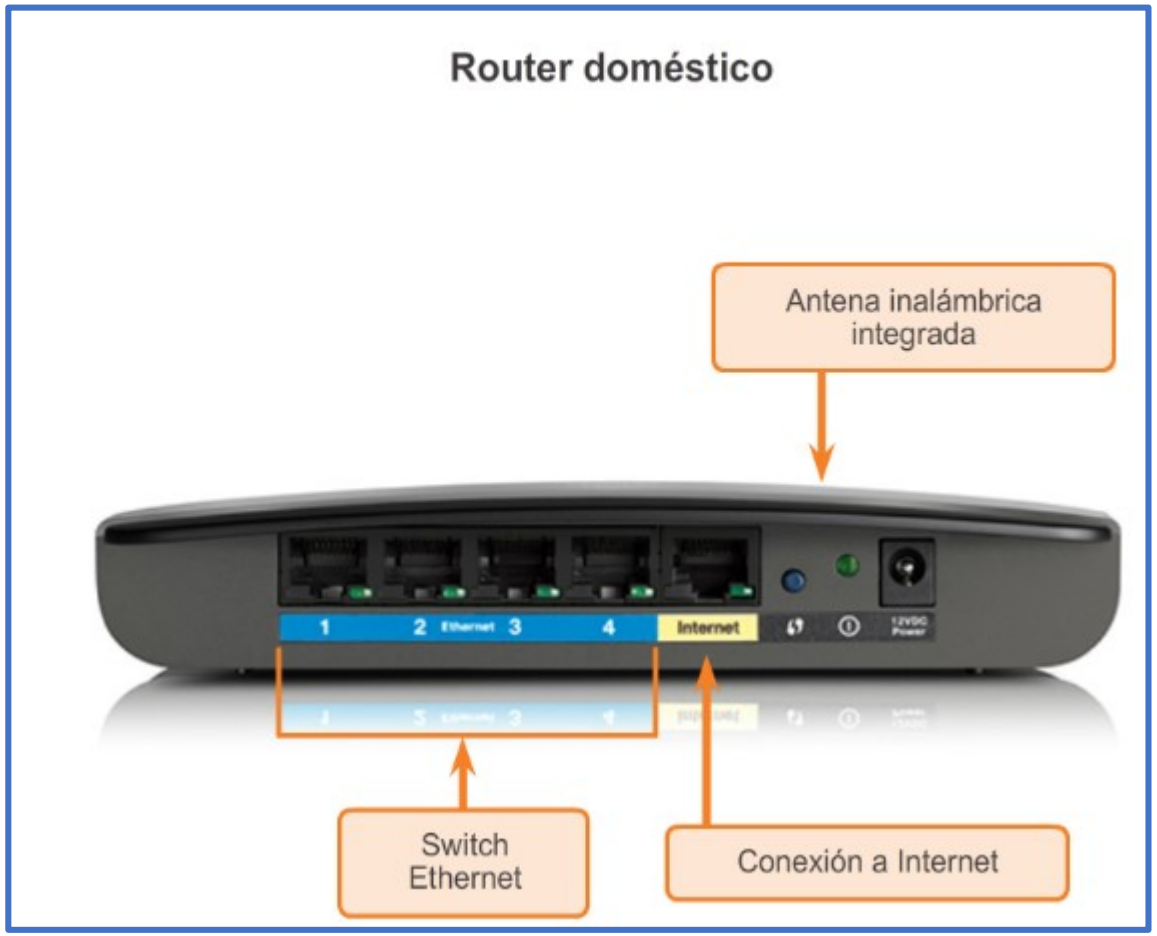
Funcionamiento de Ethernet

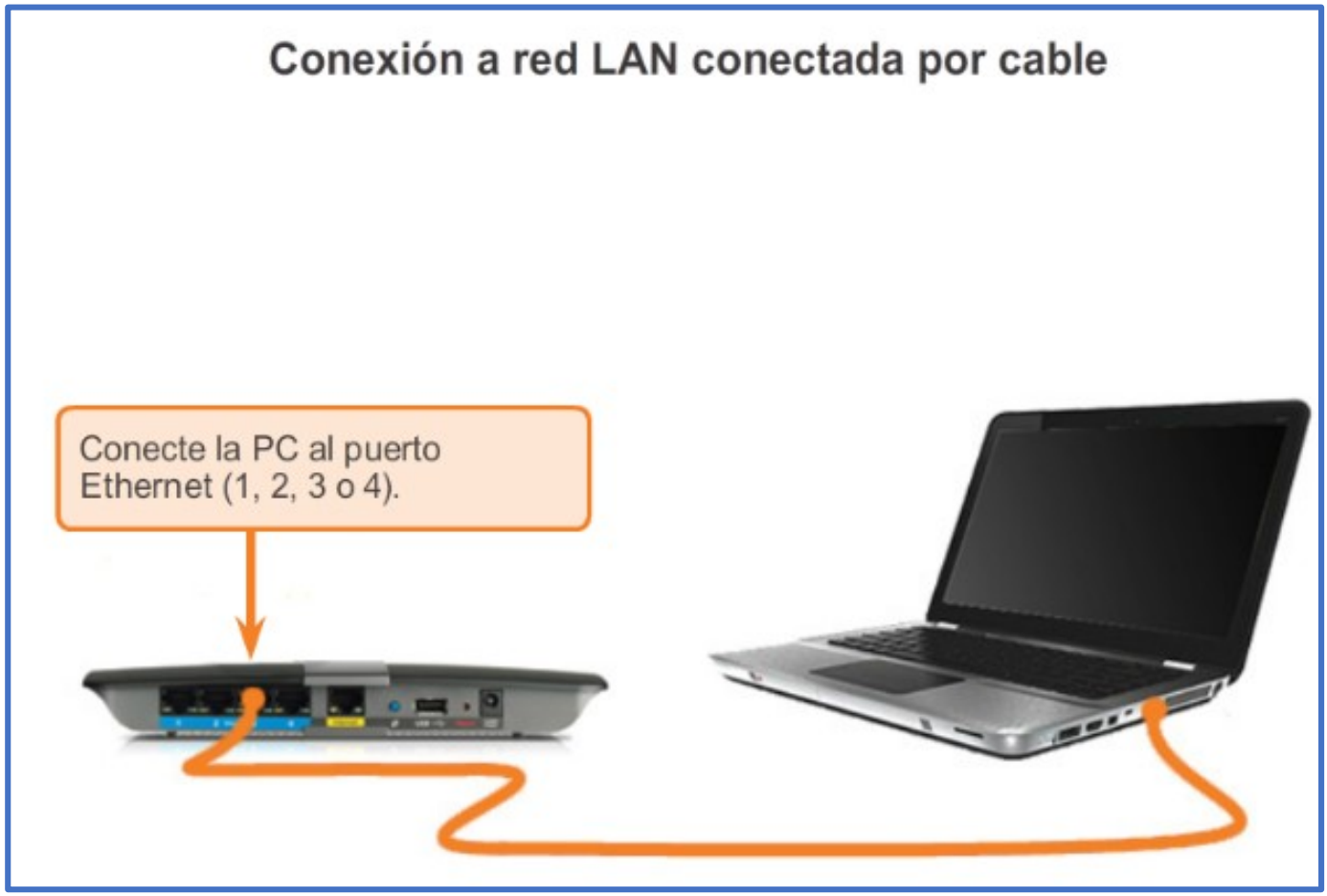
Subcapa MAC

Control de acceso al medio

- Responsable de la ubicación y la remoción de tramas en los medios.
- Se comunica directamente con la capa física.
- Si hay varios dispositivos en un único medio que intentan reenviar datos simultáneamente, los datos colisionan, lo que provoca que estos se dañen y no se puedan utilizar.
- Ethernet proporciona un método para controlar la forma en que los nodos comparten el acceso mediante el uso de una tecnología de acceso múltiple por detección de portadora (CSMA).

Protocolos de Redes Ethernet

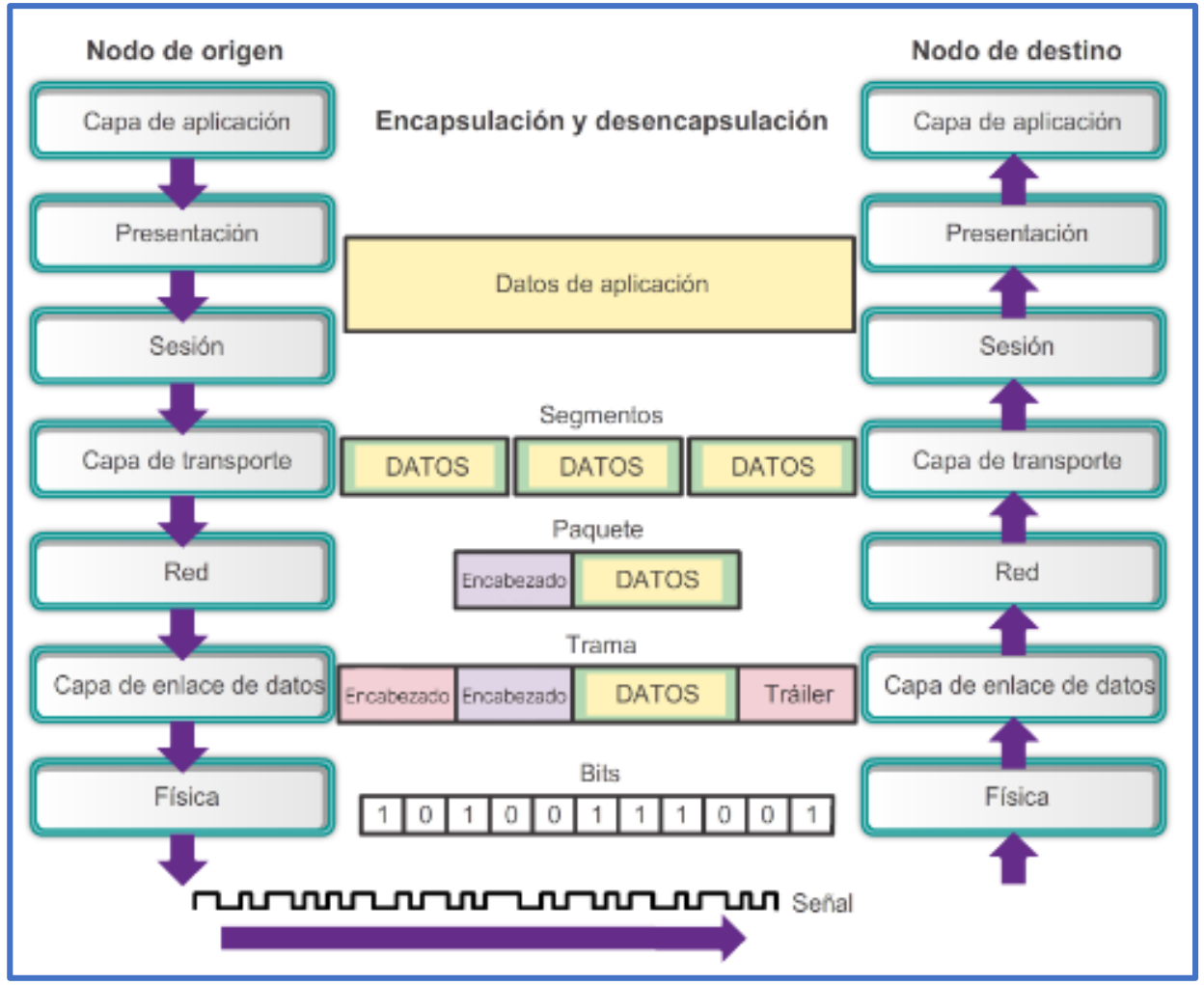




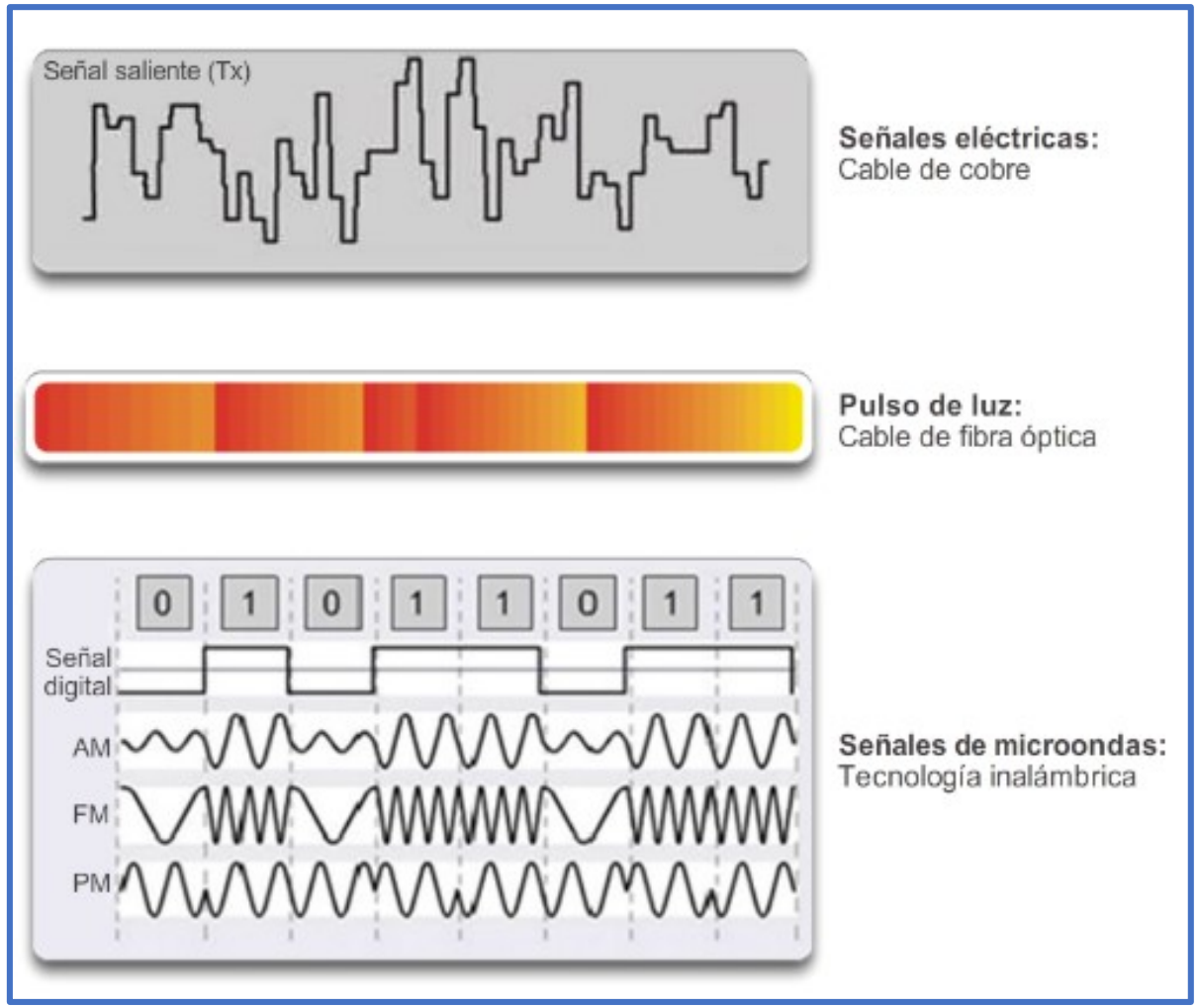
Protocolos de Redes Ethernet

Propósito de la capa física

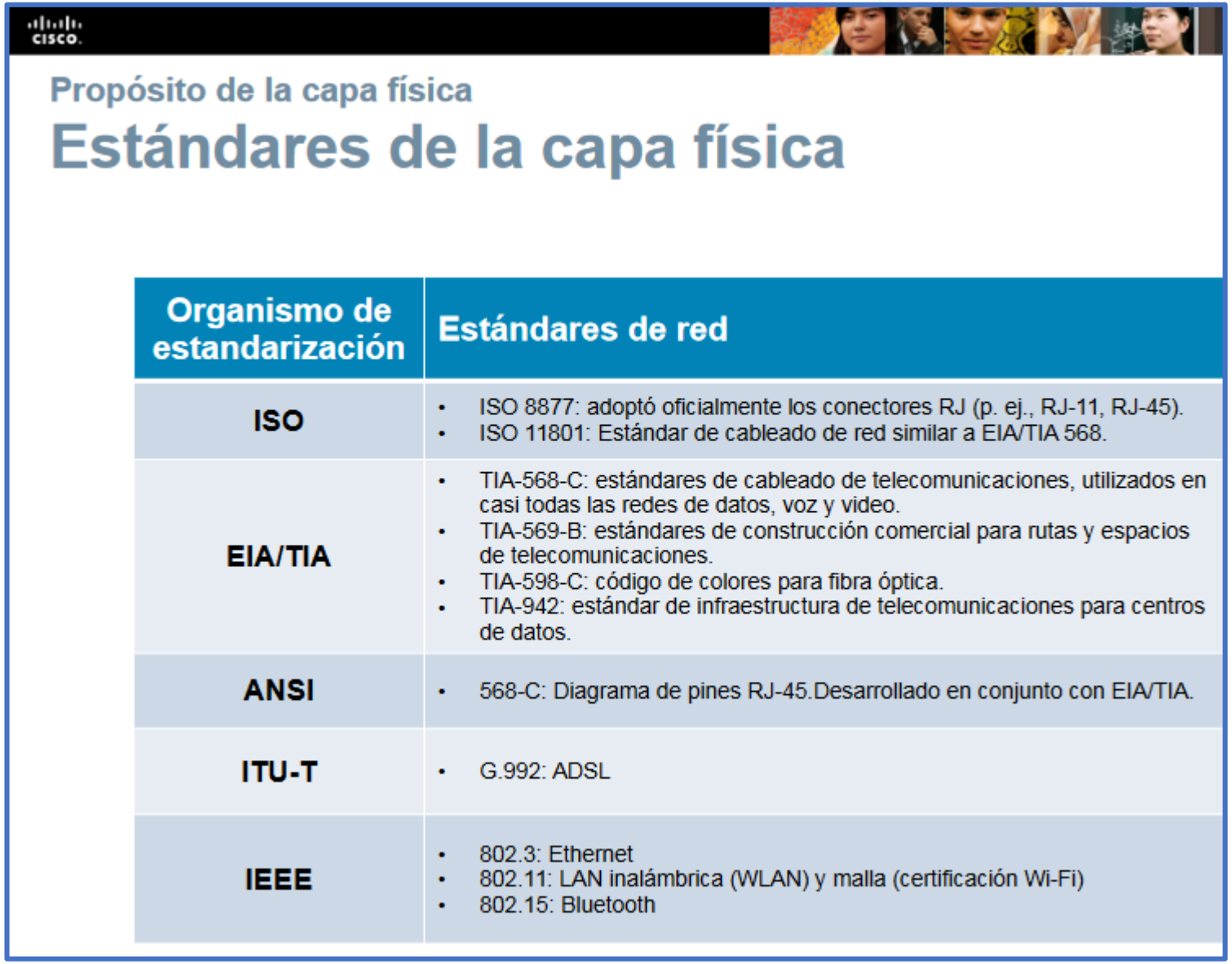
Capa física



Medios de la capa física



Protocolos de Redes Ethernet



Asymmetric digital subscriber line (ADSL) is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voiceband modem can provide.

Stands for the "Institute of Electrical and Electronics Engineers" and is produced "I triple E." The **IEEE** is a professional association that develops, defines, and reviews electronics and computer science **standards**

Velocidad de transmisión y performance

Transmission speed is the rate at which data packets cross a computer network from one server to another.

Transmission speed is typically measured in megabits per second (Mbps), which equals one million bits per second, although gigabit and even terabit **speeds** are becoming common.

Unidad de ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1bps=unidad fundamental de ancho de banda
Kilobits por segundo	kbps	1kbps=1000bps = 10^3bps
Megabits per second, megabits por segundo	Mbps	1Mbps =1000000bps=10^6bps
Gigabits per second, gigabits por segundo	Gbps	1Gbps=1000000000bps=10^9bps
Terabits per second, terabits por segundo	Tbps	1Tbps=1000000000000bps=10^12bps

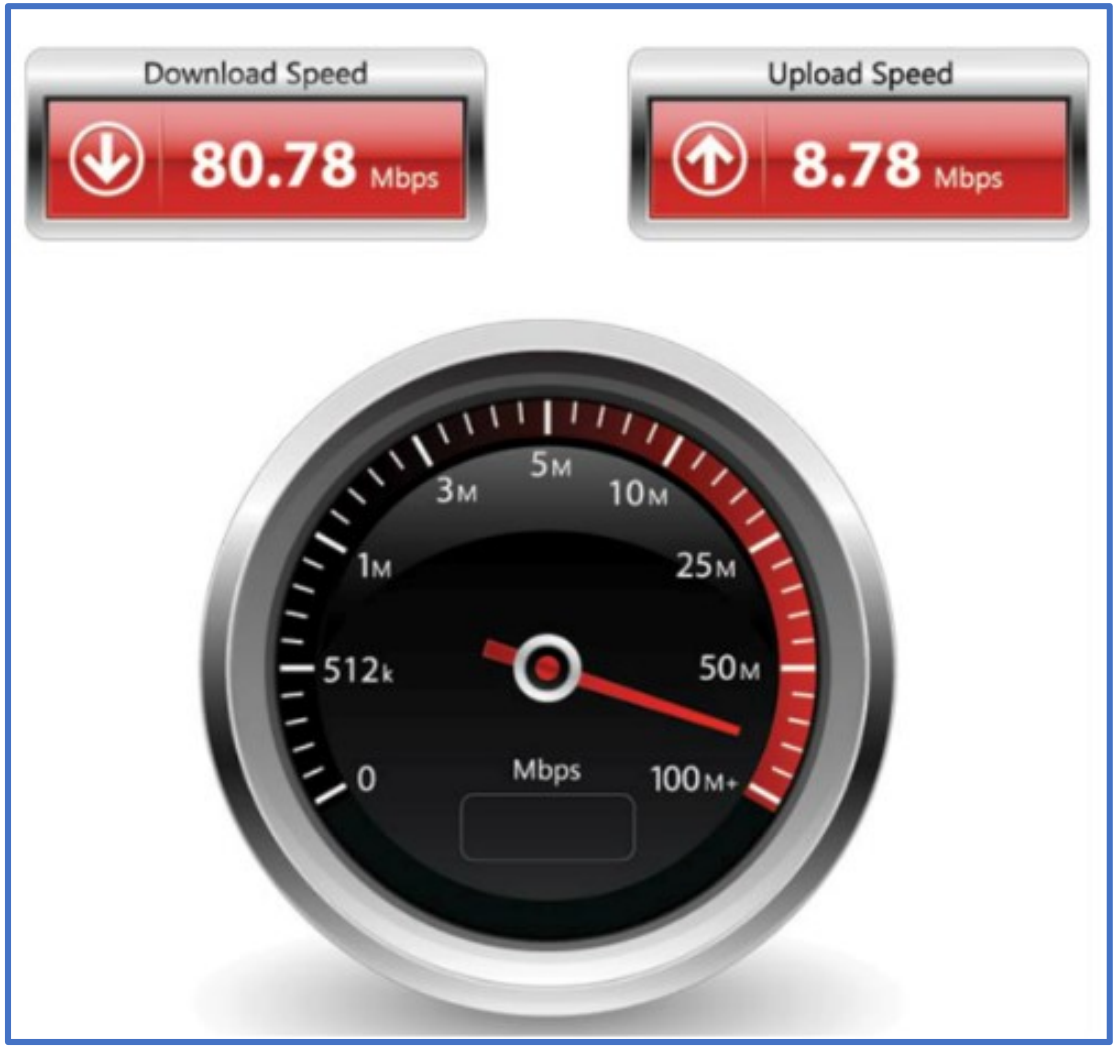
Bandwidth: It is a range of frequencies within a given band, in particular that used for transmitting a signal.

Velocidad de transmisión y performance

PERFORMANCE OF THE NET.

The **download speed** is how fast you can pull data from the server to you. Most connections are designed to download much faster than they upload, since the majority of online activity, like loading web pages or streaming videos, consists of downloads. Download speed is measured in megabits per second (Mbps).

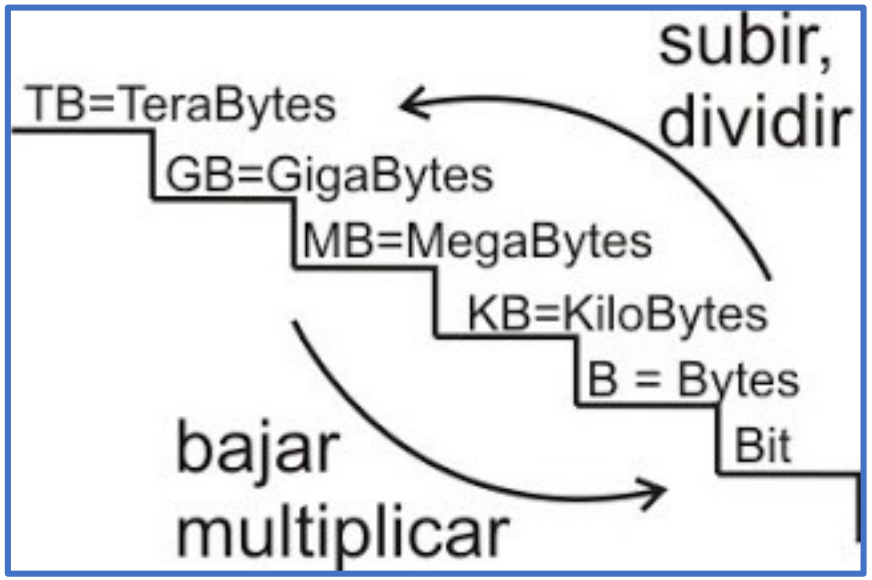
The **upload speed** is how fast you send data from you to others. Uploading is necessary for sending big files via email, or in using video-chat to talk to someone else online (since you have to send your video feed to them). Upload speed is measured in megabits per second (Mbps).



Velocidad de transmisión y performance

Unidad básica de medida de la memoria y almacenamiento

Medida	Simbologia	Equivalencia
byte	b	8 bits
kilobyte	Kb	1024 bytes
megabyte	MB	1024 KB
gigabyte	GB	1024 MB
terabyte	TB	1024 GB
Petabyte	PB	1024 TB
Exabyte	EB	1024 PB
Zetabyte	ZB	1024 EB
Yottabyte	YB	1024 ZB
Brontobyte	BB	1024 YB
Geopbyte	GB	1024 BB



Velocidad de transmisión y performance

VELOCIDAD DE TRANSMISIÓN:
Cantidad de bits transmitidos en una unidad de tiempo.
Ejemplos: 9600 bps, 64 Kbps, 2 Mbps, etc.
Depende del esquema de codificación o modulación.

Ley de Hartly-Shannon: máxima velocidad de transmisión de un canal en presencia de ruido térmico o blanco es:

$$C = W * Lg_2(1 + S/N)$$

S= Potencia de la señal transmitida.
N=Potencia del Ruido.

Ej: En el sistema telefónico convencional se maneja una relación de ruido de 30dB que equivalen a un S/N=1000/1.
Por tanto
$C = 3100 * Lg_2(1 + 1000) = 30.894$ bps.

- **What is a Megabit per second (Mbps)?**
  - A Megabit per second is a unit used to measure data transfer rates and is based on "Decimal multiples of bits". The symbol for Megabit per second is Mbps or Mb/s or Mbit/s. There are 8 Megabits per second in a Megabyte per second.
- **What is a Megabyte per second (MBps)?**
  - A Megabyte per second is a unit used to measure data transfer rates and is based on "Decimal multiples of bits". The symbol for Megabyte per second is MBps or MB/s. There are 0.125 Megabytes per second in a Megabit per second.

Velocidad de transmisión y performance

Ejercicios:

¿Cuantos Kbps representan 7Mbps?

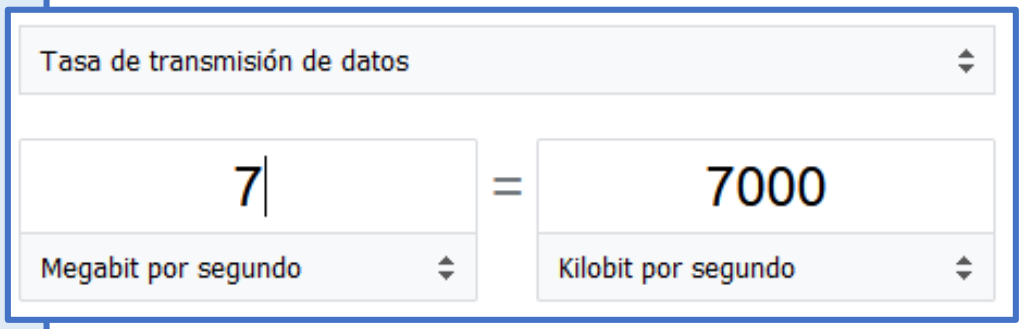
Si 1 Mpbs=1000 Kbps

7 ~~Mpbs~~ *1000 Kbps

\-------

1.0 ~~Mbps~~

R=7000Kbps



¿En un enlace de 10 Gbps, calcular en KBps?

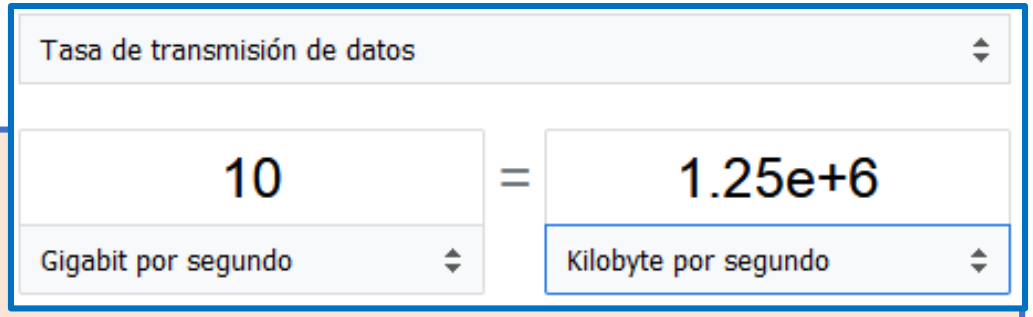
Si 1 Gpbs=1000 Mbps

10 ~~Gbps~~ *1000 ~~Mbps~~*1000 ~~Kbps~~ 1 KBps

\------- ------- * -------

1.0 ~~Gbps~~ 1.0~~Mbps~~ 8 ~~kbps~~

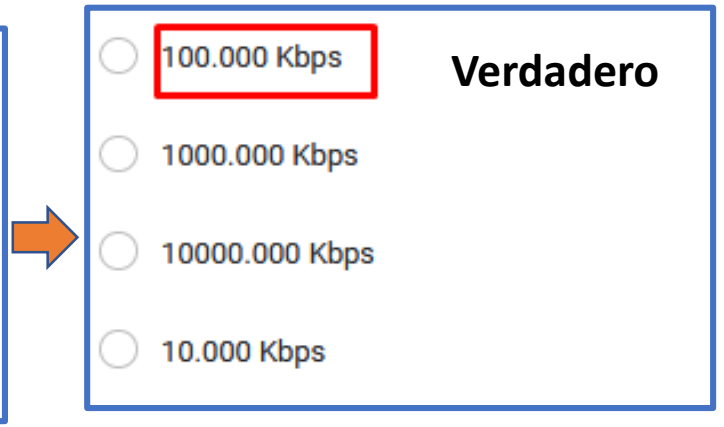
R=1.250000 **KB**ps



Velocidad de transmisión y performance

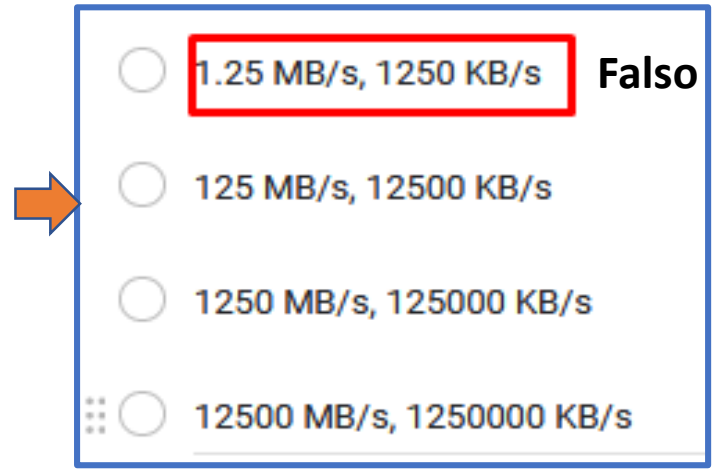
Ejercicio 3:

- Usted dispone de una conexión 100BASET4 a 100 Mbps. Realice la conversión necesaria para conocer: La capacidad de transmisión en Kbps?



Ejercicio 4:

- Usted dispone de una conexión IEEE 802.3ae. Realice la conversión necesaria para conocer La capacidad de transmisión en MBps y en Kbps.



Velocidad de transmisión y performance

Desarrollo:

¿Cuantos Kbps representan 100 Mbps?

Si 1 Mpbs=1000 Kbps

100 ~~Mpbs~~ *1000 Kbps

\-------

1.0 ~~Mbps~~

R=100.000 Kbps

¿En un enlace de 10 Gbps, calcular en MBps y Kbps?

Si 1 Gpbs=1000 Mbps

10 ~~Gbps~~ *1000 ~~Mbps~~*1000 ~~Kbps~~

\-------

1.0 ~~Gbps~~

\-------

1.0~~Mbps~~

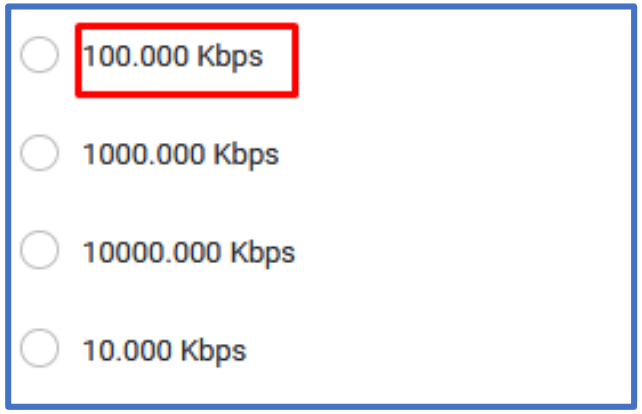
*

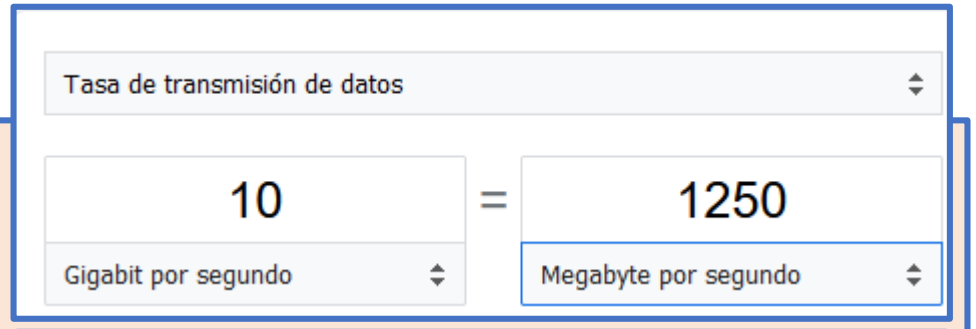
1 MBps

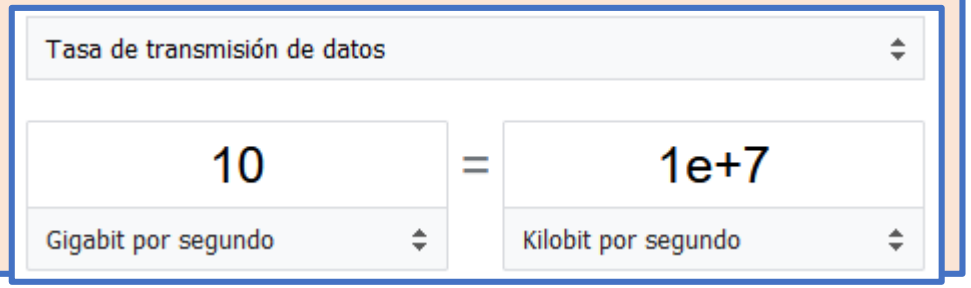
\-------

8000 ~~kbps~~

Verificación







Velocidad de transmisión y performance

❑Ejercicio 5

Se dispone de un video de 700 MB de almacenamiento. ¿Que tiempo se tarda en descargarlo si el enlace dispone de 4 Mbps?

Desarrollo:

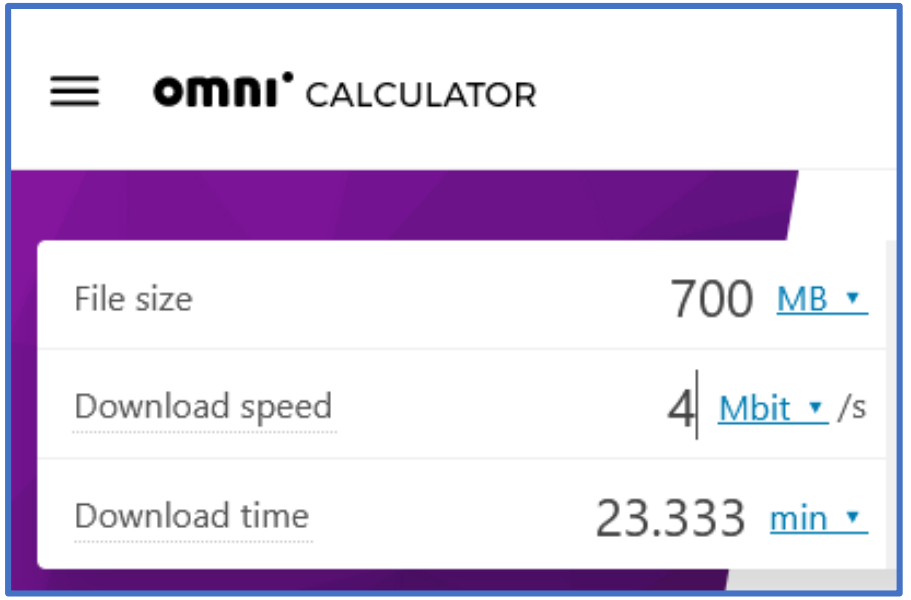
Se tienen 700 MB

Si 1 MB=8 Mb

$$\frac{700\ \cancel{MB} * 8\ \cancel{Mb}}{1.0\ \cancel{MB}} * \frac{1\ seg}{4\ \cancel{Mb}} = \frac{5600\ seg}{4} = 1400\ seg/60 = 23{,}33\ min$$

Verificación

URL:
https://www.omnicalculator.com/other/download-time



Velocidad de transmisión y performance

❑Ejercicio 6

Se dispone de información en un HDD de 7 GB de almacenamiento. ¿Que tiempo se tarda en descargarlo si el enlace que dispone es de 8 Mbps?

Desarrollo:

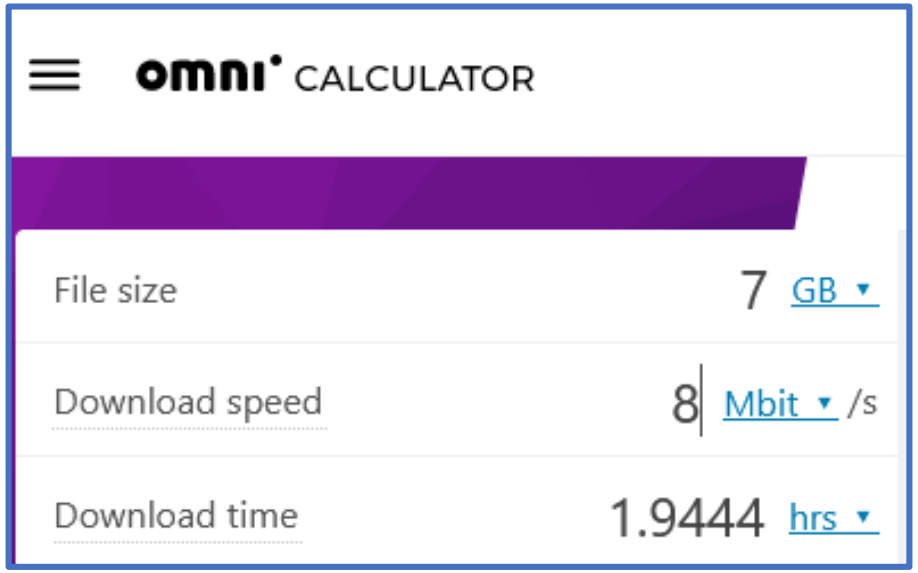
Se tienen 7 GB

Si 1 GB=1024 MB; 1 MB=8Mb

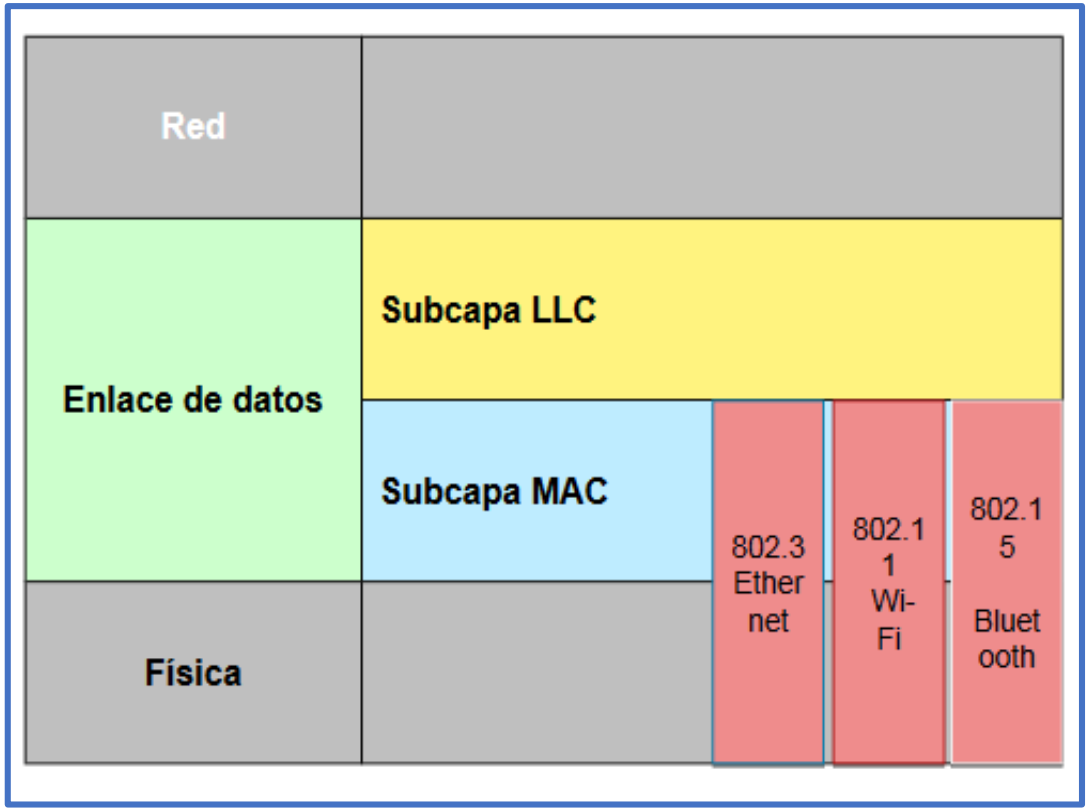
$$7\ \cancel{GB} \times \frac{1024\ \cancel{MB}}{1.0\ \cancel{GB}} \times \frac{8\ \cancel{Mb}}{1\ \cancel{MB}} \times \frac{1\ s}{8\ \cancel{Mb}} = \frac{57344\ s}{8} = \frac{7168}{3600} = 1.99 \text{ horas}$$

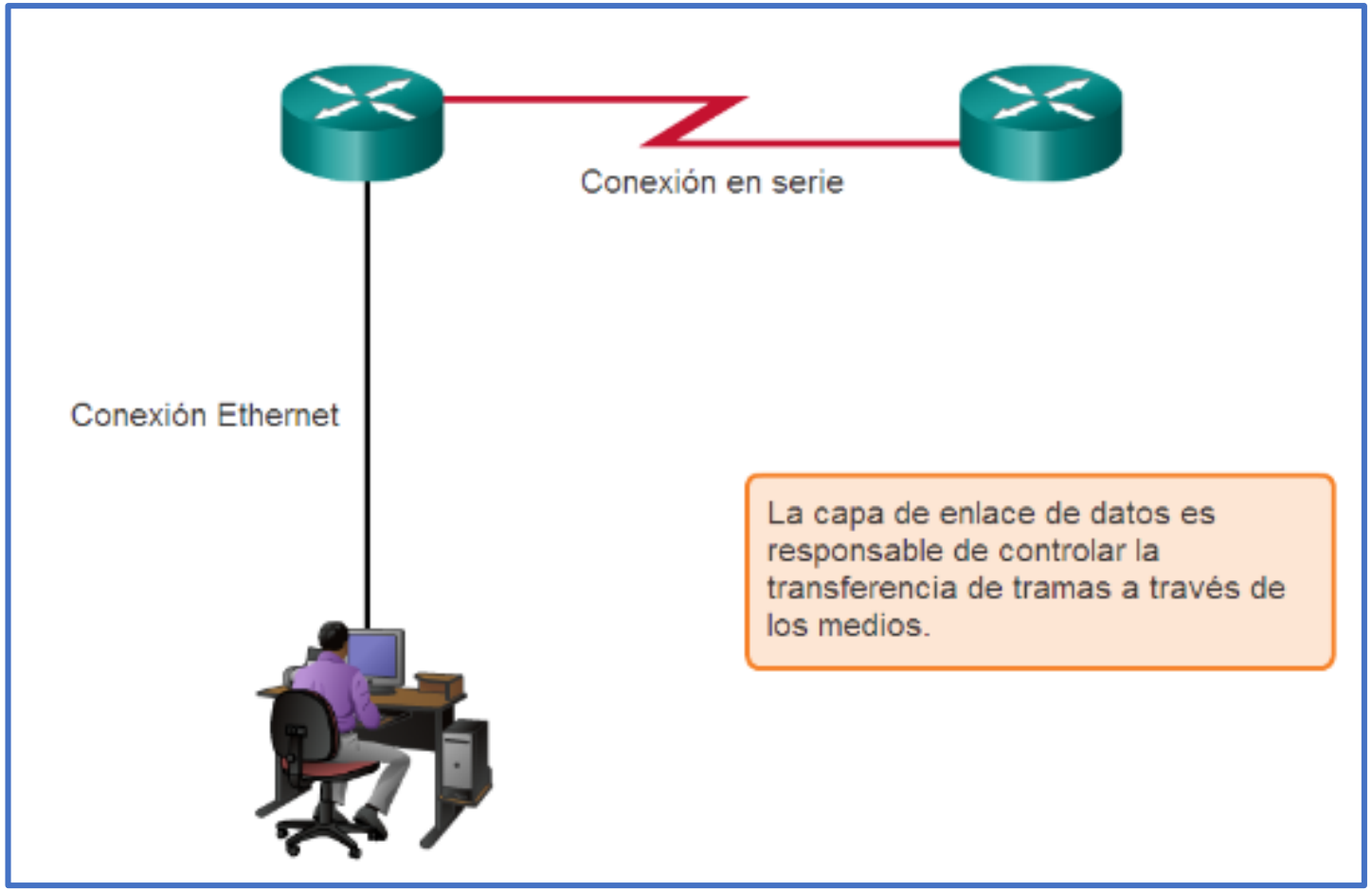
Verificación

URL:
https://www.omnicalculator.com/other/download-time

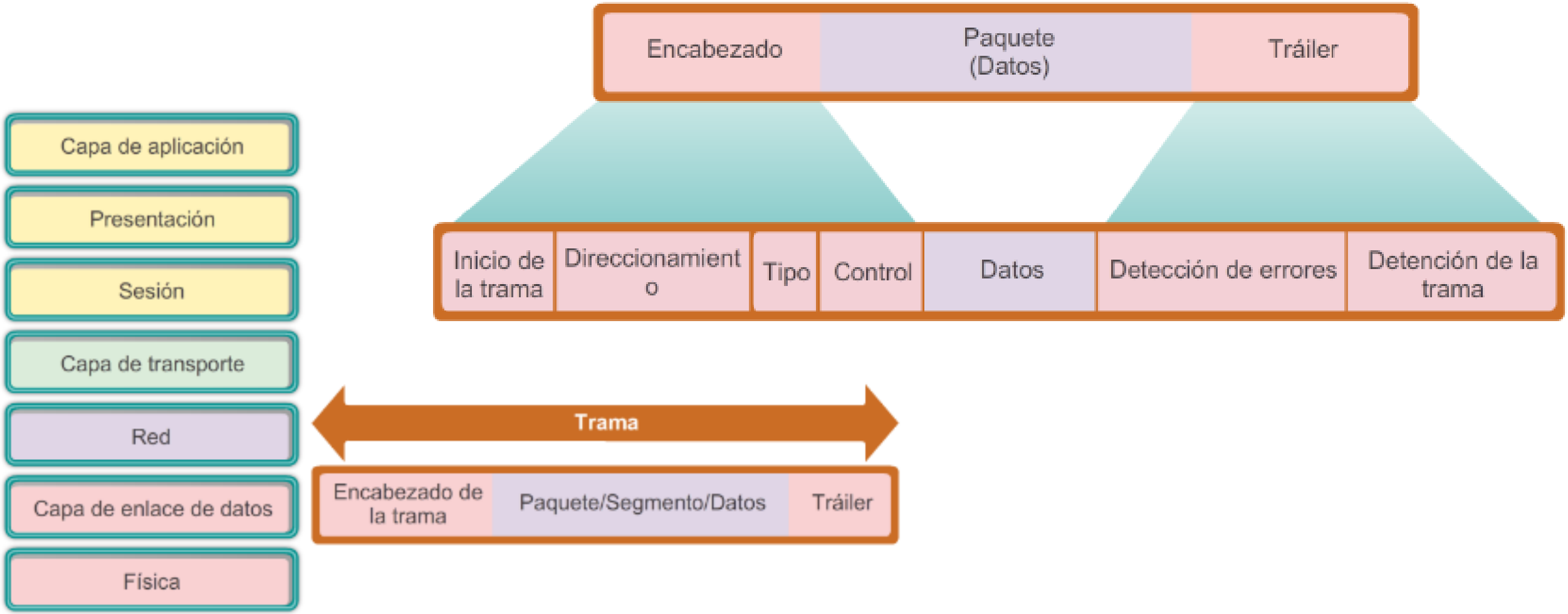


Protocolos de Redes Ethernet

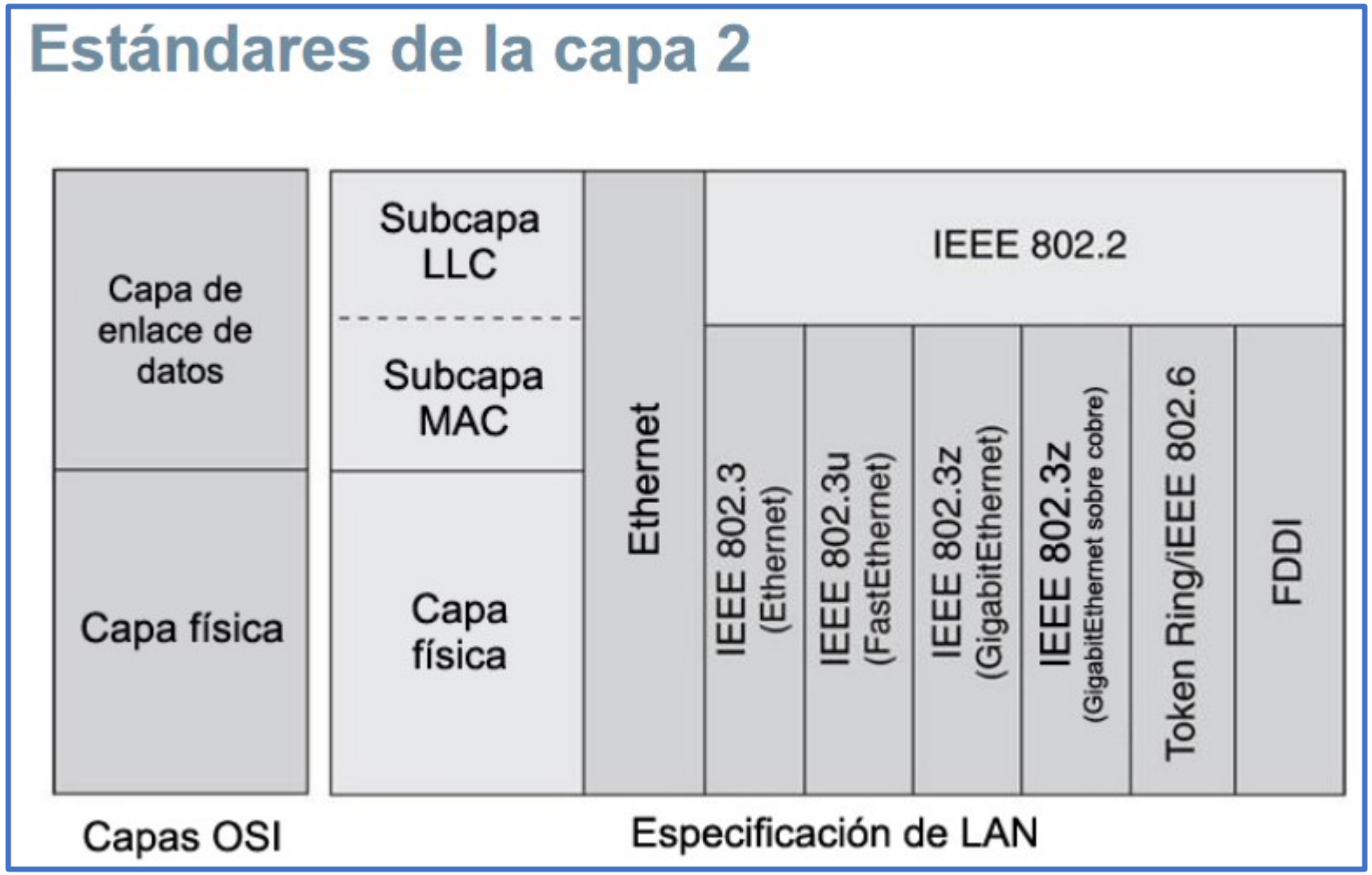




Protocolos de Redes Ethernet



Protocolos de Redes Ethernet

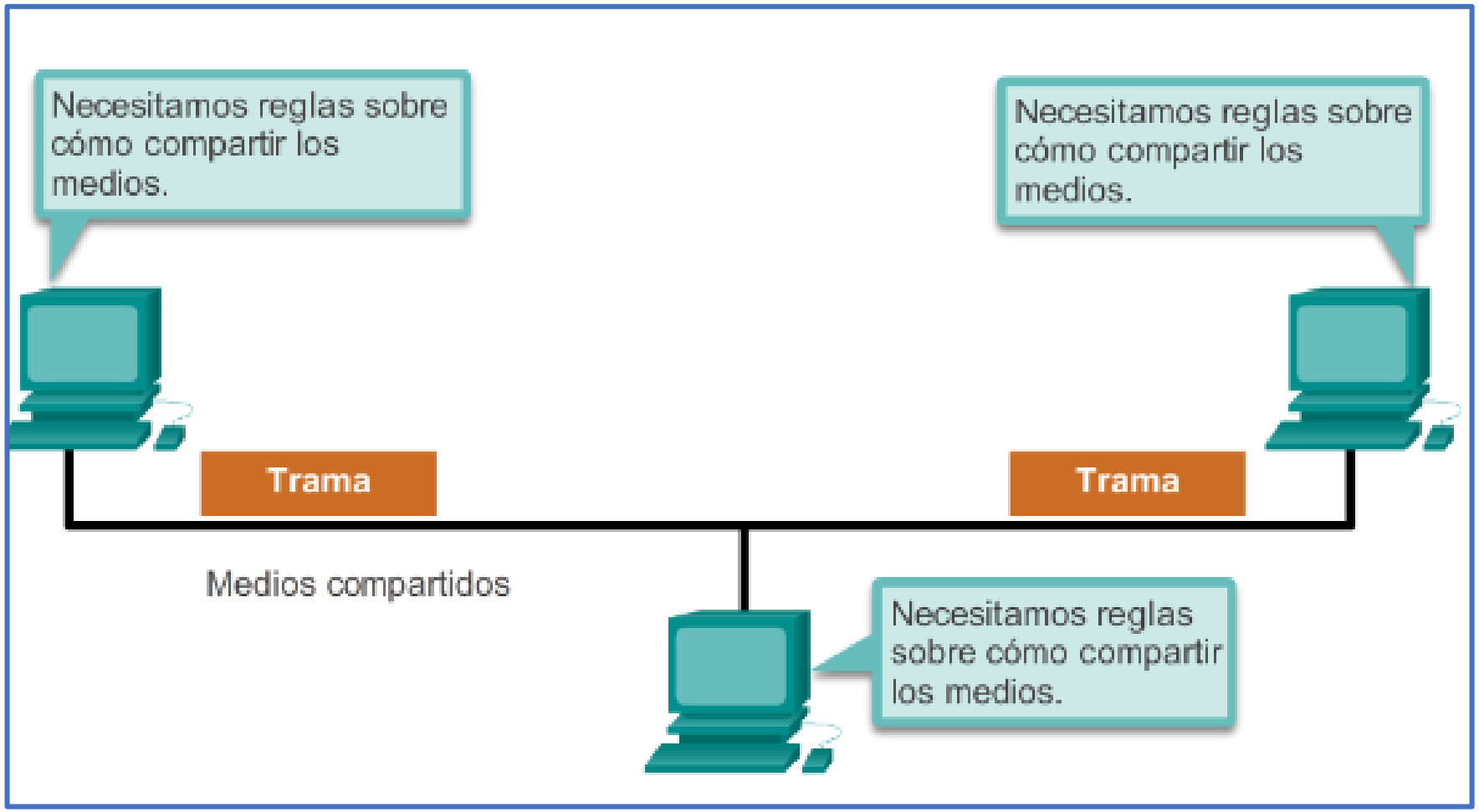


IEEE 802.2 is the original name of the ISO/IEC 8802-2 standard which defines logical link control (LLC) as the upper portion of the data link layer of the OSI Model.

The original standard developed by IEEE in collaboration with the ANSI was adopted by the International Organization for Standardization (ISO) in 1998, but it still remains an integral part of the family of IEEE 802 standards for local and metropolitan networks.

Protocolos de Redes Ethernet

Control de acceso a los medios

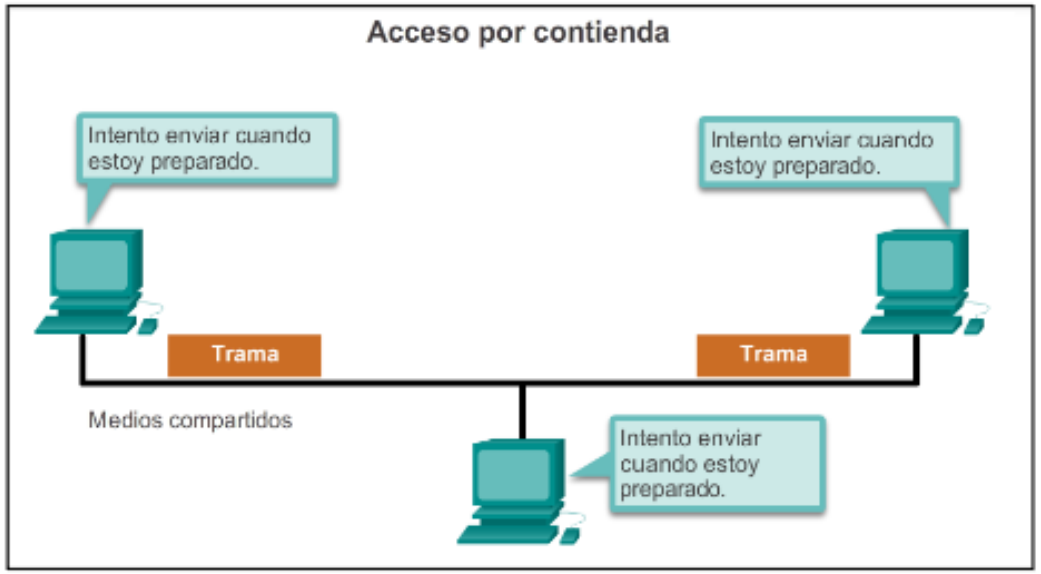


A **media access control** is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable. The media access control policy involves sub-layers of the data link layer 2 in the OSI reference model.

The essence of the **MAC** protocol is to ensure non-collision and eases the transfer of data packets between two computer terminals. A collision takes place when two or more terminals transmit data/information simultaneously. This leads to a breakdown of communication, which can prove costly for organizations that lean heavily on data transmission.

Protocolos de Redes Ethernet

Acceso por contienda



Características	Tecnologías de contienda
• Las estaciones pueden transmitir en cualquier momento. • Existe colisión. • Existen mecanismos para resolver la contienda por los medios.	• CSMA/CD para redes Ethernet 802.3 • CSMA/CA para redes inalámbricas 802.11

Carrier-sense multiple access with collision detection (CSMA/CD) is a media access control (MAC) method used most notably in early Ethernet technology for local area networking. It uses carrier-sensing to defer transmissions until no other stations are transmitting.

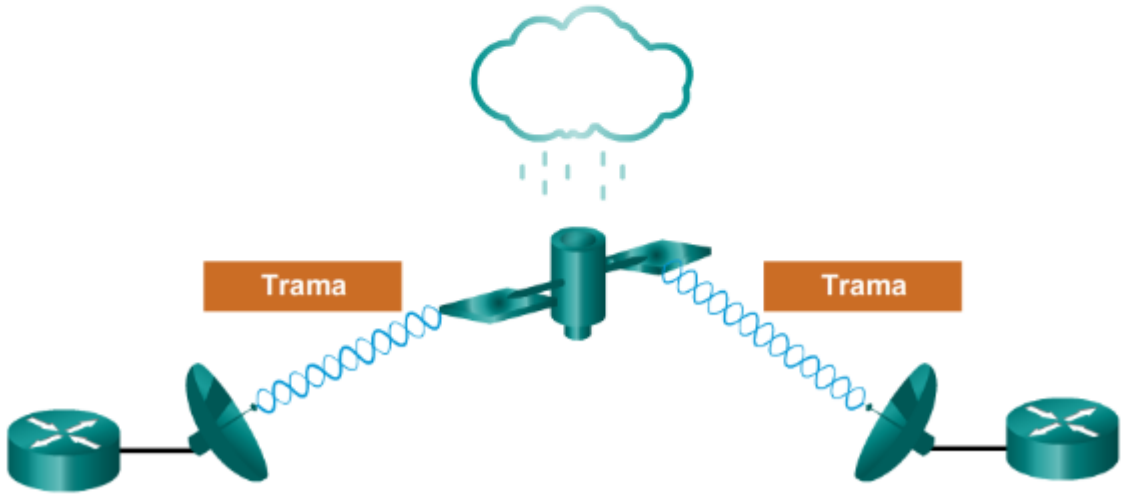
This is used in combination with collision detection in which a transmitting station detects collisions by sensing transmissions from other stations while it is transmitting a frame. When this collision condition is detected, the station stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame.

Protocolos de Redes Ethernet

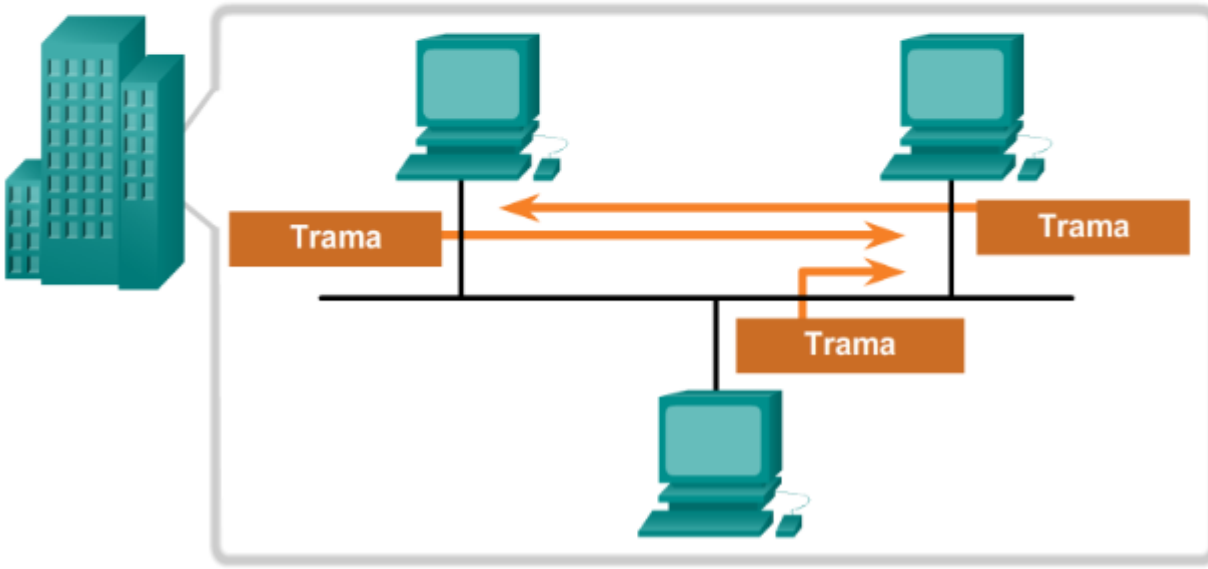
Trama de enlace de datos

La trama

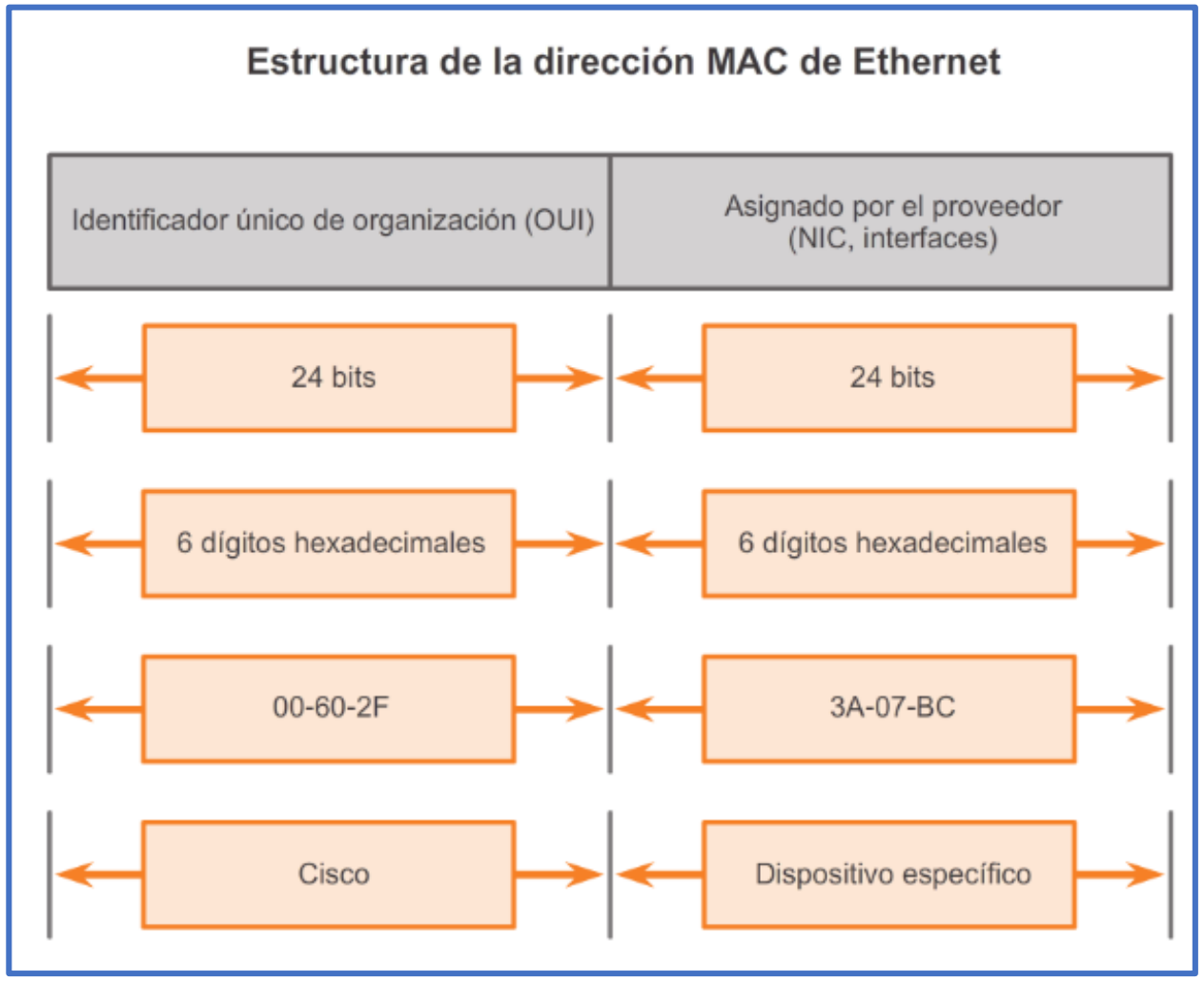
Se necesita un mayor esfuerzo para asegurar la entrega = mayor sobrecarga = velocidades de transmisión más lentas

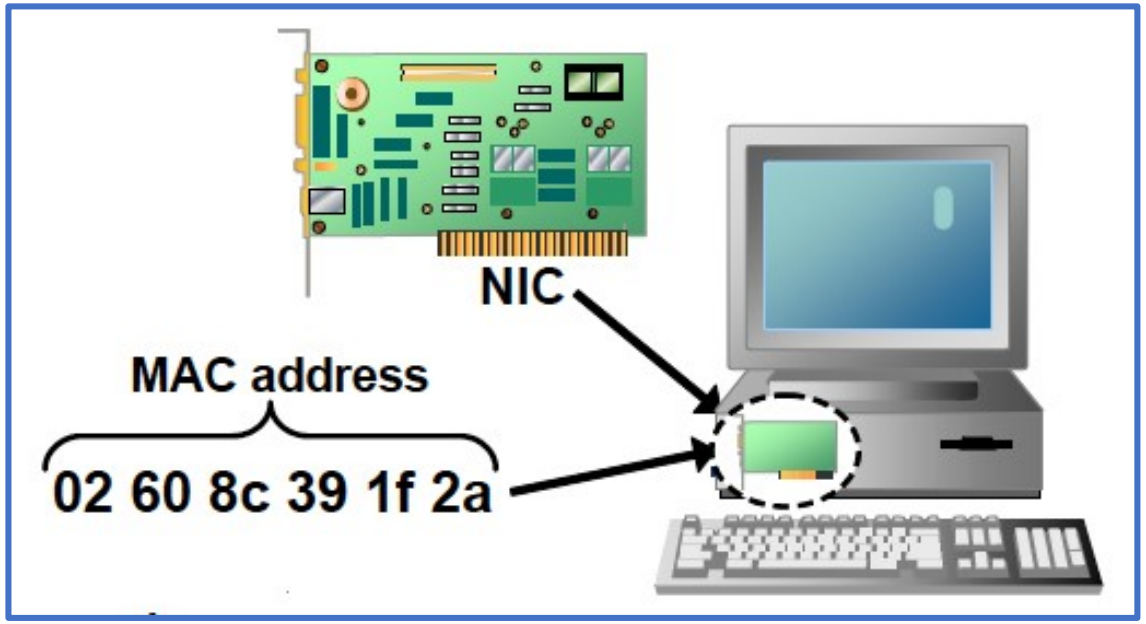


Se necesita un menor esfuerzo para asegurar la entrega = menor sobrecarga = velocidades de transmisión más rápidas



Protocolos de Redes Ethernet





MAC addresses act as the physical addresses for local communications. They show up in most IEEE 802 networks including: 802.3 (as well as Ethernet II), 802.5, 802.11 (Wi-Fi), 802.15 (Bluetooth), and the ITU-T G.hn standards.

Protocolos de Redes Ethernet

	Trama					
Nombre de campo	Preámbulo	Destino	Origen	Tipo	Datos	Secuencia de verificación de trama
Tamaño	8 bytes	6 bytes	6 bytes	2 bytes	46 bytes a 1500 bytes	4 bytes

Preámbulo: se utiliza para la sincronización; también contiene un delimitador para marcar el final de la información de temporización.
Dirección de destino: dirección MAC de 48 bits para el nodo de destino.
Dirección de origen: dirección MAC de 48 bits para el nodo de origen.
Tipo: valor para indicar qué protocolo de capa superior recibirá los datos una vez que finalice el proceso Ethernet.
Datos o contenido: esto es la PDU, normalmente un paquete IPV4, que se debe transportar a través de los medios.
Secuencia de verificación de trama (FCS): un valor utilizado para verificar si hay tramas dañadas.

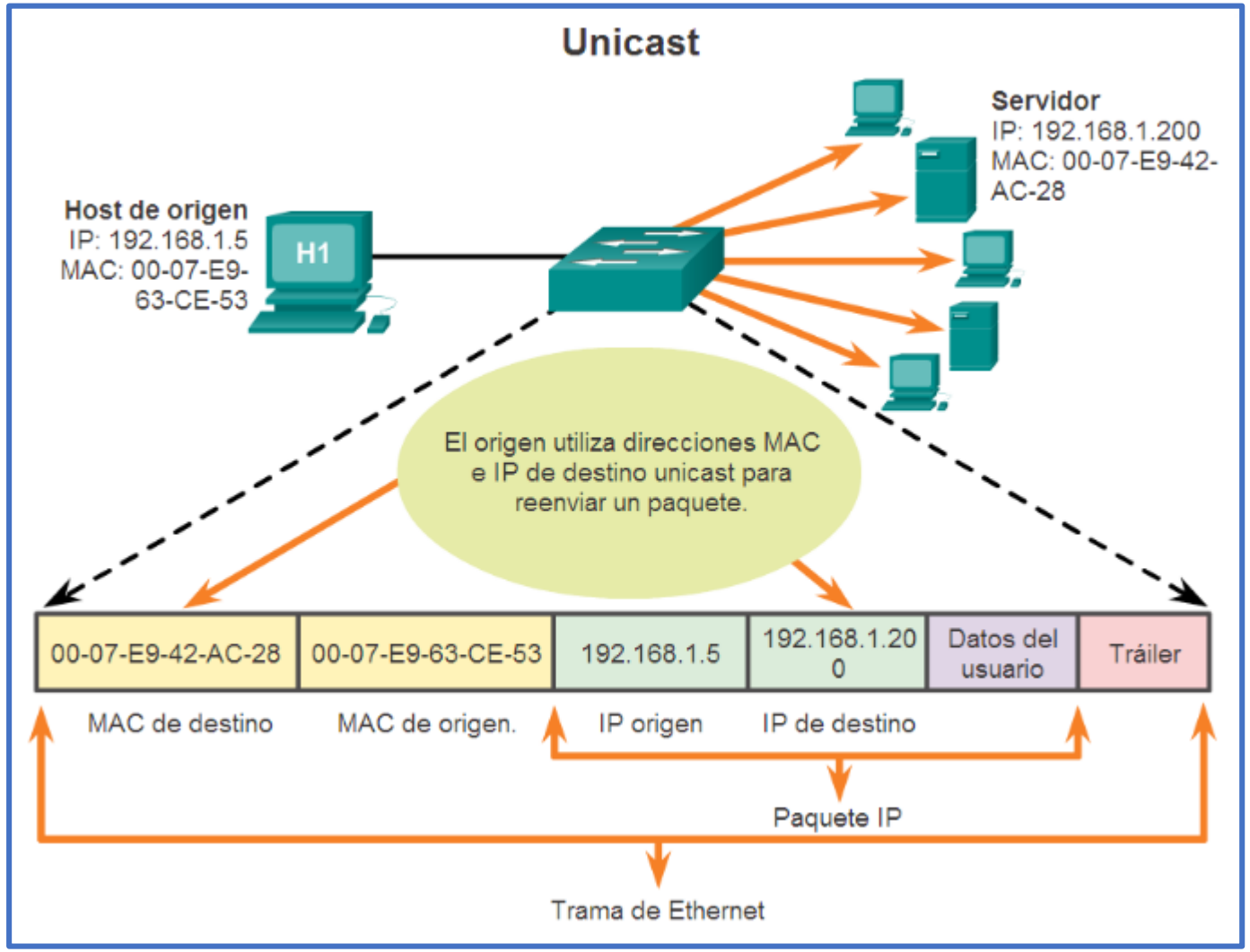
Ethernet Frame:
When transmitting data over Ethernet, the Ethernet frame is primarily responsible for the correct rulemaking and successful transmission of data packets.
Essentially, data sent over Ethernet is carried by the frame. An Ethernet frame is between **64 bytes** and **1,518 bytes** big, depending on the size of the data to be transported.

Protocolos de Redes Ethernet

IEEE 802.3 is a set of standards put forth by the IEEE that define Ethernet-based networks as well as the name of the working group assigned to develop these standards.

IEEE 802.3 is otherwise known as the Ethernet standard and defines the physical layer and the media access control (MAC) of the data link layer for wired Ethernet networks, generally as a local area network (LAN) technology.

Protocolos de Redes Ethernet



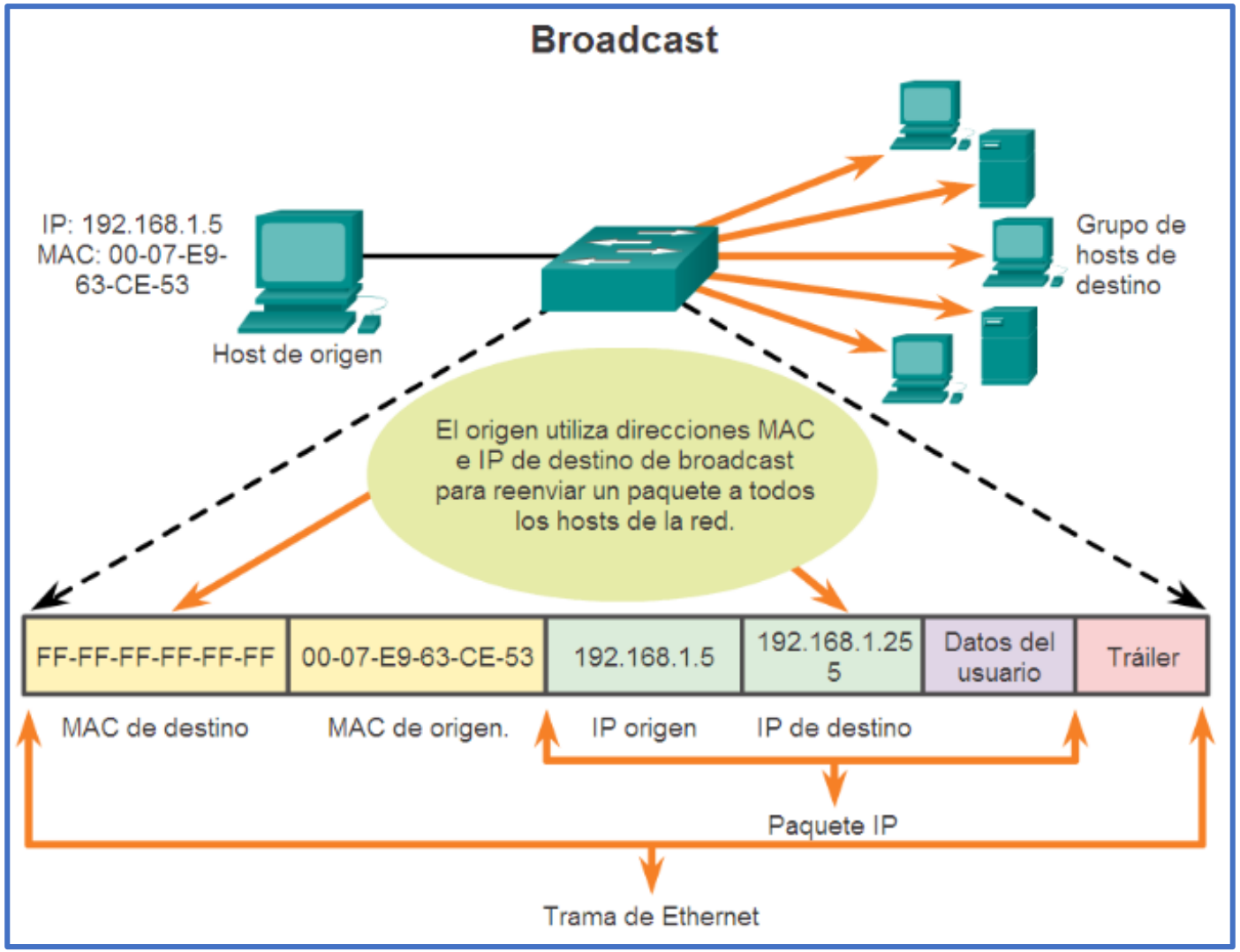
UNICAST

In computer networking, unicast is a one-to-one transmission from one point in the network to another point; that is, one sender and one receiver, each identified by a network address.

Unicast is in contrast to multicast and broadcast which are one-to-many transmissions.

Internet Protocol unicast delivery methods such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are typically used.

Protocolos de Redes Ethernet

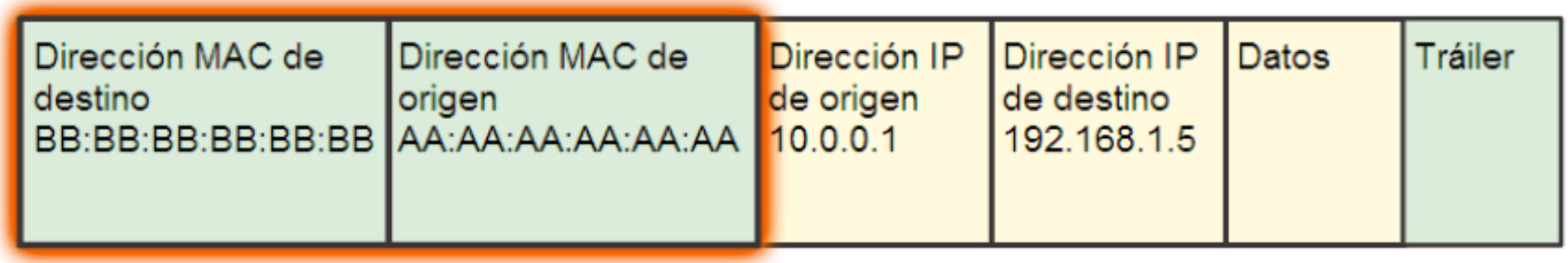


Broadcast:

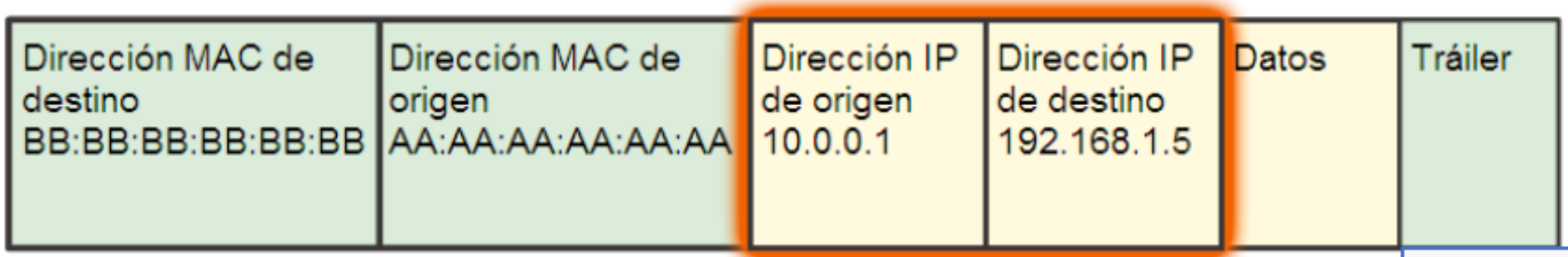
In computer networking, telecommunication and information theory, broadcasting is a method of transferring a message to all recipients simultaneously.

Broadcasting can be performed as a high-level operation in a program, for example, broadcasting in Message Passing Interface, or it may be a low-level networking operation, for example broadcasting on Ethernet.

Conectividad de extremo a extremo, MAC e IP



Un switch examina las direcciones MAC.

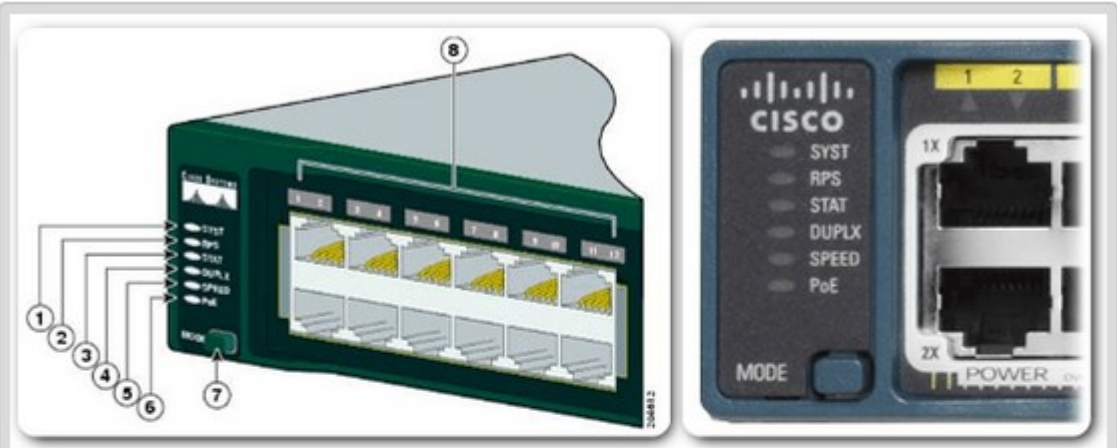


Un router examina las direcciones IP.

Configuración básica de Switch

- Los switches de Cisco son de configuración automática y no necesitan ninguna configuración adicional para comenzar a funcionar.
- Sin embargo, los switches Cisco ejecutan Cisco IOS y se pueden configurar manualmente para satisfacer mejor las necesidades de la red.
- Esto incluye el ajuste de los requisitos de velocidad, de ancho de banda y de seguridad de los puertos.

Configuración básica de Switch



LED del switch Catalyst 2960

1	LED del sistema	5	LED de velocidad del puerto
2	LED de RPS (si el switch admite RPS)	6	LED de estado de alimentación por Ethernet (si el switch la admite)
3	LED de estado del puerto (este es el modo predeterminado)	7	Botón Mode
4	LED de modo dúplex del puerto	8	LED del puerto

Imagen 1: LED del Switch

Características de los switches:

- ✓ **Puertos:** (10/100/1000/10000) en par trenzado y fibra
- ✓ **Velocidad:** (10/100/1000/10000) en par trenzado y fibra.
- ✓ **Puertos modulares: GBIC** (*Gigabit Interface Converter*); **SFP** (*Small Form-factor Puggable*)
- ✓ **Power Over Ethernet, IEEE 802.3af** en 2003, **IEEE 802.3at**. En 2009.
- ✓ **Configurable:** VLANS, STP, Monitorización de puertos (Port Mirroring), Link Aggregation / Port Trunking), Seguridad IEEE 802.1X

Figura 3. Motor supervisor de Cisco Nexus 9500

Módulo supervisor	
Procesador	Romley, 1,8 GHz, 4 núcleos
Memoria del sistema	16 GB, actualizables a 48 GB
Puertos seriales RS-232	Uno (RJ-45)
Puertos de administración 10/100/1000	Uno (RJ-45)
Interfaz USB 2.0	Dos
Almacenamiento SSD	64 GB

Configuración básica de Switch

Modos de configuración de un switch

Imagen 2: Administración Remota de Switch

Tabla Configuración de la interfaz de administración de un switch.

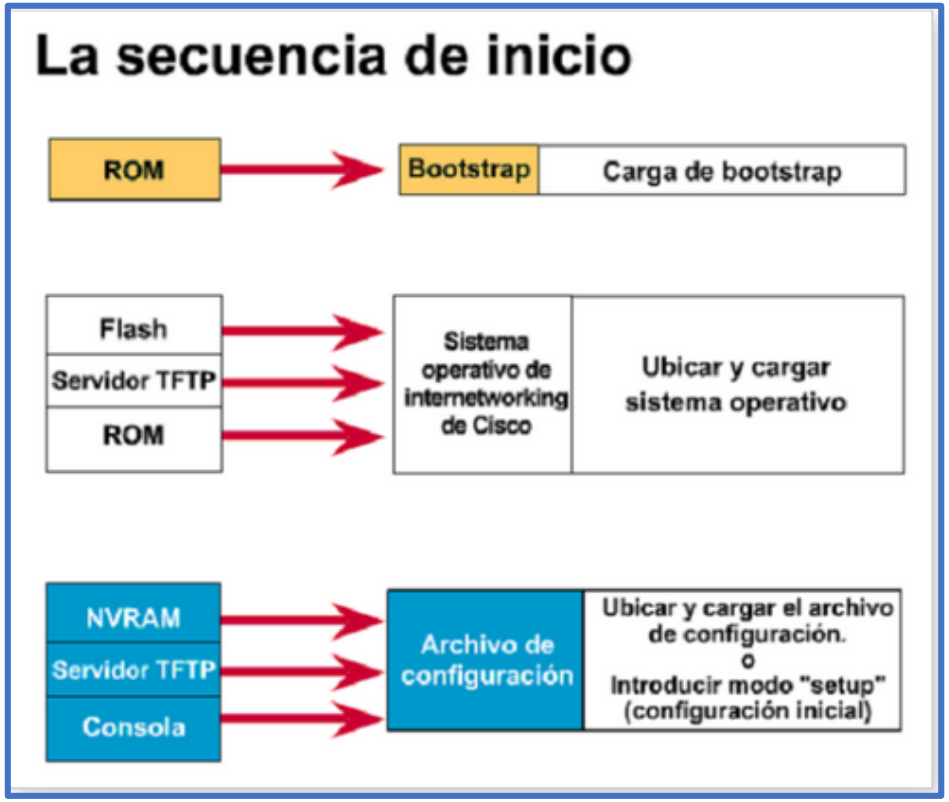
Descripción	Comando
Ingresar al modo de configuración global.	S1# configure terminal
Ingrese al modo de configuración de interfaz para la SVI.	S1(config)# interface vlan 99
Configura la dirección IP de la interfaz de administración.	S1(config-if)# ip address 172.17.99.11 255.255.255.0
Habilita la interfaz de administración.	S1(config-if)# no shutdown
Vuelva al modo EXEC privilegiado.	S1(config-if)# end
Guarda la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config

Configuración de parámetros iniciales de un switch

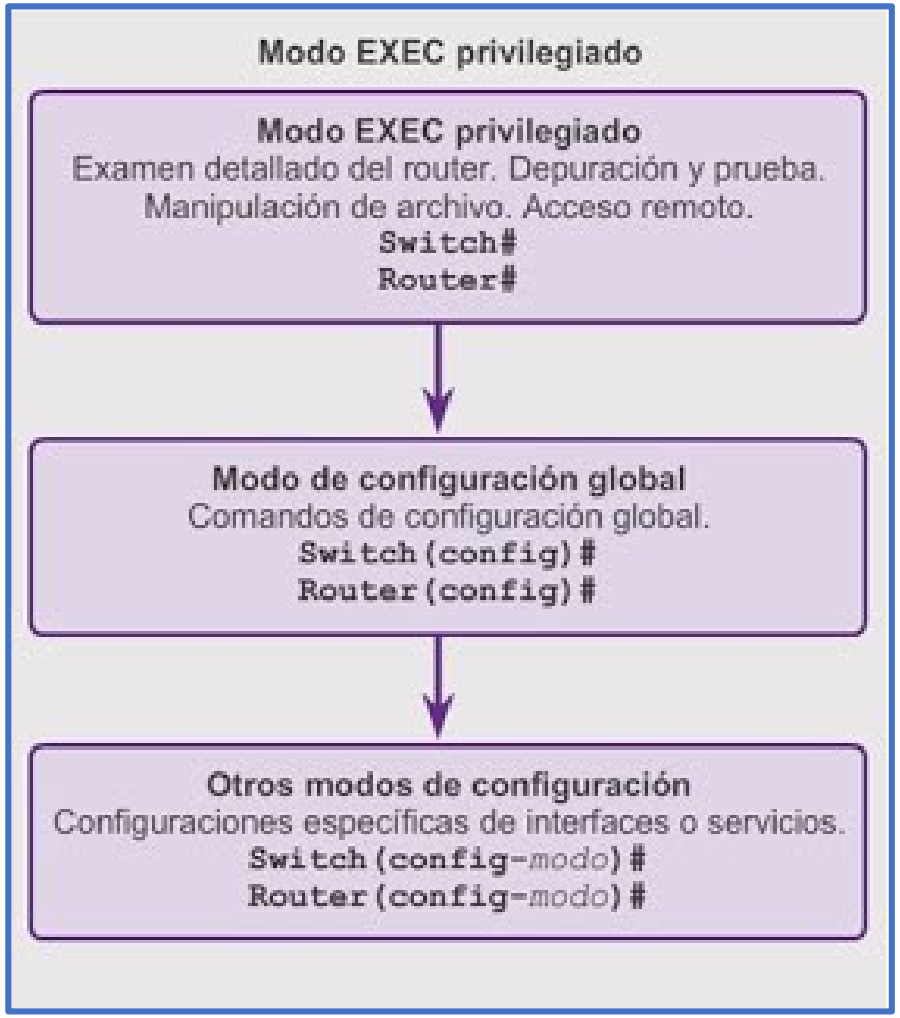
Secuencia de arranque de un switch

Una vez que se enciende el switch Cisco, lleva a cabo la siguiente secuencia de arranque:

- Primero, el switch carga un programa de autodiagnóstico al encender (POST) almacenado en la memoria ROM. El POST verifica el subsistema de la CPU. Este comprueba la CPU, la memoria DRAM y la parte del dispositivo flash que integra el sistema de archivos flash.
- A continuación, el switch carga el software del cargador de arranque. El cargador de arranque es un pequeño programa almacenado en la memoria ROM que se ejecuta inmediatamente después de que el POST se completa correctamente.
- El cargador de arranque lleva a cabo la inicialización de la CPU de bajo nivel. Inicializa los registros de la CPU, que controlan dónde está asignada la memoria física, la cantidad de memoria y su velocidad.
- El cargador de arranque inicia el sistema de archivos flash en la placa del sistema.
- Por último, el cargador de arranque localiza y carga una imagen de software del sistema operativo de IOS en la memoria y delega el control del switch a IOS.



Configuración básica de Switch




```
Switch_Basico#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_Basico(config)#line console 0
Switch_Basico(config-line)#pass c0ns014
Switch_Basico(config-line)#login
Switch_Basico(config-line)#exit
Switch_Basico(config)#
Switch_Basico(config)#line vty 0 15
Switch_Basico(config-line)#pass t3ln3t
Switch_Basico(config-line)#login
Switch_Basico(config-line)#exit
Switch_Basico(config)#exit
Switch_Basico#
```

```
Switch_Basico#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_Basico(config)#int vlan 100
Switch_Basico(config-if)#ip address 192.168.1.1 255.255.255.0
Switch_Basico(config-if)#no shutdown
Switch_Basico(config-if)#exit
Switch_Basico(config)#exit
Switch_Basico#
```

Configuración básica de Switch

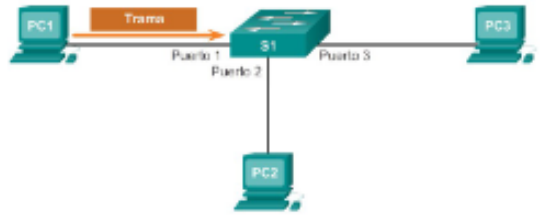
Conmutación

Tabla de direcciones MAC del switch

1. El switch recibe una trama de broadcast de la PC 1 en el puerto 1.
2. El switch ingresa la dirección MAC de origen y el puerto del switch que recibió la trama en la tabla de direcciones.
3. Dado que la dirección de destino es broadcast, el switch satura todos los puertos enviando la trama, excepto el puerto que la recibió.
4. El dispositivo de destino responde al broadcast con una trama de unicast dirigida a la PC 1.

Conmutación

Tabla de direcciones MAC del switch



5. El switch introduce en la tabla de direcciones la dirección MAC de origen de la PC 2 y el número del puerto de switch que recibió la trama. En la tabla de direcciones MAC pueden encontrarse la dirección de destino de la trama y su puerto asociado.
6. Ahora el switch puede enviar tramas entre los dispositivos de origen y destino sin saturar el tráfico, ya que cuenta con entradas en la tabla de direcciones que identifican a los puertos asociados.

Configuración básica de Switch

Conmutación

Métodos de reenvío de tramas en switches Cisco

Almacenamiento y envío

Un switch de almacenamiento y envío recibe la trama completa y calcula la CRC. Si la CRC es válida, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Conmutación

Conmutación por método de corte

Método de corte

El switch que utiliza el método de corte envía la trama antes de recibirla en su totalidad. Como mínimo, la dirección de destino de la trama debe leerse antes de que la trama pueda enviarse.

Existen dos variantes:

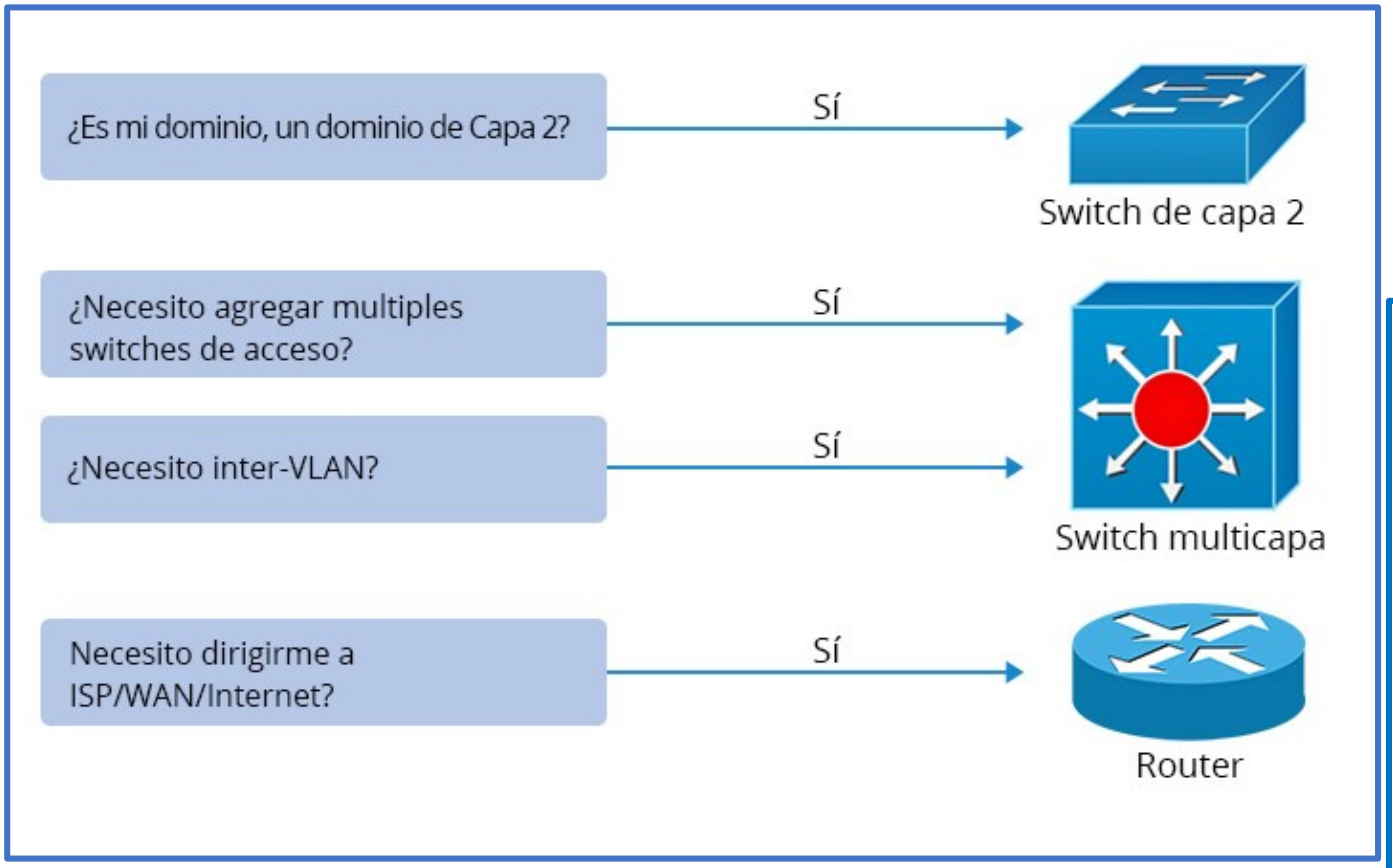
Conmutación por envío rápido:

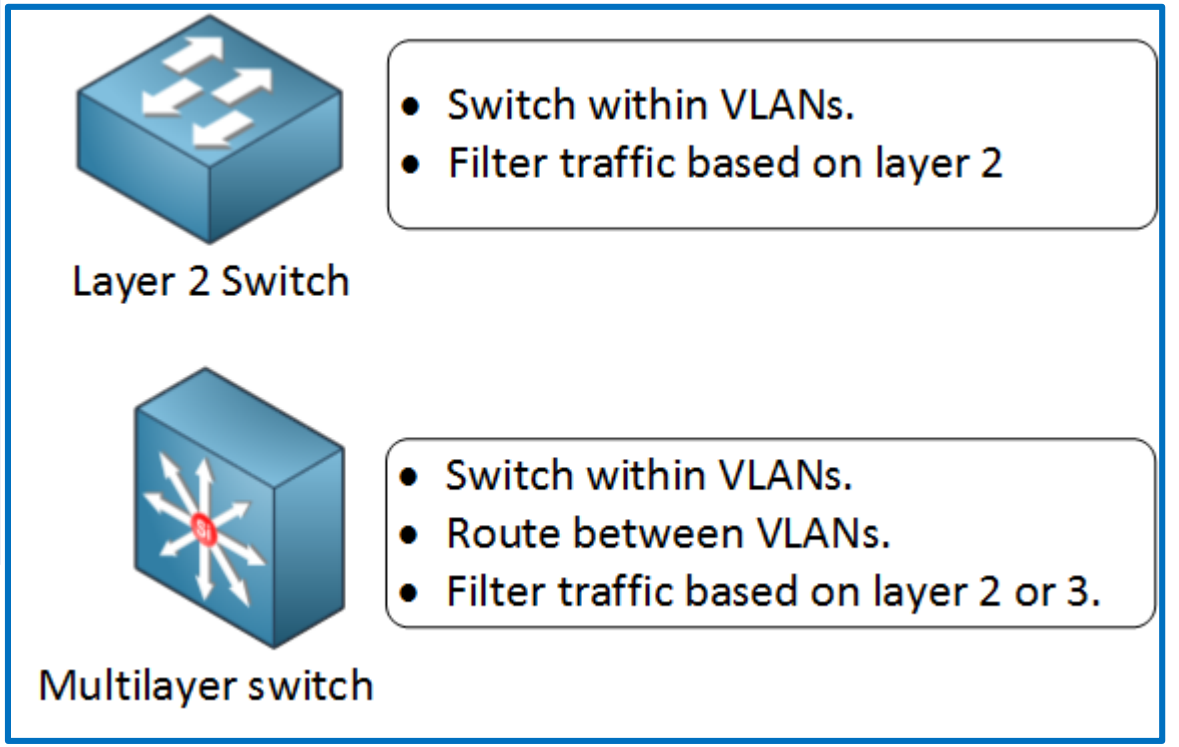
- El nivel más bajo de latencia reenvía un paquete inmediatamente después de leer la dirección de destino; método típico de conmutación por método de corte.

Conmutación libre de fragmentos:

- El switch almacena los primeros 64 bytes de la trama antes de reenviar; la mayoría de los errores y las colisiones de red se producen en los primeros 64 bytes.

Configuración básica de Switch





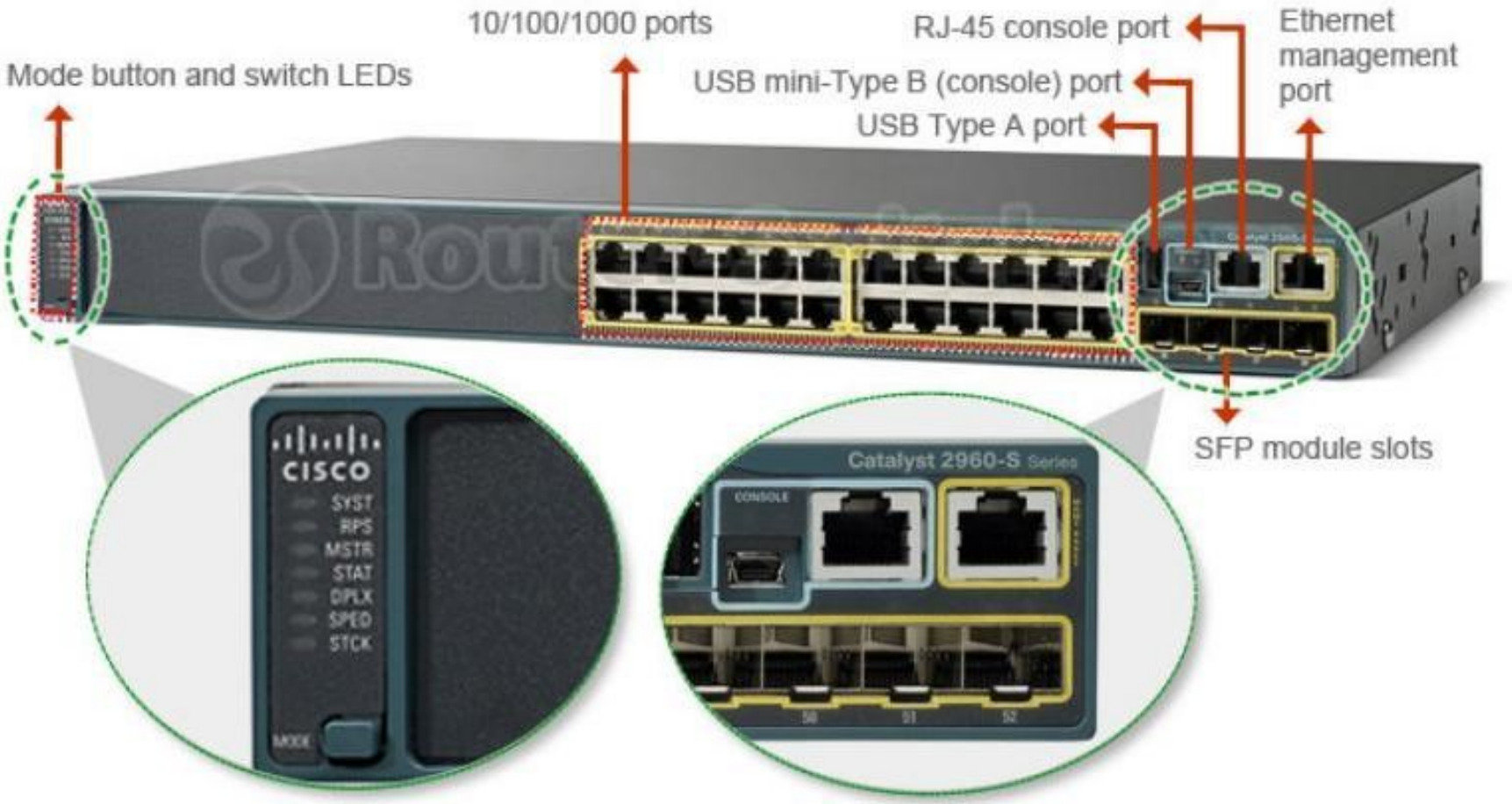
Fuente: https://community.fs.com/es/blog/layer-2-switch-vs-layer-3-switch-what-is-the-difference.html

Switches

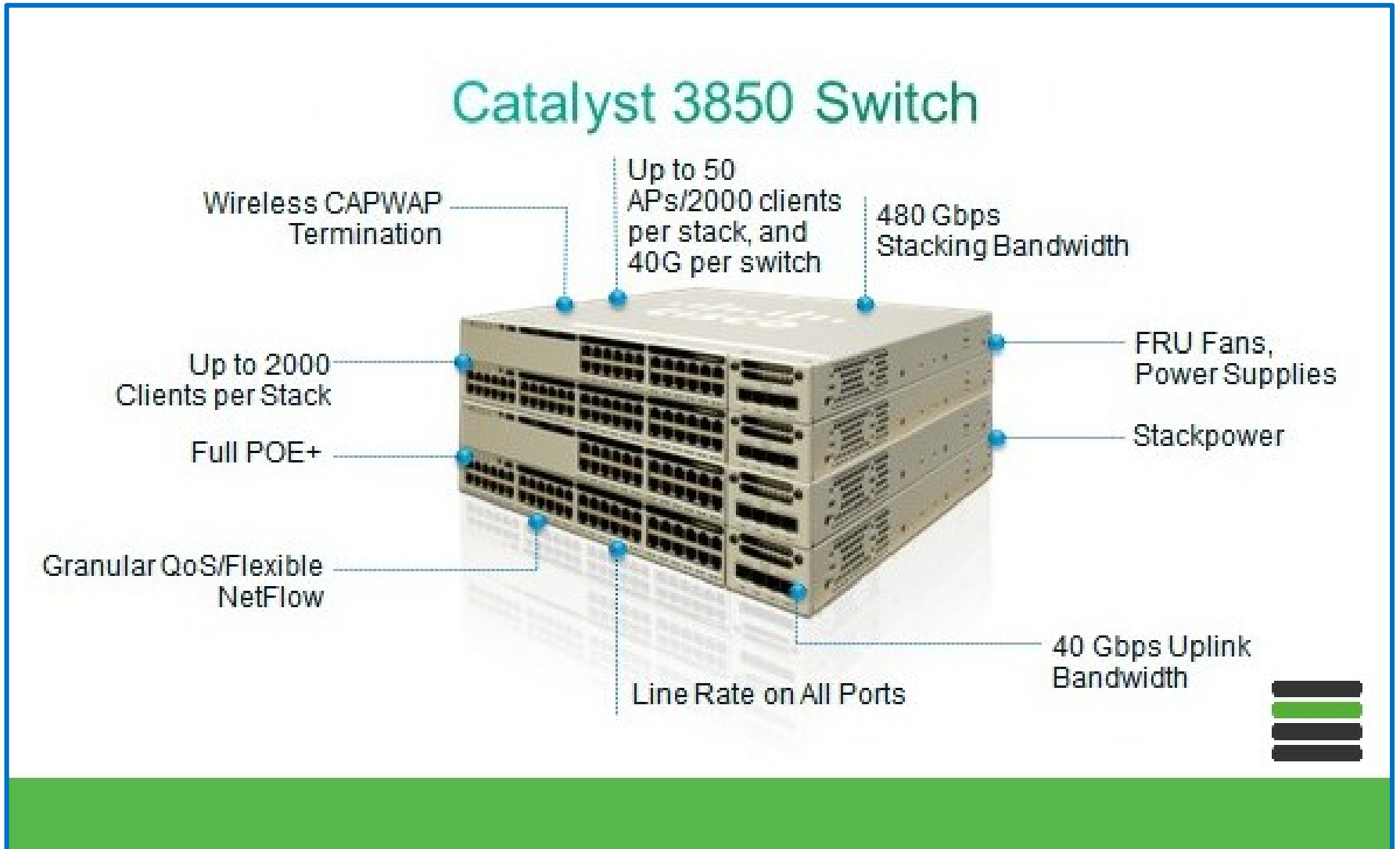
WS-C2960S-24TS-L

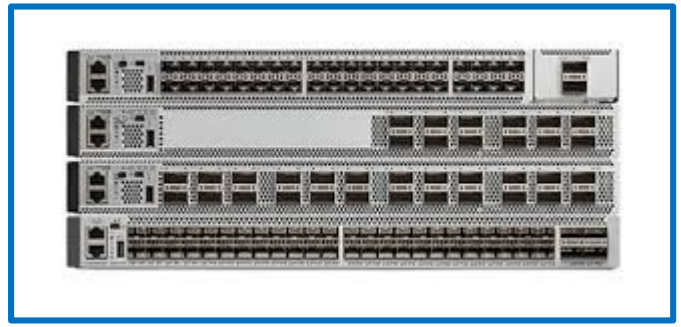
Cisco Catalyst 2960-S Series Switch

- 24 Gigabit Ethernet ports
- Two 1G Small Form-Factor Pluggable (SFP)
- USB interfaces for management and file transfers
- LAN Base or LAN Lite Cisco IOS Software feature set
- SmartOperations tools that simplify deployment and reduce the cost of network administration

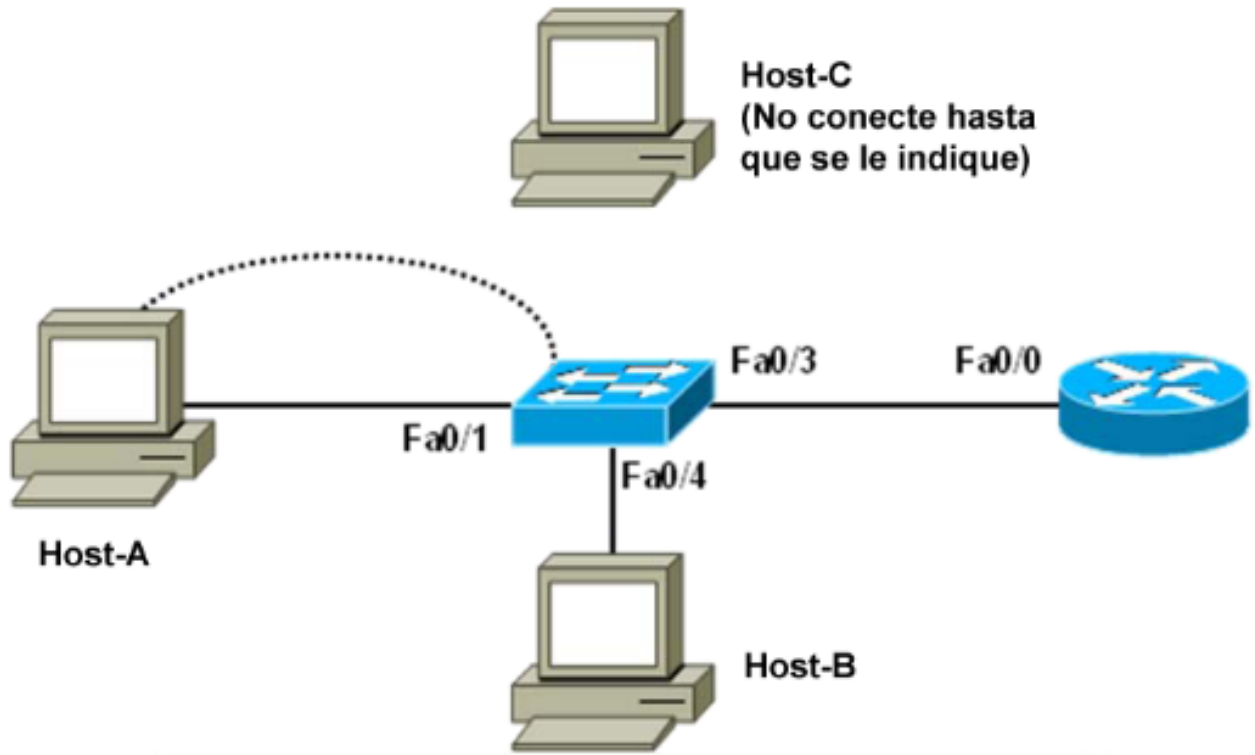


Configuración básica de Switch



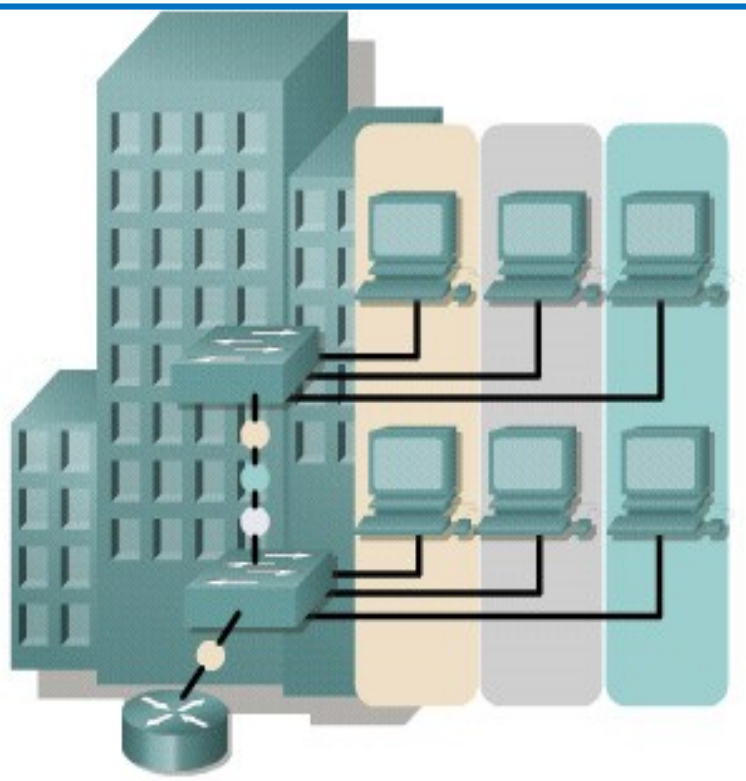


Práctica de laboratorio 5.4.4 Configurar el switch Cisco 2960



VLANs, Introduction

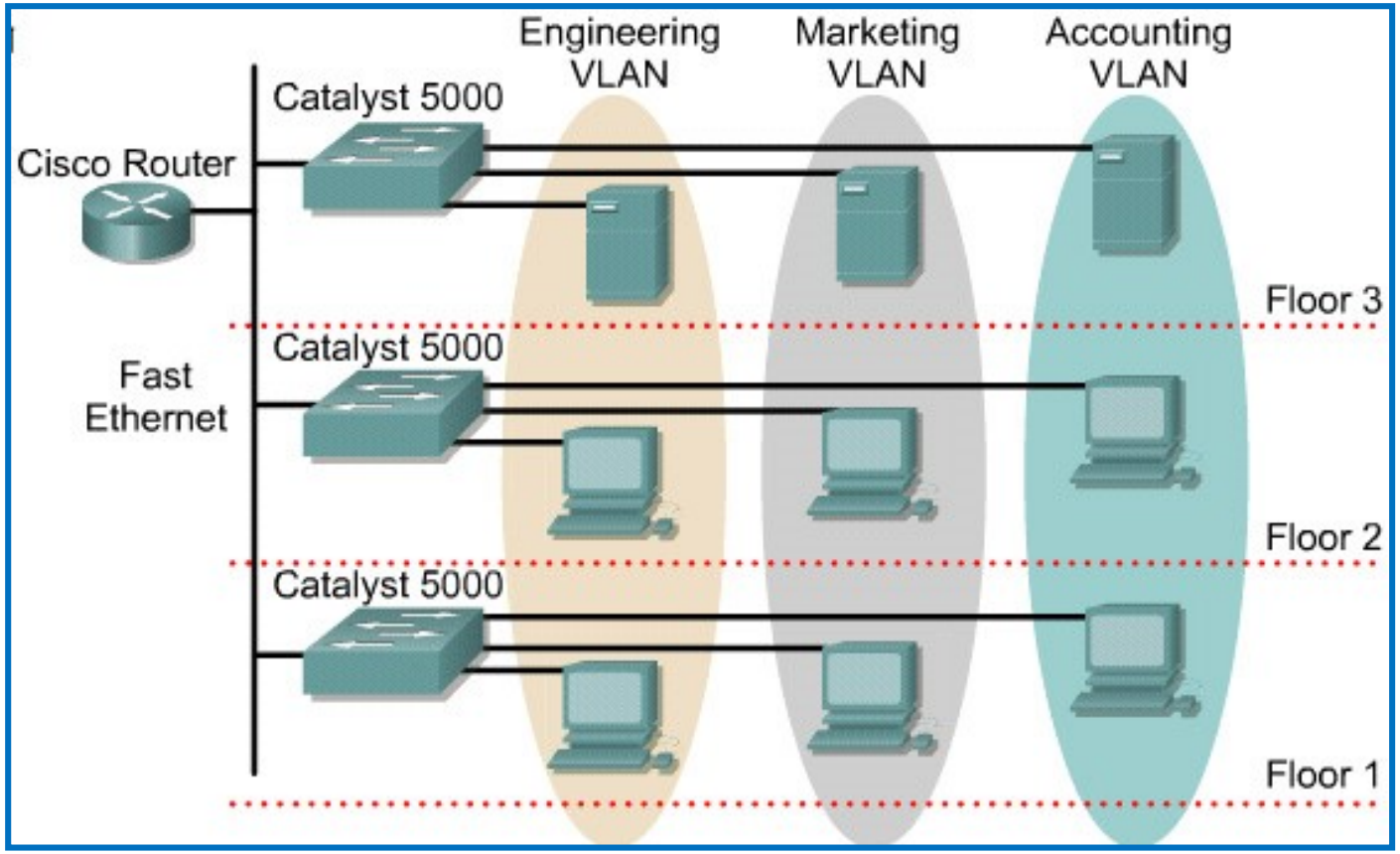
- VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.
- A workstation in a VLAN group is restricted to communicating with file servers in the same VLAN group.
- VLANs function by logically segmenting the network into different broadcast domains so that packets are only switched between ports that are designated for the same VLAN.



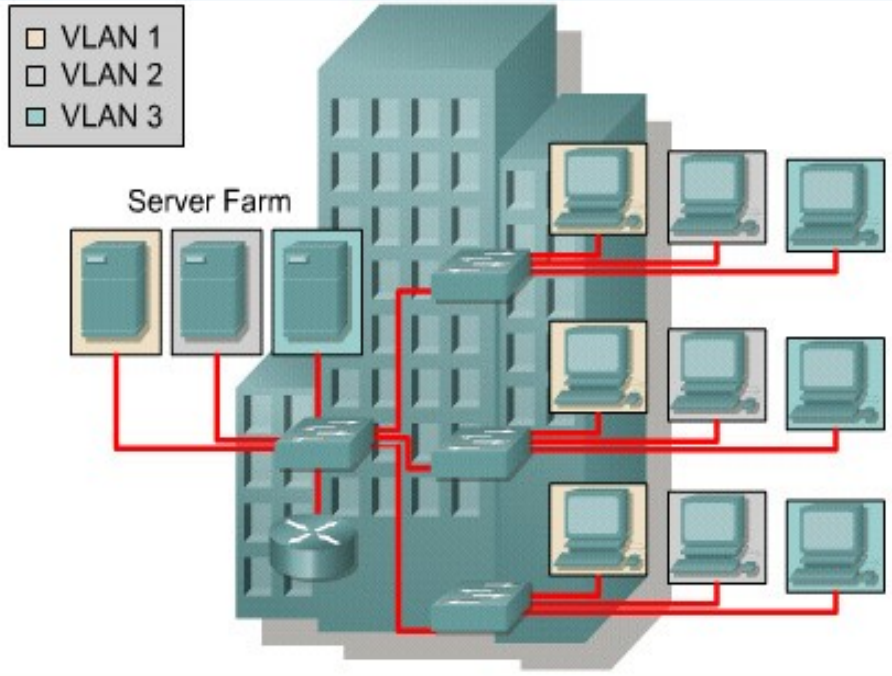
- A group of ports or users in same broadcast domain
- Can be based on port ID, MAC address, protocol, or application
- LAN switches and network management software provide a mechanism to create VLANs
- Frame tagged with VLAN ID

VLANs, Introduction

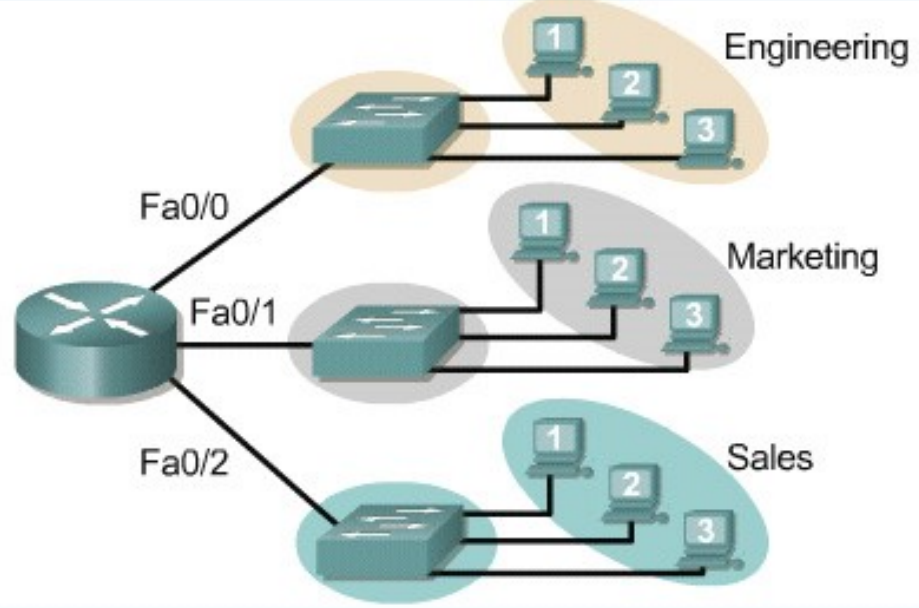
- Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- VLANs address scalability, security, and network management.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain.
- Traffic should only be routed between VLANs.
- A VLAN is a broadcast domain created by one or more switches.
- Layer 3 routing allows the router to send packets to the three different broadcast domains.



VLANs, Introduction



- A switch creates a broadcast domain
- VLANs help manage broadcast domains
- VLANs can be defined on port groups, users, or protocols
- LAN switches and network management software provide a mechanism to create VLANs

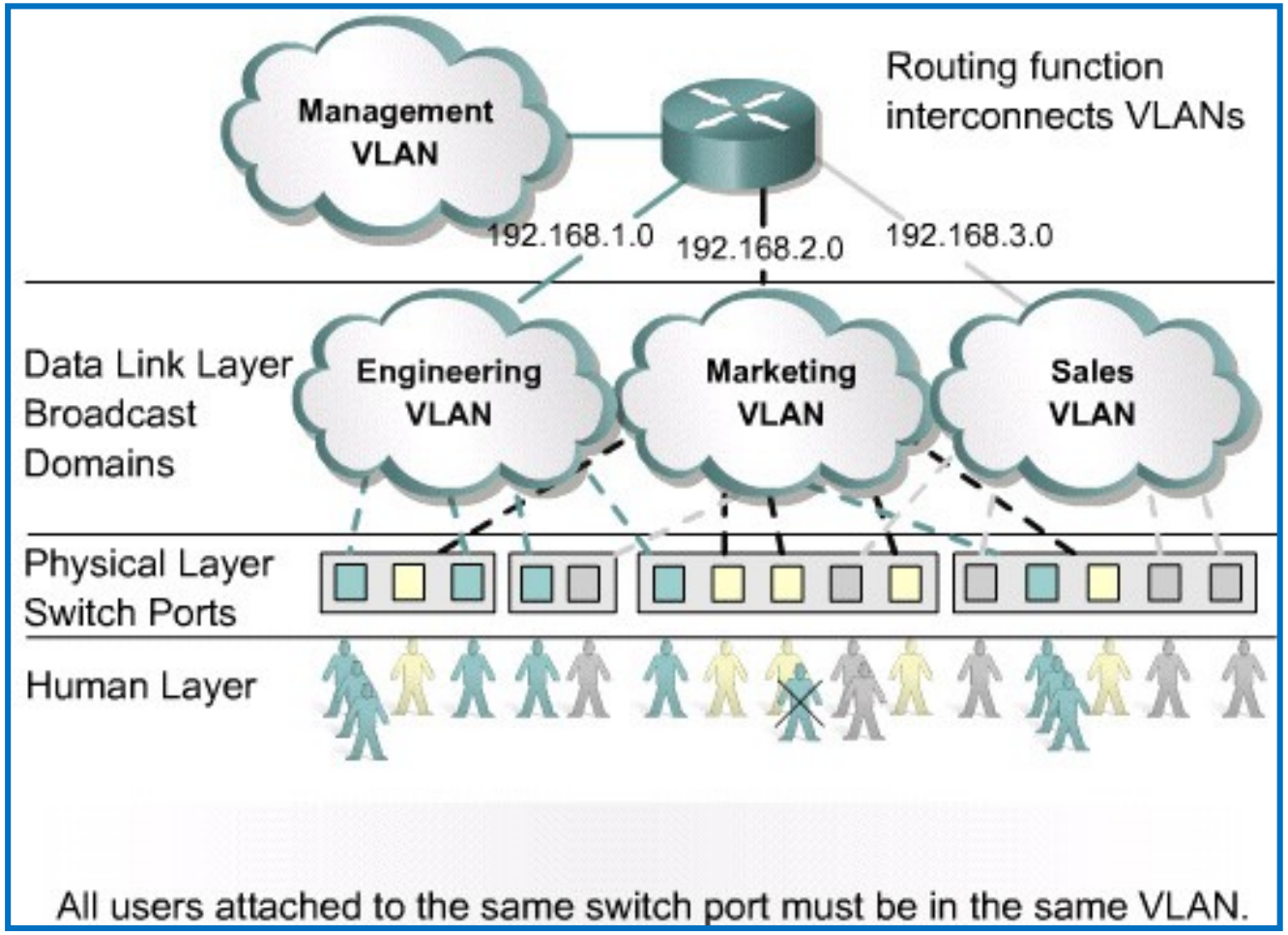


Three switches and one router could be used without VLANs:

- Switch for Engineering
- Switch for Sales
- Switch for Marketing
- Each switch treats all ports as members of one broadcast domain
- Router is used to route packets among the three broadcast domains

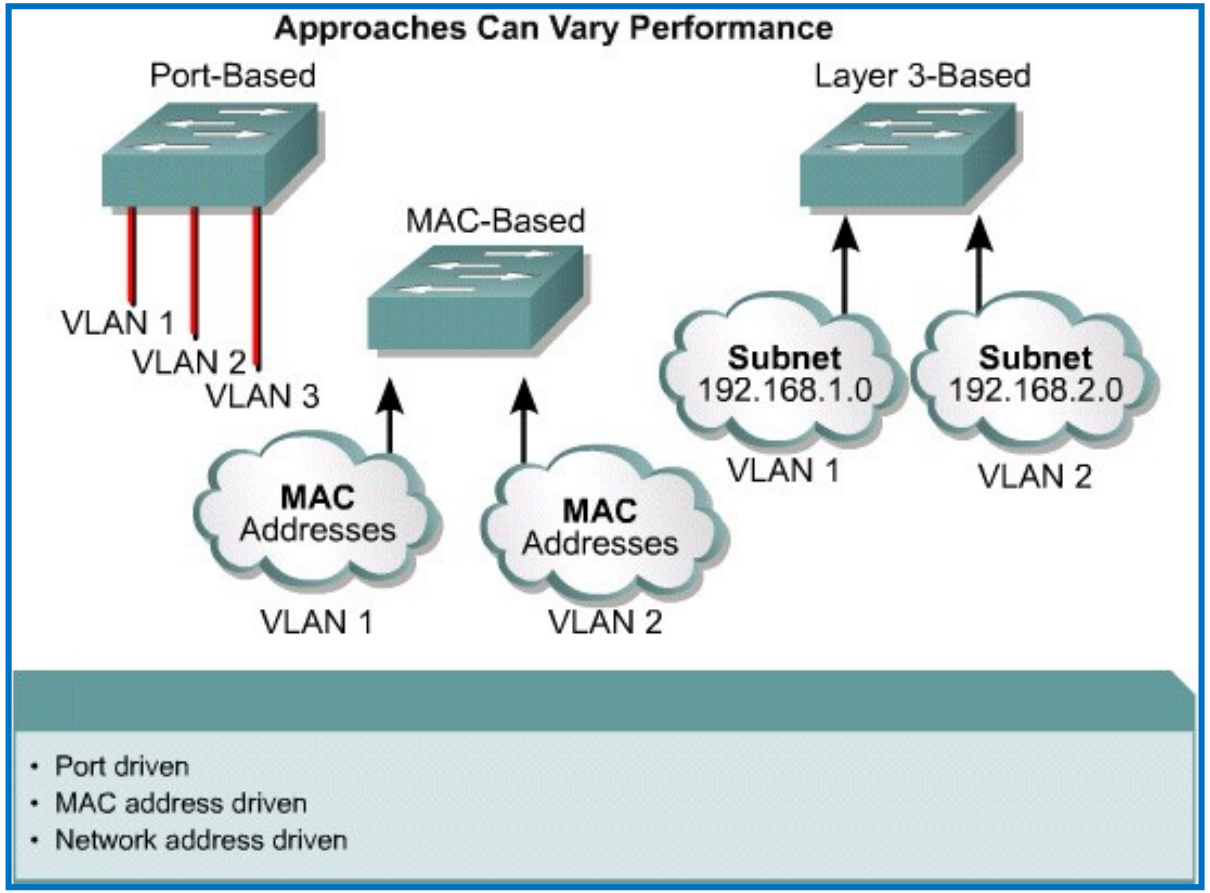
Benefits of VLANs

- The key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically.
- VLANs offer a method of segregating a physical network into a logical network infrastructure. By deploying VLANs, you can create multiple virtual LANs in your Ethernet infrastructure.
- VLANs help reduce traffic. Decrease costs, improve performance, increase security, provide more connectivity options, and reduce the size of fault domain, improving the diagnostic process.
- As the use of VLAN technology has become more common, designing and maintaining networks must now involve being aware of the presence of VLANs.

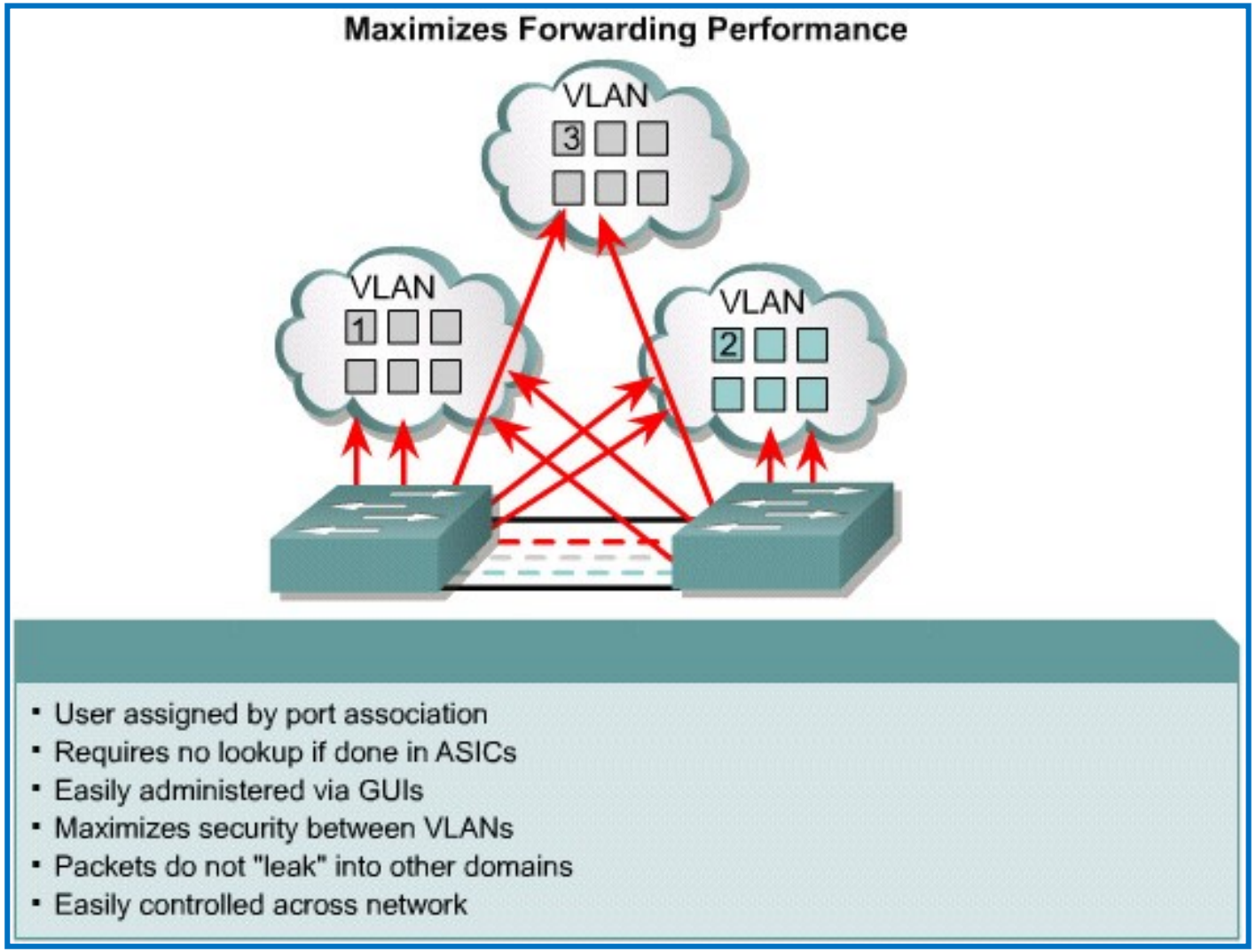


VLAN types

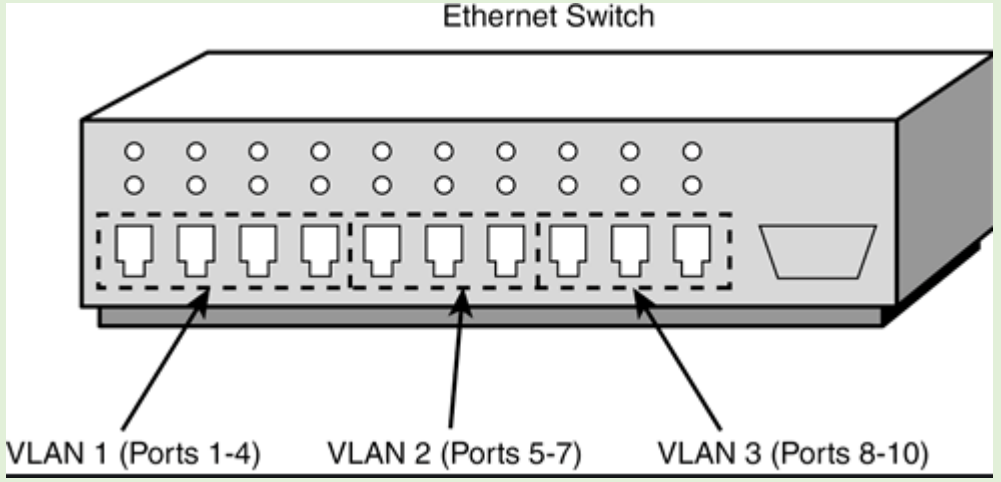
- Port-based VLANs
- MAC address based VLANs
- Protocol based VLANs
- The number of VLANs in a switch vary depending on several factors:
  - Traffic patterns
  - Types of applications
  - Network management needs
  - Group commonality
- An important consideration in defining the size of the switch and the number of VLANs is the IP addressing scheme.
- Because a one-to-one correspondence between VLANs and IP subnets is strongly recommended, there can be no more than 254 devices in any one VLAN.
- It is further recommended that VLANs should not extend outside of the Layer 2 domain of the distribution switch.



Membership by Port



- Port-based VLANs require that specific ports on a network switch be assigned to a VLAN.
- For example, ports 1 through 4 might be assigned to marketing, ports 5 through 7 might be assigned to sales, and so on.
- Using this method, a switch determines VLAN membership by taking note of the port used by a particular packet. Figure 1 shows an example of a port-based VLAN.

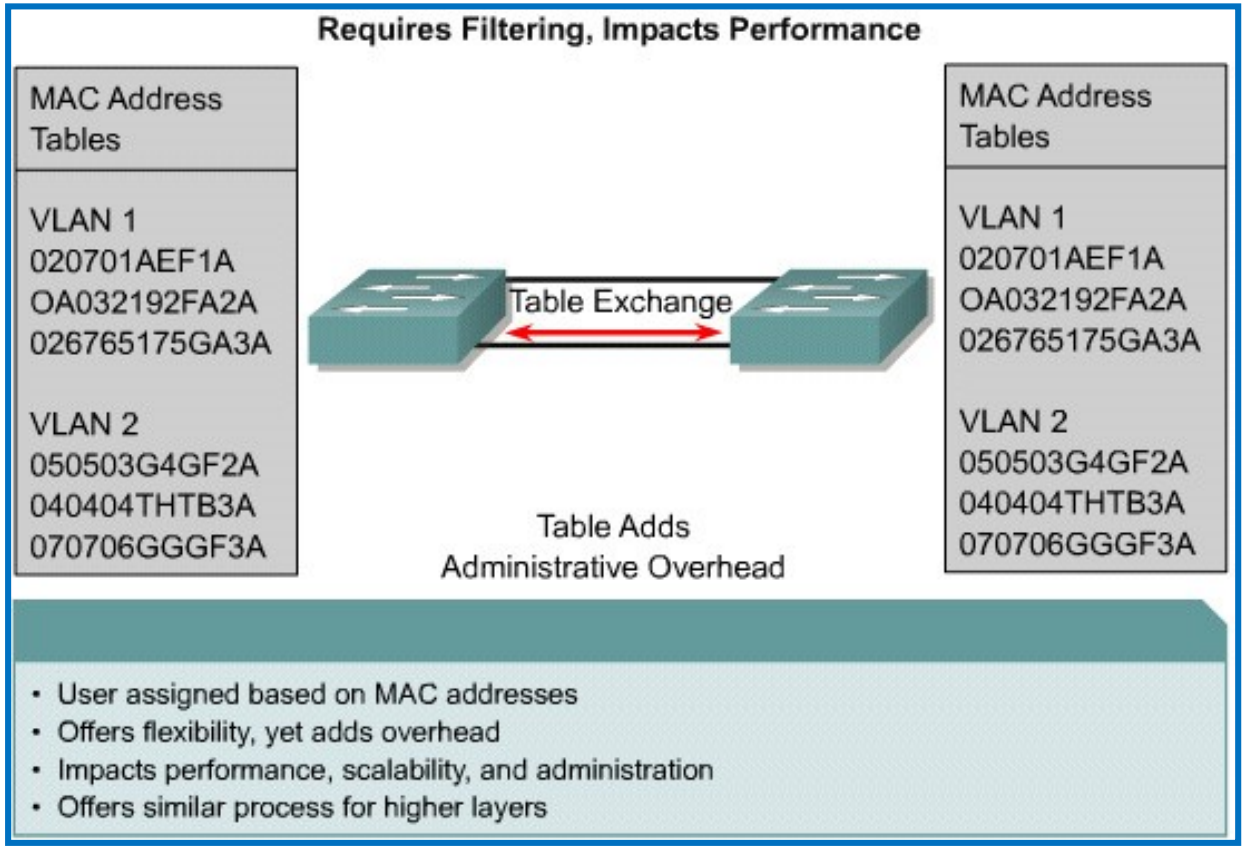


VLAN types

- There are two major methods of frame tagging, Inter-Switch Link (ISL) and 802.1Q.
- ISL used to be the most common, but is now being replaced by 802.1Q frame tagging.

Tagging	Method	Media	Description
Inter-Switch Link (ISL)	Fast Ethernet	ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header	Frame is lengthened.
802.IQ	Fast Ethernet	IEEE defined Ethernet VLAN protocol	Header is modified.
802.IQ	FDDI	IEEE defined standard: The 802.10 protocol incorporates a mechanism whereby LAN traffic can carry a VLAN identifier	VLAN ID is the essential piece of required header information.
LAN Emulation (LANE)	ATM	No tagging	Virtual connection implies a VLAN ID.

Membership by MAC-Addresses



VLAN Commands

Create a VLAN

- SW1(config)#**vlan 20**
- SW1(config-vlan)#**name Finance**
- SW1(config-vlan)#**end**
- VLAN will be saved in VLAN database rather than running config.

Assign port to VLAN

- SW1(config)#**int fa 0/14**
- SW1(config-if)#**switchport mode access**
- SW1(config-if)#**switchport access vlan 20**
- SW1(config-if)#**end**

show vlan brief

- List of VLANs with ports

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
20   student                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

VLAN Commands

Show commands

- show vlan brief (list of VLANs and ports)
- show vlan summary
- show interfaces vlan (up/down, traffic etc)
- Show interfaces fa0/14 switchport (access mode, trunking)

Delete a VLAN

- SW1(config)#**no vlan 20**
- SW1(config)#**end**
- VLAN 20 is deleted.

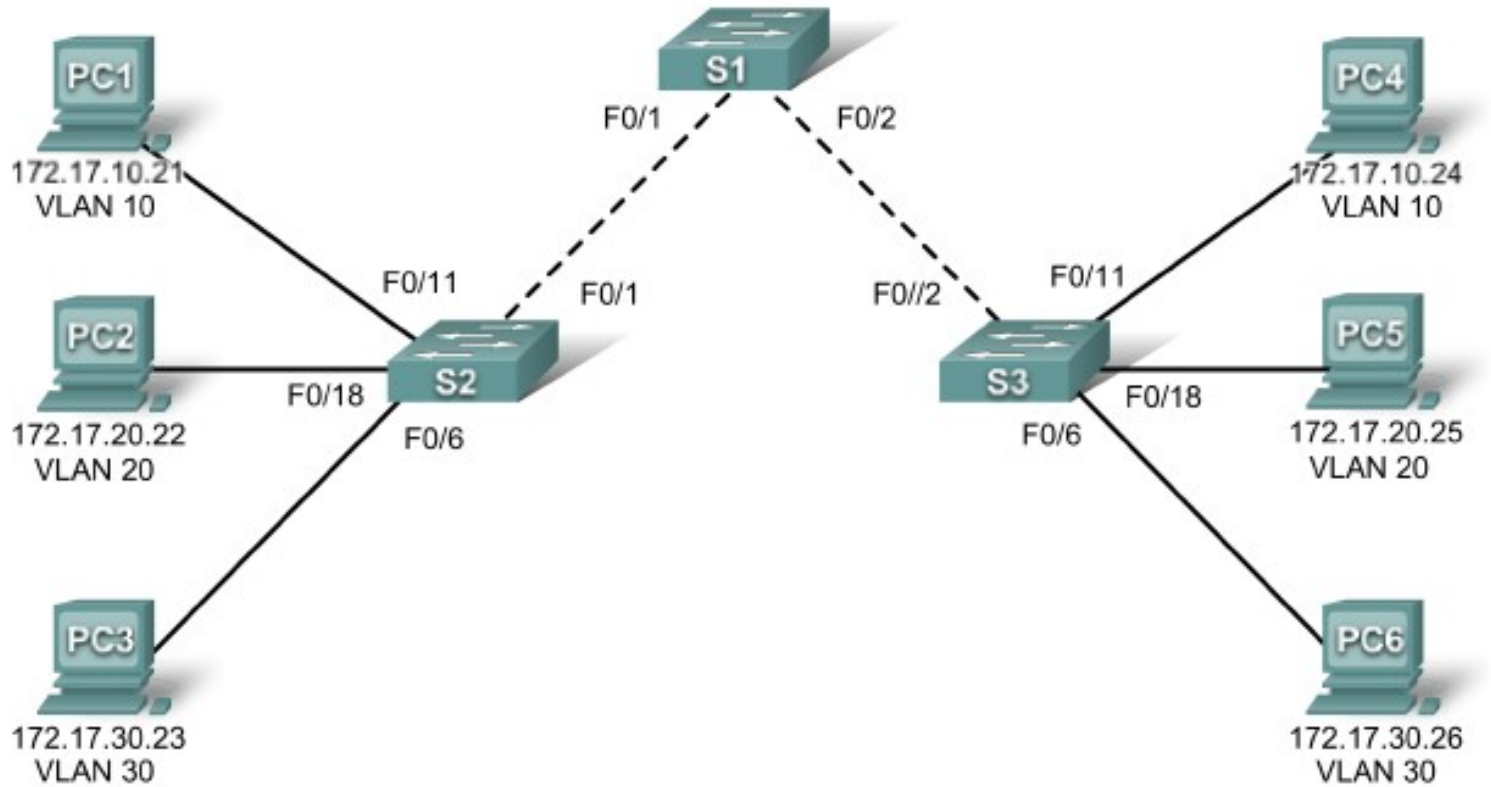
Remove port from VLAN

- SW1(config)#**int fa 0/14**
- SW1(config-if)#**no switchport access vlan**
- SW1(config-if)#**end**
- The port goes back to VLAN 1.
- If you assign a port to a new VLAN, it is automatically removed from its existing VLAN.

Cisco | Networking Academy®
Mind Wide Open™

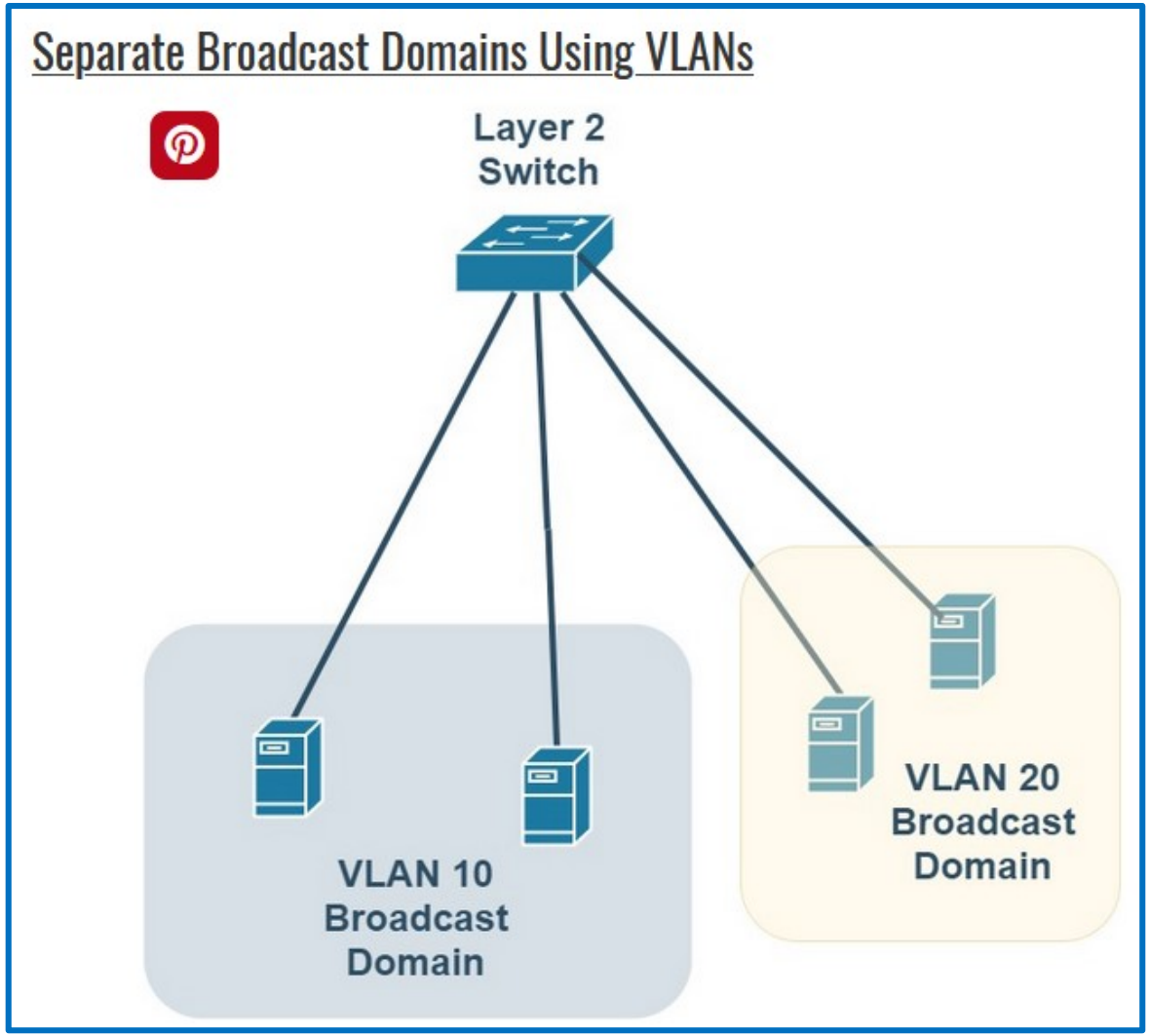
Práctica de laboratorio 3.5.1: Configuración básica de una VLAN

Diagrama de topología

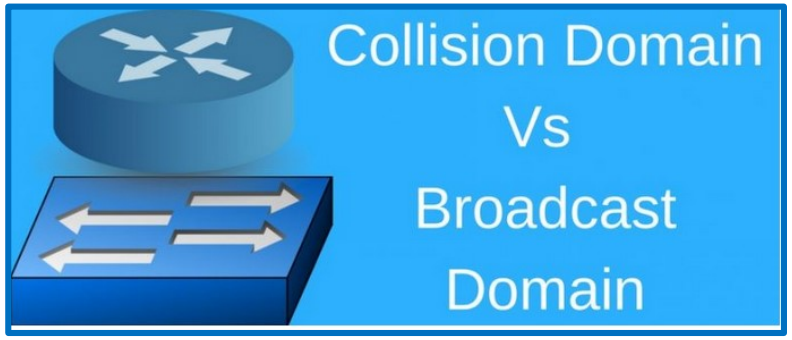


Broadcast domains with VLANs and routers

- Traffic should only be routed between VLANs.
- A VLAN is a broadcast domain created by one or more switches.
- Layer 3 routing allows the router to send packets to the three different broadcast domains.
- Each VLAN is an individual broadcast domain because a broadcast in a given VLAN will never reach any ports in other VLANs.
- Normally, a port carries traffic only for the single VLAN to which it belongs.
- For a VLAN to span multiple switches on a single connection, a trunk is required to connect two switches.

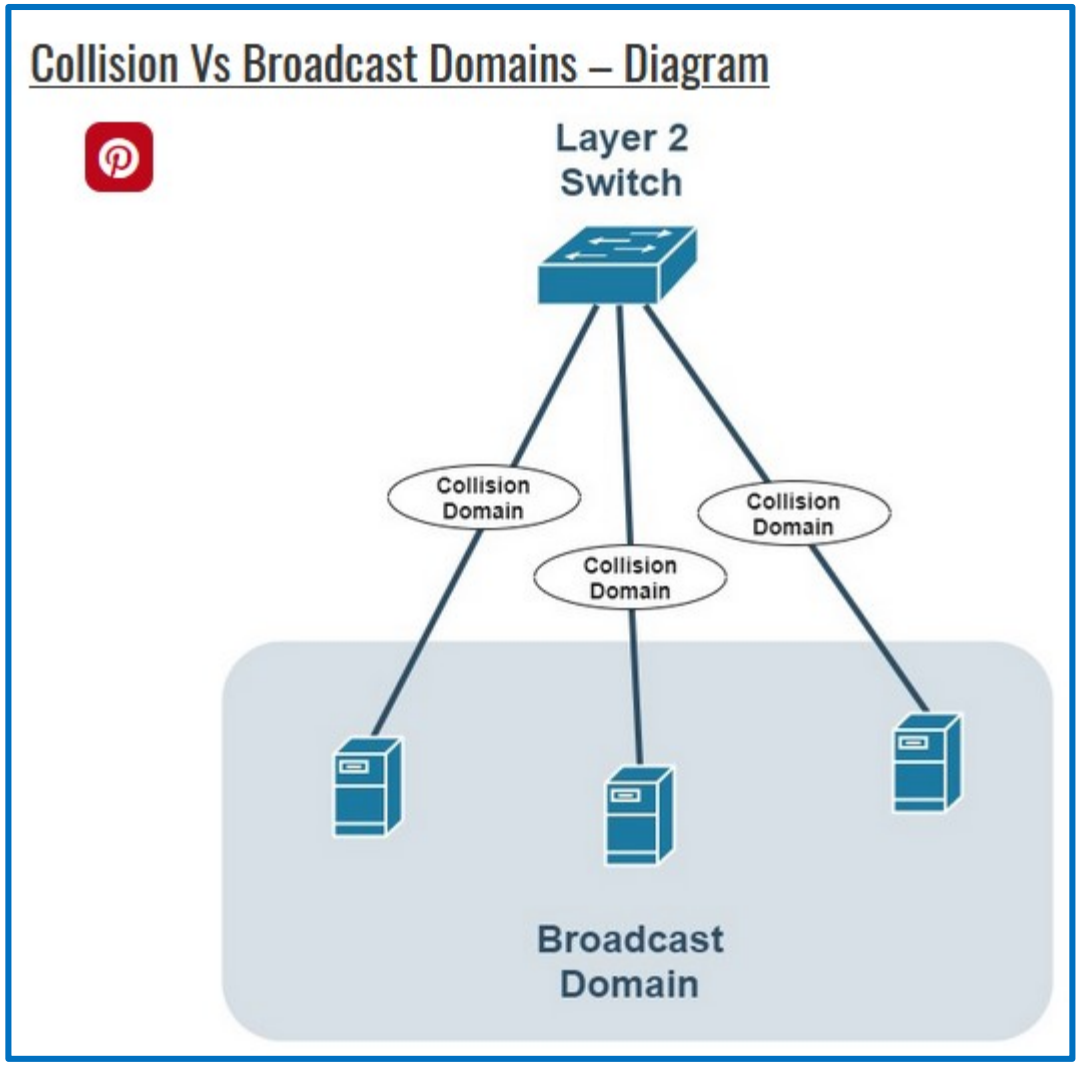


Collision Domains and Broadcast Domains



Source: Collision Domains and Broadcast Domains Explained, URL: https://www.networkstraining.com/collision-domain-vs-broadcast-domain/

- The diagram shows a Layer 2 switch having one Broadcast Domain and three Collision Domains.
- Basically, all hosts connected to the same switch (in the same Layer 2 VLAN) belong to the same broadcast domain. This means, all broadcast packets sent by one host will be received by all other hosts in the same broadcast domain (same VLAN).
- On the other hand, each physical port link connecting a single host to the switch is considered a collision domain. If you have 3 hosts connected to the switch, there are 3 separate collision domains.



Collision Domains and Broadcast Domains

❖**What is a Collision Domain?**

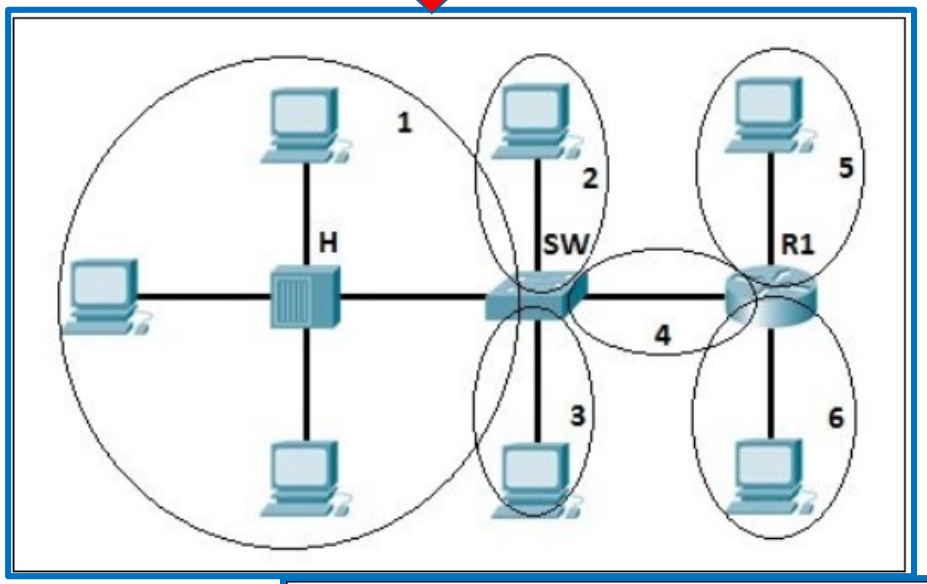
- ❖The term collision domain is basically used in LAN Switching, which occurs in Layer 2 of the OSI reference model.
- ❖Layer 2 switches are most commonly used in modern LAN networks, and this eliminates collisions. On an Ethernet Switch, a collision domain exists only on each physical switch-port, not on the whole switched network (as shown on the diagram above).
- ❖Because usually only a single host is connected to each switch port, there are no collisions in Ethernet Switches.

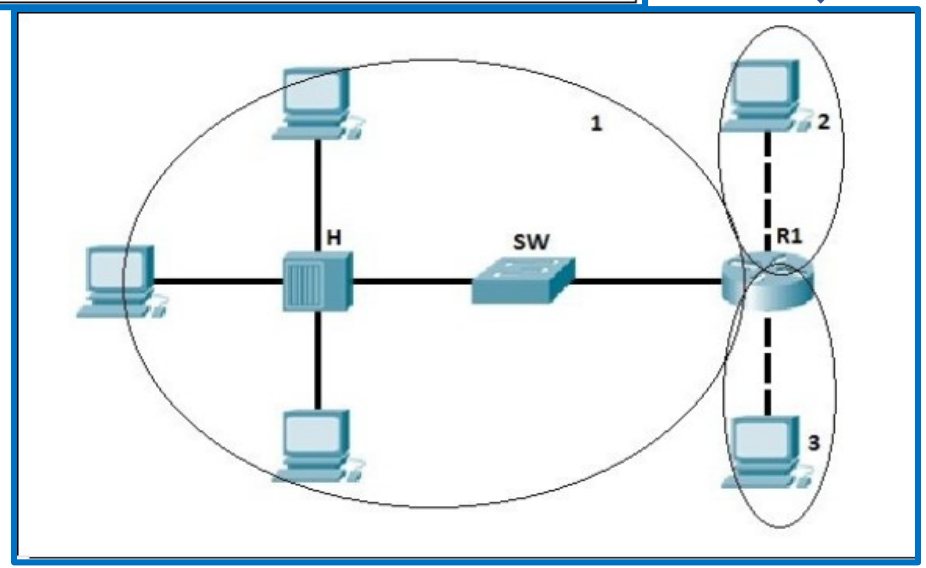
❖**What is a Broadcast Domain?**

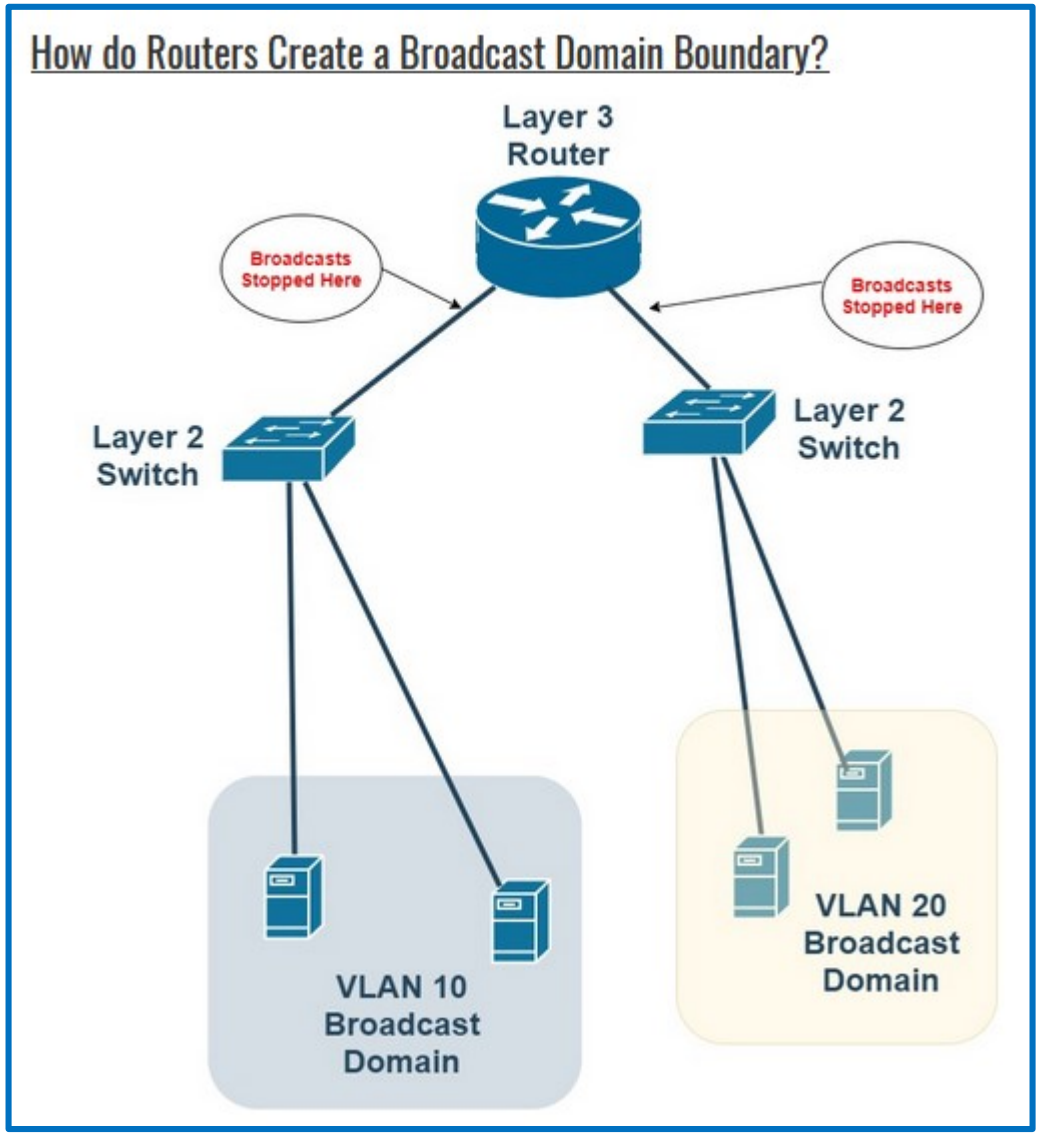
- ❖In terms of network devices, a router is used for creating multiple broadcast domains. This simply means that each router interface is considered as a border of each broadcast domain. Therefore a router interface is the boundary of the broadcast domain.
- ❖Routers can be quite expensive, which means you cannot rely on using many routers to create multiple broadcast domains. This brings about the concept of VLANs.
- ❖A mechanism known as Carrier Sense Multiple Access/ Collision Detection (CSMA/CD) is used on LAN segments to detect and prevent collisions from happening.

Source: Collision Domains and Broadcast Domains Explained, URL: https://www.networkstraining.com/collision-domain-vs-broadcast-domain/

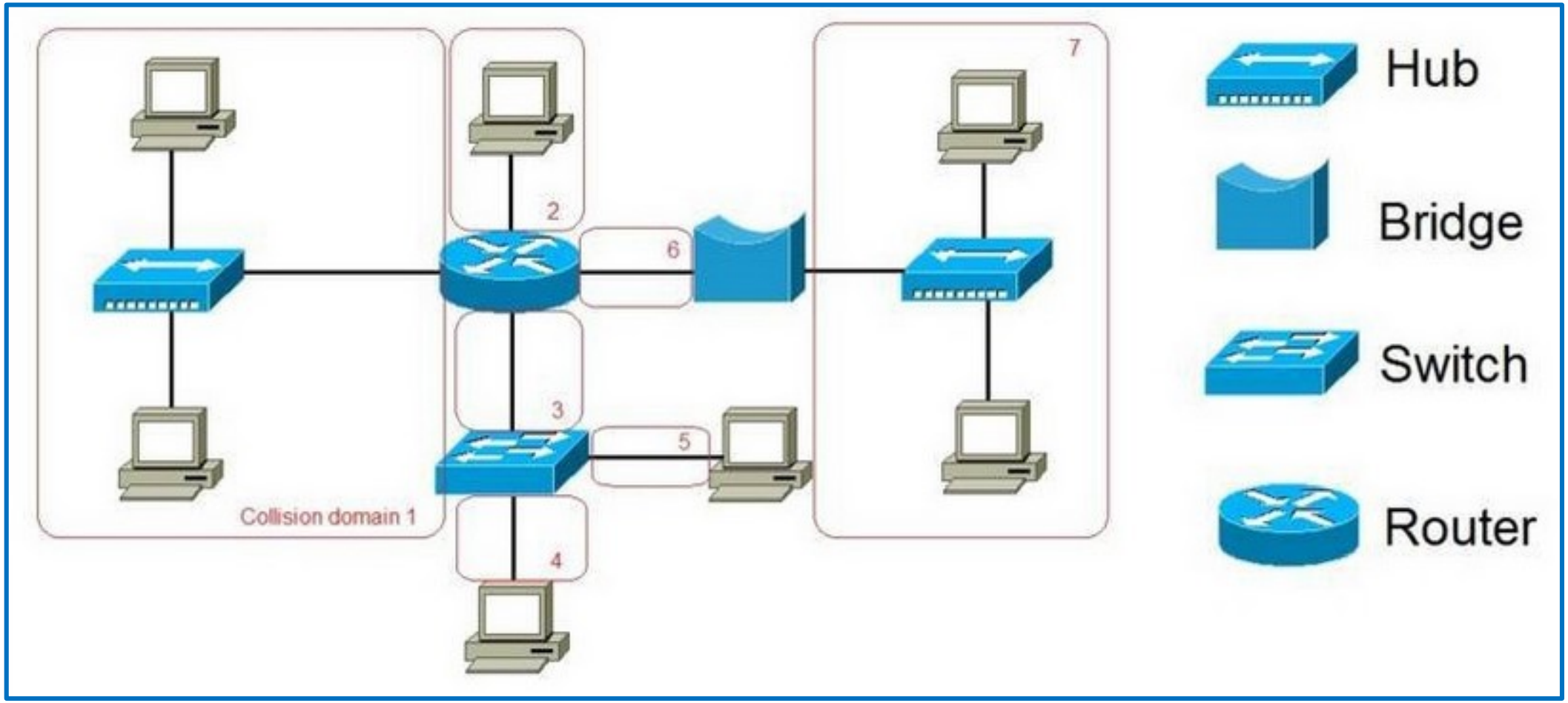
Collision Domains and Broadcast Domains



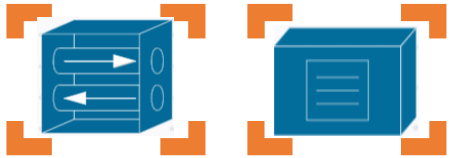




Collision Domains and Broadcast Domains



Collision Domains and Broadcast Domains



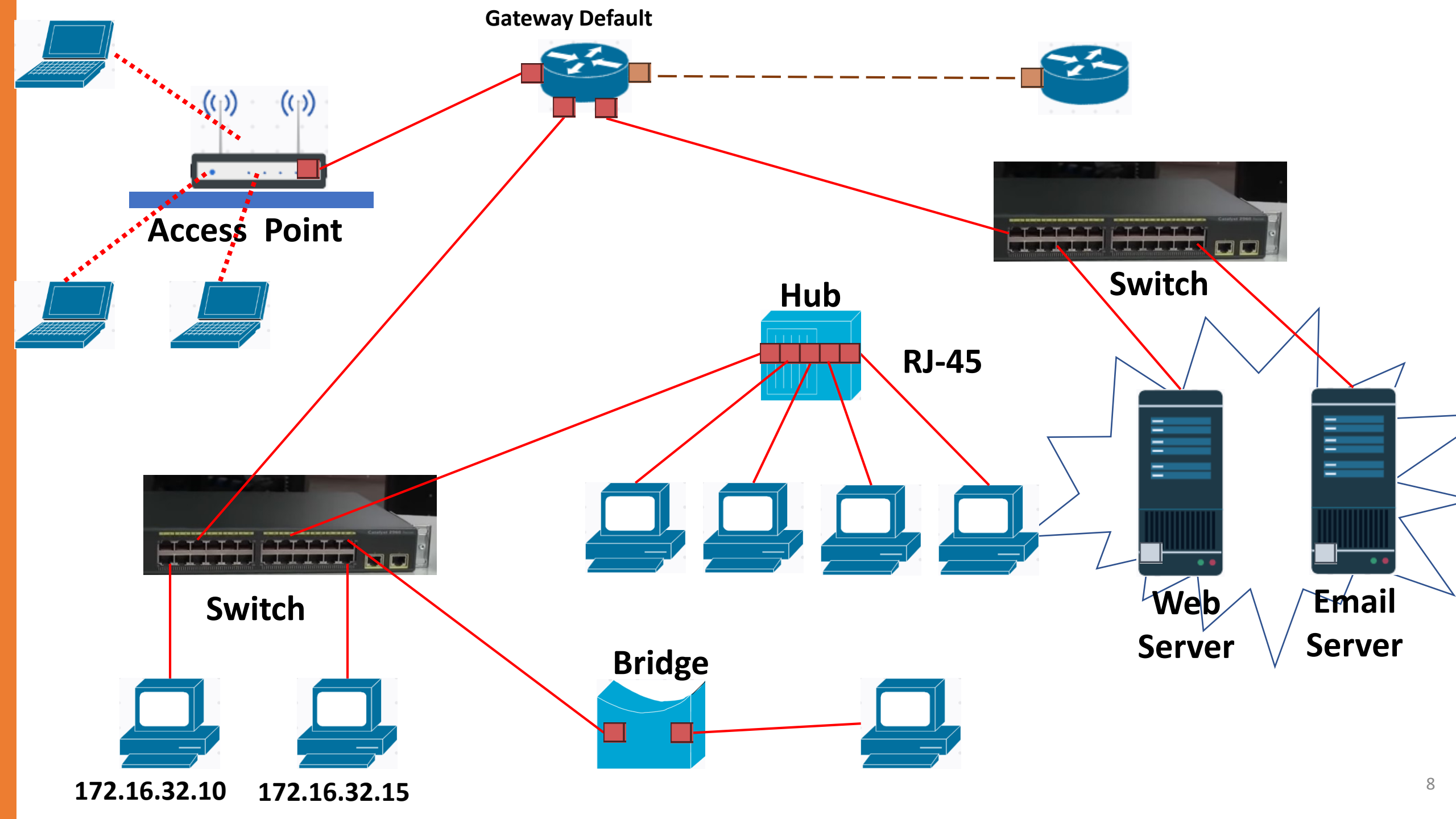
Hubs and Repiters
They forward all the transmitted data in between and thus extend the collision domains. Share all ports in a single collision domain

Switch y Router
They segment the collision domains. Each port is a single collision domain

Bridge
It contains 2 ports so it divides the collision domains by each port

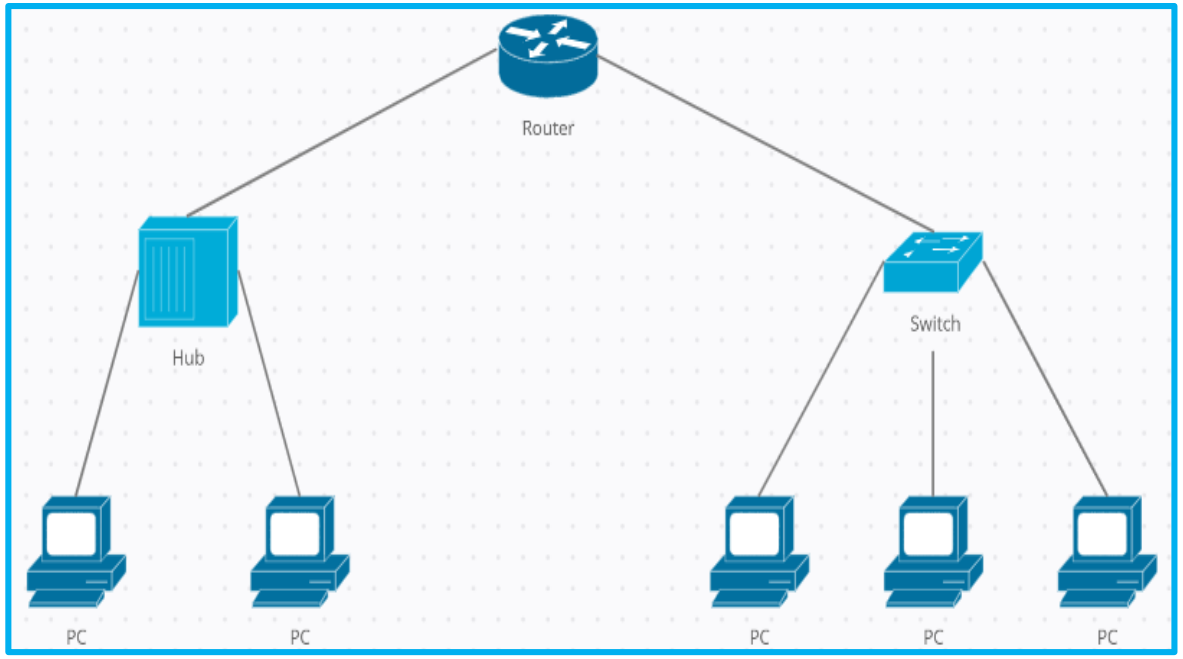
Hub, Switch y Bridge
By default they belong to the same broadcast domain.

Router
They separate or limit broadcast domains for each Ethernet or Serial interface.


Gateway Default
Access Point
Switch
Hub
RJ-45
Switch
Web Server
Email Server
Bridge
172.16.32.10
172.16.32.15

Base o Enunciado

¿Cuál de las siguientes opciones es correcta en la figura mostrada a continuación? (2 opciones)

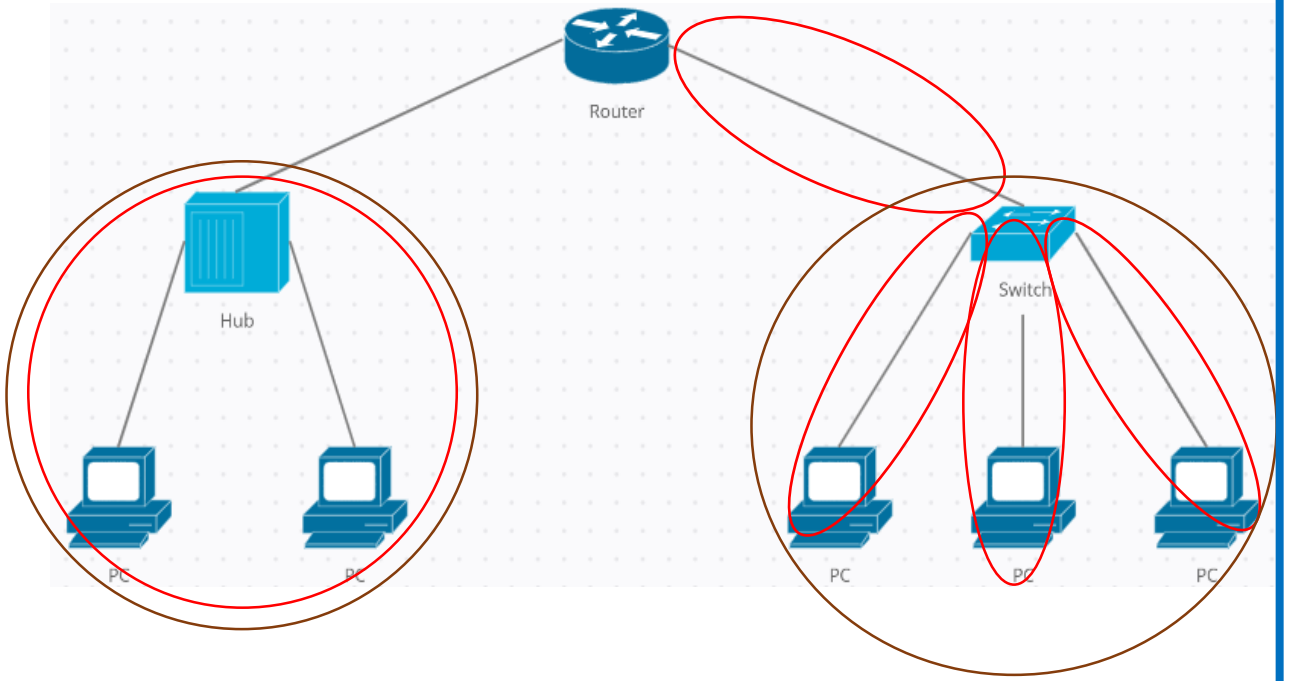


Opciones

a. Existen 2 dominios de broadcast
b. Existen 4 dominios de broadcast
c. Existen 7 dominios de colisión
d. Existen 5 dominios de colisión

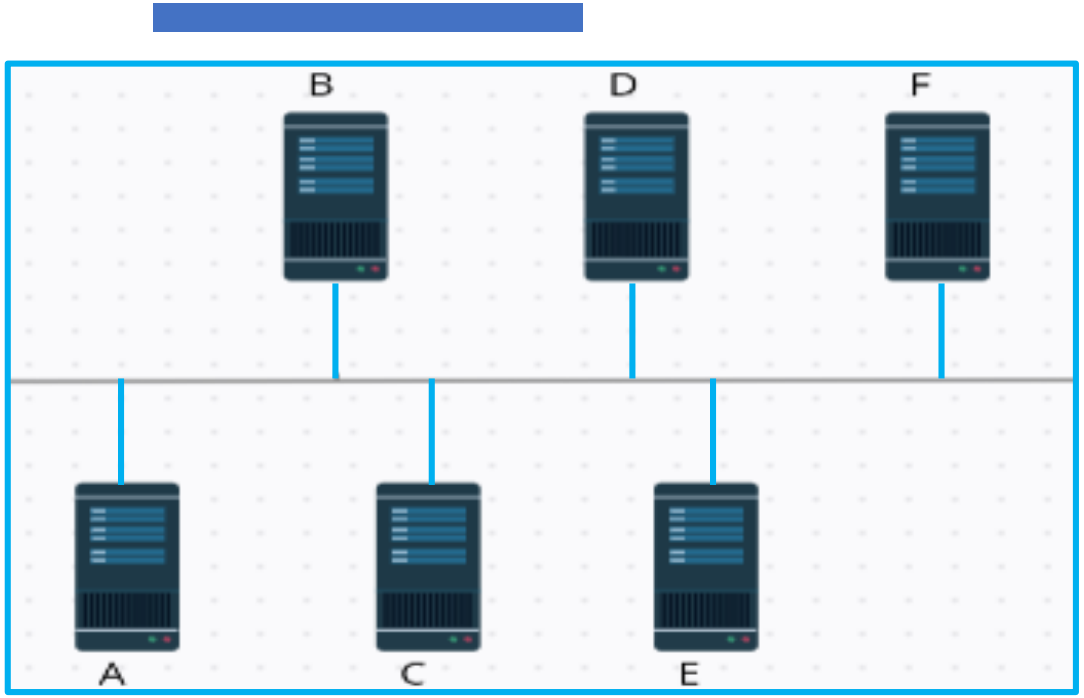
Respuesta

a. Existen 2 dominios de broadcast
b. Existen 5 dominios de colisión



Base o Enunciado

¿Cuál de las siguientes opciones es correcta en la figura mostrada a continuación?



Opciones

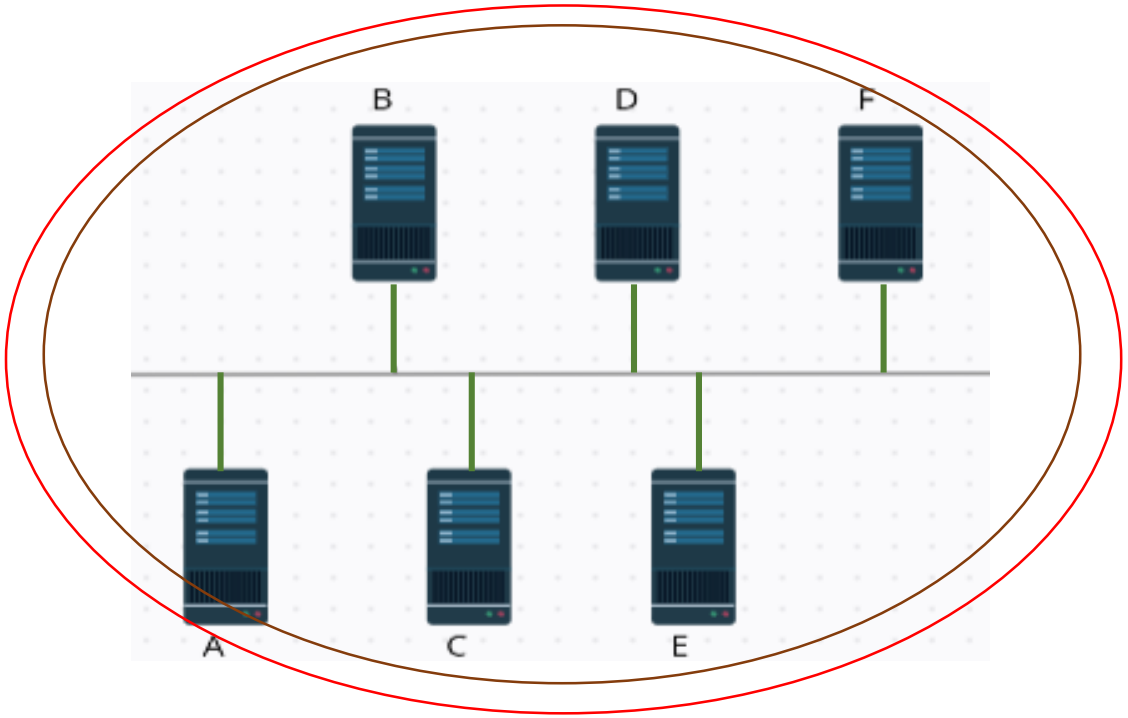
a. Existen 1 dominios de broadcast y 1 dominio de colisión

b. Existen 6 dominios de broadcast y 1 dominio de colisión

c. Existen 1 dominios de broadcast y 6 dominio de colisión

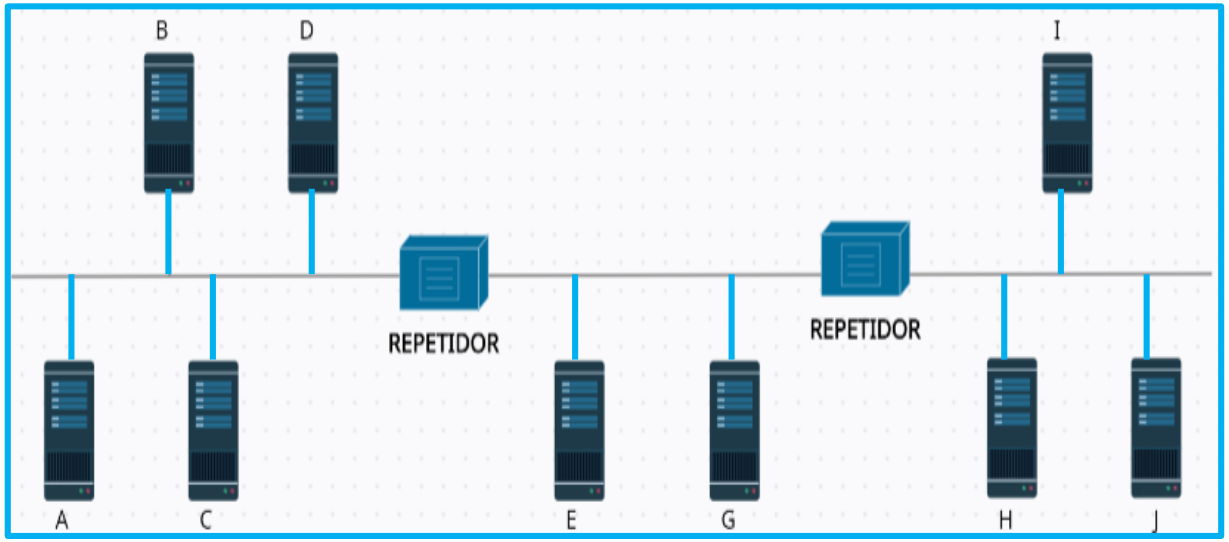
Respuesta

a. Existen 1 dominios de broadcast y 1 dominio de colisión



Base o Enunciado

¿Cuál de las siguientes opciones es correcta en la figura mostrada a continuación?



Opciones

a. Existen 1 dominios de broadcast y 3 dominio de colisión

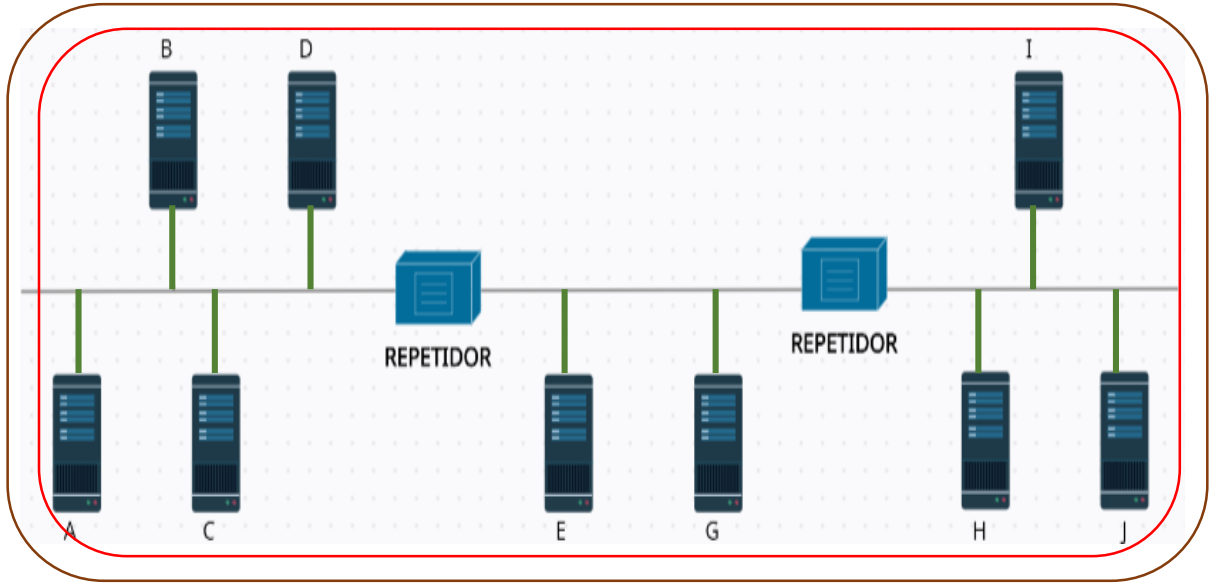
b. Existen 3 dominios de broadcast y 1 dominio de colisión

c. Existen 1 dominios de broadcast y 1 dominio de colisión

d. Existen 9 dominios de broadcast y 3 dominio de colisión

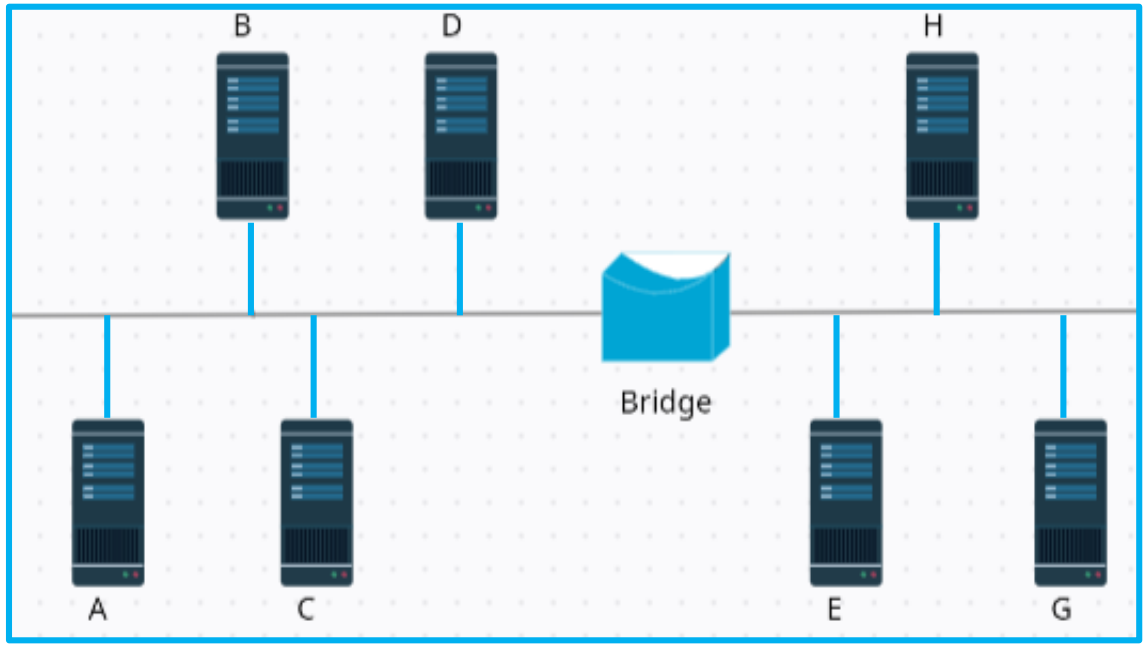
Respuesta

c. Existen 1 dominios de broadcast y 1 dominio de colisión



Base o Enunciado

¿Cuál de las siguientes opciones es correcta en la figura mostrada a continuación? (2 opciones)

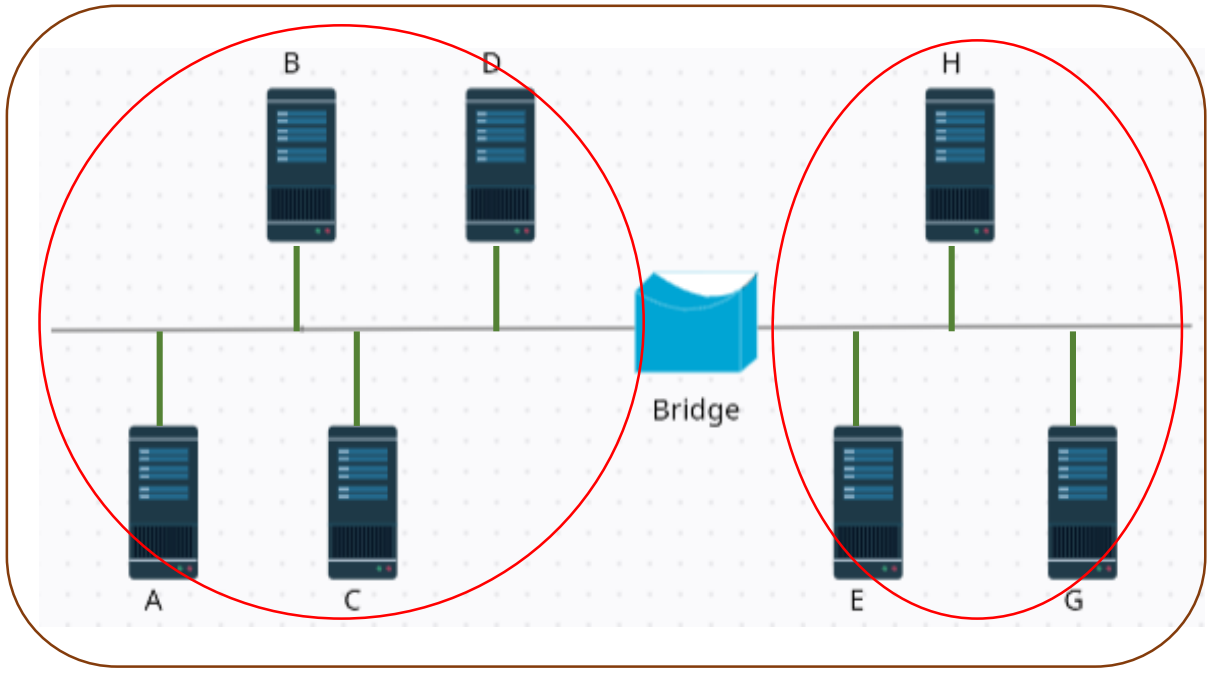


Opciones

a. Existen 2 dominios de broadcast
b. Existen 1 dominios de broadcast
c. Existen 2 dominios de colisión
d. Existen 7 dominios de colisión

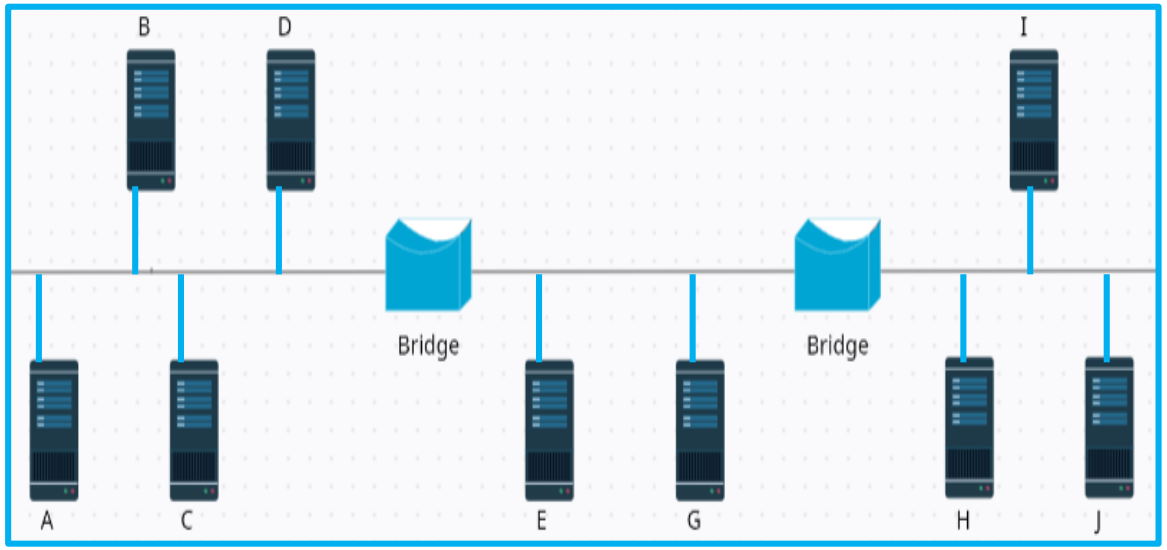
Respuesta

b. Existen 1 dominios de broadcast
c. Existen 2 dominios de colisión



Base o Enunciado

¿Cuál de las siguientes opciones es correcta en la figura mostrada a continuación? (2 opciones)

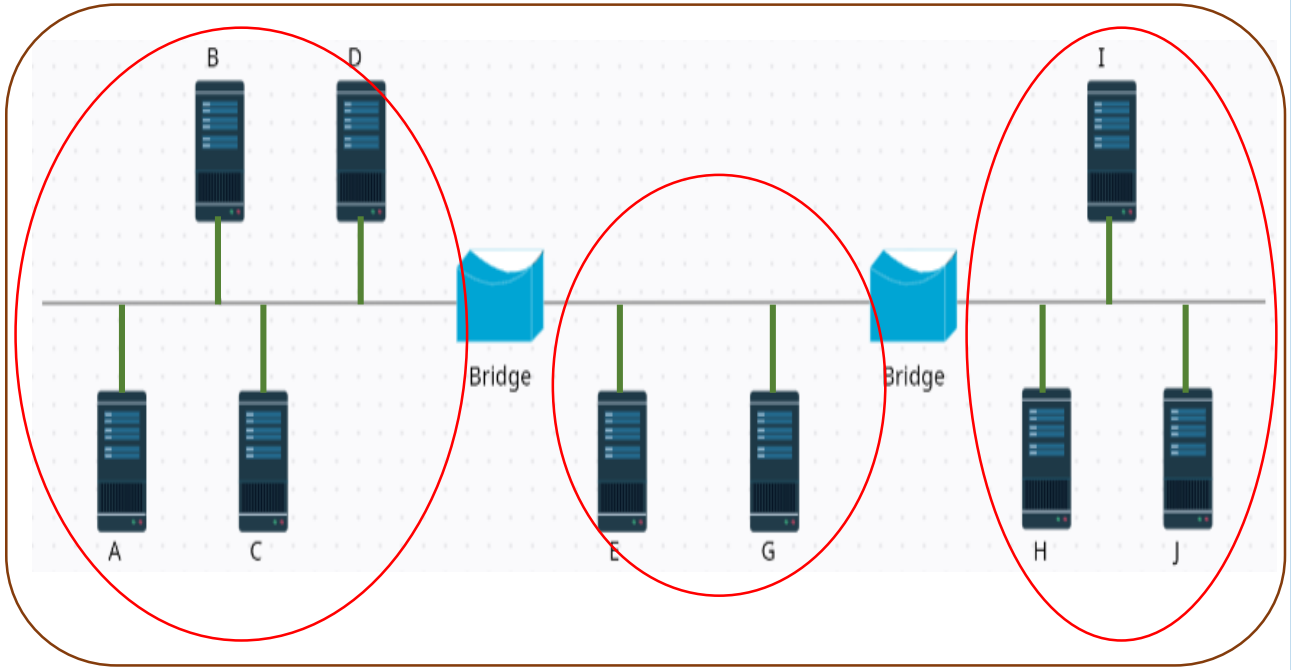


Opciones

a. Existen 1 dominios de broadcast
b. Existen 3 dominios de broadcast
c. Existen 7 dominios de colisión
d. Existen 3 dominios de colisión

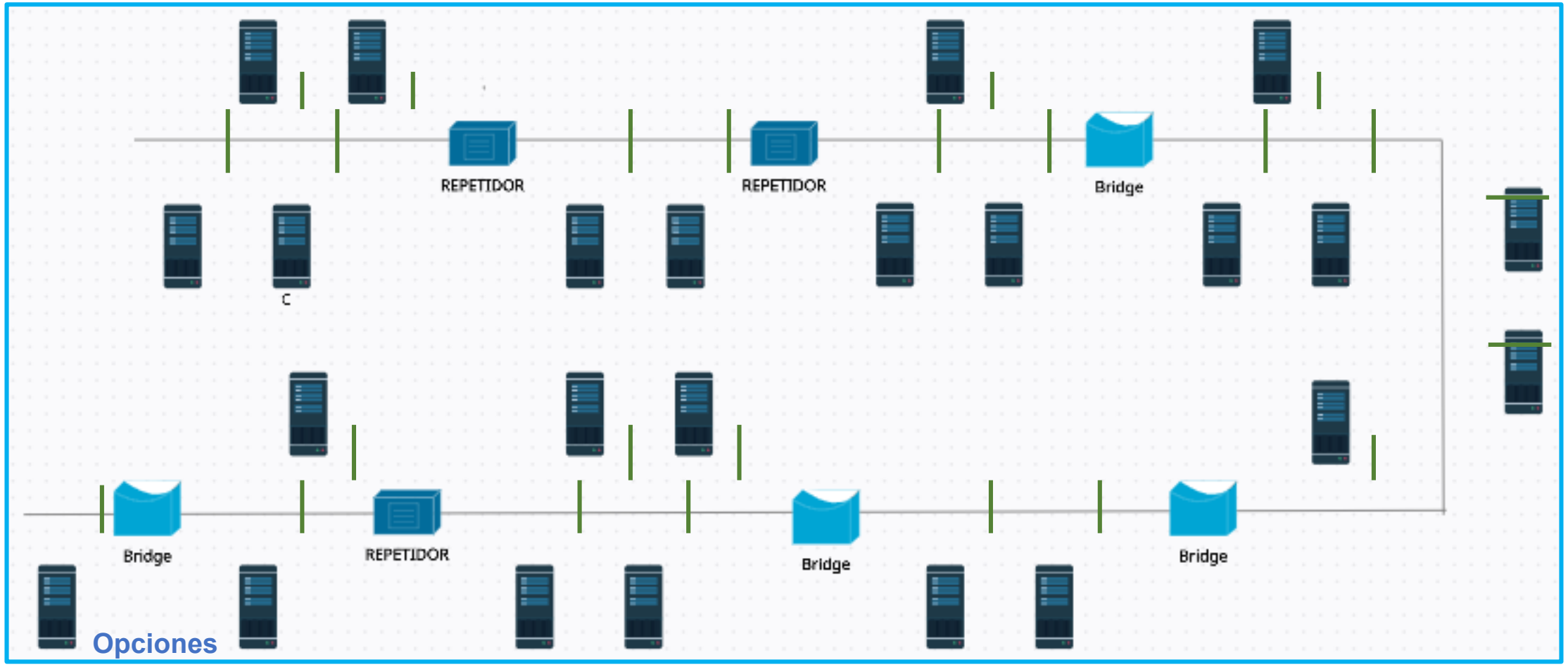
Respuesta

a. Existen 1 dominios de broadcast
d. Existen 3 dominios de colisión



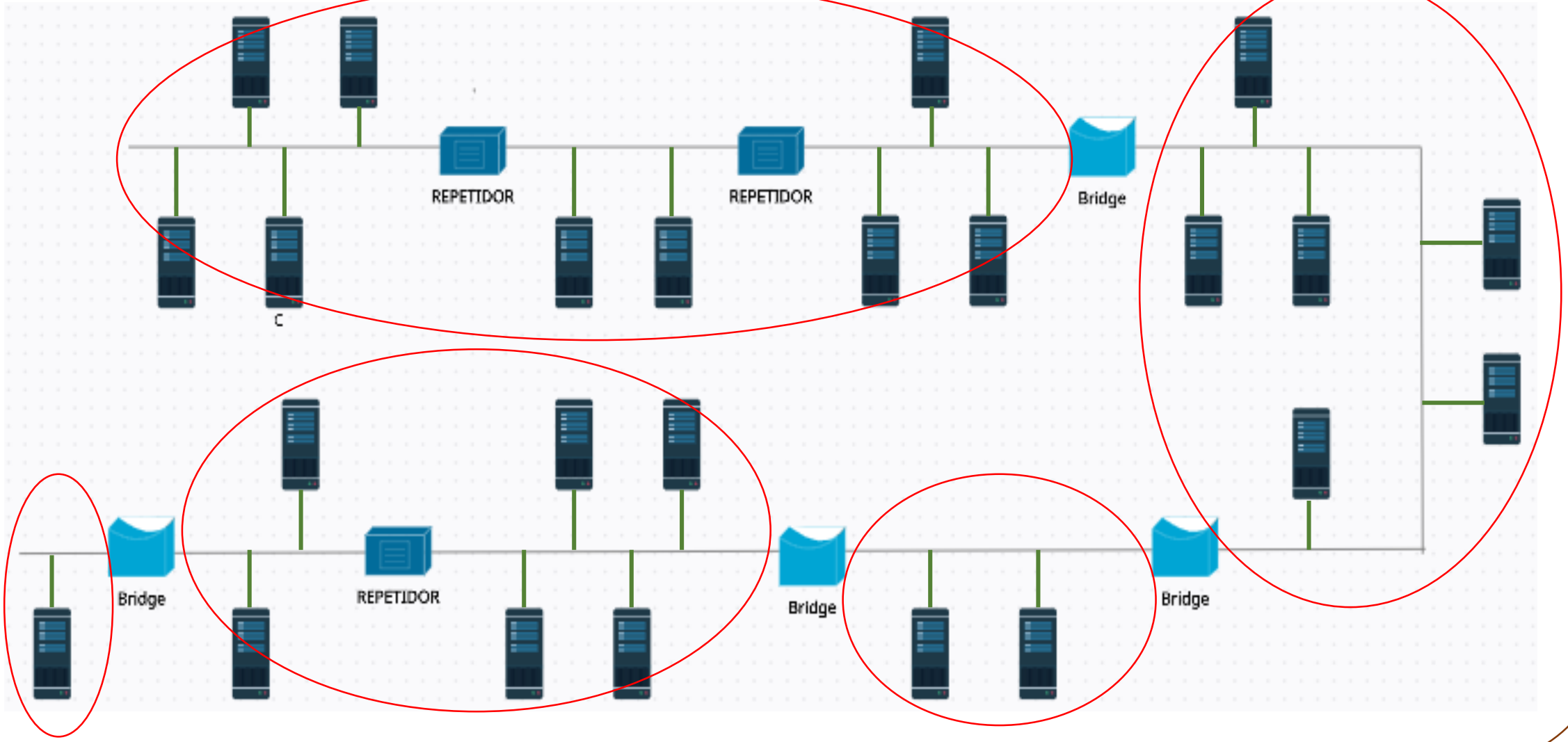
Base o Enunciado

¿Cuál de las siguientes opciones es correcta, elija continuación? (2 opciones)



Opciones

a. Existen 5 dominios de colisión
b. Existen 8 dominios de broadcast
c. Existen 1 dominios de broadcast
d. Existen 4 dominios de colisión



Respuesta

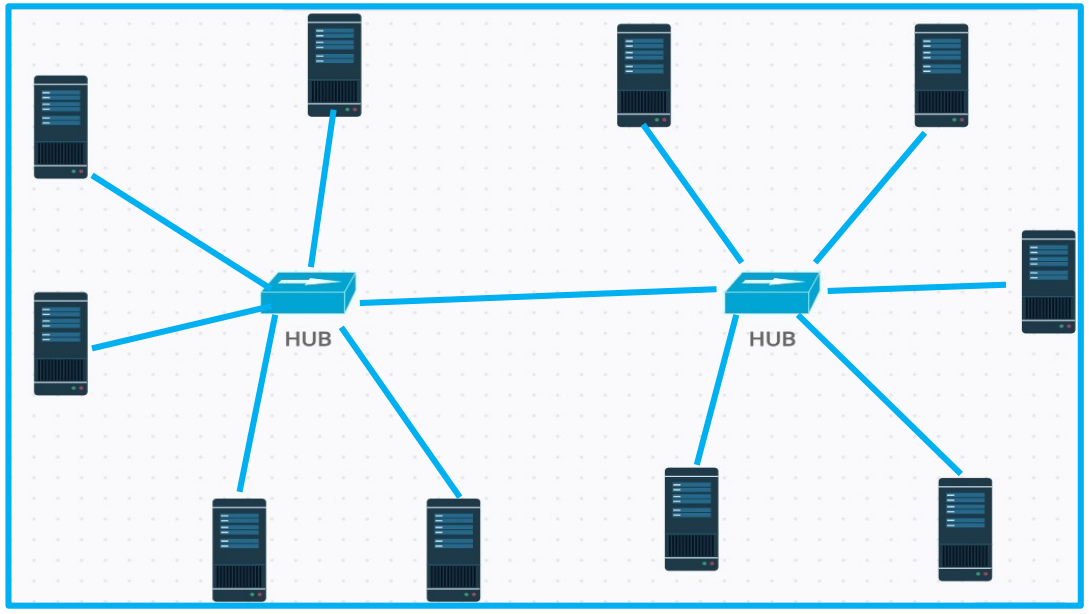
a. Existen 5 dominios de colisión

c. Existen 1 dominios de broadcast

Colisión	
Broadcast	

Base o Enunciado

¿Cuál de las siguientes opciones es correcta en la figura mostrada a continuación?



Opciones

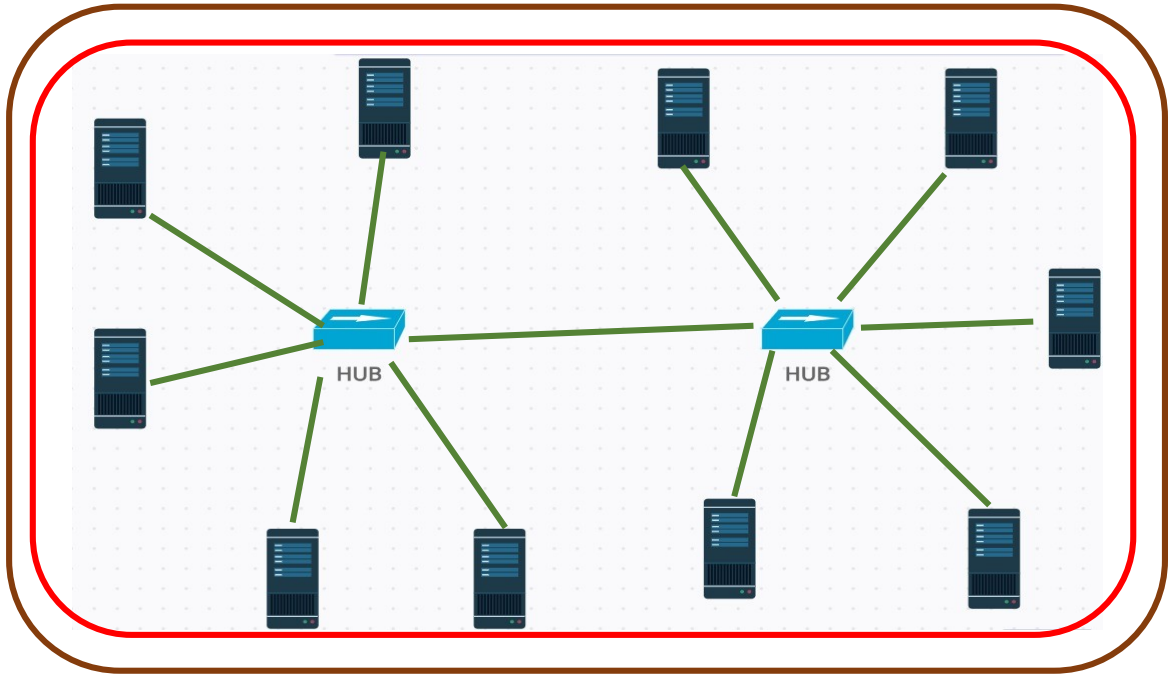
a. Existen 3 dominios de broadcast y 10 dominio de colisión

b. Existen 1 dominios de broadcast y 11 dominio de colisión

c. Existen 1 dominios de broadcast y 1 dominio de colisión

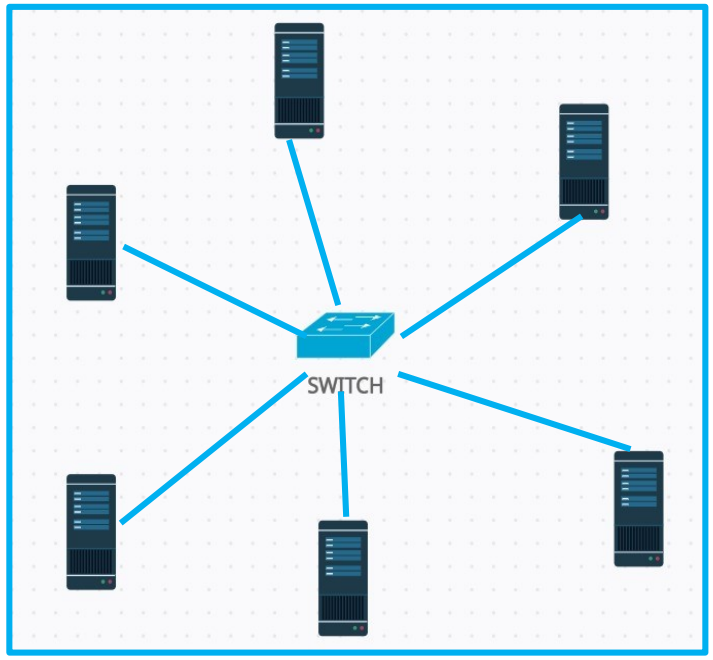
Respuesta

c. Existen 1 dominios de broadcast y 1 dominio de colisión



Base o Enunciado

¿Cuál de las siguientes opciones es correcta en la figura mostrada a continuación?



Opciones

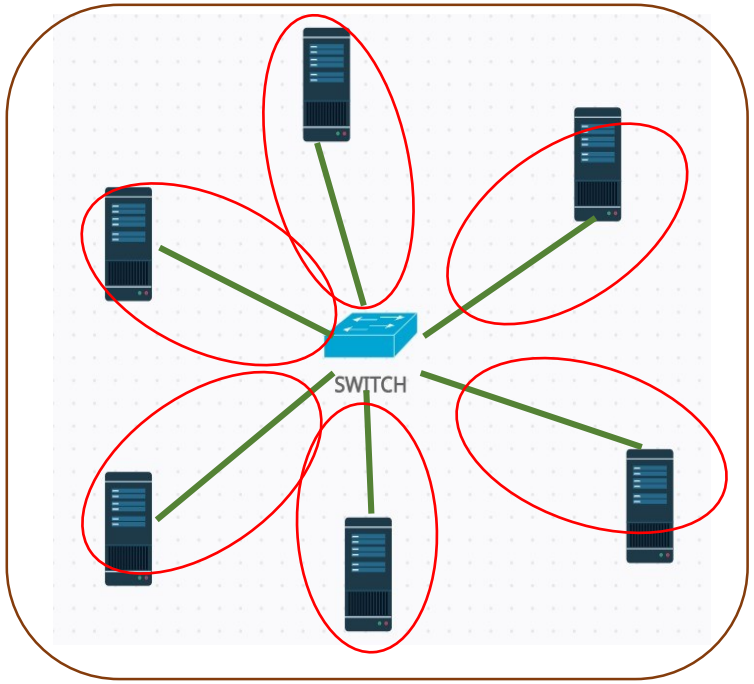
a. Existen 1 dominios de broadcast y 1 dominio de colisión

b. Existen 1 dominios de broadcast y 6 dominio de colisión

c. Existen 6 dominios de broadcast y 1 dominio de colisión

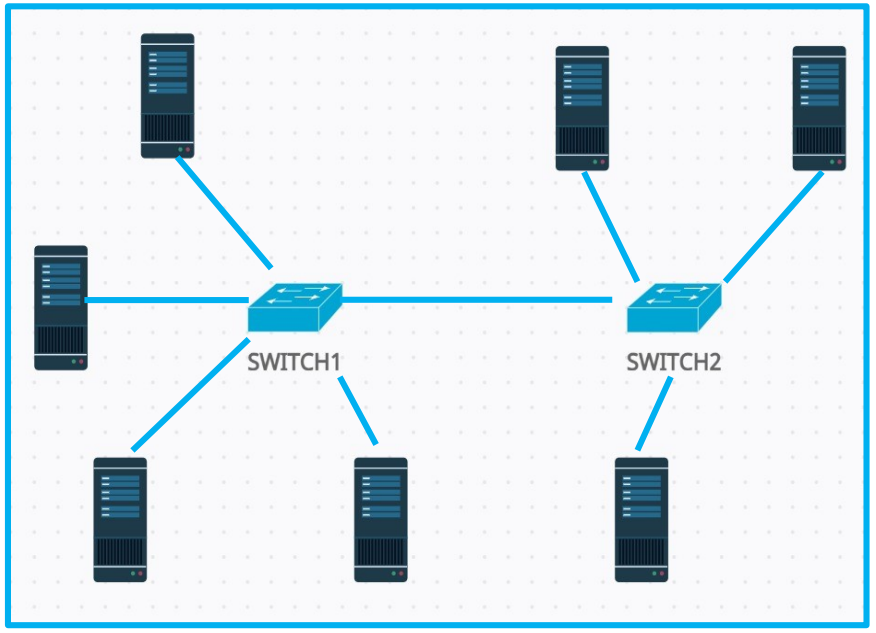
Respuesta

b. Existen 1 dominios de broadcast y 6 dominio de colisión



Base o Enunciado

¿Cuál de las siguientes opciones es correcta en la figura mostrada a continuación? (2 opciones)

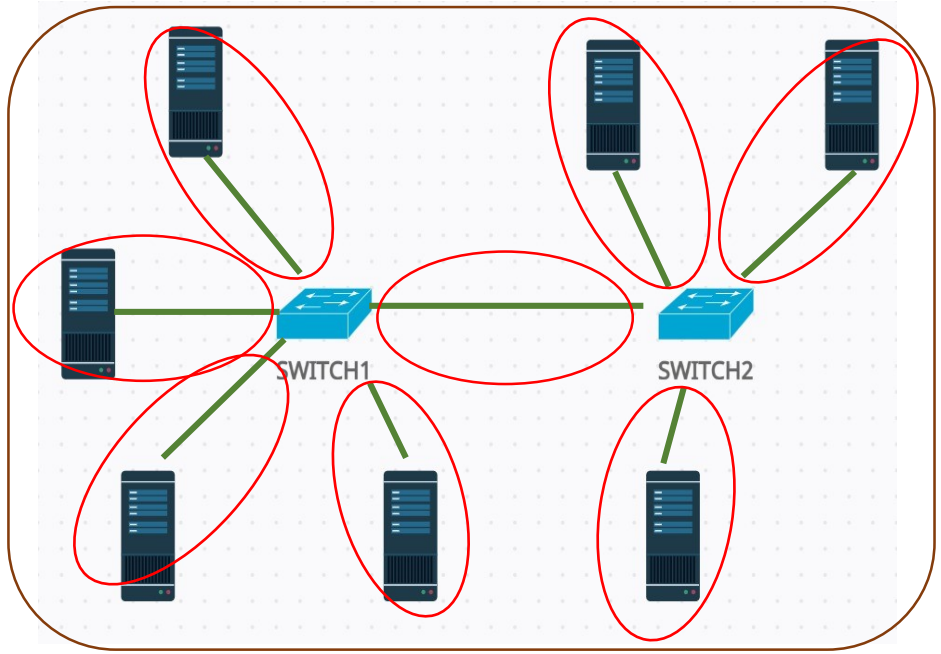


Opciones

a. Existen 1 dominios de broadcast
b. Existen 2 dominios de broadcast
c. Existen 7 dominios de colisión
d. Existen 8 dominios de colisión

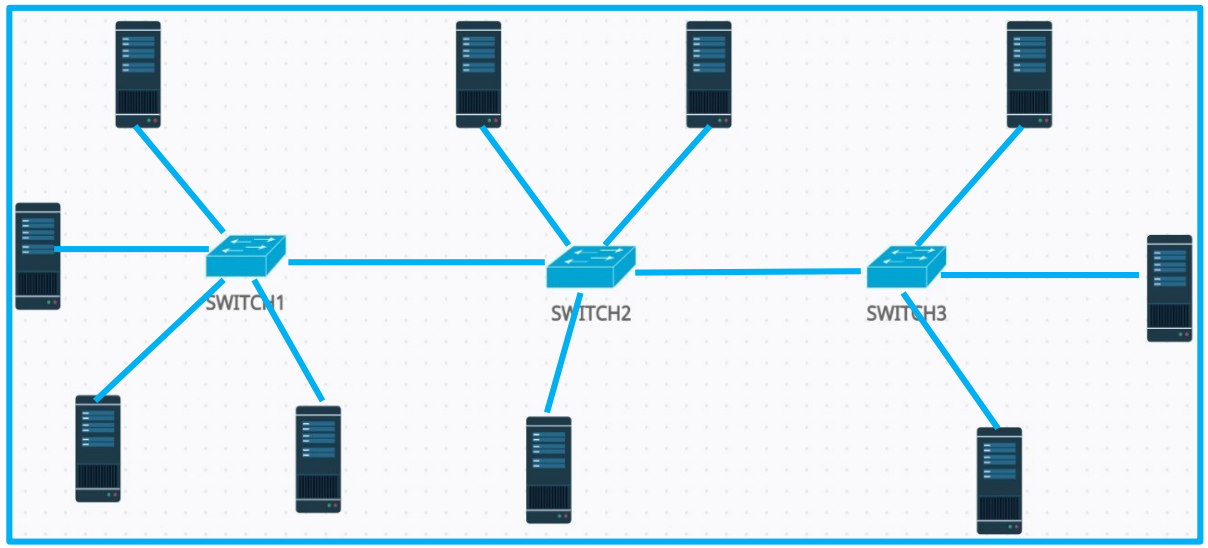
Respuesta

a. Existen 1 dominios de broadcast
c. Existen 8 dominios de colisión



Base o Enunciado

¿Cuál de las siguientes opciones es correcta en la figura mostrada a continuación?



Opciones

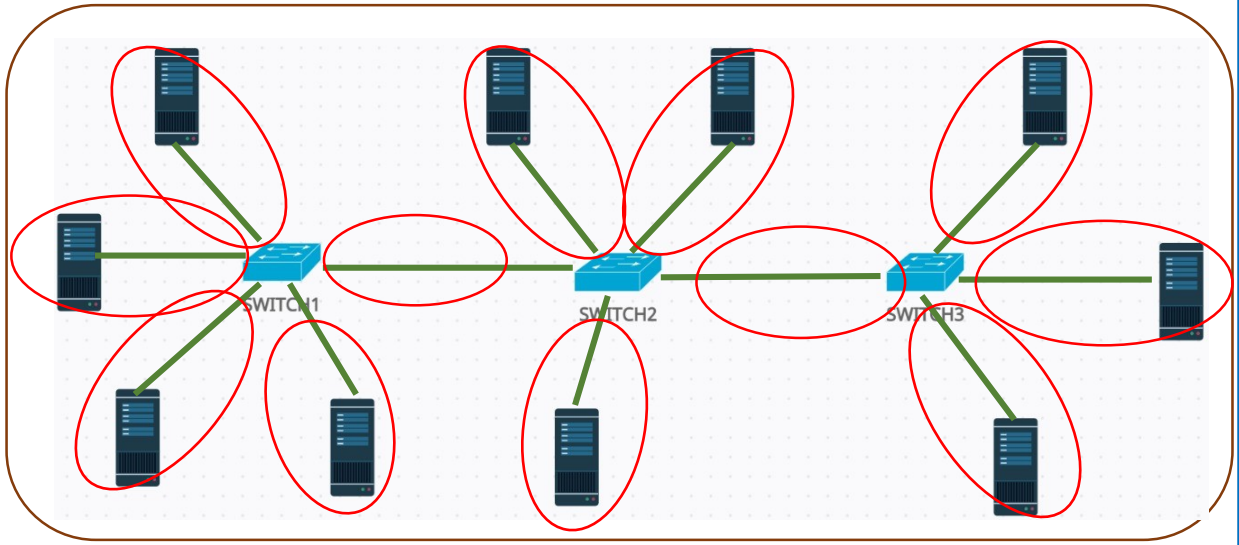
a. Existen 1 dominios de broadcast y 12 dominio de colisión

b. Existen 1 dominios de broadcast y 13 dominio de colisión

c. Existen 3 dominios de broadcast y 10 dominio de colisión

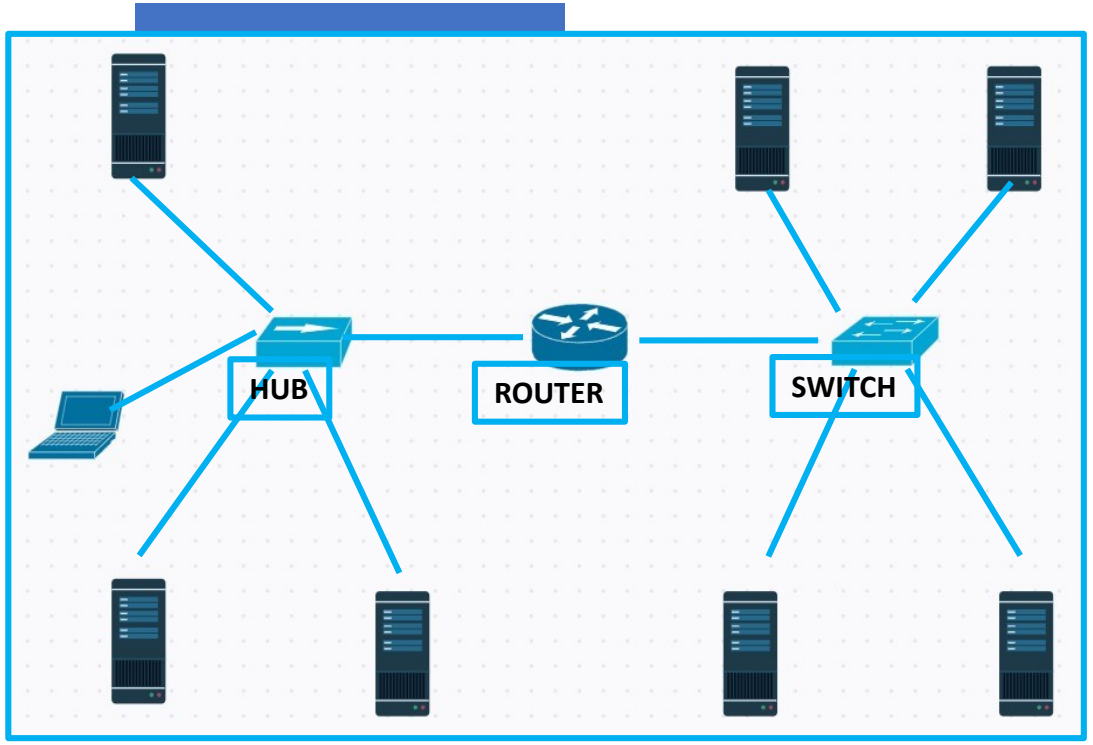
Respuesta

a. Existen 1 dominios de broadcast y 12 dominio de colisión



Base o Enunciado

¿Cuál de las siguientes opciones es correcta en la figura mostrada a continuación? (2 opciones)

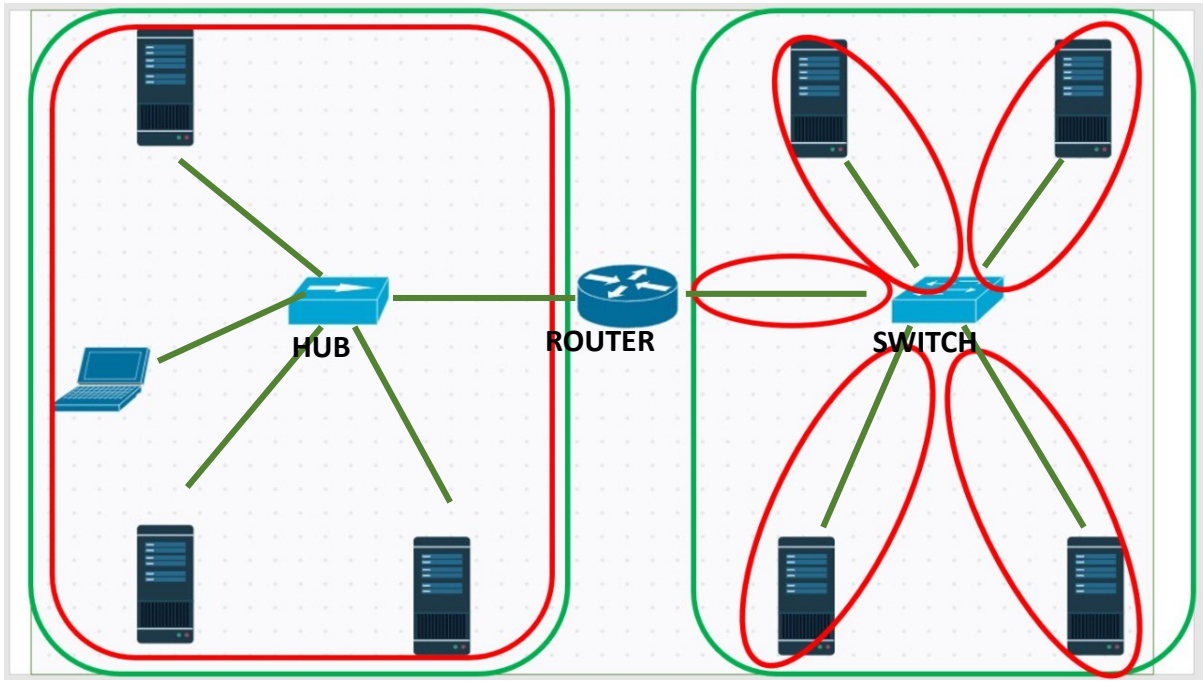


Opciones

a. Existen 1 dominios de broadcast
b. Existen 2 dominios de broadcast
c. Existen 6 dominios de colisión
d. Existen 9 dominios de colisión

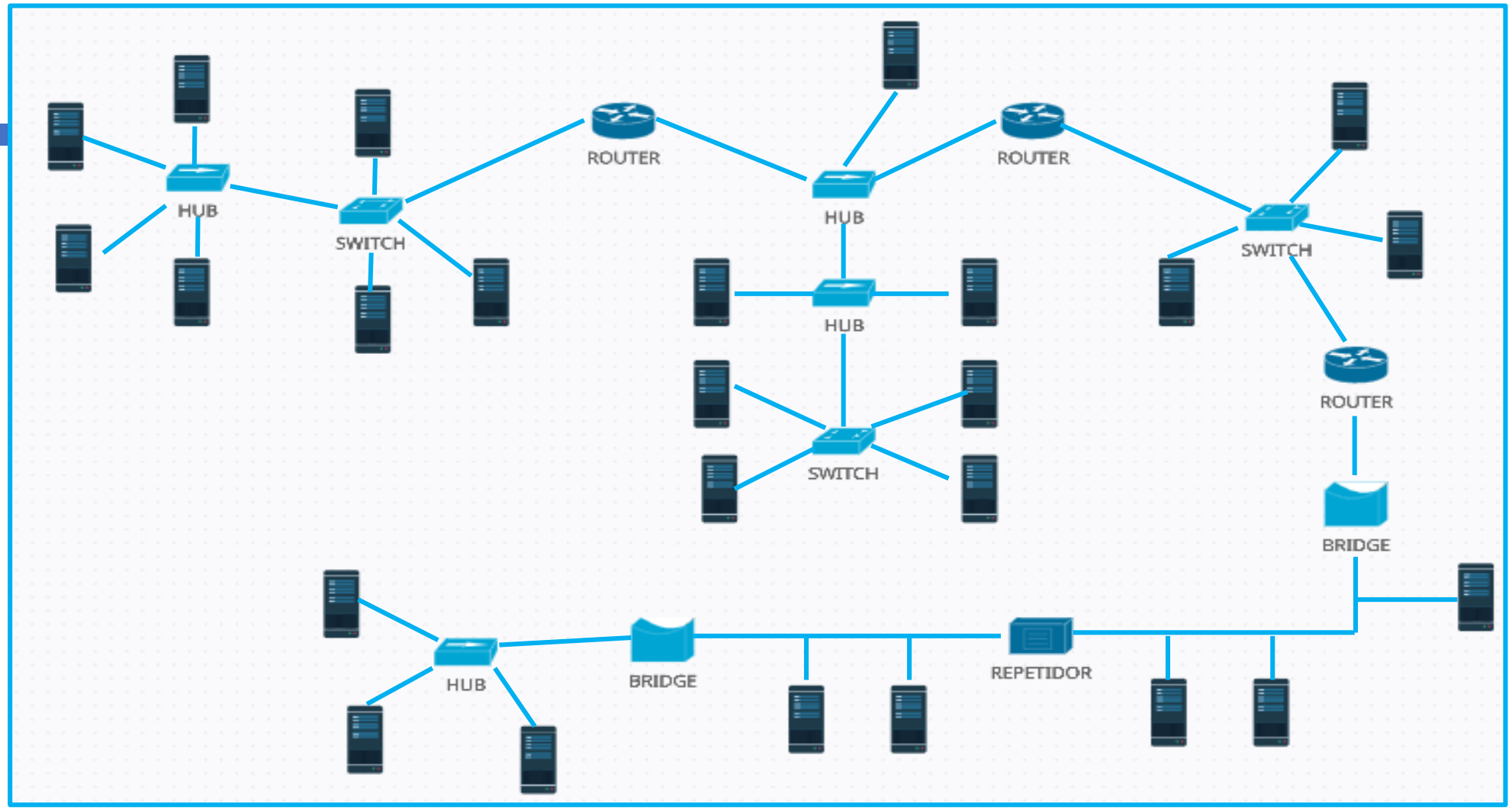
Respuesta

b. Existen 2 dominios de broadcast
c. Existen 6 dominios de colisión



Base o Enunciado

¿Cuál de las siguientes opciones es correcta en esta topología? (2 opciones)

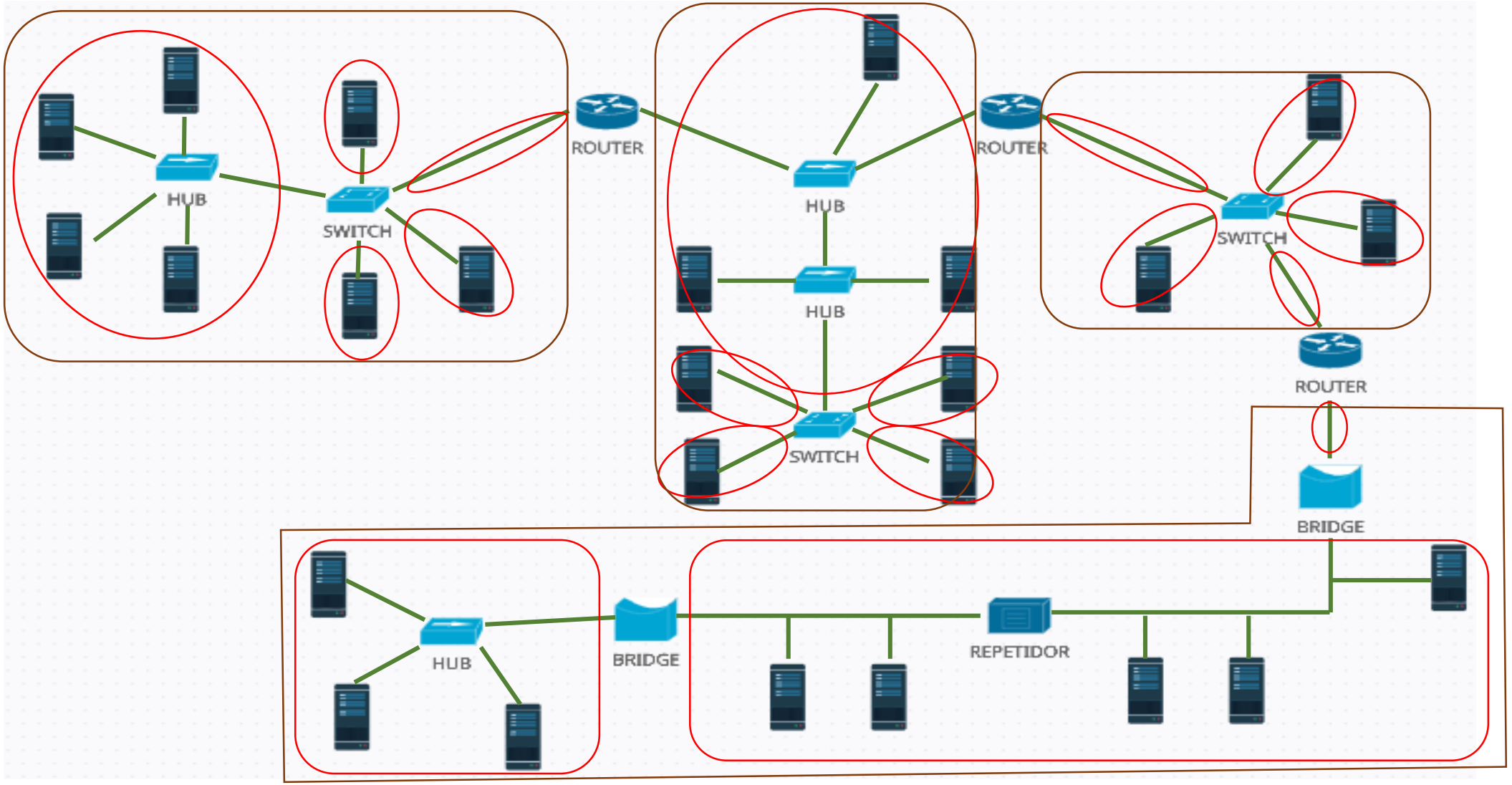


Opciones

a. Existen 4 dominios de broadcast y 18 dominio de colisión

b. Existen 8 dominios de broadcast y 18 dominio de colisión

c. Existen 9 dominios de broadcast y 33 dominio de colisión



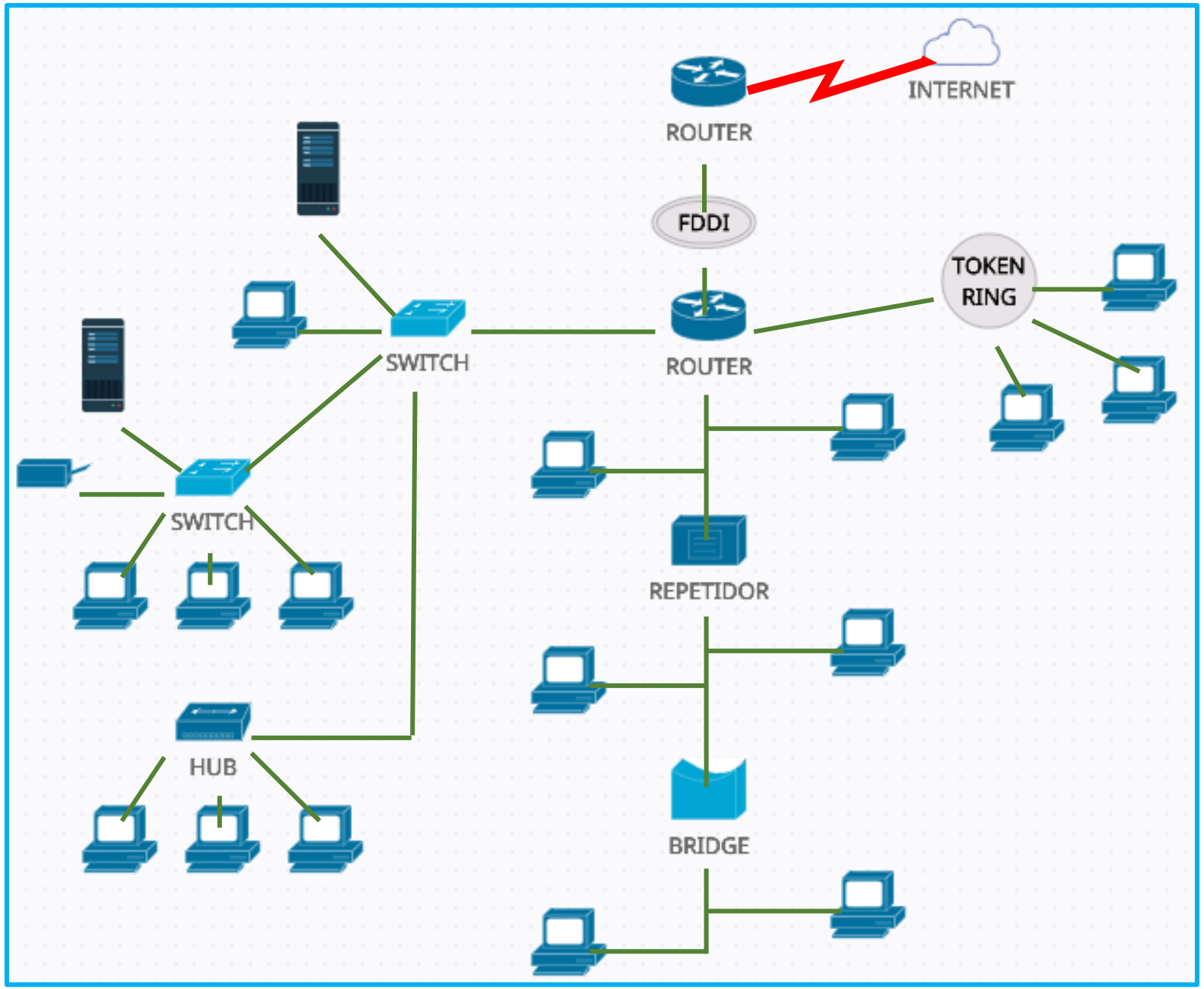
Respuesta

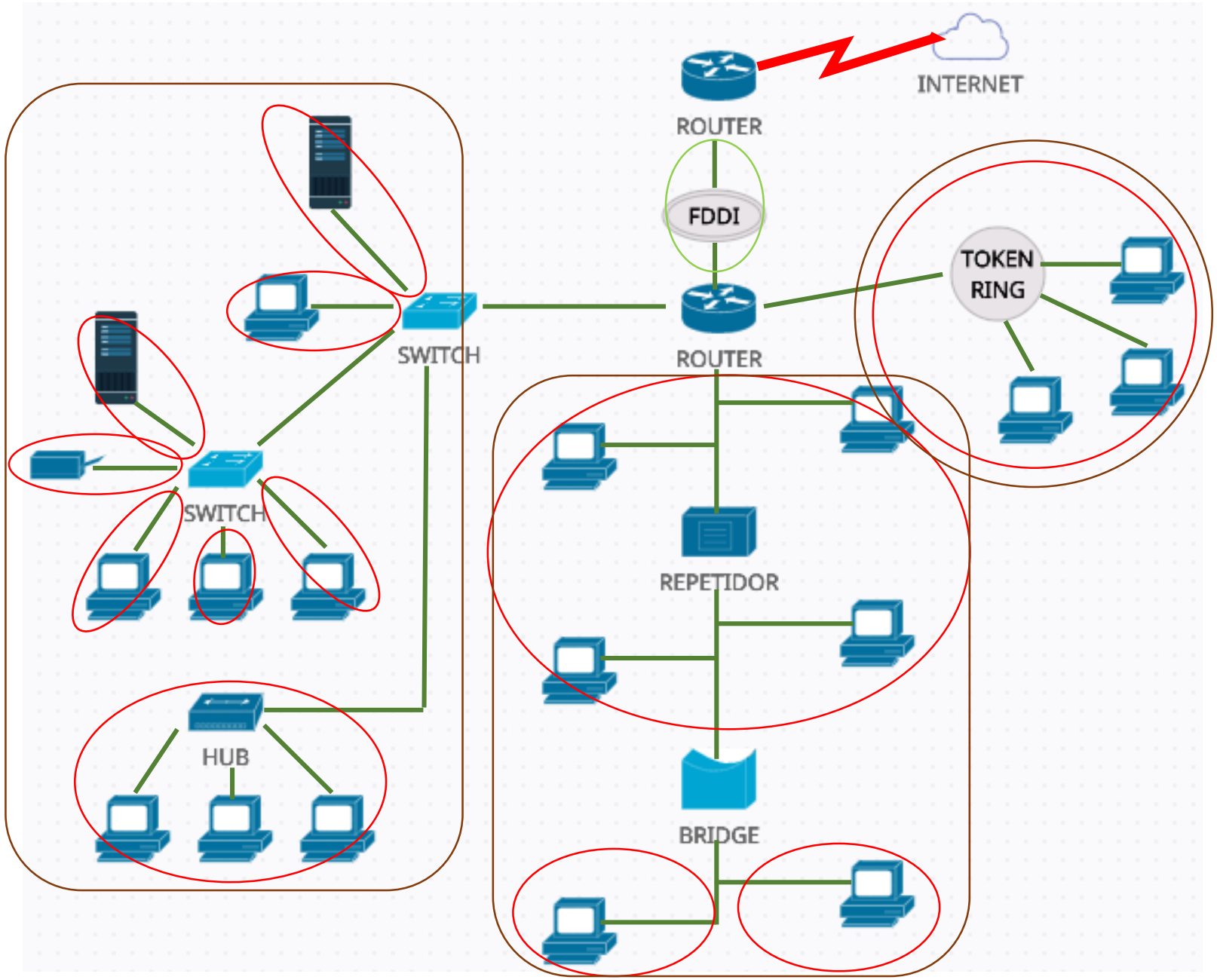
a. Existen 4 dominios de broadcast y 18 dominio de colisión

Colisión	
Broadcast	

Base o Enunciado

¿Cuál de las siguientes opciones es correcta en esta topología? (2 opciones)





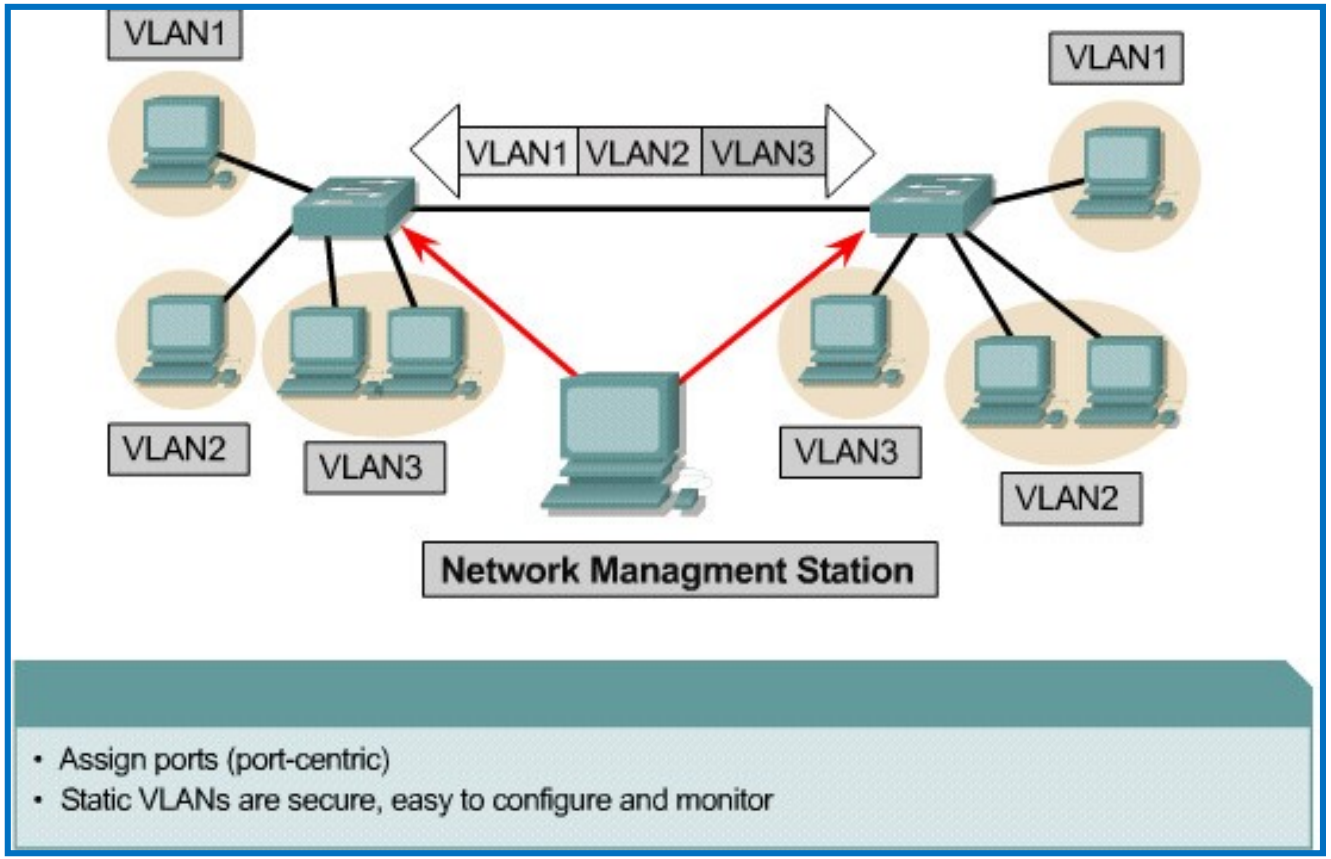
Dominio de Colisión y de Broadcast

- Existen **X** dominios de broadcast
- Existen **Y** dominios de colisión

Colisión	
Broadcast	

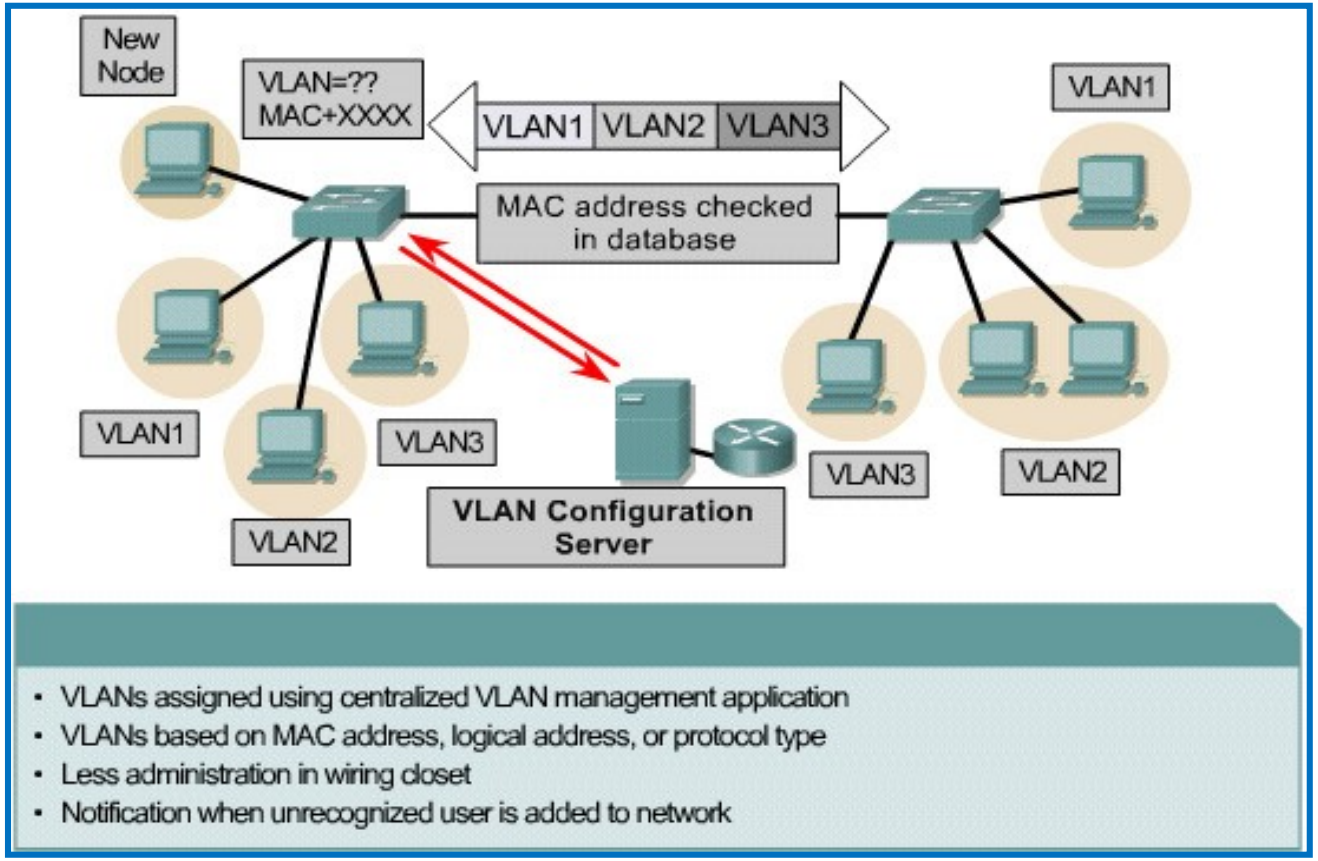
VLAN operation

- Each switch port could be assigned to a different VLAN.
- Ports assigned to the same VLAN share broadcasts.
- Ports that do not belong to that VLAN do not share these broadcasts.
- Users attached to the same shared segment, share the bandwidth of that segment.
- Each additional user attached to the shared medium means less bandwidth and deterioration of network performance.
- VLANs offer more bandwidth to users than a shared network.
- The default VLAN for every port in the switch is the management VLAN.

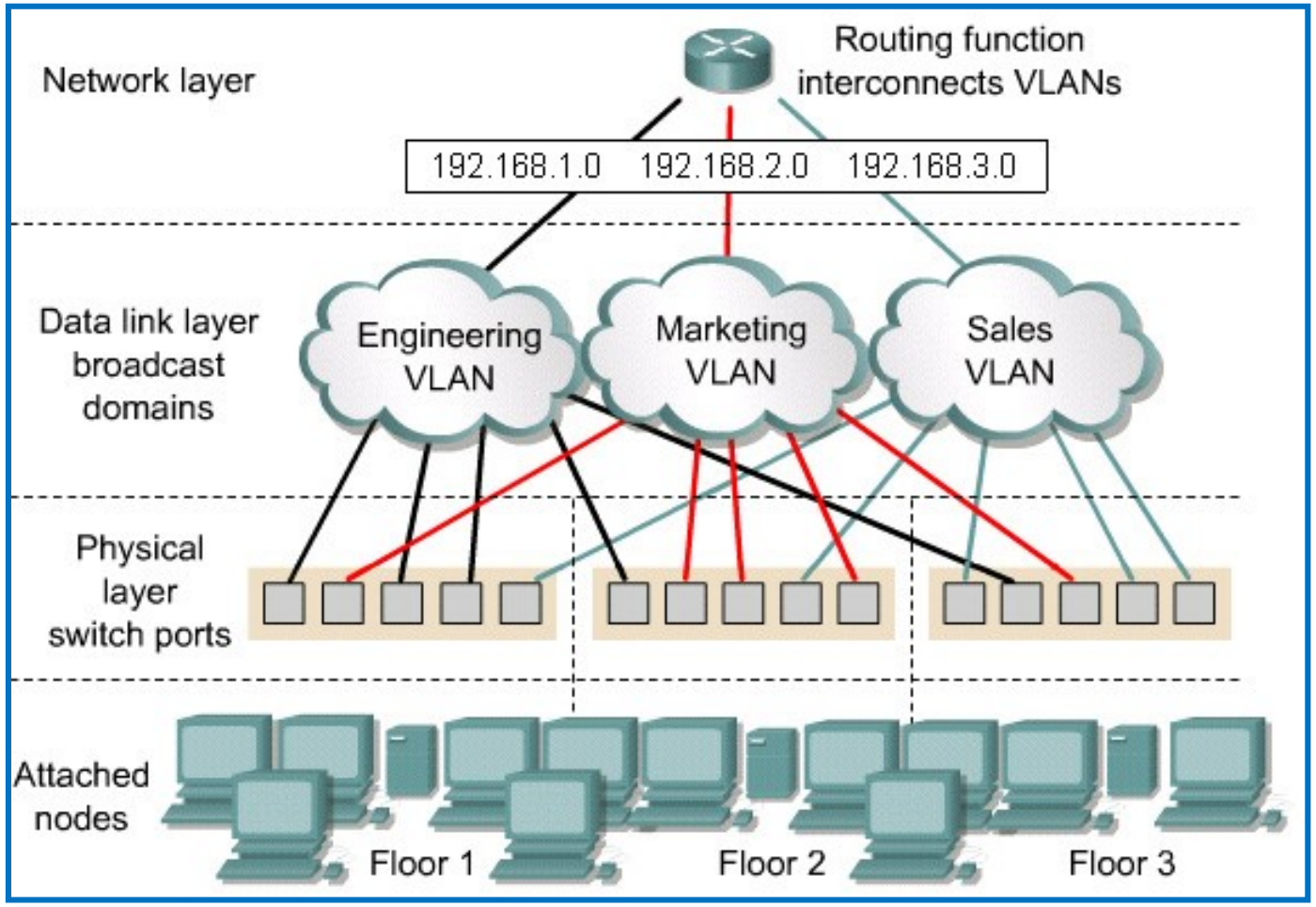


VLAN operation

- The management VLAN is always VLAN 1 and may not be deleted. All other ports on the switch may be reassigned to alternate VLANs.
- Dynamic VLANs allow for membership based on the MAC address of the device connected to the switch port.
- As a device enters the network, it queries a database within the switch for a VLAN membership.
- In port-based or port-centric VLAN membership, the port is assigned to a specific VLAN membership independent of the user or system attached to the port.
- All users of the same port must be in the same VLAN.



VLAN operation

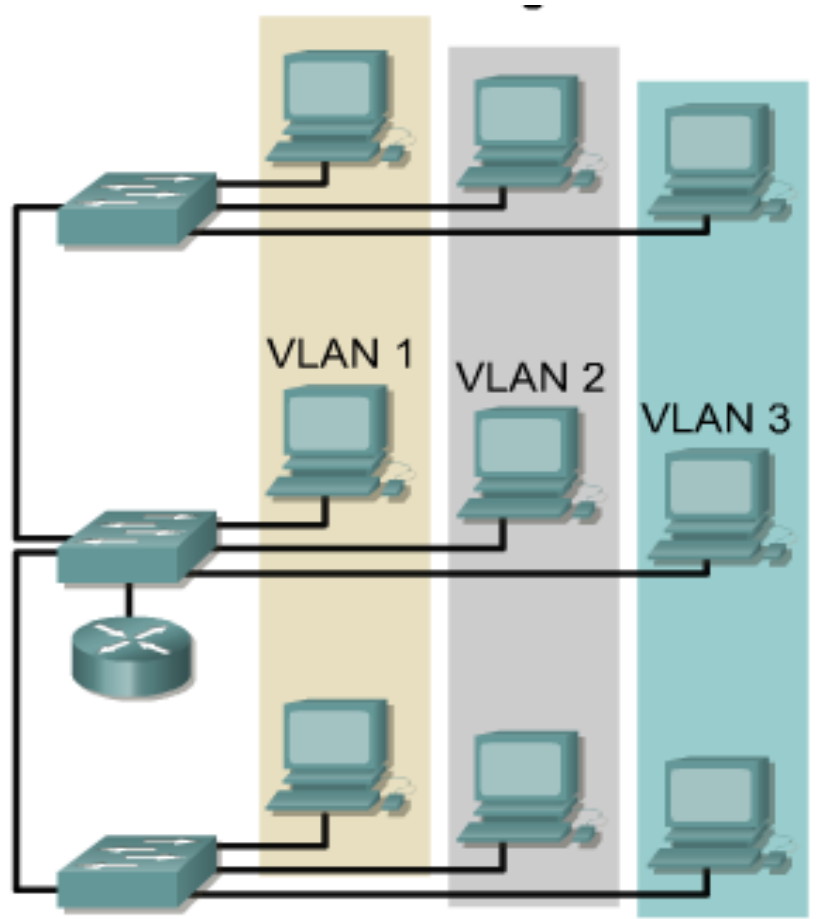


- Network administrators are responsible for configuring VLANs both manually and statically.

Configuring VLANs	Description
Statically	Network administrators configure port-by-port. Each Port is associated with a specific VLAN. The network administrator is responsible for keying in the mappings between the ports and VLANs.
Dynamically	The ports are able to dynamically work out their VLAN configuration. Uses a software database of MAC address to VLAN mappings (which the network administrator must set up first).

VLAN operation-Summary

- It is a method that allows you to create networks that are logically independent, even if they are within the same physical network, even within the same switch.
- In this way, a user could have several VLANs within the same router or switch.
- It could be said that each of these networks groups the computers of a certain network segment.
- VLAN membership can be by role and not by location. VLANs are managed by switches.
- The router is required for inter-VLAN communication.
- All hosts in a VLAN have addresses on the same subnet. A VLAN is a subnet. The transmissions remain within the VLAN. A VLAN is a broadcast domain.



Fuente: Redes Zone. URL: https://www.redeszone.net/2016/11/29/vlans-que-son-tipos-y-para-que-sirven/

VLAN operation-Summary

- The switch has a separate MAC address table for each VLAN.
- Traffic for each VLAN is kept separate from other VLANs.
- Layer 2 switches cannot be routed between VLANs.
- VLAN 1: Default Ethernet LAN, all ports start in this VLAN.
- VLAN 1002 - 1005 automatically created for Token Ring and FDDI.
- Numbers 2 to 1001 can be used for new VLANs
- Up to 255 VLANs on the Catalyst 2960 switch
- Extended range 1006 - 4094 possible but fewer features
- VLAN information is stored in the VLAN database, known as vlan.dat (stored in the switch's flash mem)

- **Static:** Based on the Port or MAC address. They are those that are assigned by the administrator manually.
- **Dynamics:** Assignment is done automatically through software packages, applications or protocol.
- **Of data:** It is a practice to segment user and device traffic (voice traffic, administration traffic)
- **Native:** Assigned to an 802.1Q trunk port.
- **Administration:** Allows access to the administrative capabilities of the switch.
- **Default:** Loads the default configuration at switch startup (POST). VLAN 1 (cisco).

VLAN-Configuration commands

Create VLANs

- ❑Switch(config)#vlan vlan_number
- ❑Switch(config-vlan)#name vlan_name
- ❑Switch(config-vlan)#exit

Assign ports to be members of the VLAN. By default, all ports are members of VLAN 1 at startup. Assign ports individually or as a range. Use the following commands to assign individual ports to VLANs:

- ❑Switch(config)#interface fa x/x
- ❑Switch(config-if)#switchport mode access
- ❑Switch(config-if)#switchport access vlan vlan_number
- ❑Switch(config-if)# exit

Assign a port range to VLAN

- ❑Switch(config)#interface range fa#/start_of_range - end_of_range
- ❑Switch(config-if)#switchport access vlan vlan_number
- ❑Switch(config-if)#exit

Assign port to VLAN

- ❖SW1(config)#**int fa 0/14**
- ❖SW1(config-if)#**switchport mode access**
- ❖SW1(config-if)#**switchport access vlan 20**
- ❖SW1(config-if)#**end**

VLAN-Configuration commands

VLAN Show commands

- ❖show vlan brief (list of VLANs and ports)
- ❖show vlan summary
- ❖show interfaces vlan (up/down, traffic etc)
- ❖Show interfaces fa0/14 switchport (access mode, trunking)

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
20   student                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Remove port from VLAN

- SW1(config)#**int fa 0/14**
- SW1(config-if)#**no switchport access vlan**
- SW1(config-if)#**end**
- The port goes back to VLAN 1.
- If you assign a port to a new VLAN, it is automatically removed from its existing VLAN.

Delete a VLAN

- SW1(config)#**no vlan 20**
- SW1(config)#**end**
- VLAN 20 is deleted.
- Any ports still on VLAN 20 will be inactive – not on any VLAN. They need to be reassigned.

VLAN-Configuration commands

Creating VLANs

Create the VLAN:

```
PxS1# config t
PxS1(config)# vlan 2
PxS1(config-vlan)# name Sales
```

Set VLAN Membership to Interfaces:

```
PxS1(config)# interface f0/1
PxS1(config-if)# switchport mode access
PxS1(config-if)# switchport access vlan 2
PxS1(config-if)# interface f0/2
PxS1(config-if)# switchport mode access
PxS1(config-if)# switchport access vlan 2
```

VLAN Access Port Configuration – Eng VLAN

Access Port Configuration – Eng VLAN

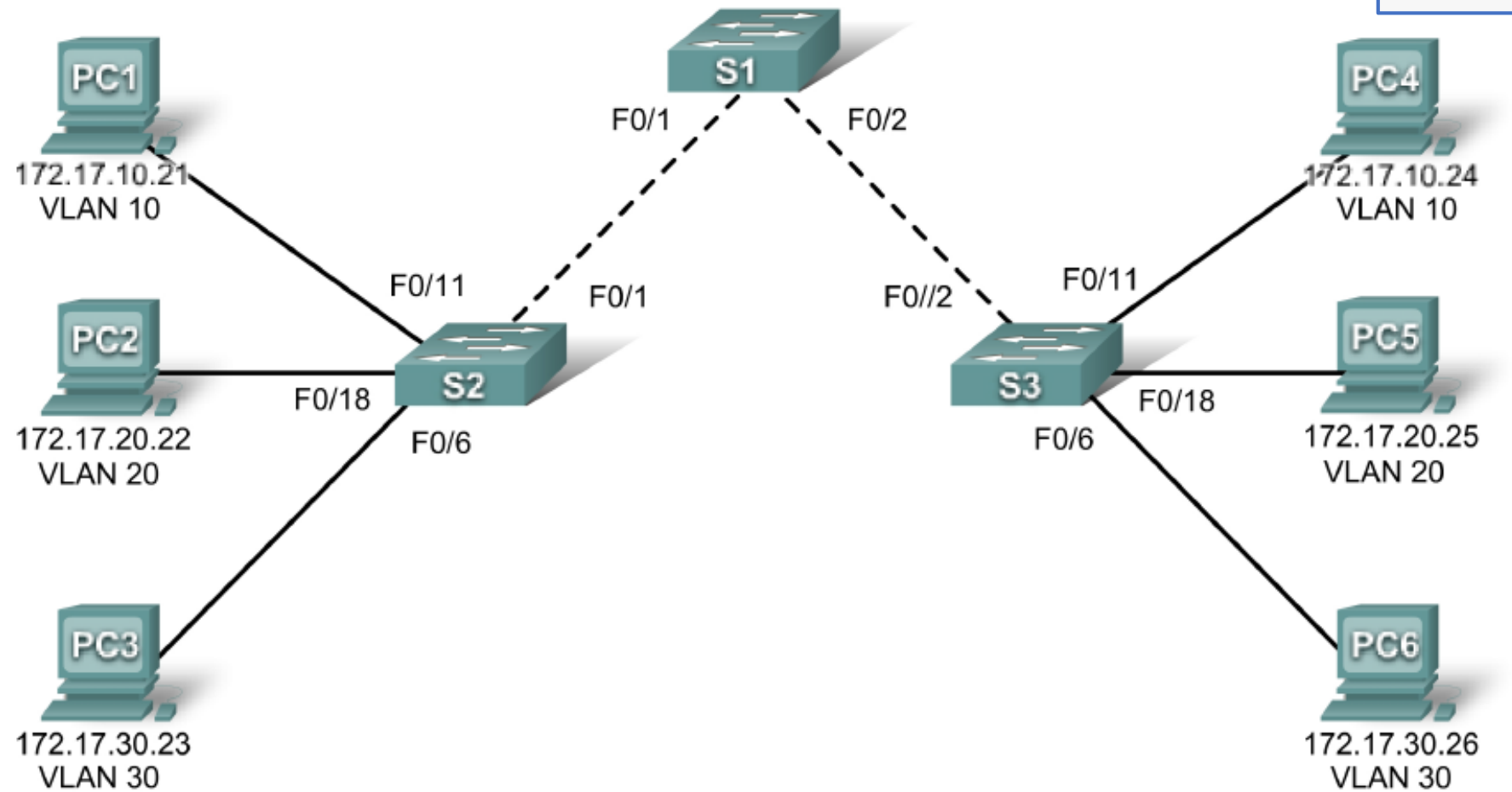
```
SW1(config)#vlan 10
SW1(config-vlan)#name Eng

SW1(config)#interface FastEthernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config)#interface range FastEthernet 0/3 - 5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
```

FLACKBOX
www.flackbox.com

Cisco | Networking Academy®
Mind Wide Open™

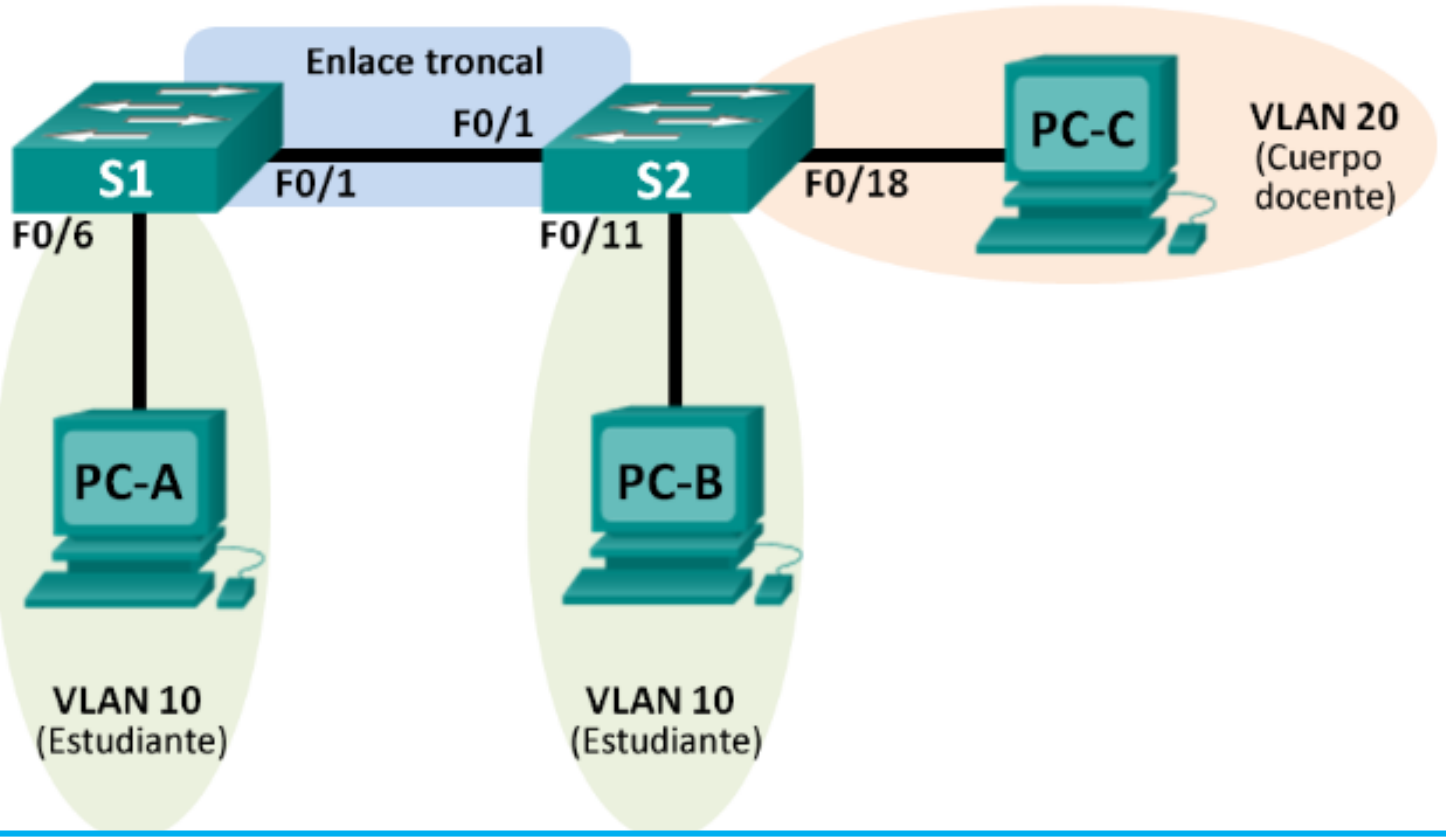
Práctica de laboratorio 3.5.1: Configuración básica de una VLAN

Diagrama de topología



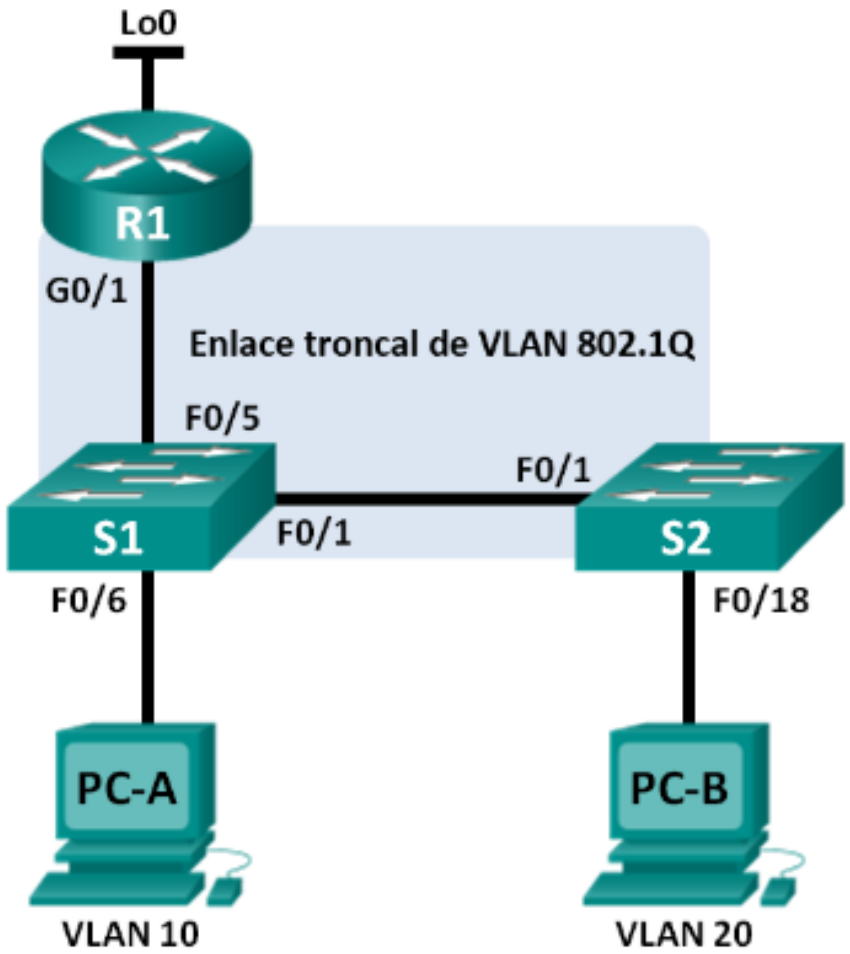
Práctica de laboratorio: configuración de redes VLAN y enlaces troncales

Topología

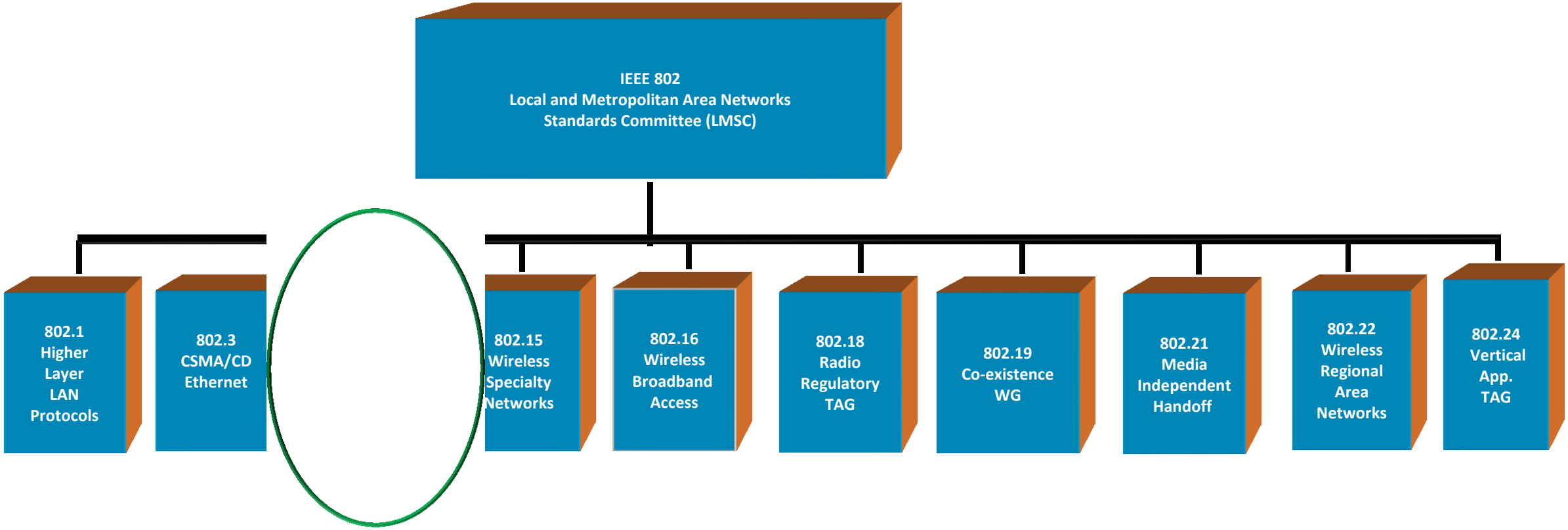


Práctica de laboratorio: configuración de routing entre VLAN basado en enlaces troncales 802.1Q

Topología



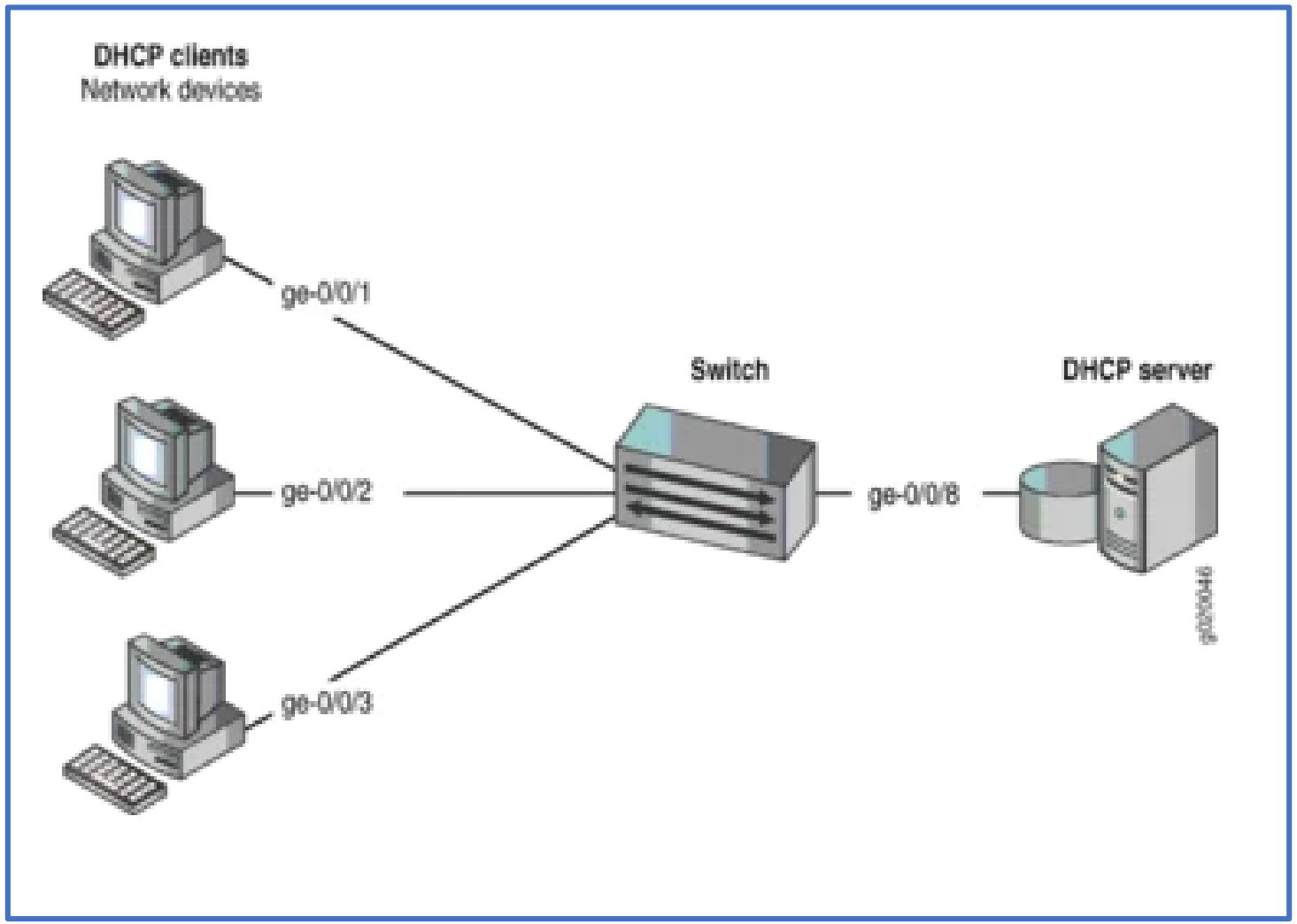
Introducing WLAN



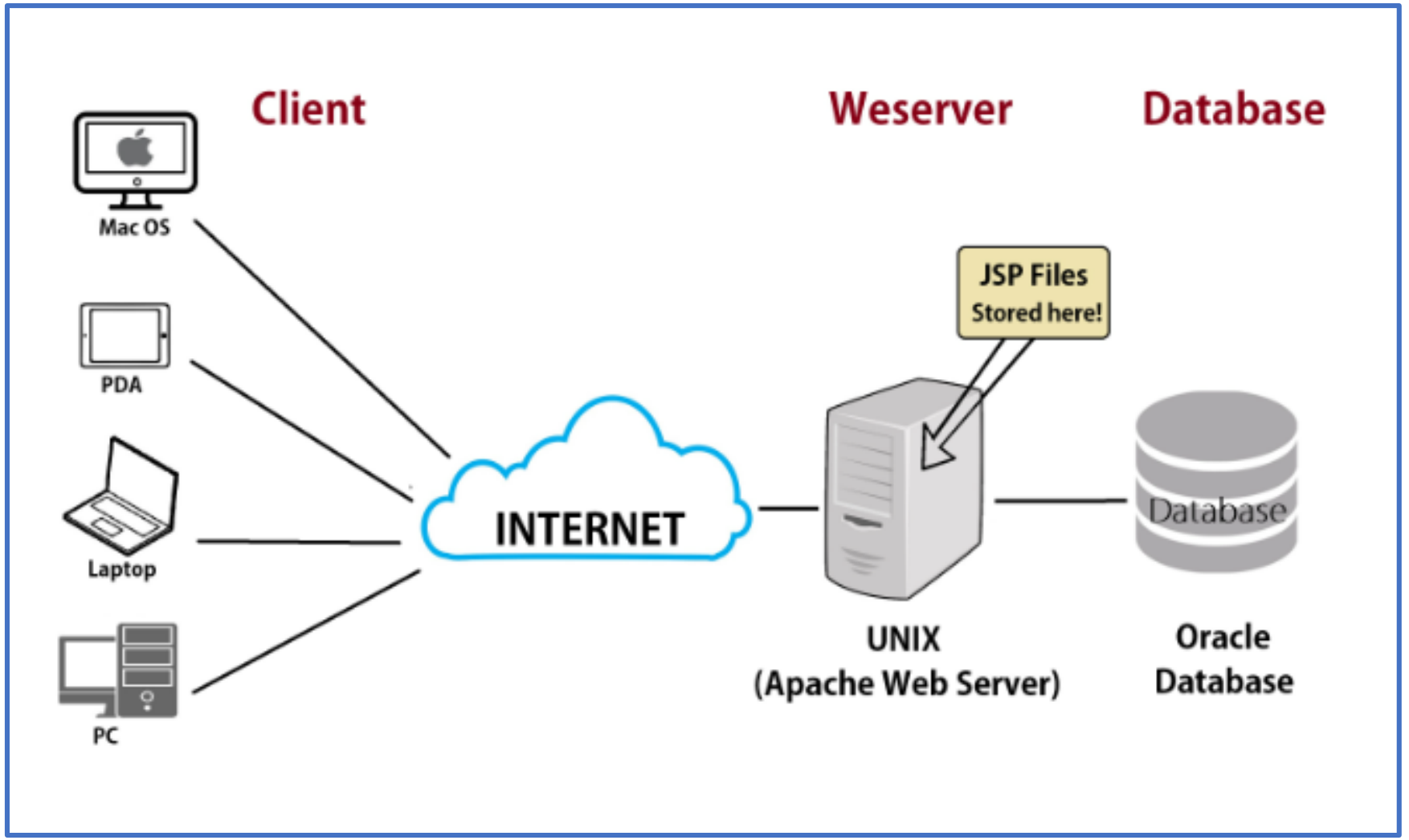
IEEE 802.11 WG Voting Members: 300+

Network Servises

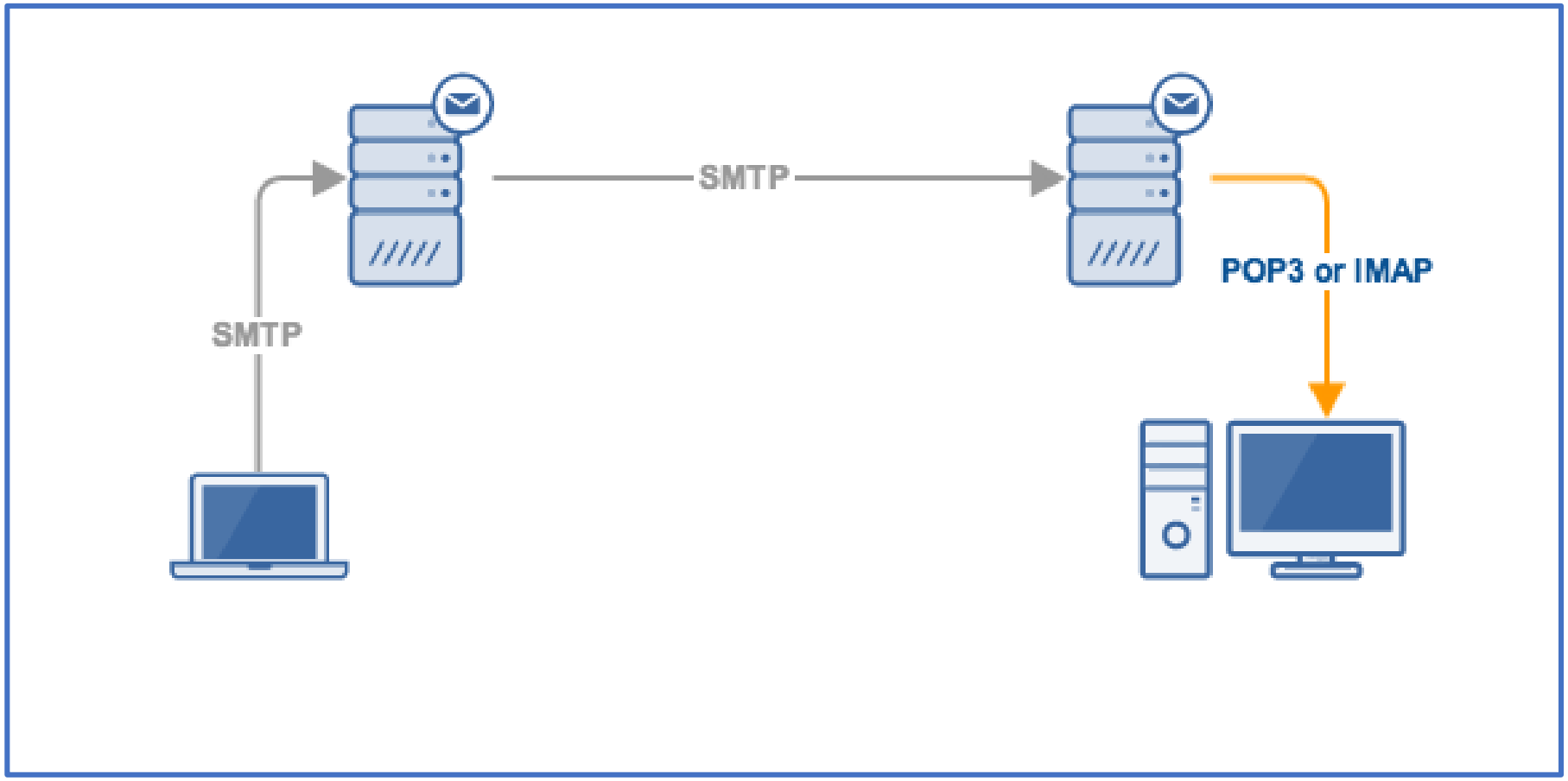
DHCP Server


DHCP clients
Network devices
ge-0/0/1
ge-0/0/2
ge-0/0/3
Switch
ge-0/0/8
DHCP server

Web Server


Client
Weserver
Database
Mac OS
PDA
Laptop
PC
INTERNET
JSP Files
Stored here!
Database
UNIX
(Apache Web Server)
Oracle
Database

Email Server



Introducing WLAN

Standard Organization

- **The International Telecommunication Union Radiocommunication Sector (ITU-R)** and **Federal Communications Commission (FCC)** - regulate frequencies, power levels, and transmission methods

- **Institute of Electrical and Electronics Engineers (IEEE)** - Standard and compatibility between equipment

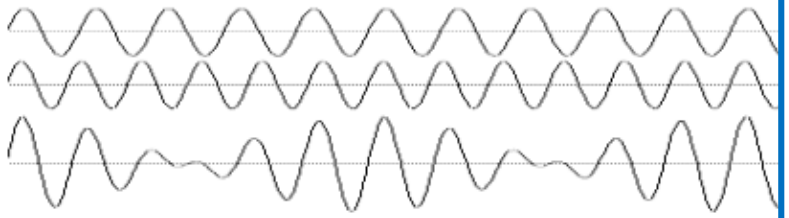
- **Wi-Fi Alliance** – Certification testing for wireless equipment

- **International Organization for Standardization (ISO)** – OSI 7 layers for data communication

- **Internet Engineering Task Force (IETF)** - creating Internet standards (RFC)

高科中实
GAOKE ZHONGSHI

- Wireless technologies use electromagnetic waves



Radio Fundamental

- Physical layer is radio frequency (RF) communications.
- Wired vs Wireless

travel across the bounded medium contains or confines the signal.

travel across the unbounded medium.

Wi-Fi ONBOARD

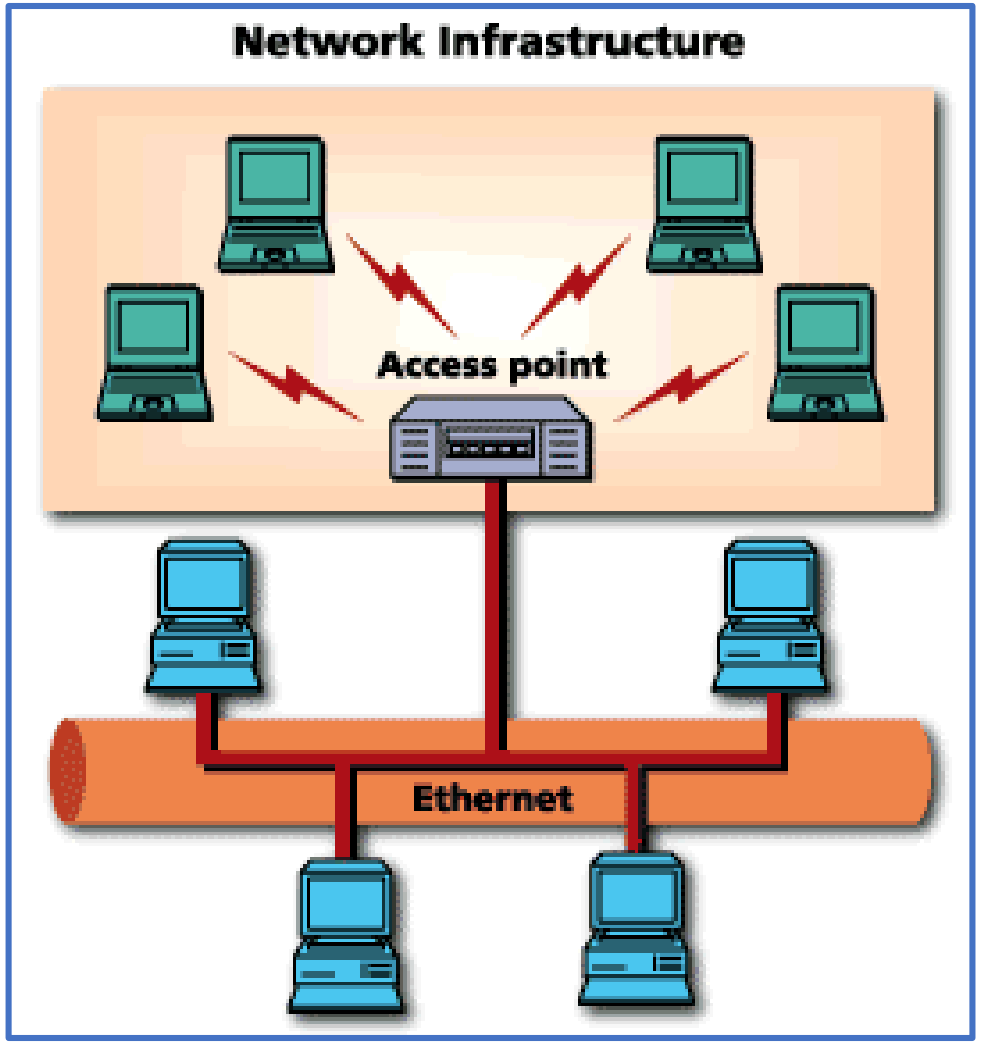
a b g Wi Fi n
CERTIFIED®

Frequency in LAN?

- ISM – Industrial Scientific Medical
  - Free to transmit
  - http://en.wikipedia.org/wiki/ISM_band
- 2.4GHz and 5 GHz bands
- Disadvantage:
  - They are very occupied
  - The frequencies are high

Introducing WLAN

- WLAN stands for Wireless Local Area Network.
- They use electromagnetic waves as a transmission medium.
- It is a flexible data communication system widely used as an alternative to or as an extension of the wired LAN.
- It uses radio frequency technology that allows greater mobility for users by minimizing wired connections.
- Every day this type of network is recognized more and more in a large number of businesses and a great extension of them is predicted.



Introducing WLAN

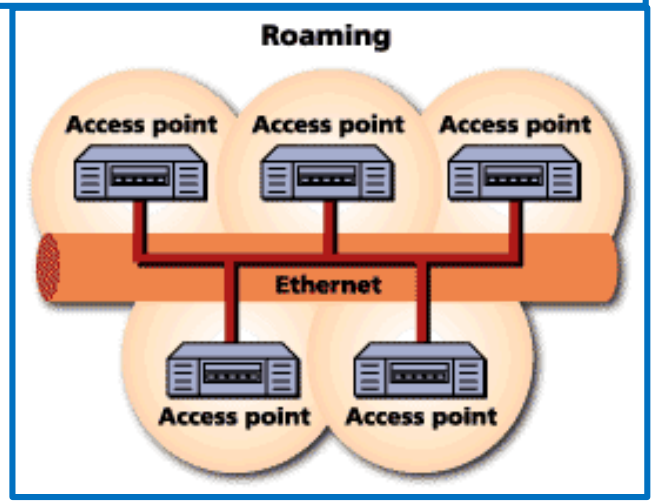
Why use WLAN?

Compared to the traditional network, the wireless network offers the following advantages:

- Mobility: Information in real time anywhere in the organization or company for all users of the network.
- Ease of installation: Avoid works to run cable through walls and ceilings.
- Flexibility: It allows you to go where the cable cannot.
- Scalability: Changing the network topology is easy and treats small and large networks the same.
- Price?

Roaming

- Users maintain a continuous connection as they roam from one physical area to another;
- Mobile nodes automatically register with the new access point;
- Methods: DHCP, Mobile IP;
- IEEE 802.11 standard does not address roaming, you may need to purchase equipment from one vendor if your users need to roam from one access point to another.



Introducing WLAN

Wireless Technologies

- PAN/WPAN (Personal Area Network)
  Bluetooth, IEEE 802.15.4
- **LAN (Local Area Network)**
  IEEE 802.11
- MAN (Metropolitan Area Network)
  IEEE 802.11, IEEE 802.16, IEEE 802.20
- WAN (Wide Area Network)
  GSM, CDMA, Satelite
- http://www.ieee.org/index.html

Explosive Mobile Device Growth

- In 2020 there will be **50 billion** connected devices
- Smartphone & Tablet adoption growing **70%+ annually**.**
- In 2014, more than **60%** of network devices shipped without a wired port.***

History of Wireless LAN

- In 1970, the University of Hawaii developed the first wireless network, called ALOHAnet
- 400 MHz frequency range
- IEEE ratified the original 802.11 standard (1997) - 2Mbps

802.11

- Legacy – released in 1997
- Specified in infrared and wireless
- Spread Spectrum – FHSS/DSSS
- Speed: 1-2 Mbps
- Frequency: 2.4 Ghz and 900 Mhz

802.11g

- Standardized in 2003
- Best of both worlds (a & b)
- Frequency band: 2.4 GHz
- Bandwidth: 54 Mbps
- Modulation: OFDM

Cisco Systems Networking Academy

- 802.11a

  Introduces OFDM and takes speed up to 54 Mbps

  Frequency band: 5 GHz

  Distance to transmit signal: 25m

- 802.11b

  Bandwidth: 11 Mbps

  Frequency band: 2.4 GHz

  Became very popular – called WiFi

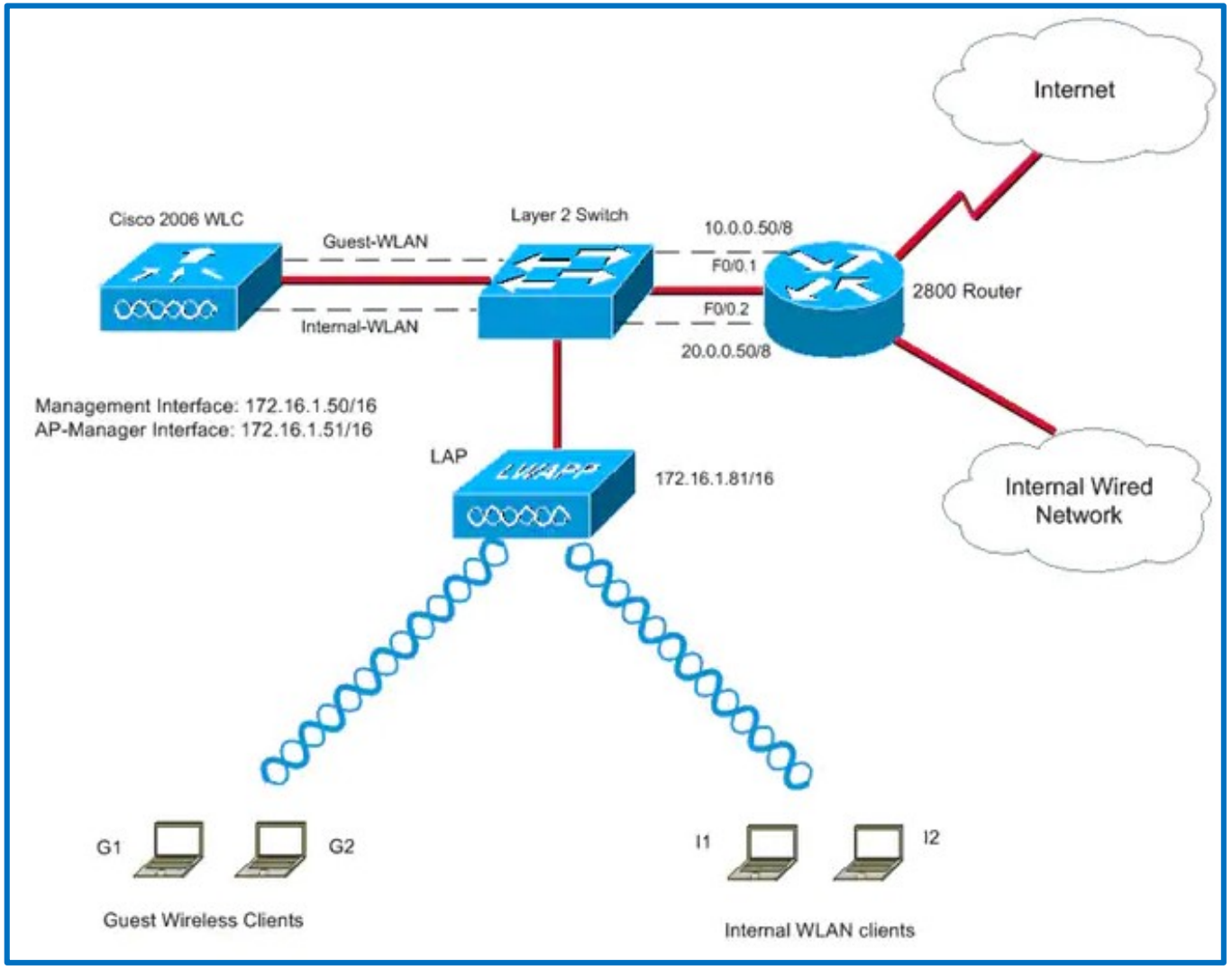
802.11n

- 802.11n – standardized 29 October 2009
- Far greater speeds: theoretical maximum 600 Mbps
- Better coverage and density of the signal
- Backwards compatible with 802.11 a/b/g
- Uses multiple antenaes and MIMO technology
- Increased channel width to 40 Mhz

Introducing WLAN

Wireless Devices

- As wireless devices have grown in popularity, so have WLANs. In fact, most routers sold are now wireless routers;
- A wireless router serves as a base station, providing wireless connections to any Wi-Fi-enabled devices within range of the router's wireless signal;
- This includes laptops, tablets, smartphones, and other wireless devices, such as smart appliances and smart home controllers;
- Wireless routers often connect to a cable modem or other Internet-connected device to provide Internet access to connected devices.



Introducing WLAN

Advantages of WLANs

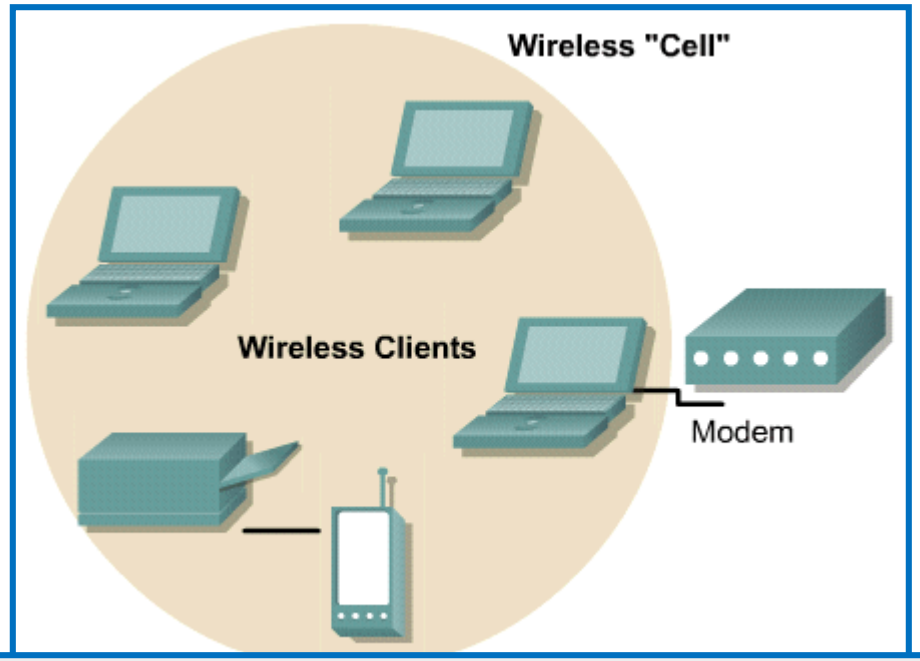
- The most obvious advantage of a WLAN is that devices can connect wirelessly, eliminating the need for cables.
- This allows homes and businesses to create local networks without wiring the building with Ethernet.
- It also provides a way for small devices, such as smartphones and tablets, to connect to the network.
- WLANs are not limited by the number of physical ports on the router and therefore can support dozens or even hundreds of devices.
- The range of a WLAN can easily be extended by adding one or more repeaters.
- Finally, a WLAN can be easily upgraded by replacing routers with new versions — a much easier and cheaper solution than upgrading old Ethernet cables.

Disadvantages of WLANs

- Wireless networks are naturally less secure than wired networks.
- Any wireless device can attempt to connect to a WLAN, so it is important to limit access to the network if security is a concern.
- This is typically done using wireless authentication such as WEP or WPA, which encrypts the communication.
- Additionally, wireless networks are more susceptible to interference from other signals or physical barriers, such as concrete walls. Thus, they have minor transmission speed.

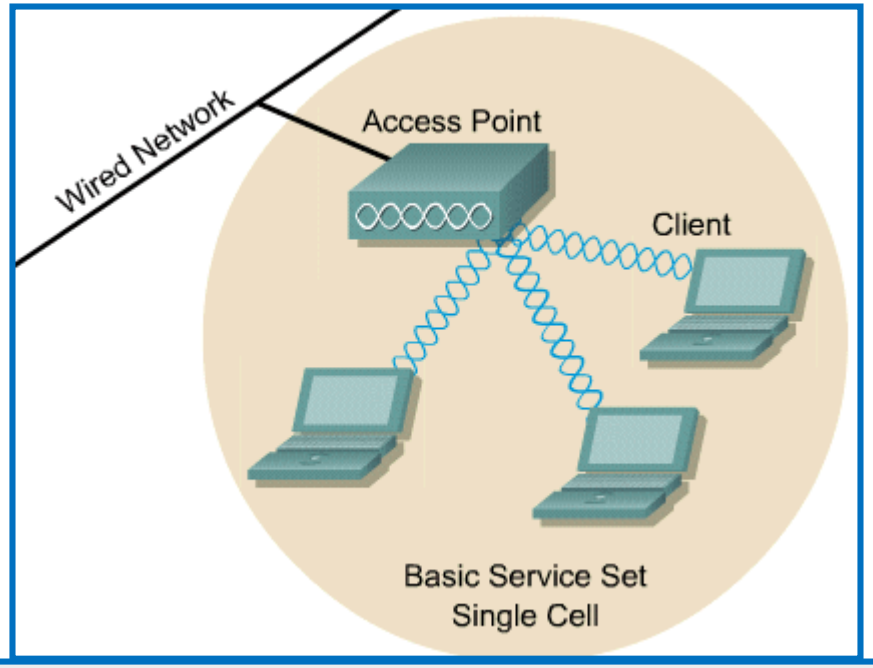
Introducing WLAN

Ad Hoc Topology



- Peer-to-Peer (Ad Hoc) Topology (IBSS)
- It can consist of 2 or more PCs with wireless network adapters.
- Sometimes called an Independent (Basic Service Set) BSS.
- Limited range.

Basic Infrastructure Topology (BSS)



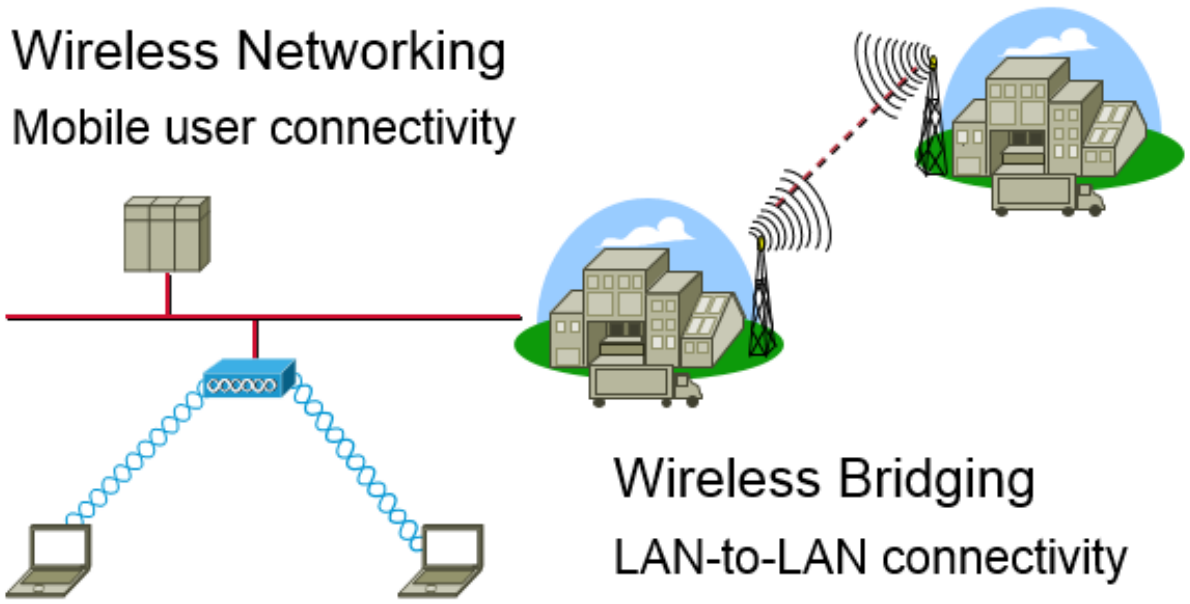
- Building block of an 802.11 LAN that covers a single cell
- When a device moves out of its BSS, it can no longer communicate with other members of the BSS.
- Uses infrastructure mode, requires an access point (AP).
- A BSS has one service set ID (SSID).

Introducing WLAN

Wireless LAN Implementations

Wireless Networking

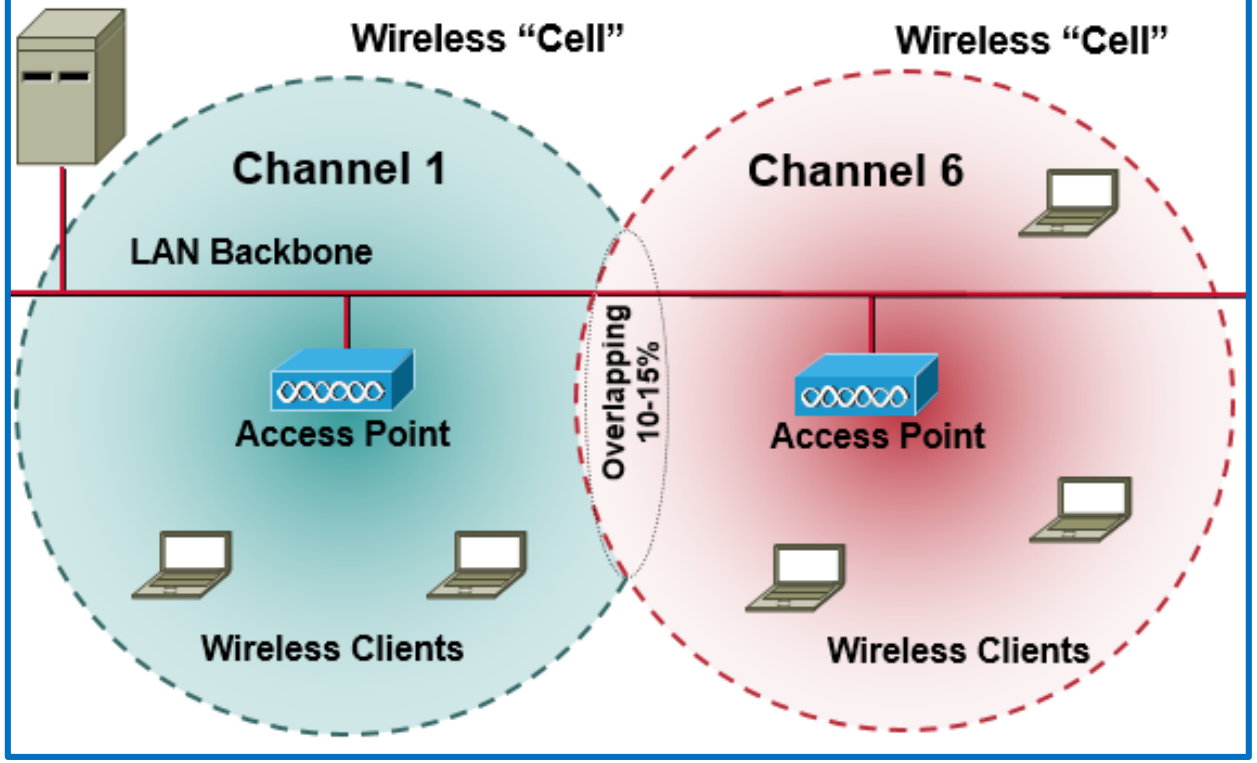
Mobile user connectivity



Wireless Bridging

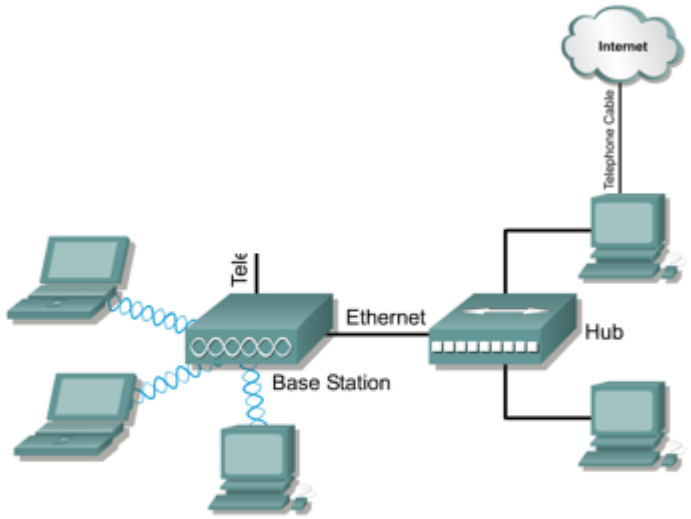
LAN-to-LAN connectivity

Typical WLAN Topologies



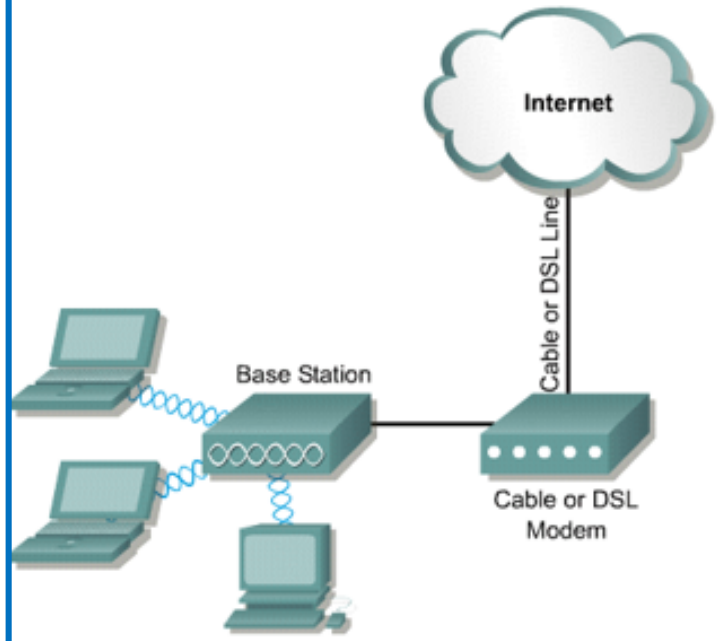
Introducing WLAN

Base Station-Dial-up



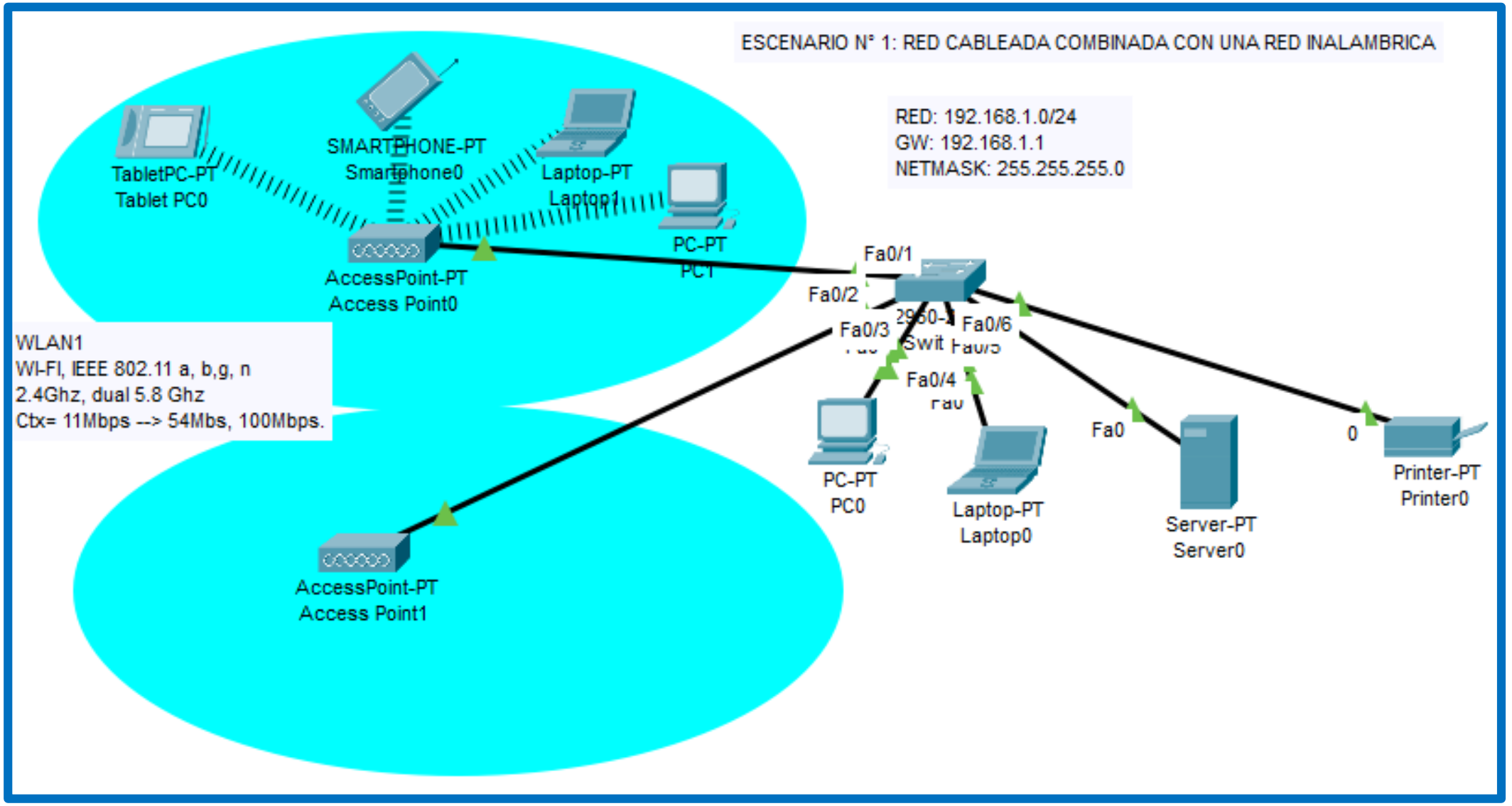
Designed for the small office/home office (SOHO). Gives telecommuters, SOHOs, and home users the convenience of wireless connectivity.

Base Station—DSL

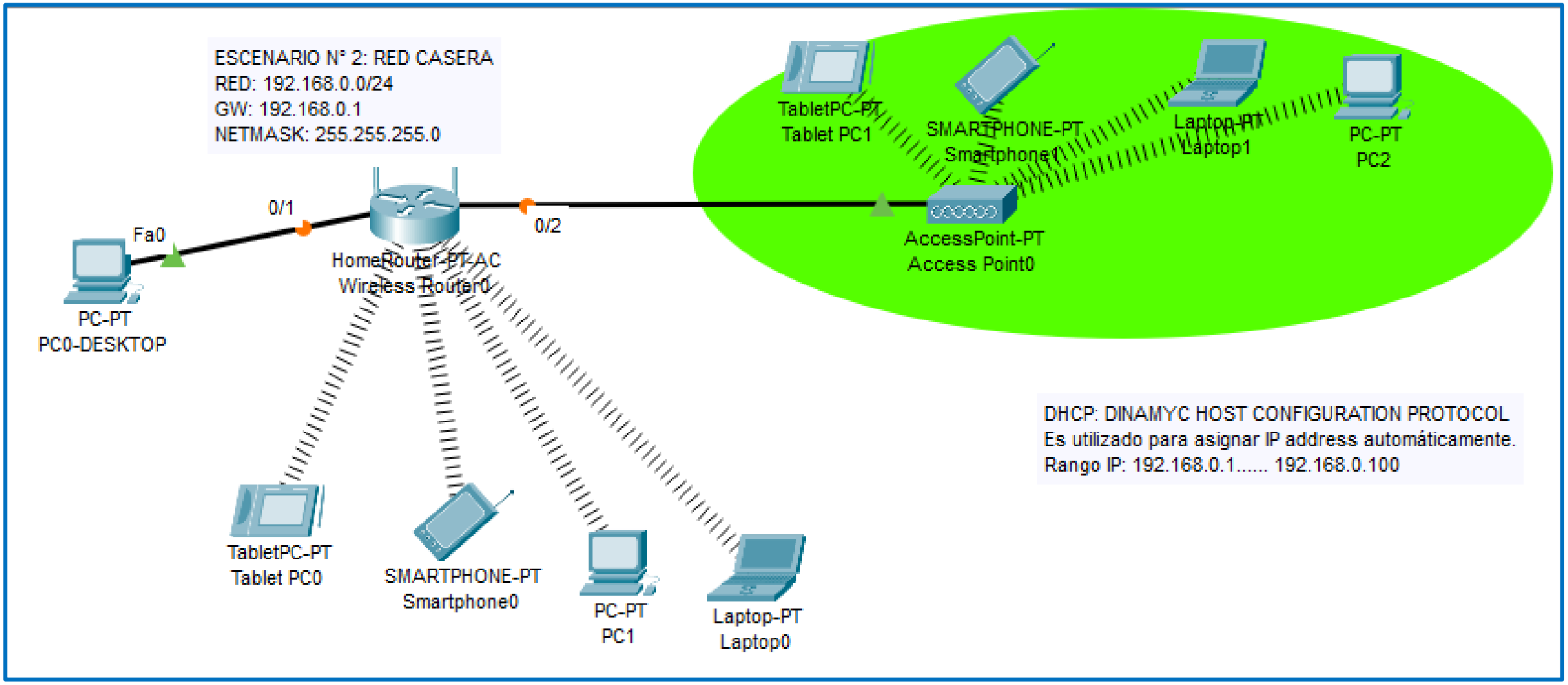


- Offers support for a Cable or DSL modem
- Will only support wireless clients.
- DHCP functionality is supported, but access to the wired network is not provided, as the Ethernet port must be used to connect to the Cable/DSL modem.
- Support for PPP over Ethernet.

Introducing WLAN: Packet Tracert Exercices



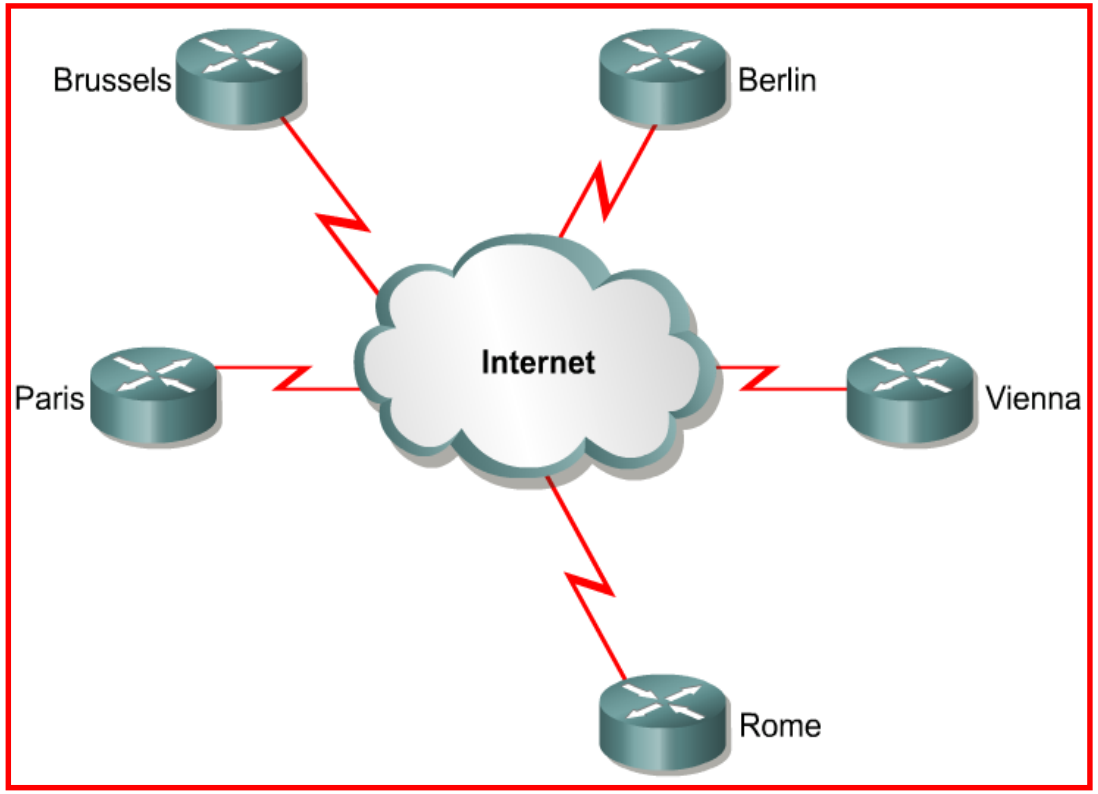
Introducing WLAN: Packet Tracert Exercices



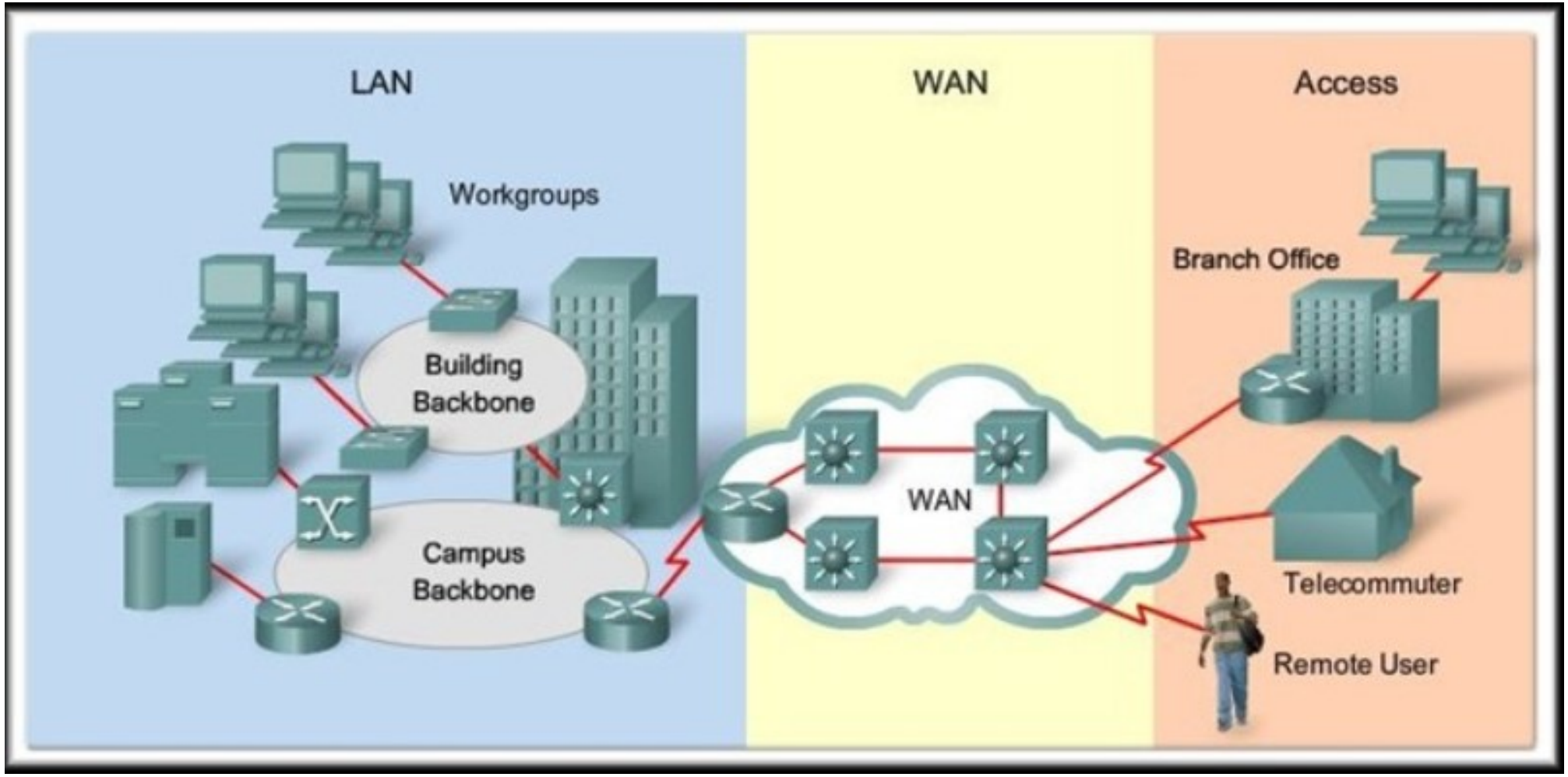
Introducing Wide Area Networks

Overview

- Differentiate between a LAN and WAN
- Identify the devices used in a WAN
- List WAN standards
- Describe WAN encapsulation
- Classify the various WAN link options
- Differentiate between packet-switched and circuit-switched WAN technologies
- Compare and contrast current WAN technologies
- Describe equipment involved in the implementation of various WAN services
- Recommend a WAN service to an organization based on its needs
- Describe DSL and cable modem connectivity basics
- Describe a methodical procedure for designing WANs
- Compare and contrast WAN topologies
- Compare and contrast WAN design models
- Recommend a WAN design to an organization based on its needs

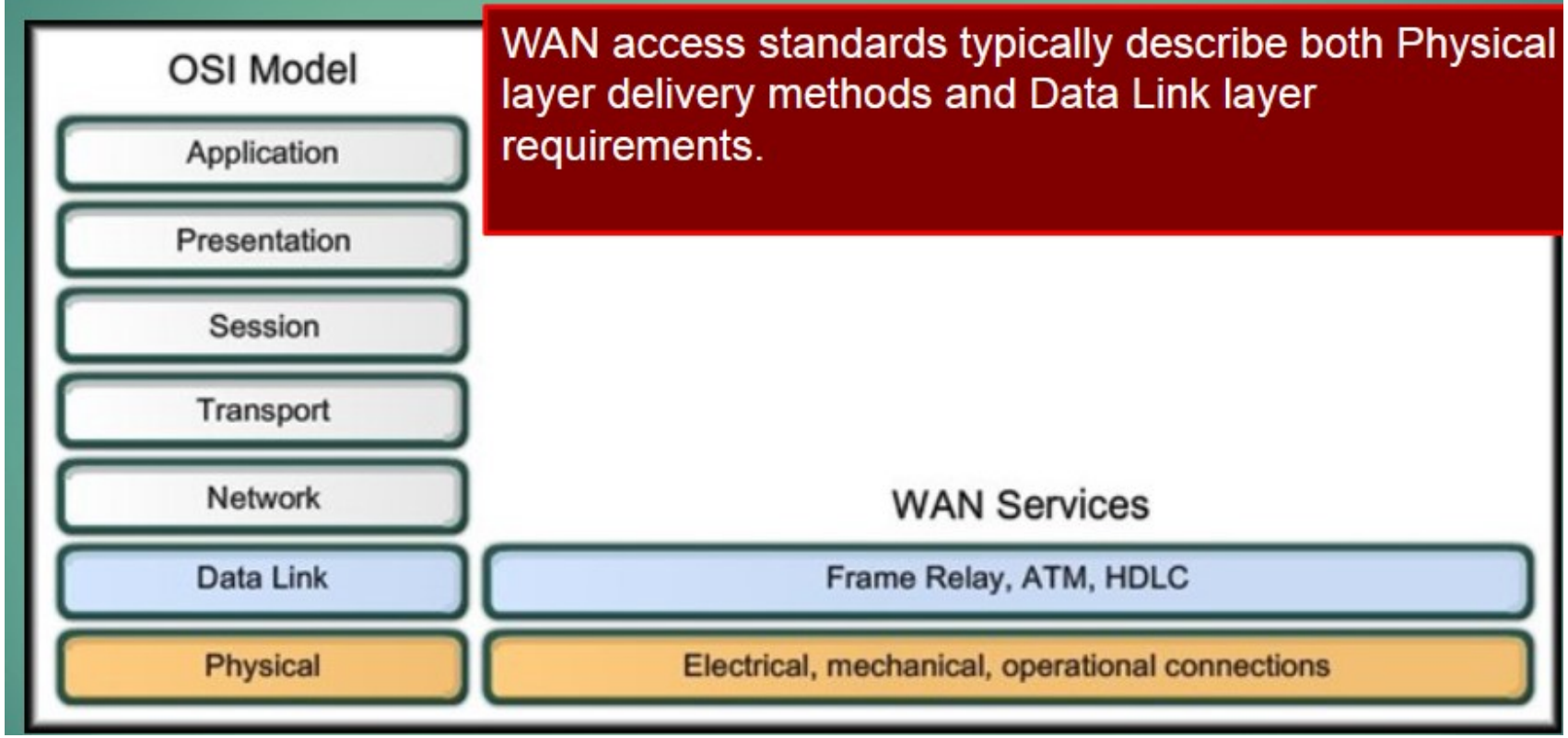


Introducing Wide Area Networks



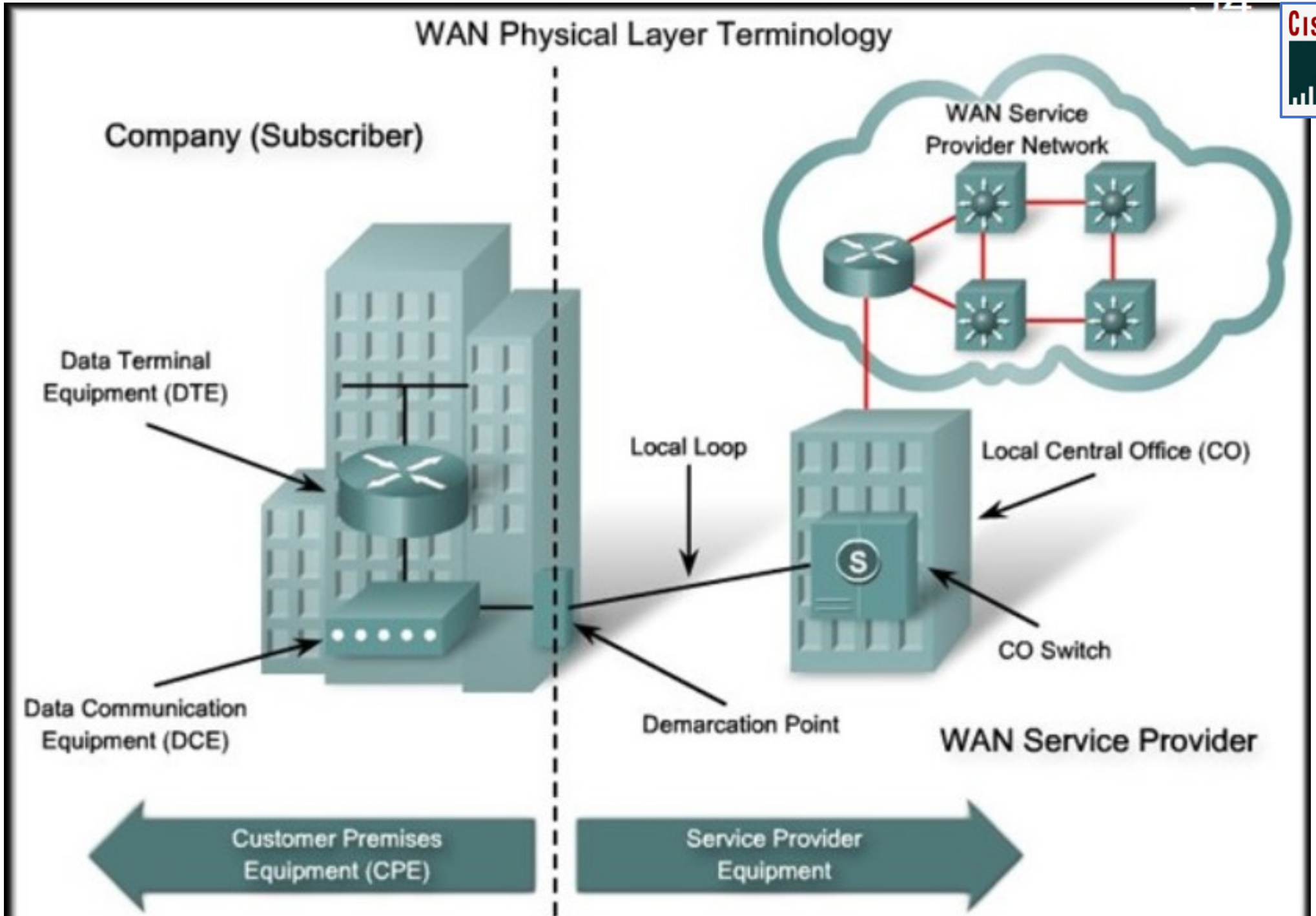
Introducing Wide Area Networks

- WAN and the OSI Model:
  - In relation to the OSI reference model, WAN operations focus on Layer 1 and Layer 2.



A wide area network (also known as WAN), is a large network of information that is not tied to a single location. WANs can facilitate communication, the sharing of information and much more between devices from around the world through a WAN provider.

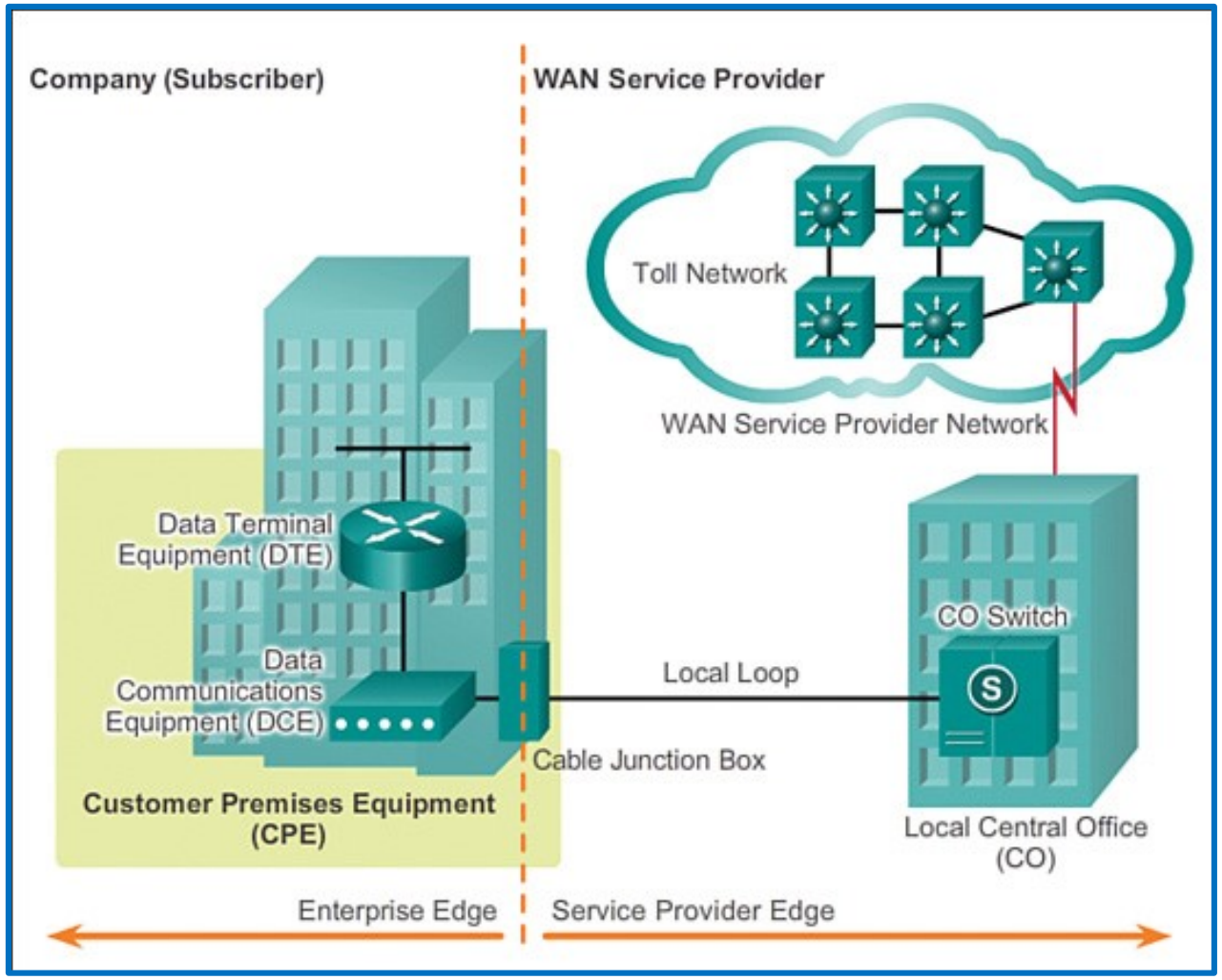
Whereas WANs can exist globally, without ties to a physical location through the use of a leased network provider, LANs exist within a limited area. LANs can be used to access a greater WAN (such as the internet), but only within the area where the LAN's infrastructure can reach.



Cisco Systems | Networking Academy

- Devices on the subscriber premises are called **customer premises equipment (CPE).**
- The subscriber owns the CPE or leases the CPE from the service provider.
- A copper or fiber cable connects the CPE to the service provider's nearest exchange or **central office (CO).**
- This cabling is often called the local loop, or **"last-mile".**

Introducing Wide Area Networks



Customer premises equipment (CPE): The devices and inside wiring located on the enterprise edge connecting to a carrier link.

Data communications equipment (DCE): The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud.

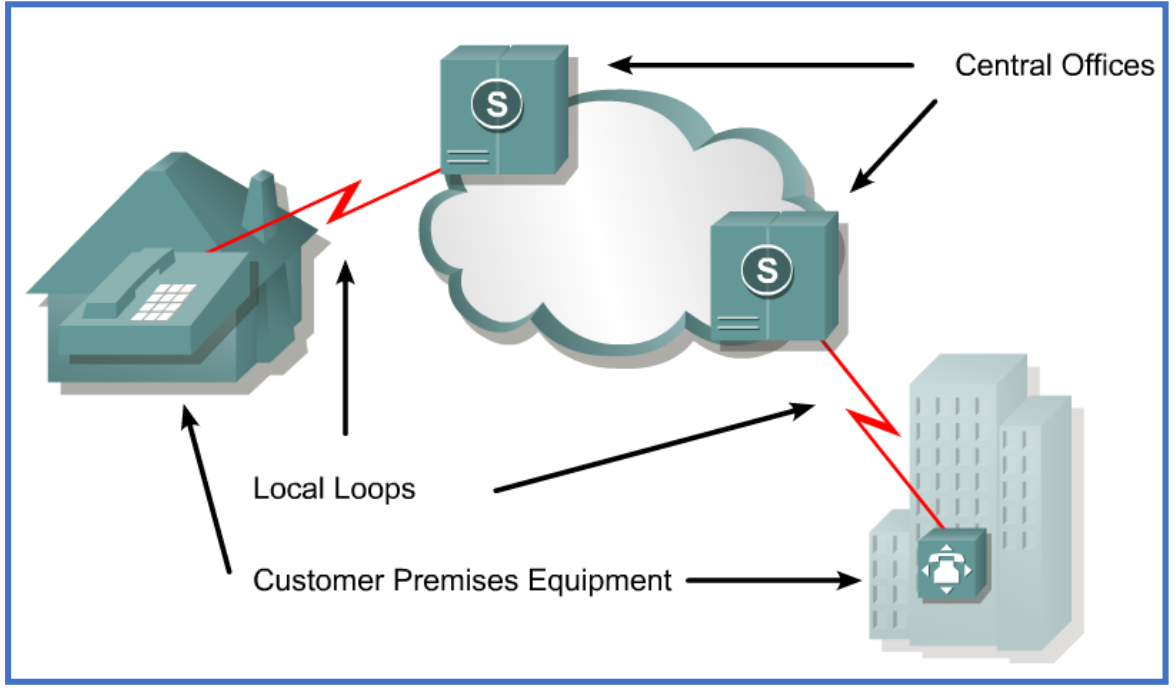
Data terminal equipment (DTE): The DTE connects to the local loop through the DCE.

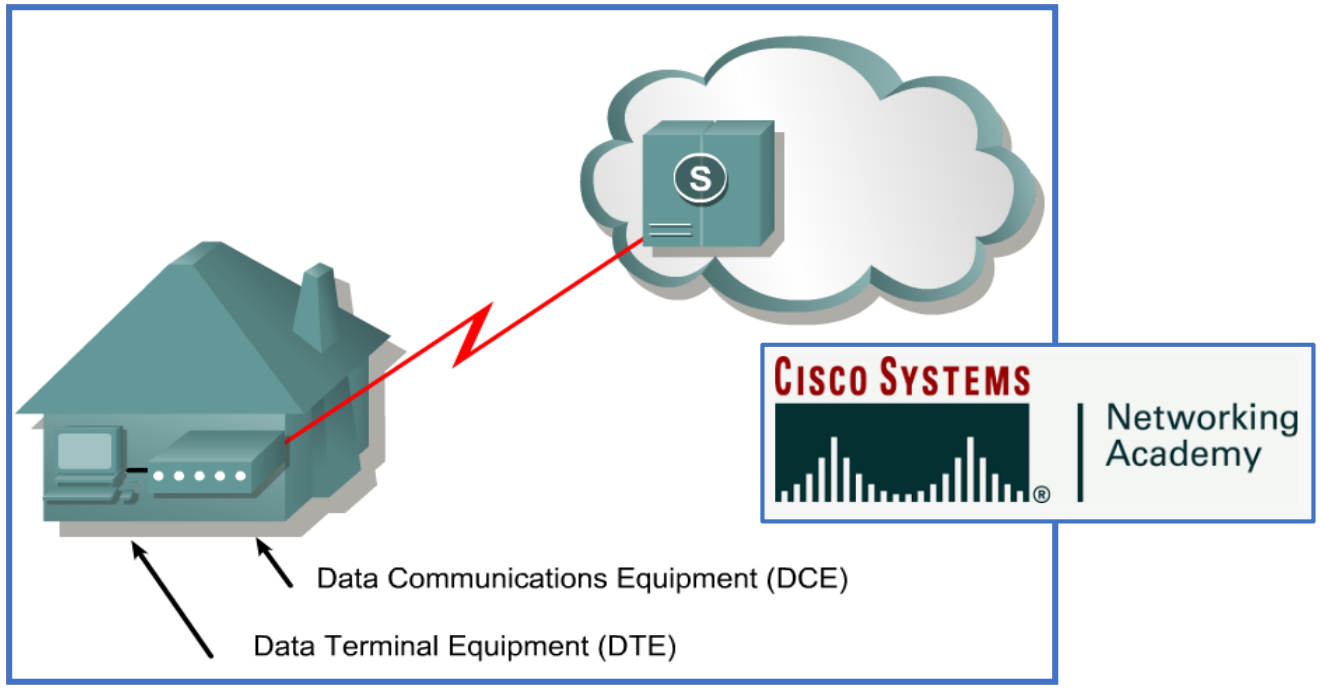
Demarcation point: Is the place where the responsibility for the connection changes from the user to the service provider.

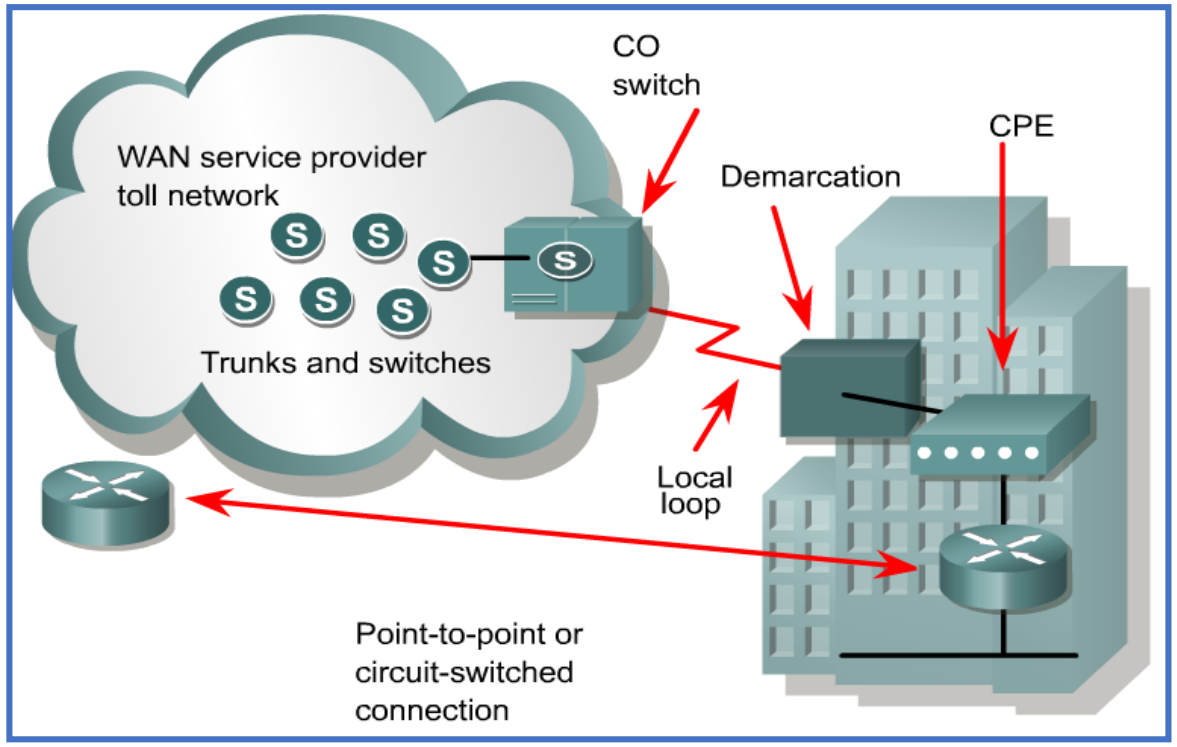
Local loop: The actual copper or fiber cable that connects the CPE to the CO of the service provider (last mile)

Central office (CO): The CO is the local service provider facility or building that connects the CPE to the provider network.

Toll network: This consists of the long-haul, all-digital, fiber-optic communications lines, switches, routers, and other equipment inside the WAN provider network.

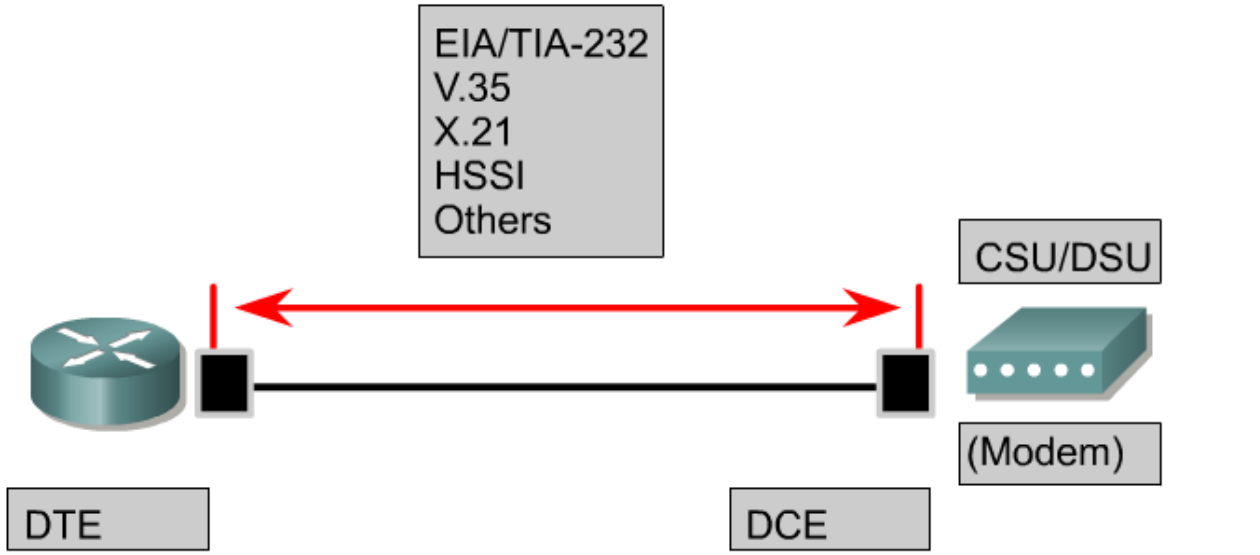






- A dialed call is connected locally to other local loops, or non-locally through a trunk to a primary center.
- It then goes to a sectional center and on to a regional or international carrier center as the call travels to its destination.
- Devices that put data on the local loop are called **data circuit-terminating equipment**, or **data communications equipment (DCE).**
- The customer devices that pass the data to the DCE are called **data terminal equipment (DTE).**
- The DCE primarily provides an interface for the DTE into the communication link on the **WAN cloud**.

Introducing Wide Area Networks



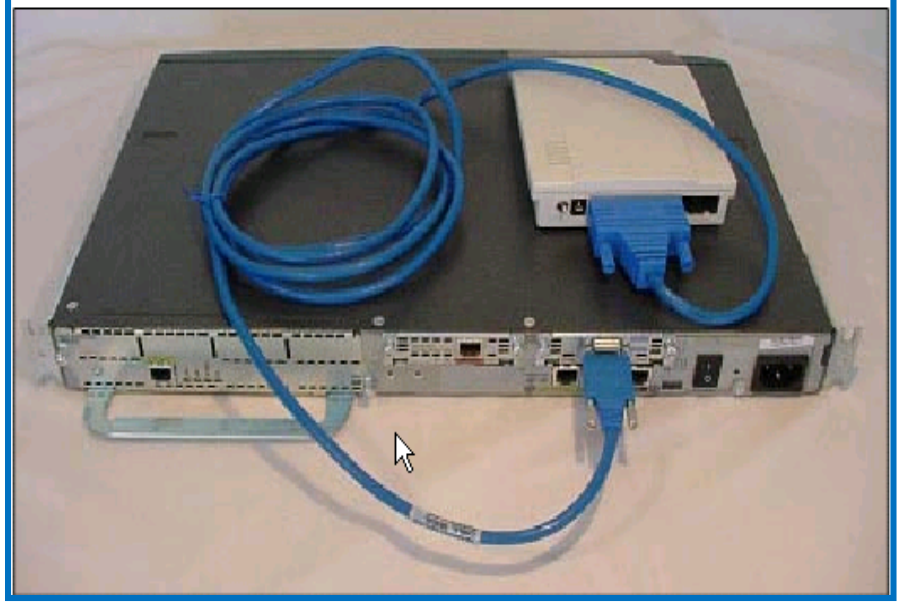
Data Terminal Equipment
User device with interface connecting to the WAN link

Data Circuit-Terminating Equipment
End of the WAN provider's side of the communication facility

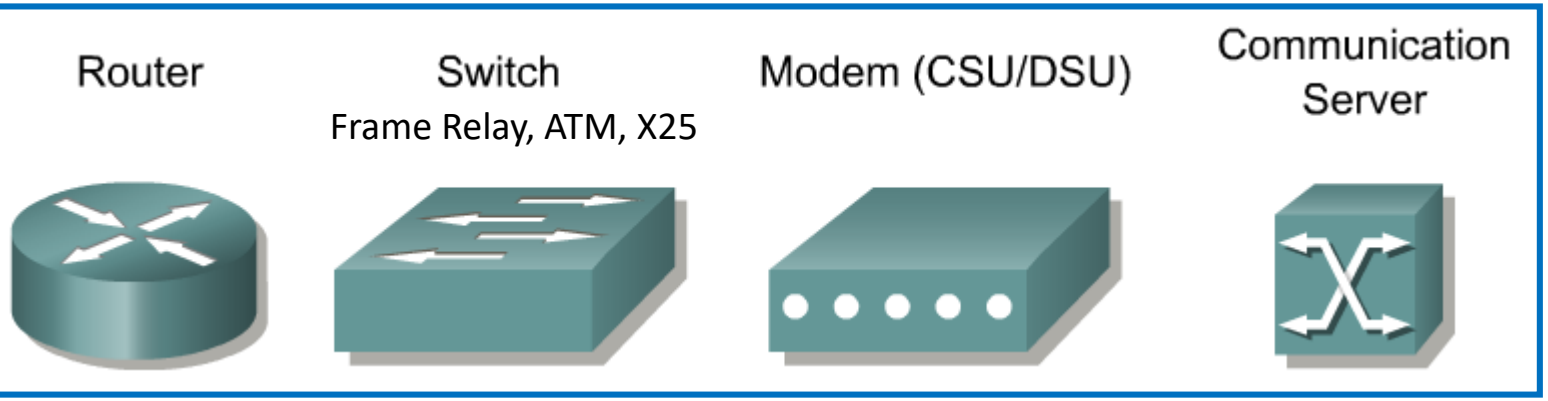
The DTE/DCE interface uses various physical layer protocols, such as High-Speed Serial Interface (HSSI) and V.35.
These protocols establish the codes and electrical parameters the devices use to communicate with each other.

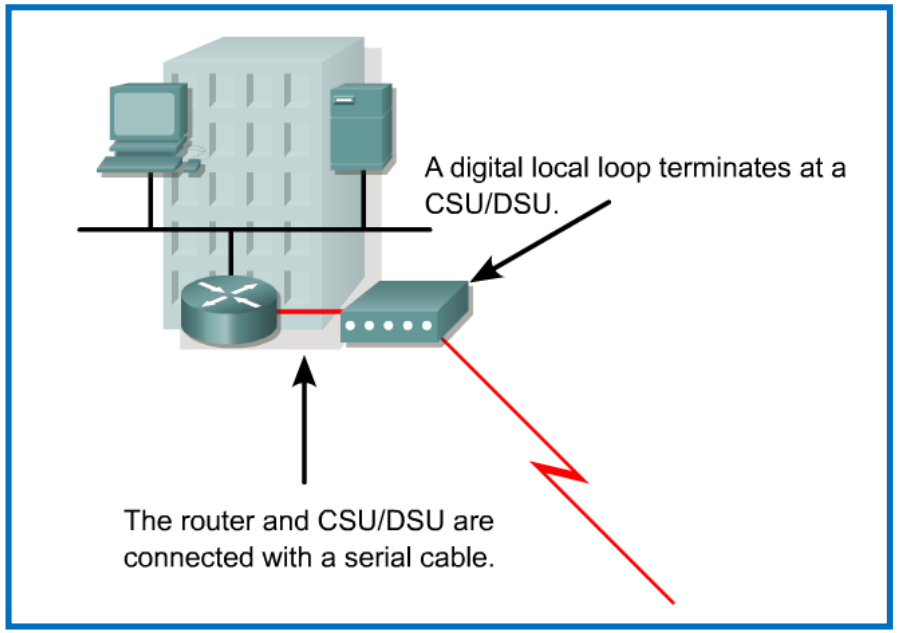
Connecting to a serial interface:
physical-layer async interface command
The Picture shows a connection between a Cisco 2620 series router and an external modem using an EIA/TIA-232 Smart Serial cable.

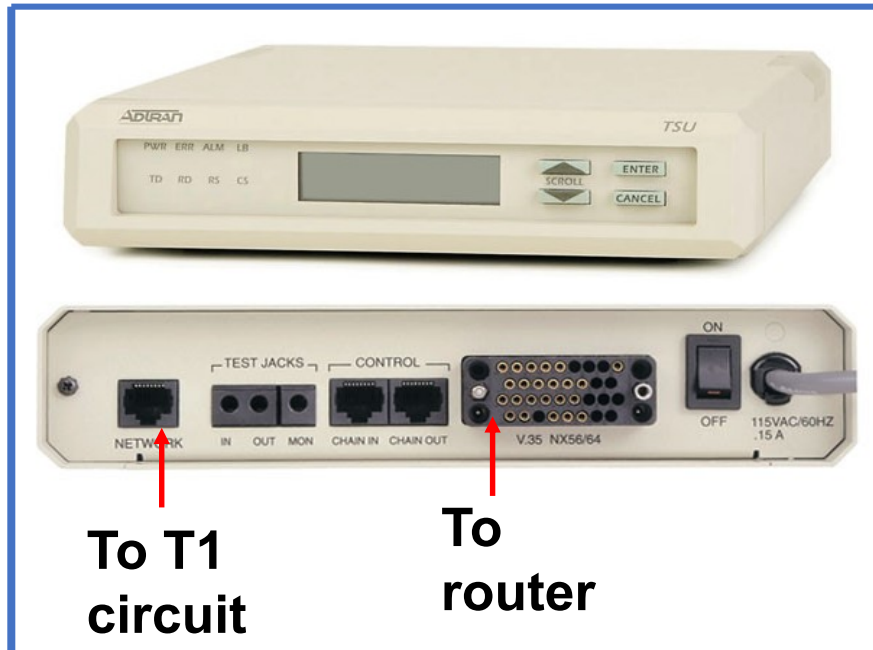
Connecting a Modem to a Router



WAN Devices







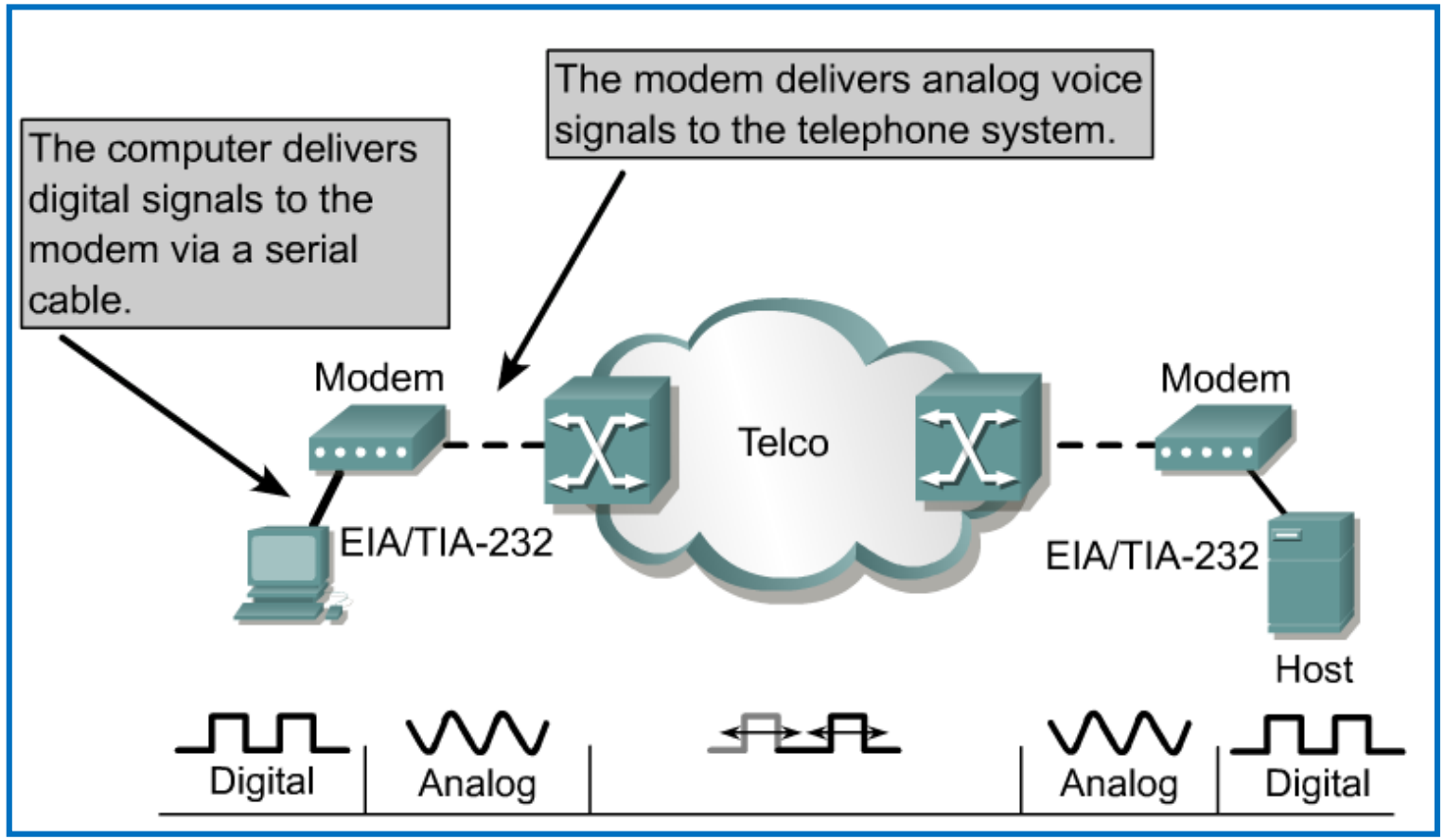
For digital lines, a **channel service unit (CSU)** and a **data service unit (DSU)** are required.
The two are often combined into a single piece of equipment, called the **CSU/DSU**.

WAN Devices

CSU/DSU Adapter

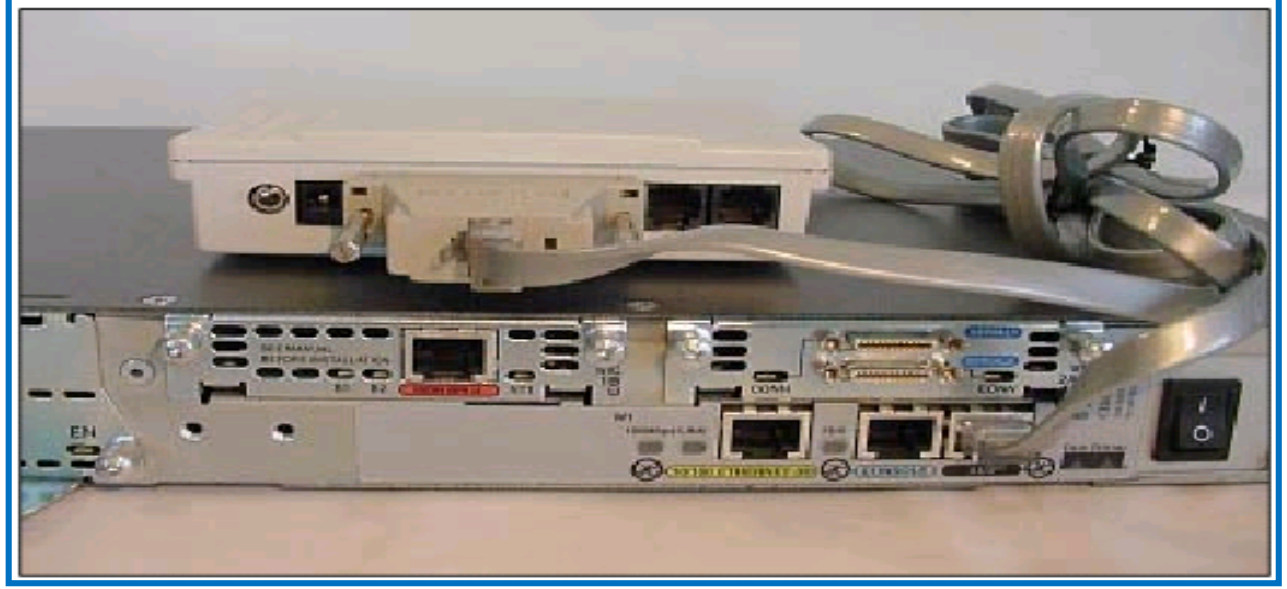
The CSU/DSU may also be built into the **interface card** in the router.

Modems



WAN Devices

Connecting a Modem to a Router

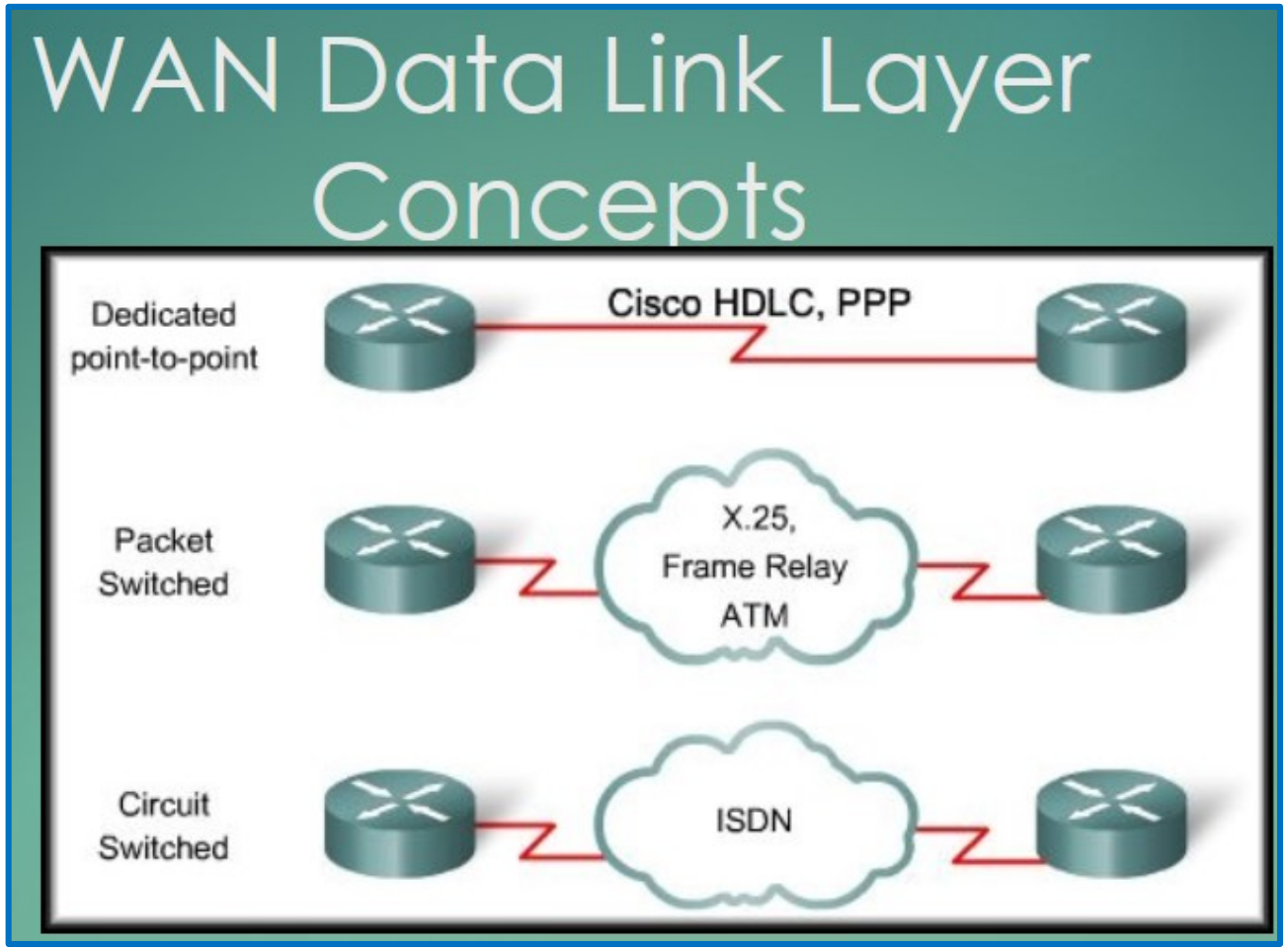


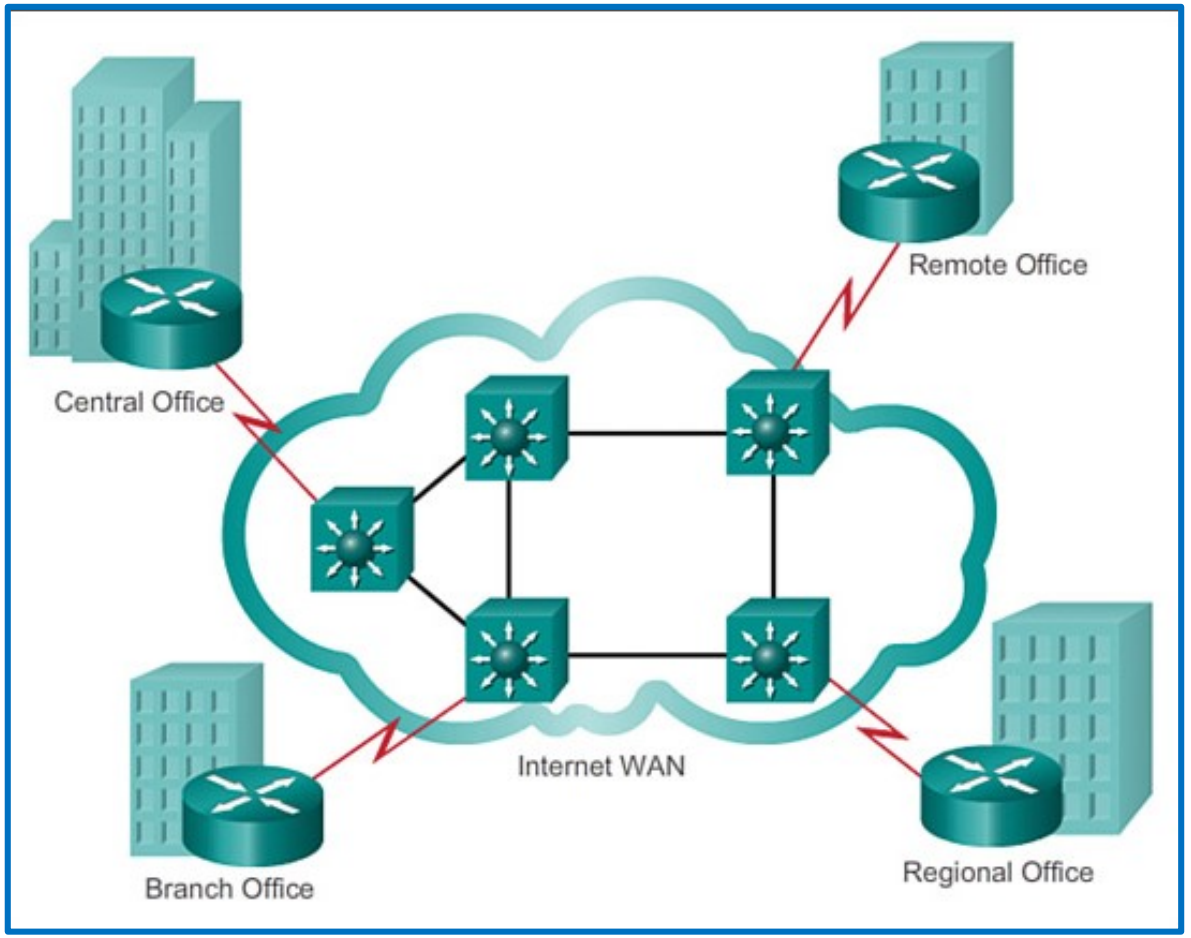
AUX (Auxiliary): To connect a modem to a Cisco router's AUX port, you typically use a rollover cable and a RJ-45-to-DB-25 male DCE modem adapter

Line Type	Signal Standard	Bit Rate Capacity
56	DS0	56 Kbps
64	DS0	64 Kbps
T1	DS1	1.544 Mbps
E1	ZM	2.048 Mbps
E3	M3	34.064 Mbps
J1	Y1	2.048 Mbps
T3	DS3	44.736 Mbps
OC-1	SONET	51.84 Mbps
OC-3	SONET	155.54 Mbps
OC-9	SONET	466.56 Mbps
OC-12	SONET	622.08 Mbps
OC-18	SONET	933.12 Mbps
OC-24	SONET	1244.16 Mbps
OC-36	SONET	1866.24 Mbps
OC-48	SONET	2488.32 Mbps

The bps values are generally full duplex

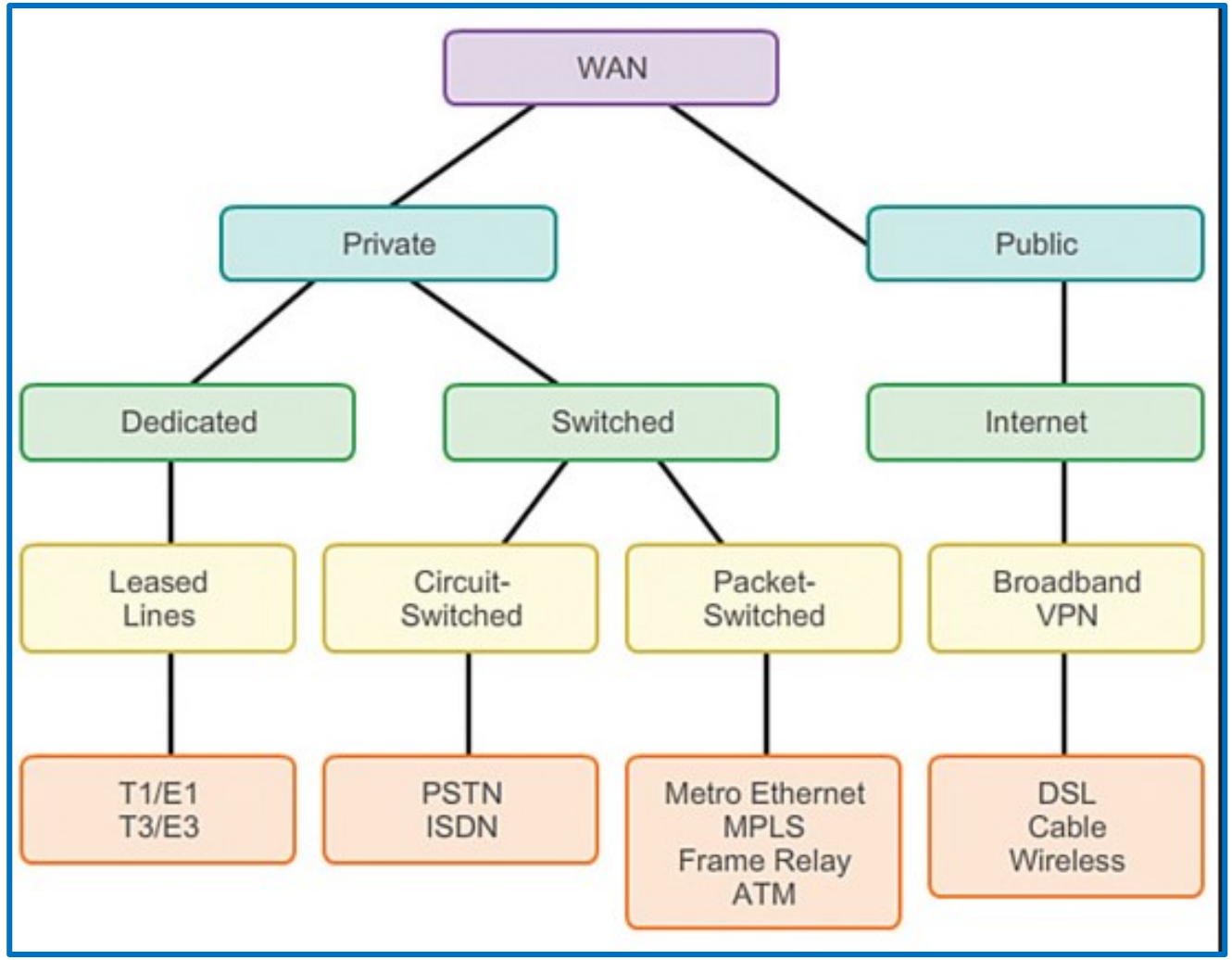
WAN Data Link options

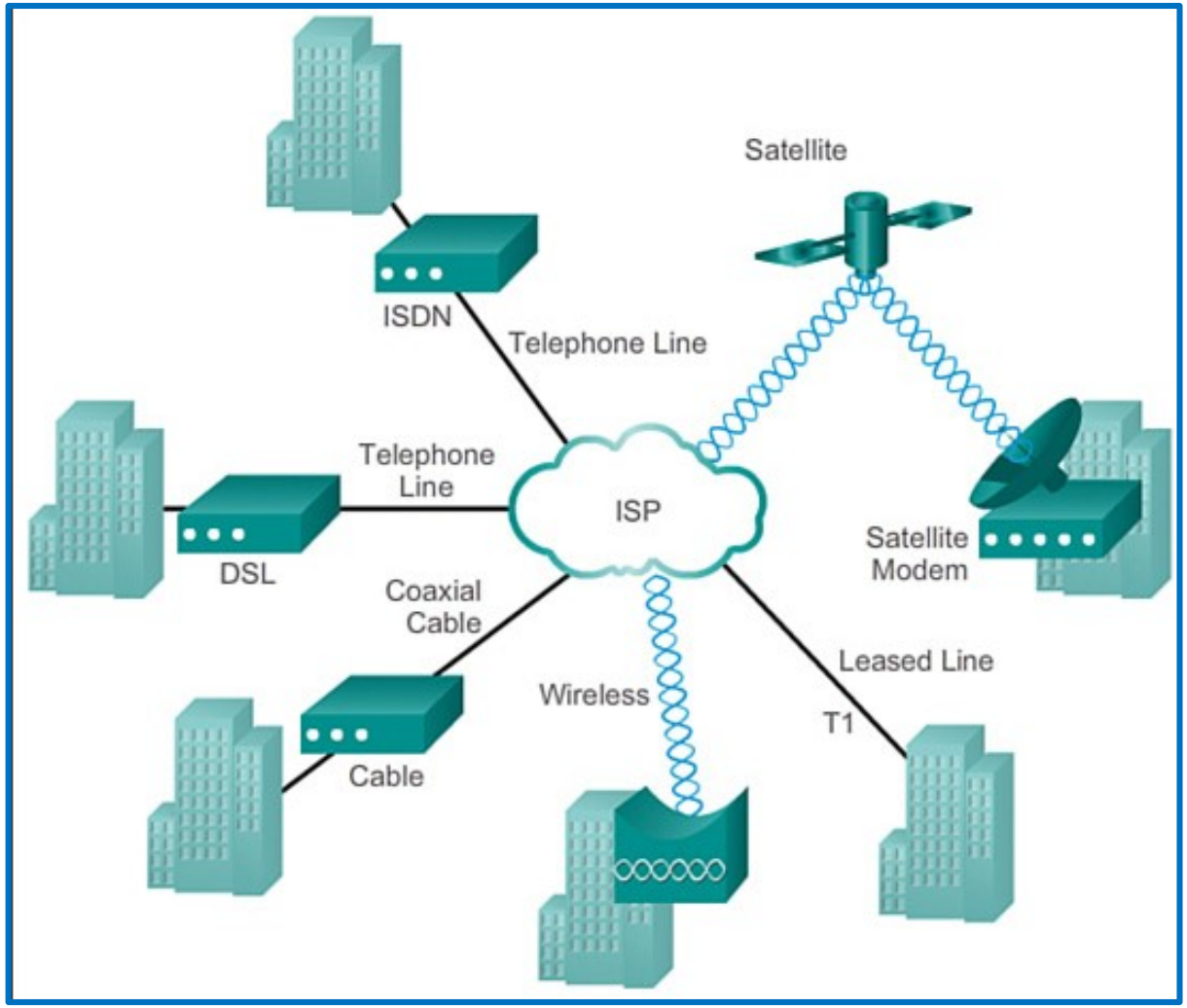




WAN Technologies Overview

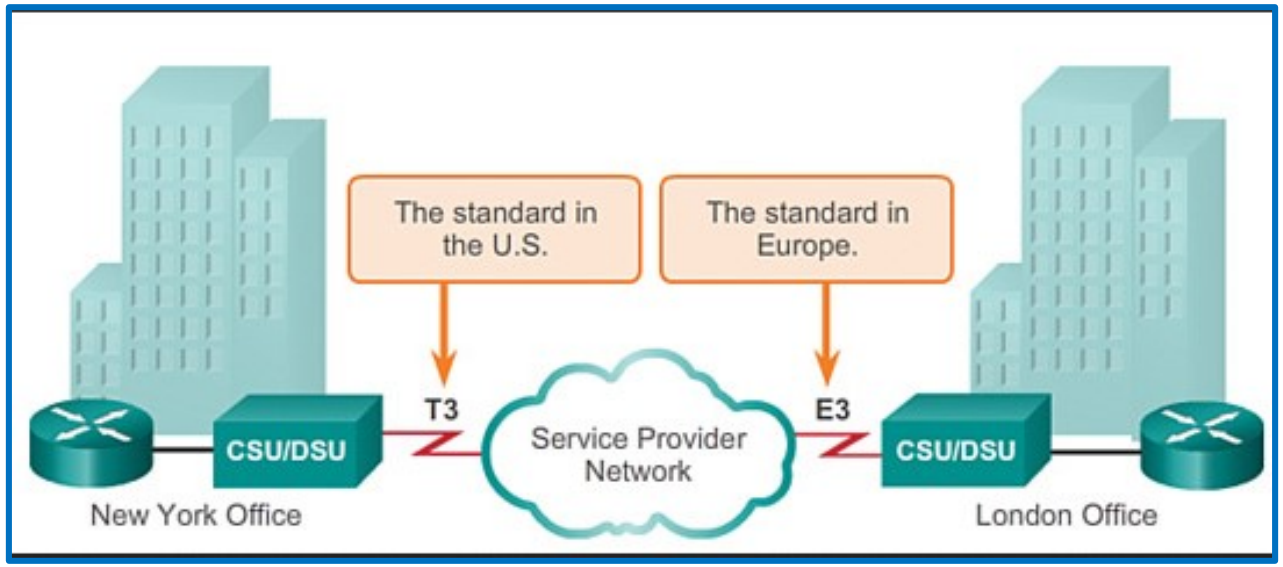
- ***Private WAN infrastructure***: Service providers may offer dedicated point-to-point leased lines, circuit-switched links, such as PSTN or ISDN, and packet-switched links, such as Ethernet WAN, ATM, or Frame Relay.
- ***Public WAN infrastructure***: Service provider may offer broadband Internet access using digital subscriber line (DSL), cable, and satellite access.





Private WAN Infrastructures

Leased Lines

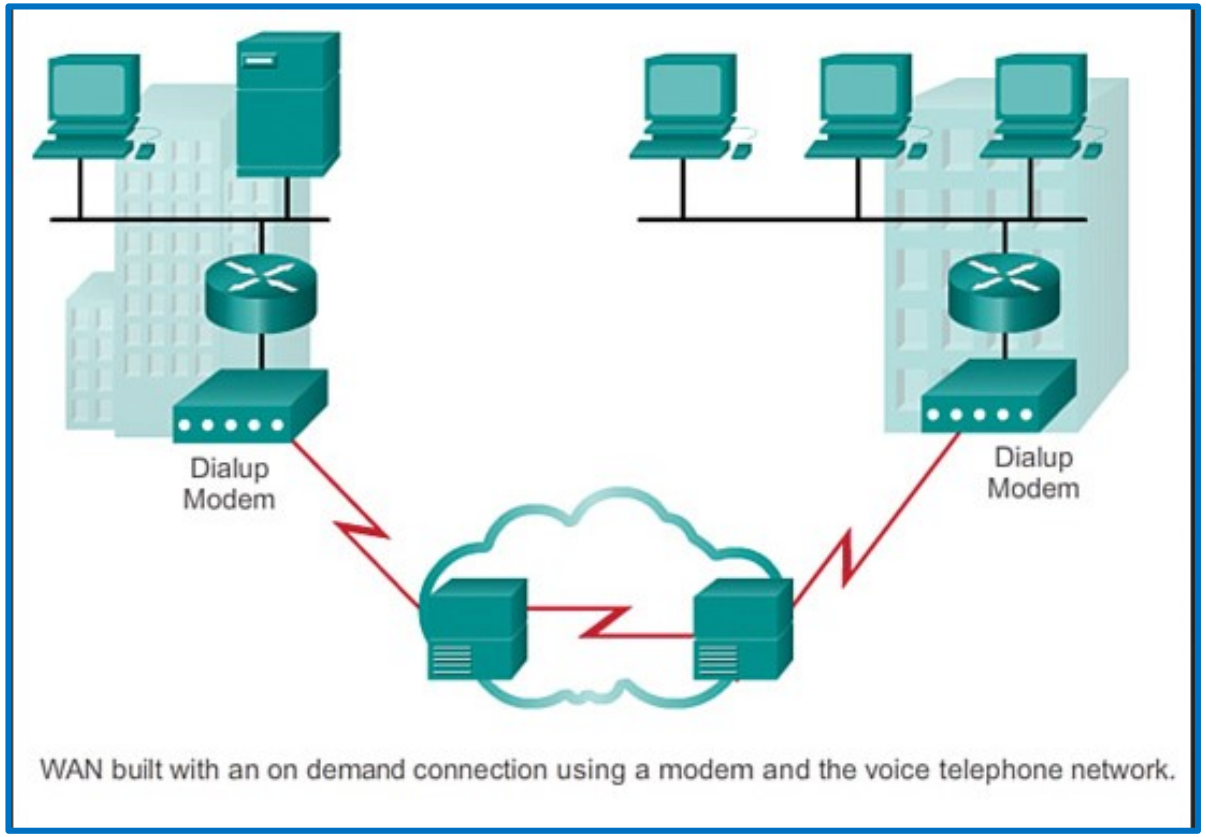


- **The advantages** of leased lines include: Simplicity, Quality, and Availability. Point-to-point communication links provide permanent, dedicated capacity, which is required for VoIP or Video over IP.
- **The disadvantage**s of leased lines include: Expensive Cost and Limited flexibility

- When permanent dedicated connections are required, a point-to-point link is used to provide a pre-established WAN communications path from the customer premises to the provider network. Point-to-point lines are usually leased from a service provider and are called leased lines.
- Leased lines are referred to by different names, such as leased circuits, serial link, serial line, point-to-point link, and T1/E1 or T3/E3 lines.
- The organization pays a monthly lease fee to a service provider to use the line.
- For instance, a T1 link supports 1.544 Mbps (in North America), an E1 supports 2.048 Mbps (Europe), a T3 supports 43.7 Mbps, and an E3 connection supports 34.368 Mbps. Optical Carrier (OC) transmission rates are used to define the digital transmitting capacity of a fiber-optic network.

Private WAN Infrastructures

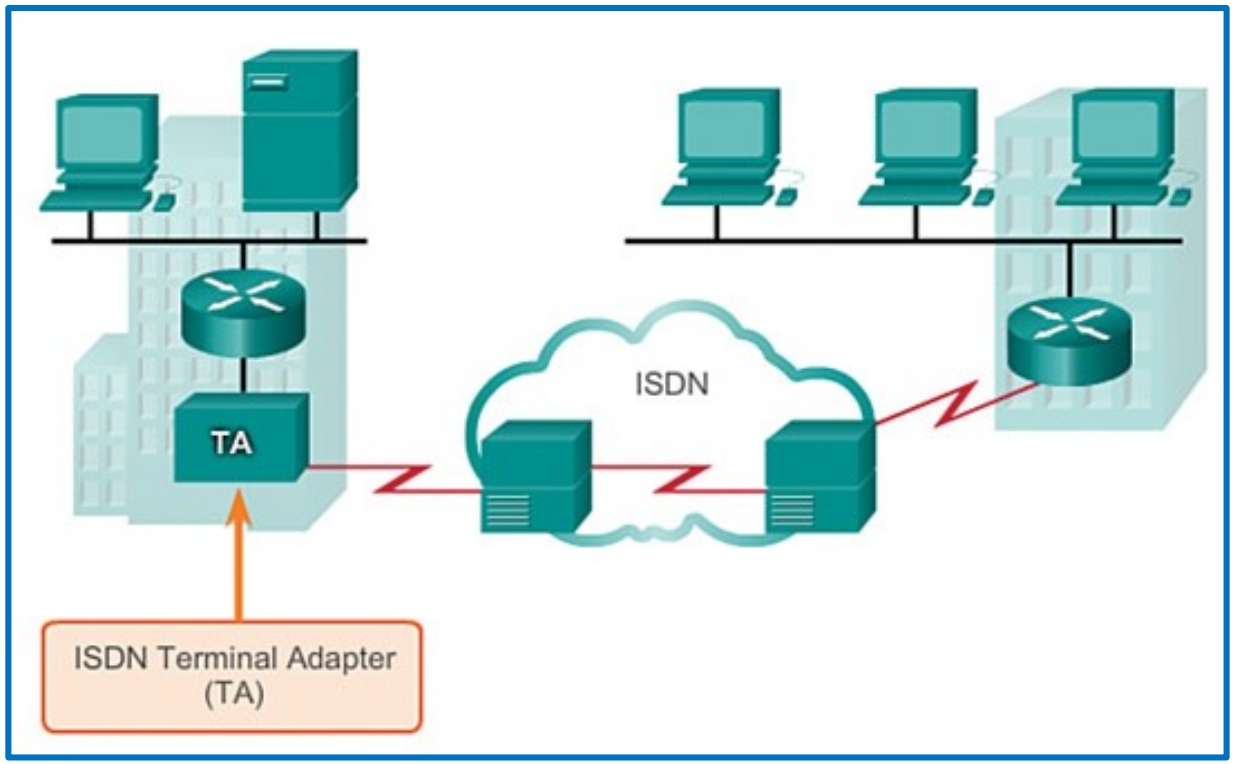
Dialup



WAN built with an on demand connection using a modem and the voice telephone network.

Traditional telephony uses a copper cable for the local loop to connect the telephone handset in the subscriber premises to the CO

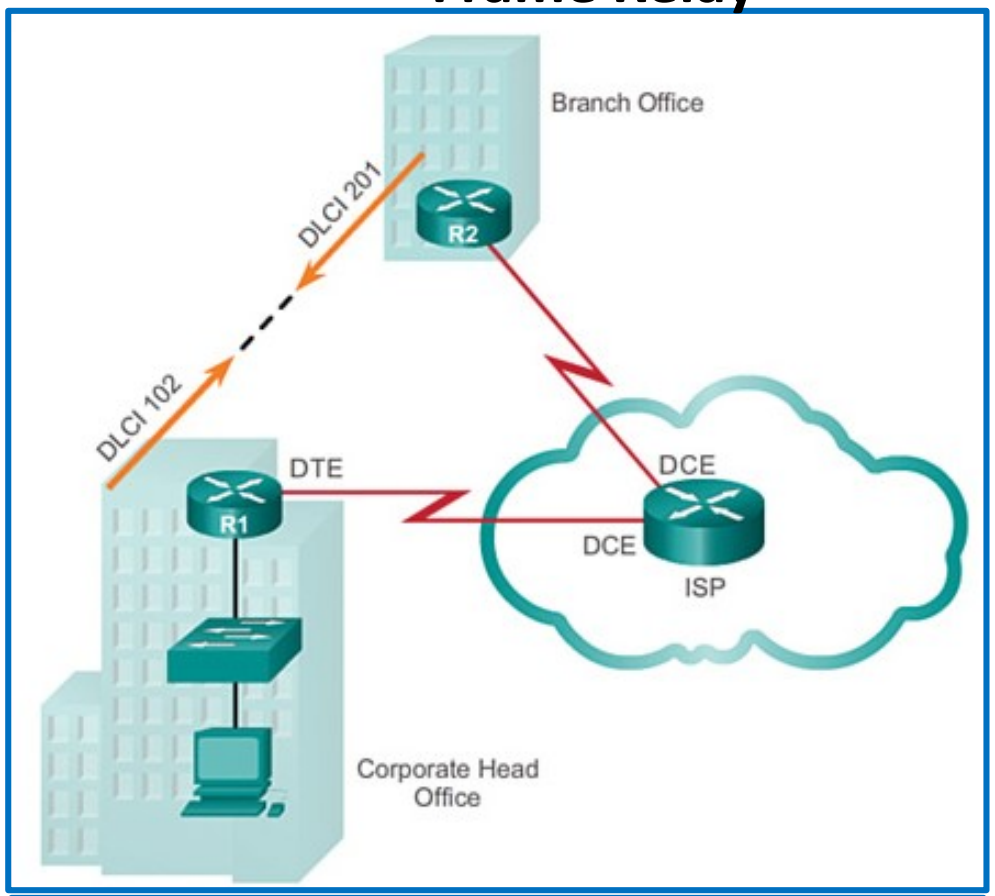
ISDN



Integrated Services Digital Network (ISDN) is a circuit-switching technology that enables the local loop of a PSTN to carry digital signals, resulting in higher-capacity switched connections.

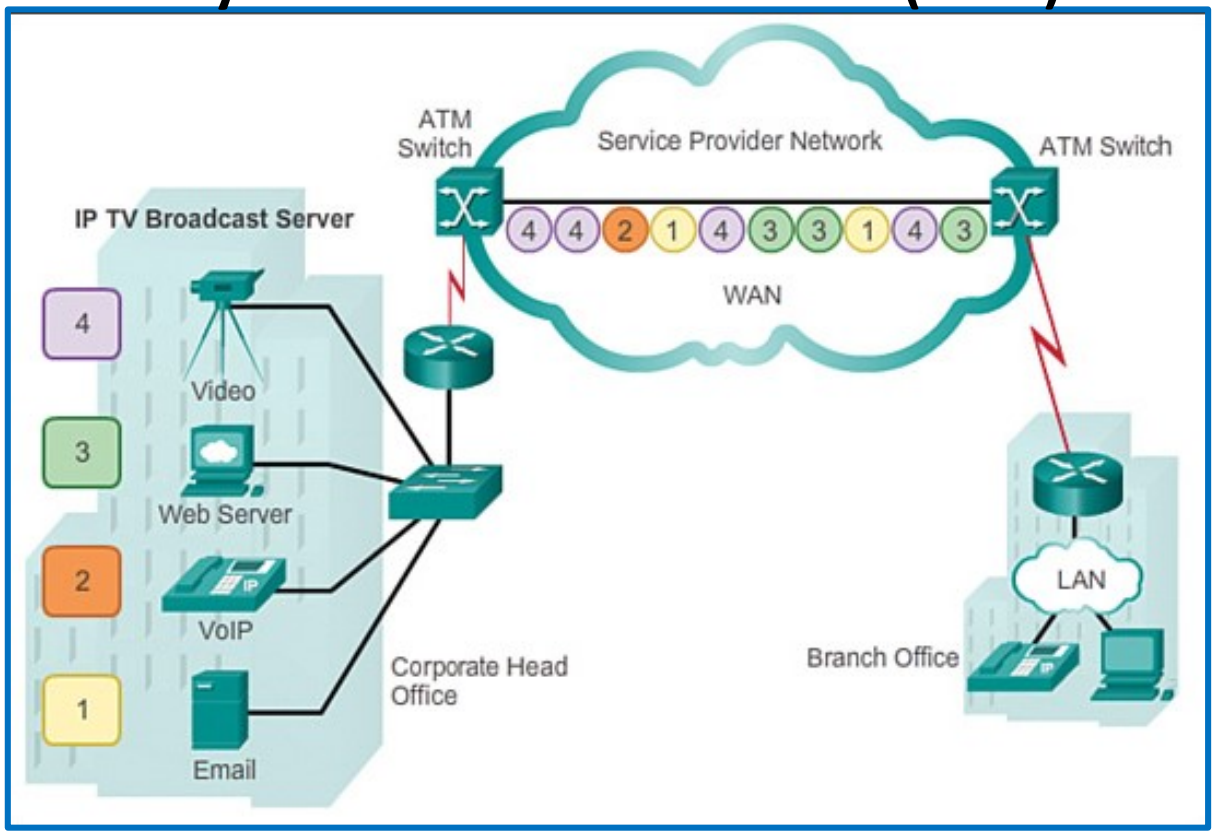
Private WAN Infrastructures

Frame Relay



It creates PVCs, which are uniquely identified DLCI. The PVCs and DLCIs ensure bidirectional communication from one DTE device to another

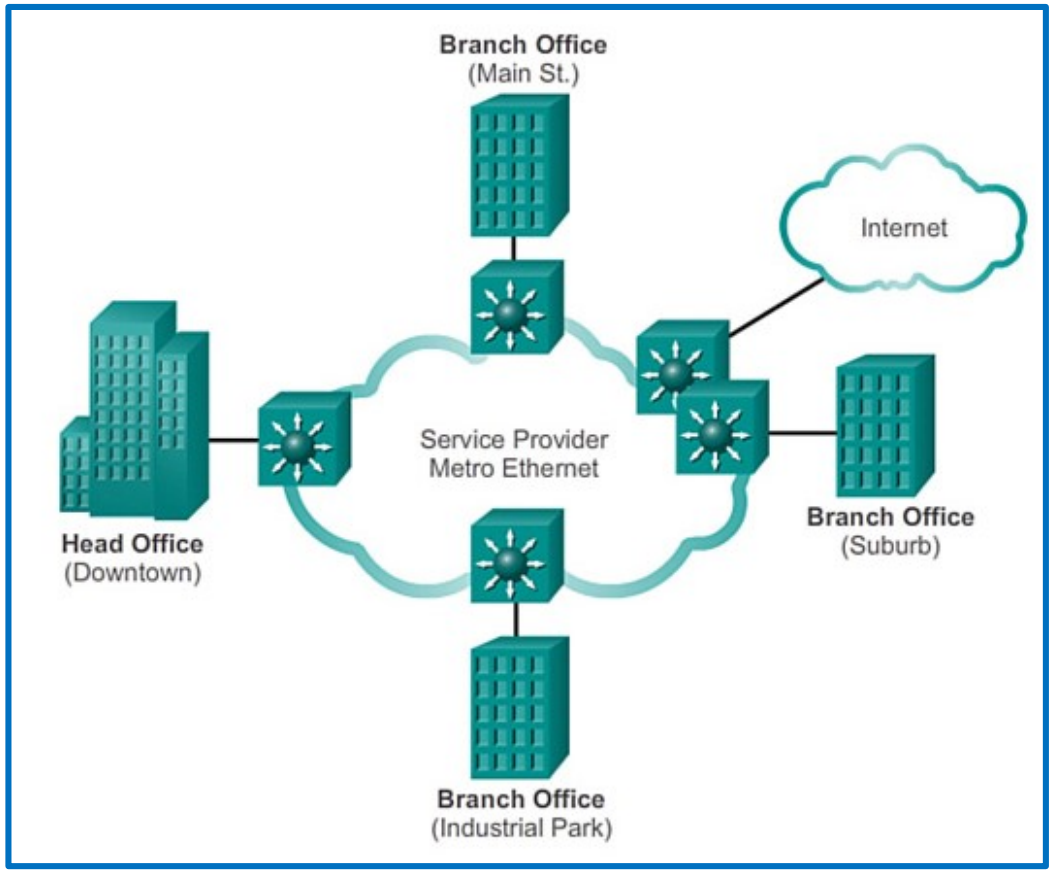
Asyncronous Transfer Mode (ATM)



It is capable of transferring voice, video, and data through private and public networks. ATM offers both PVCs and SVCs, although PVCs are more common with WANs

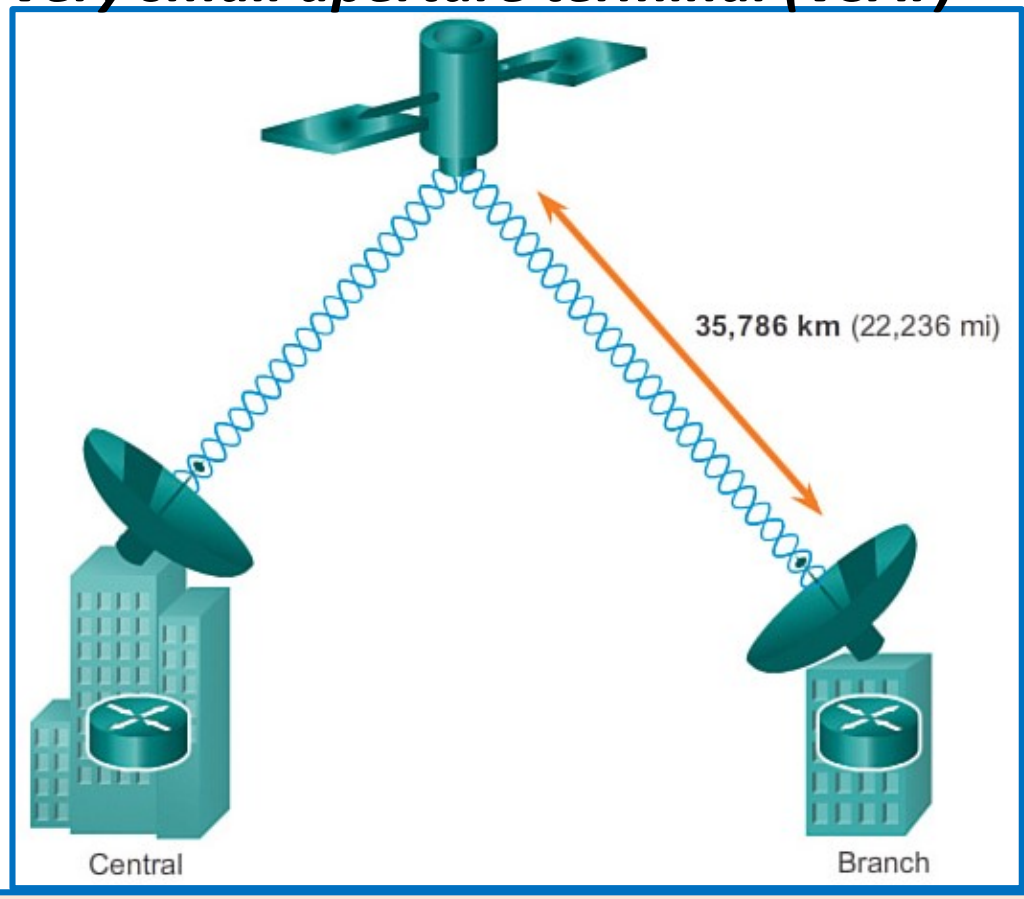
Private WAN Infrastructures

WAN Ethernet



WAN Ethernet standards using fiber-optic. E.g. the IEEE 1000BASE-LX standard supports fiber-optic cable lengths of 5 km, while the IEEE 1000BASE-ZX standard supports up to 70 km cable lengths.

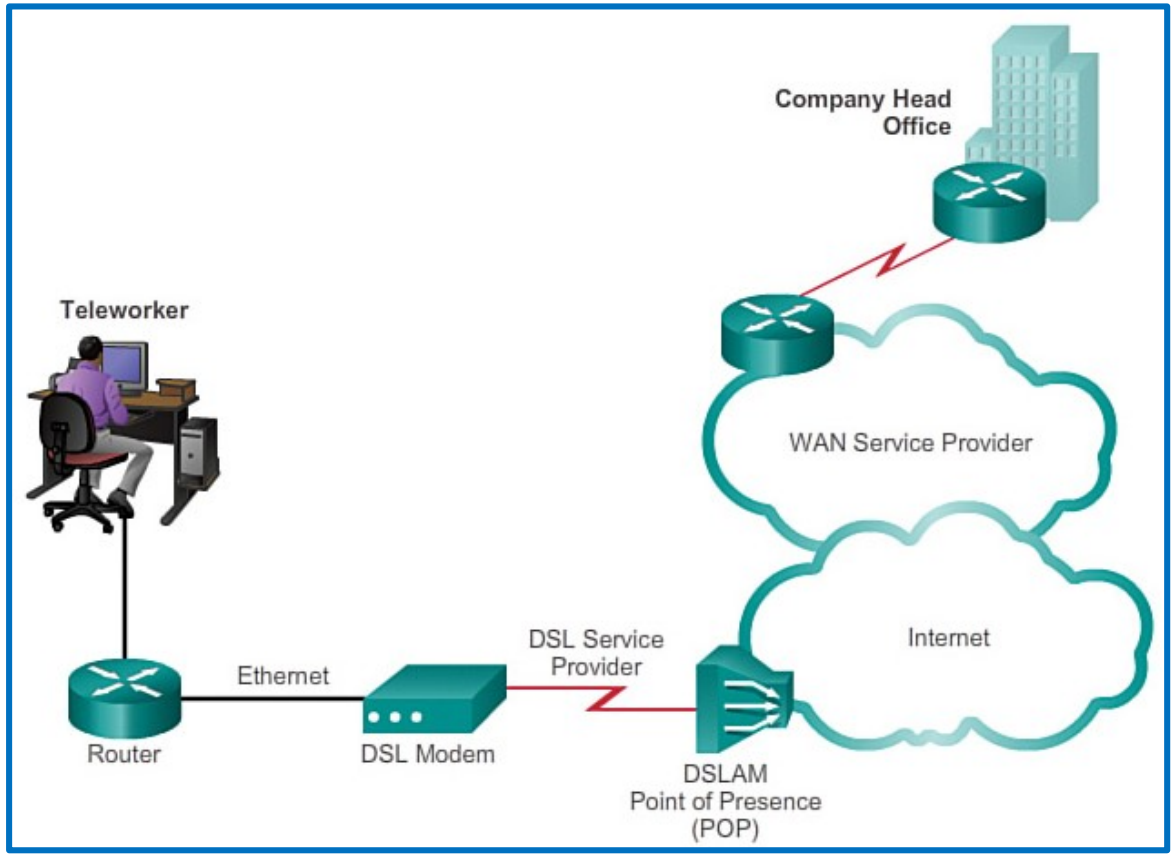
Very small aperture terminal (VSAT)



IT is a solution that creates a private WAN using satellite communications. A VSAT is a small satellite dish similar to those used for home Internet and TV.

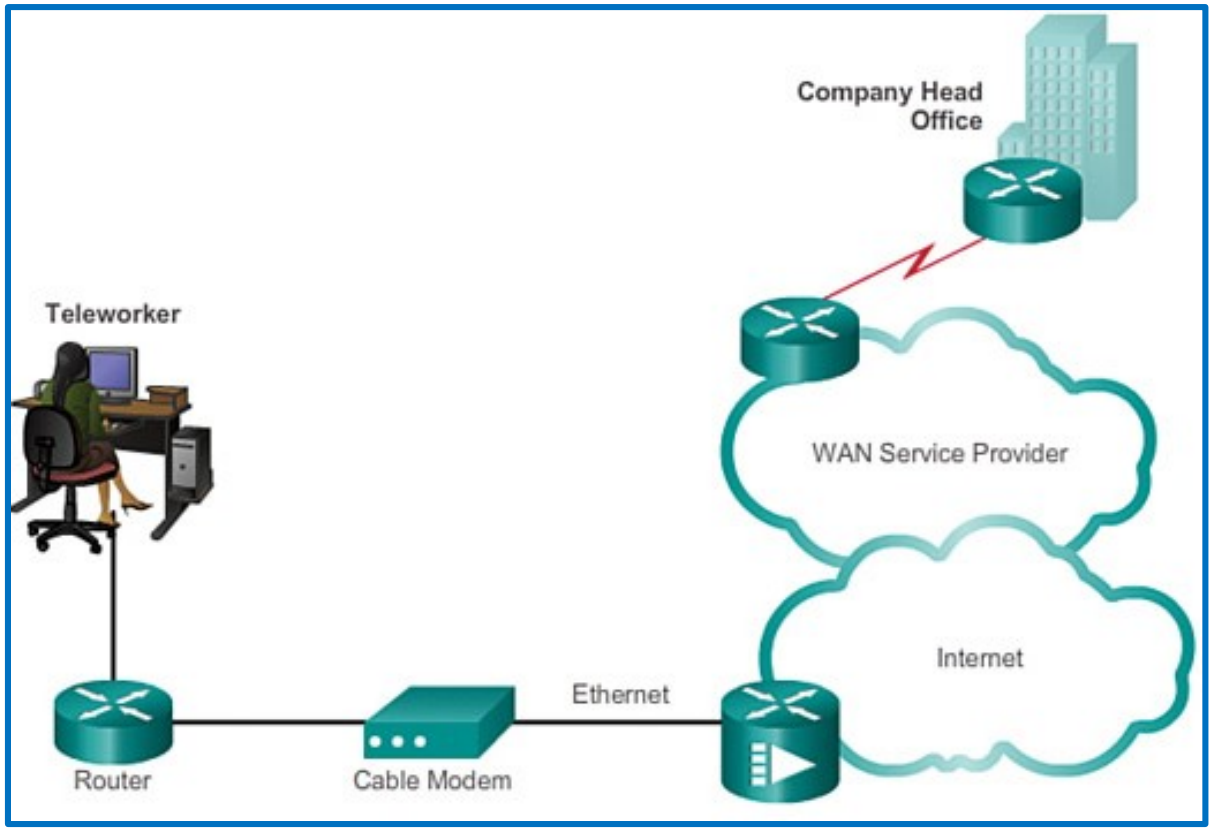
Public WAN Infrastructure

Digital Subscriber Line (DSL)



Uses existing twisted-pair telephone lines to transport high-bandwidth data, and provides IP services to subscribers. A ***DSL modem*** converts an Ethernet signal from the user device to a DSL signal, which is transmitted to the **CO**.

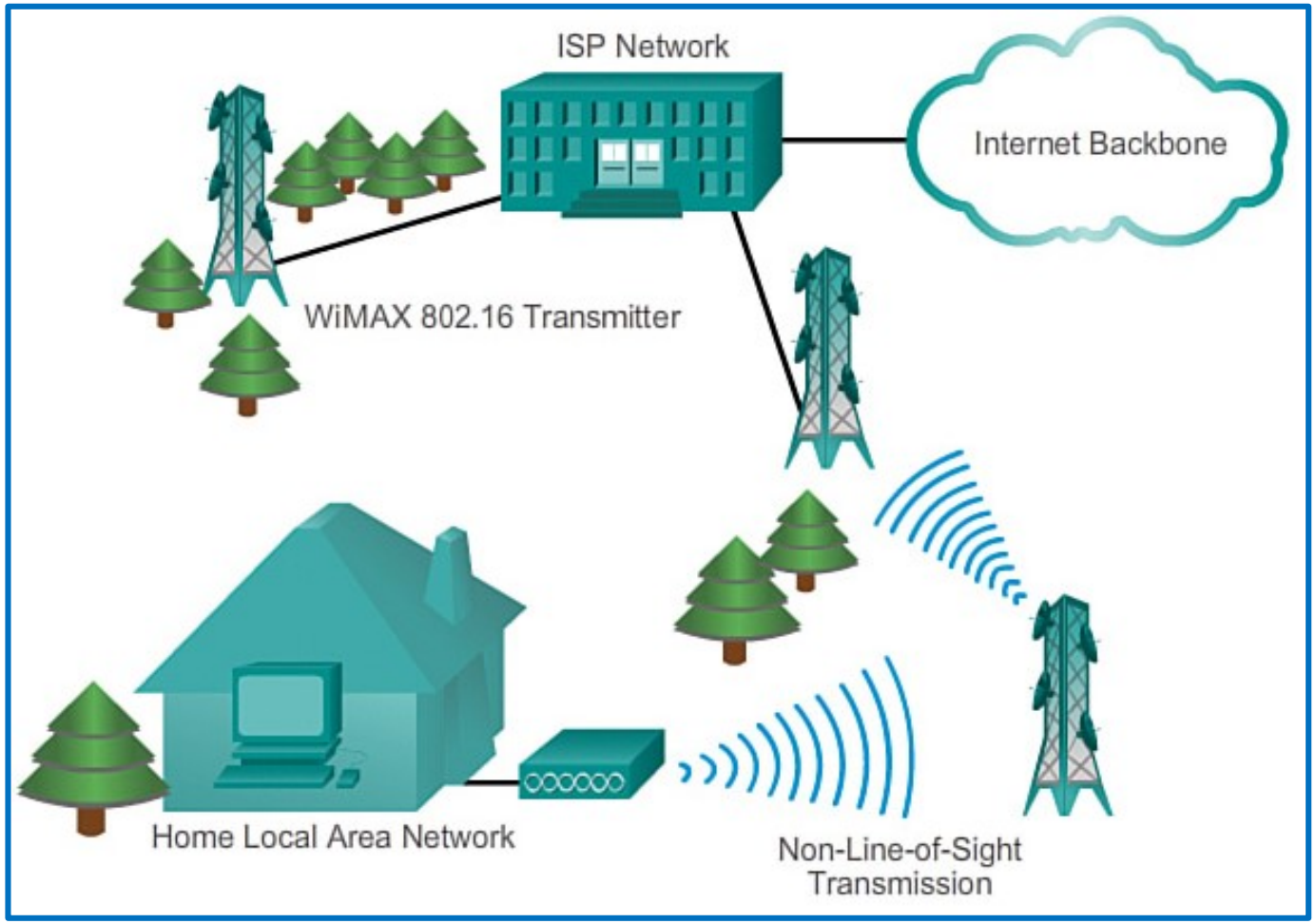
Cable



Coaxial cable is widely used in urban areas to distribute television signals. Network access is available from many cable television providers. This allows for greater bandwidth than the conventional telephone local loop.

Public WAN Infrastructure

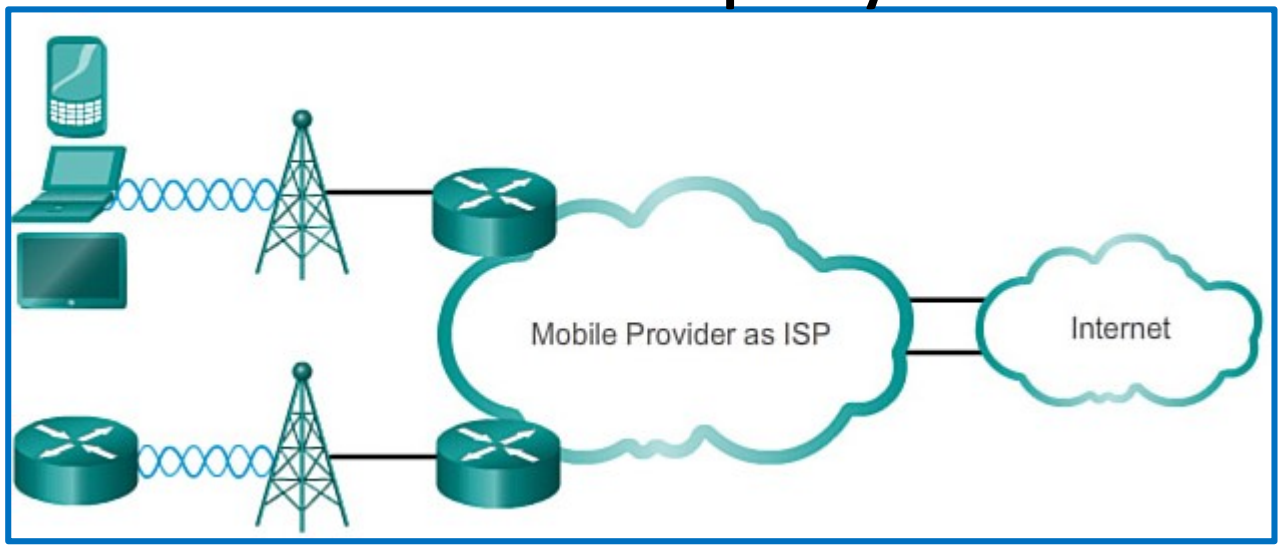
WIMAX



- **Worldwide Interoperability for Microwave Access (WiMAX)** is a new technology that is just beginning to come into use.
- It is described in the IEEE standard 802.16.
- WiMAX provides high-speed broadband service with wireless access and provides broad coverage like a cell phone network rather than through small Wi-Fi hotspots.
- WiMAX operates in a similar way to Wi-Fi, but at higher speeds, over greater distances, and for a greater number of users.
- It uses a network of WiMAX towers that are similar to cell phone towers.
- To access a WiMAX network, subscribers must subscribe to an ISP with a WiMAX tower within 30 miles of their location. They also need some type of WiMAX receiver and a special encryption code to get access to the base station.

Public WAN Infrastructure

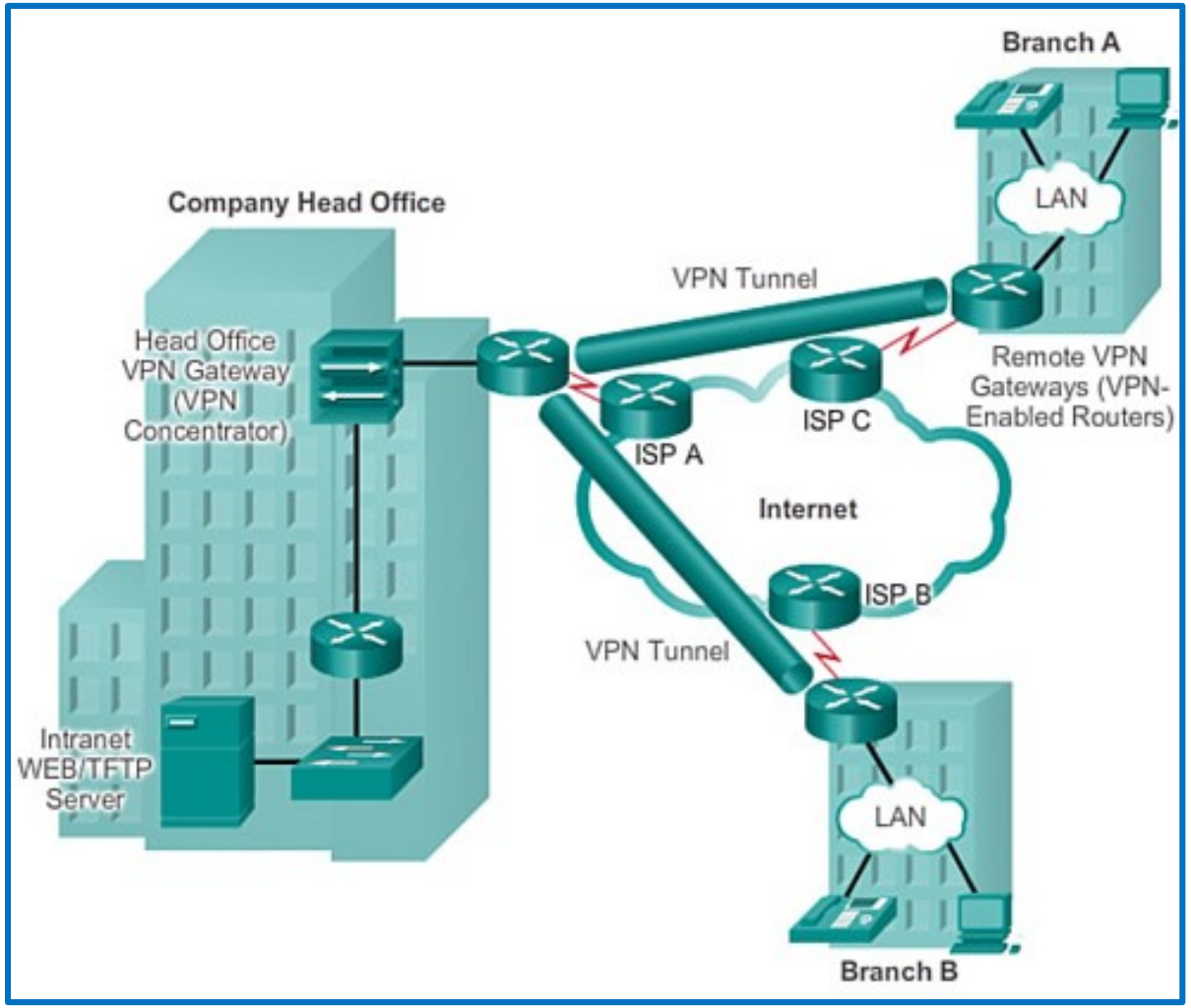
Cellular telephony



3G/4G/4G-LTE/5G Cellular

- Increasingly, cellular service is another wireless WAN technology being used to connect users and remote locations where no other WAN access technology is available.
- Many users with smartphones and tablets can use cellular data to email, surf the Web, download apps, and watch videos.
- **Long Term Evolution (LTE)**: Refers to a newer and faster technology and is considered to be part of fourth generation (4G) technology.

Virtual Private Network (VPN)



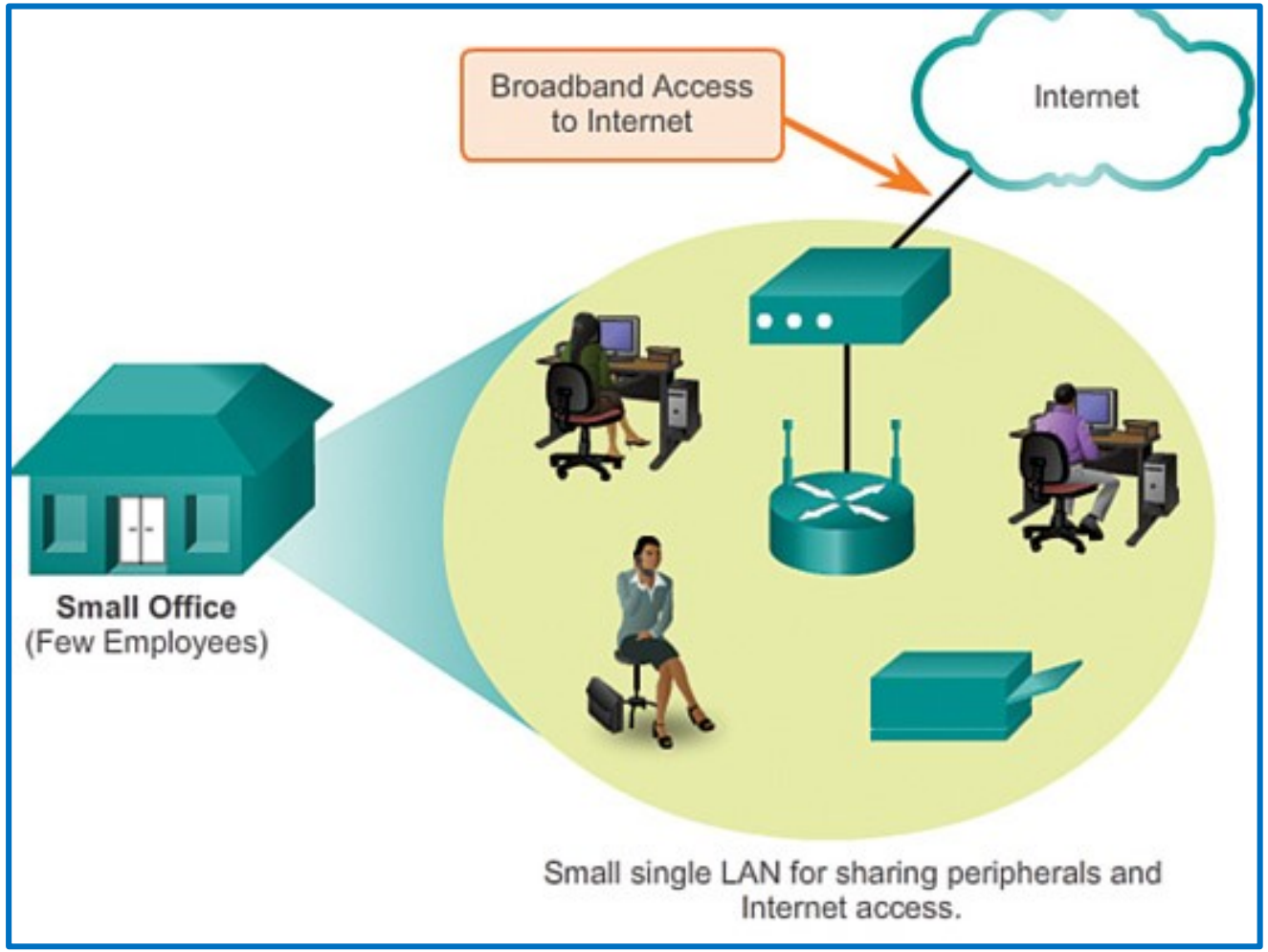
WAN Services Design Requirements

What Is the Purpose of the WAN?

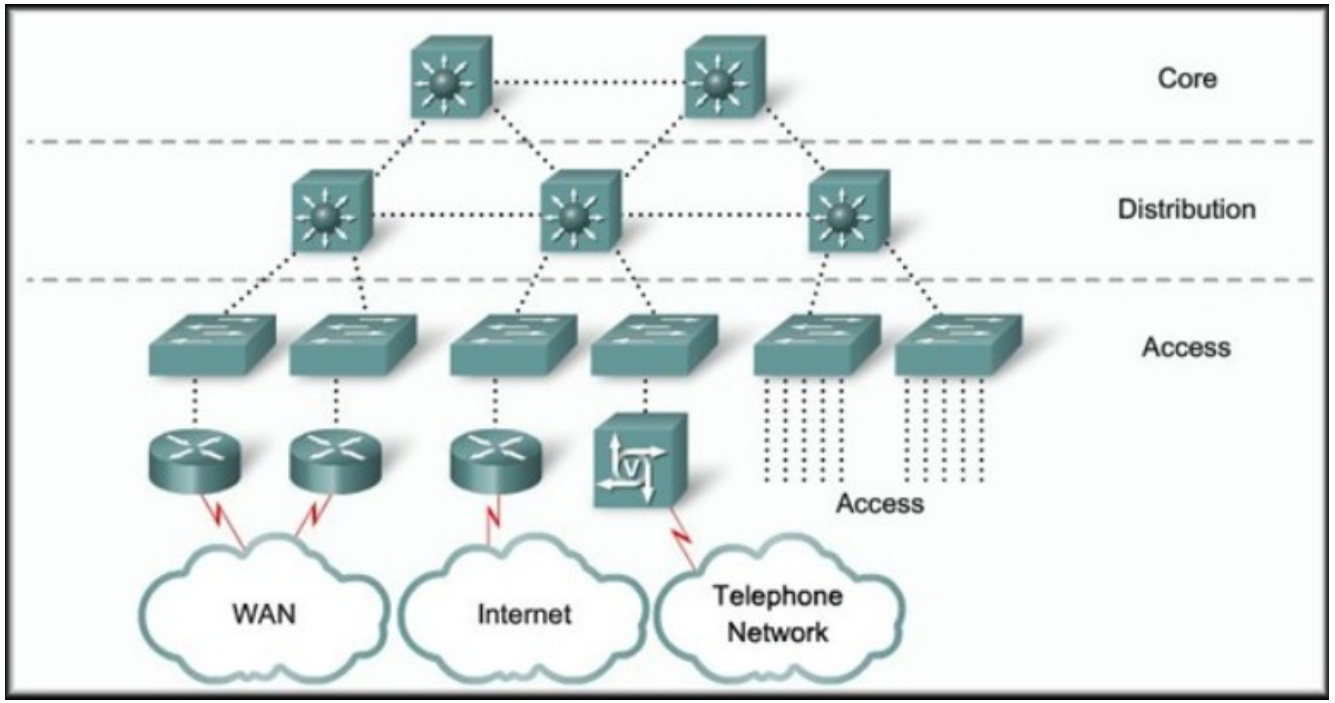
- Will the enterprise connect local branches in the same city area, connect remote branches, or connect to a single branch?
- Will the WAN be used to connect internal employees, or external business partners and customers, or all three?
- Will the enterprise connect to customers, connect to business partners, connect to employees, or some combination of these?
- Will the WAN provide authorized users limited or full access to the company intranet?

What Is the Geographic Scope?

- Is the WAN local, regional, or global?
- Is the WAN one to one (single branch), one to many branches, or many to many (distributed)?



WAN Services Design Requirements



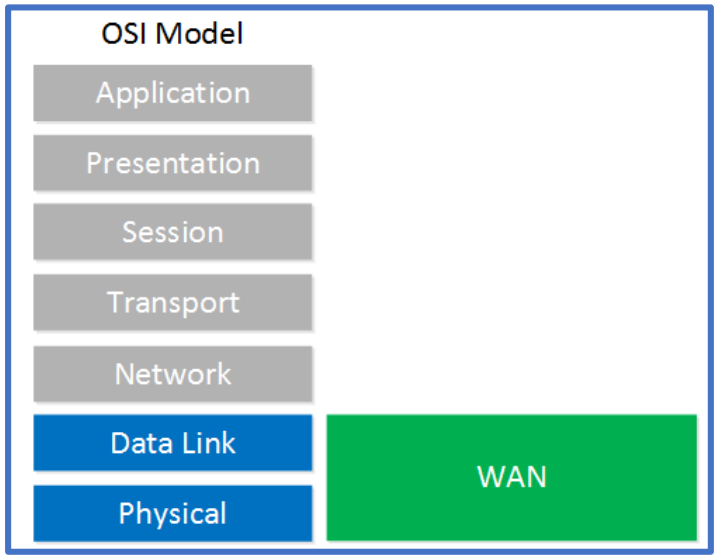
What Are the Traffic Requirements?

- What type of traffic must be supported (data only, VoIP, video, large files, streaming files)? This determines the **quality and performance requirements.**
- What volume of traffic type (voice, video, or data) must be supported for each destination? This determines the **bandwidth capacity required for the WAN connection to the ISP**.
- What quality of service is required? This may limit the choices. **If the traffic is highly sensitive to latency and jitter, eliminate any WAN connection options that cannot provide the required quality.**
- What are the security requirements (data integrity, confidentiality, and security)? These are important factors if the traffic is of a highly confidential nature, **or if it provides essential services, such as emergency response.**

Capa de Red

La capa Red:

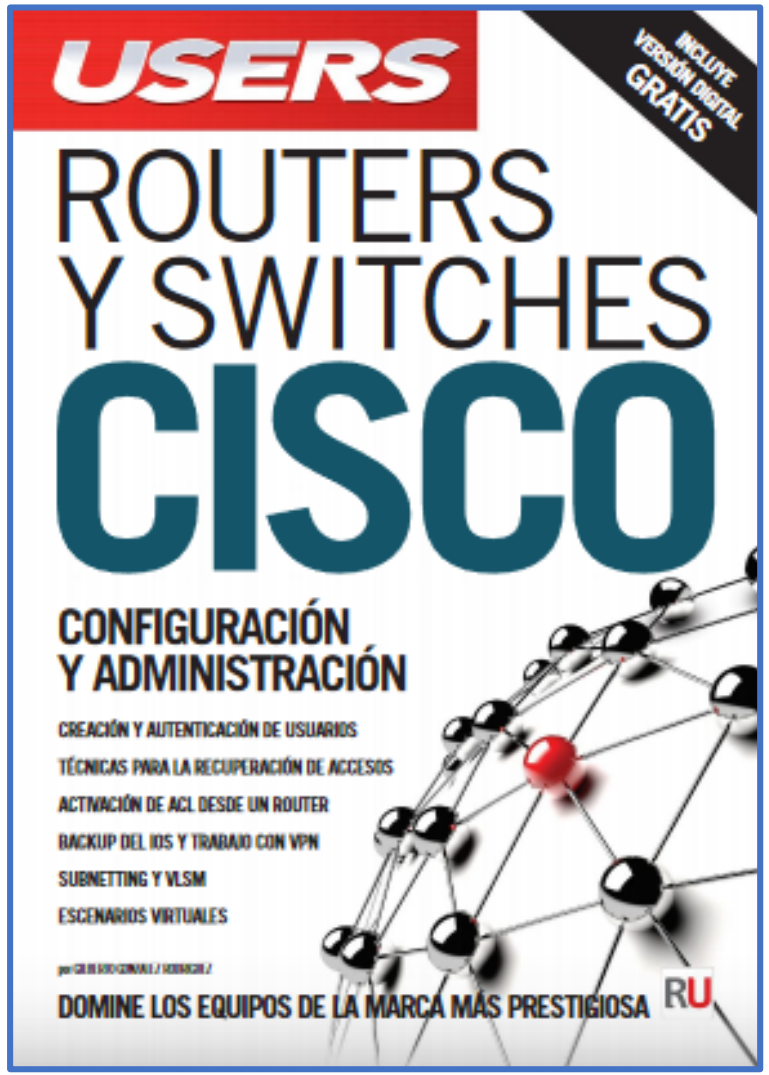
- La capa de red (capa 3 OSI) define el enrutamiento y el envío de paquetes entre redes.
- La función de la capa de red es transferir datos (paquetes) desde el host que origina los datos hacia el host que los usa, a través de varias redes separadas si fuera necesario.
- Paquete: es una unidad de tx/rx que tiene un formato específico y muchos atributos: IP-origen, IP-Destino, TTL, size, ….
- La capa de red del modelo OSI proporciona el enrutamiento de mensajes y determina si el destino de estos es la capa 4 (Transporte) o la capa 2 (Enlace de Datos).
- Para realizar este transporte de extremo a extremo la Capa de red utiliza cinco procesos básicos:
  - Direccionamiento universal (IP address);
  - Encapsulamiento (Application layer (data)--→ Transportación (messages o segments, logical ports (source, destination)) -→ Internet (packets, ip-address (source, Destin))--→ Network acceess (frame (MAC (source, dest), bits).
  - Desencapsulamiento (es el proceso inverso al encapsulamiento)
  - Enrutamiento es buscar la mejor ruta
  - Filtrado de paquetes, esquemas de seguridad, Firewall (Iptables), ACL, NAT, etc.



Fuente: https://eltallerdelbit.com/capa-de-red-capa-3-osi/

El router

- Ningún paquete puede ser enviado sin una ruta que es una IP address, que son coordenadas de servidores o routers en el ciberespacio.
- Los routers y otros dispositivos de networking, almacenan estas rutas en las tablas de enrutamiento, y las usan para determinar dónde enviar los datos.
- Los routers en su tabla de enrutamiento tienen tres características principales:
  - red de destino
  - próximo salto
  - métrica
- Un router toma una decisión de reenvío para cada paquete que llega a la interfaz del gateway. Este proceso de reenvío es denominado enrutamiento.
- El enrutamiento se hace paquete por paquete y salto por salto.
- El router hará una de tres cosas con el paquete:
  - Enviarlo al router del próximo salto
  - Enviarlo al host de destino
  - Descartarlo (filtrarlo)
- Se puede usar el Enrutamiento estático o dinámico (automático).

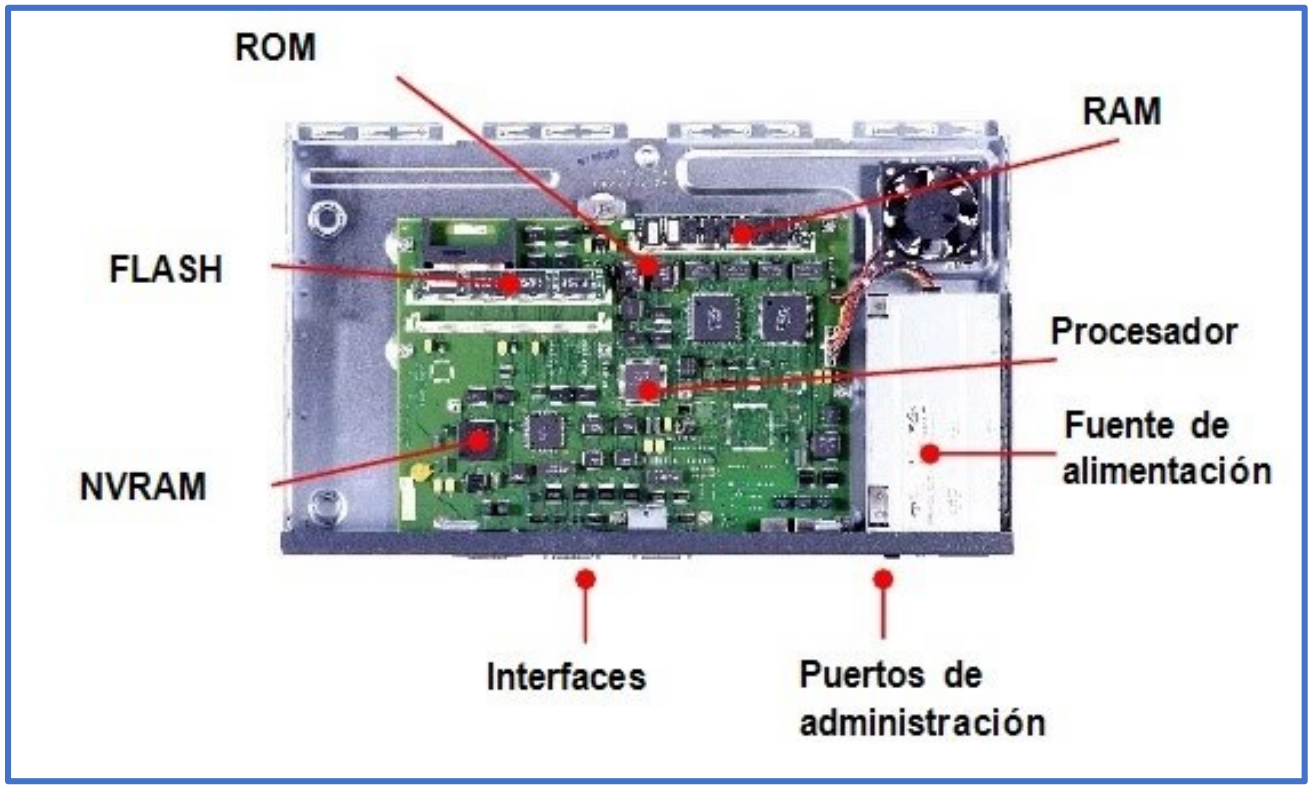


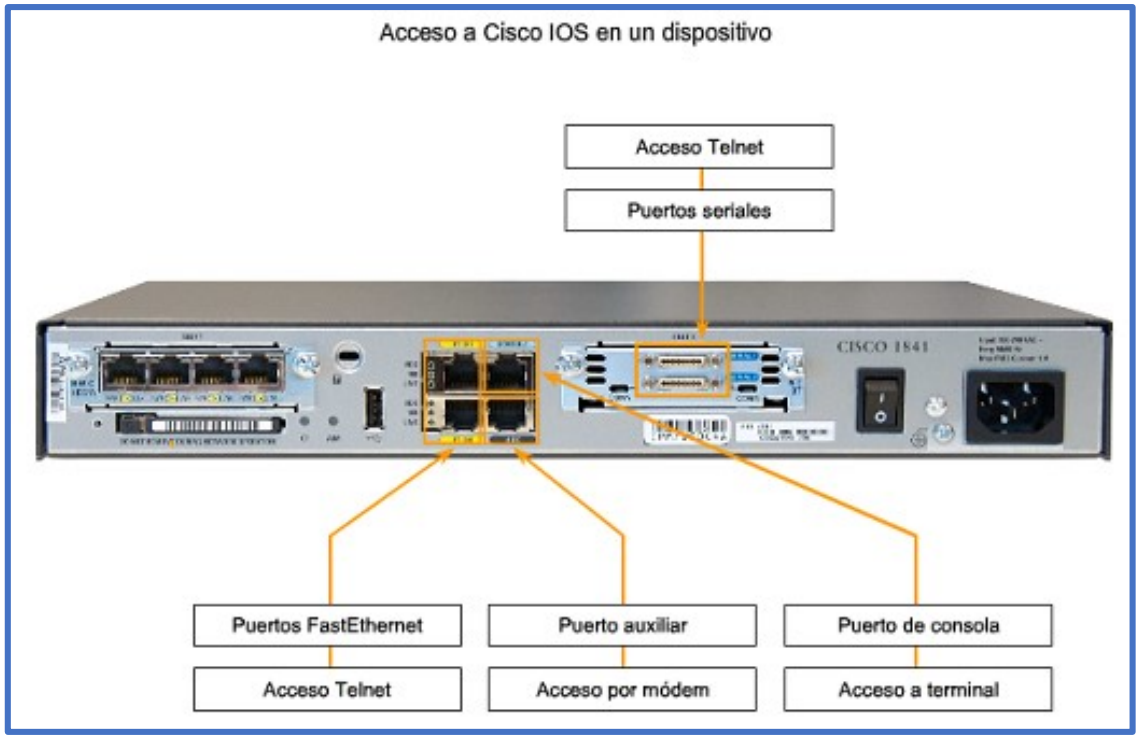
Fuente: https://eltallerdelbit.com/capa-de-red-capa-3-osi/

Router-Componentes

- **NVRAM** (memoria de acceso aleatorio no volátil): Almacena el archivo de configuración arranque (archivo startup-config) y retiene el contenido cuando se apaga o reinicia el router.
- **Memoria FLASH:** Es un tipo de ROM programable, que se puede borrar electrónicamente (EEPROM). Mantiene el contenido cuando se apaga o reinicia el router. Guarda la imagen del sistema operativo (IOS). Puede almacenar varias versiones del software IOS. La utilización de esta memoria permite que el software se actualice cargando una nueva imagen en la memoria flash, sin necesidad de retirar ni reemplazar chips en el procesador.
- **ROM** (memoria de sólo lectura): Guarda de forma permanente el código de diagnóstico de la prueba al inicio (POST), el programa bootstrap y el software básico del sistema operativo. Al ser una memoria de sólo lectura es necesario el cambio de la tarjeta de memoria para actualizaciones del software.
- **Interfaces.** Las interfaces son las conexiones de los routers con el exterior. Hay tres tipos diferentes de interfaces:
  - Interfaces LAN
  - Interfaces serial para la conexión con la red de área extensa (WAN).
  - Puertos de Consola/AUX

Router-Componentes





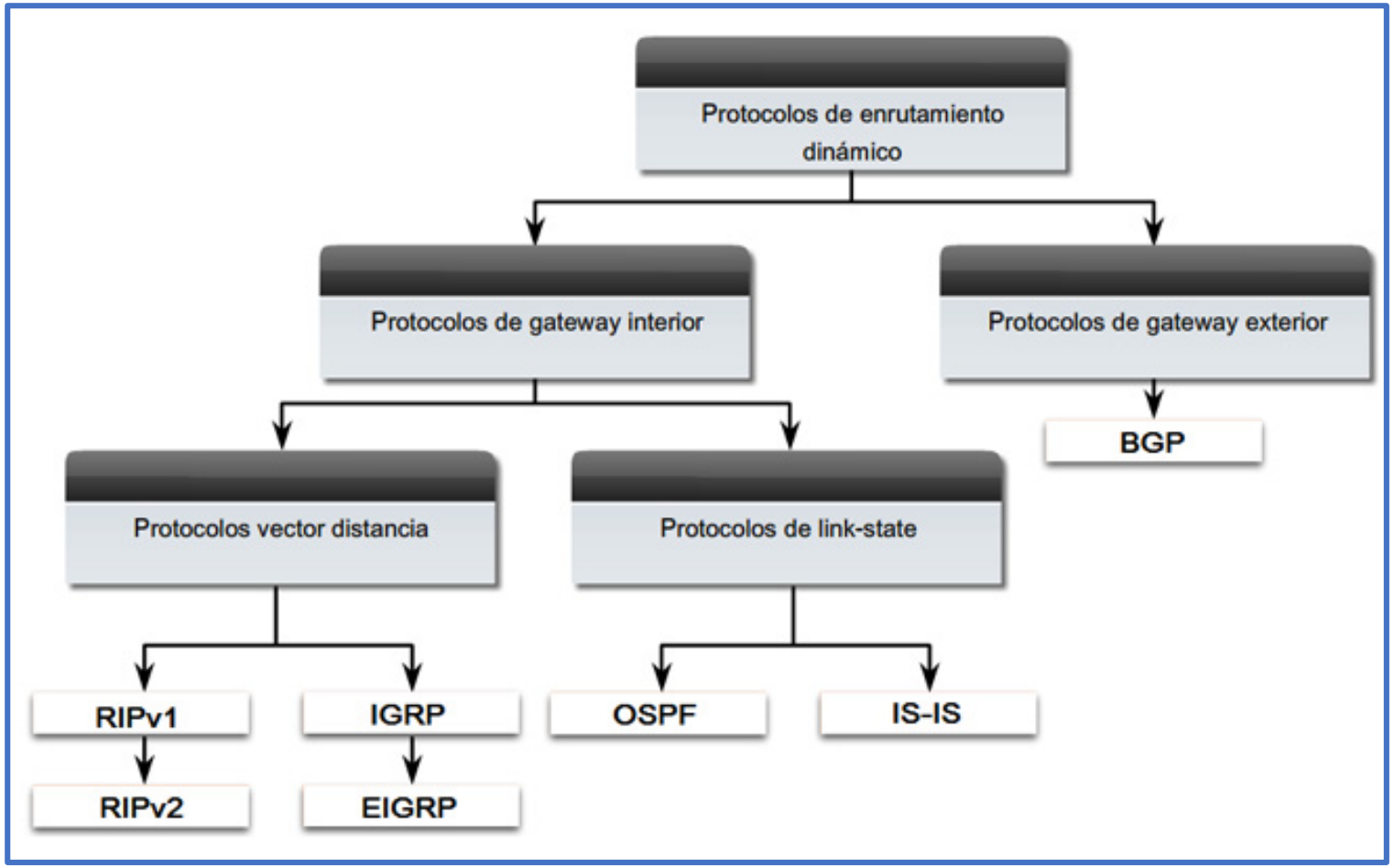
Source: https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/2-configuracion-de-routers/1-caracteristicas-y-aspectos-fisicos-de-los-routers/2-componentes-de-un-router|

Algoritmos de encaminamiento Dinámico

Enrutamiento Dinámico:

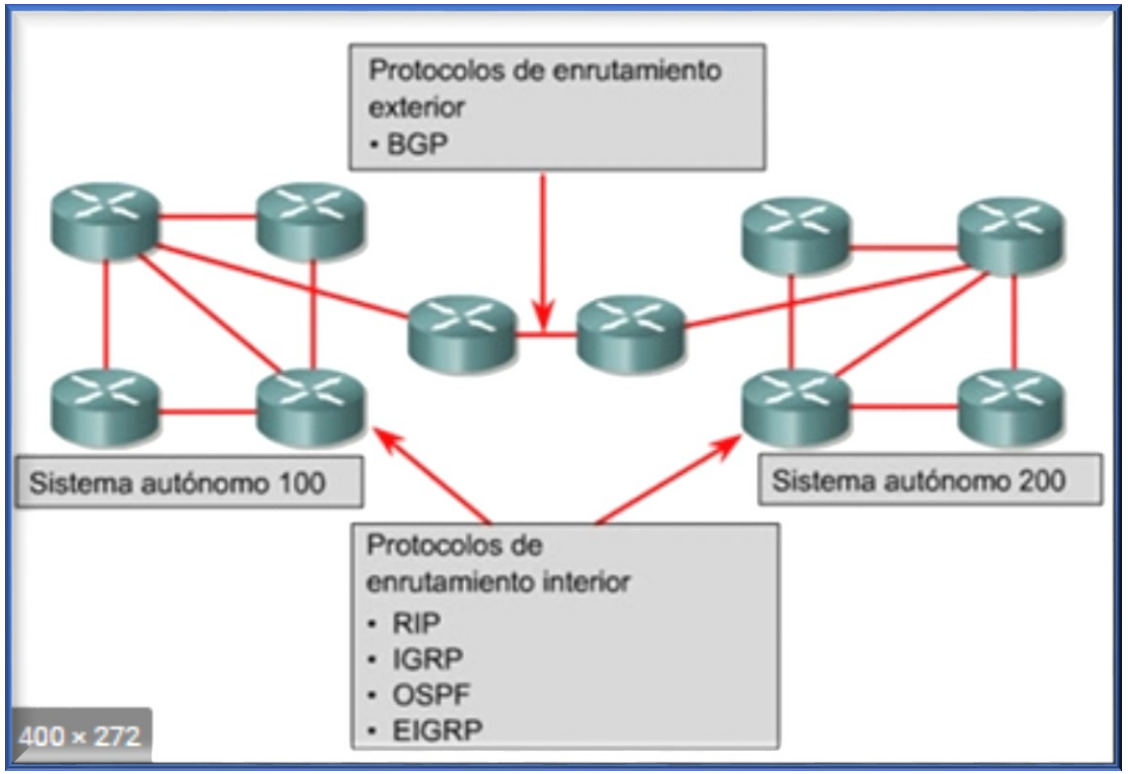
Entre los protocolos de enrutamiento comunes se incluyen:

- Protocolo de información de enrutamiento (RIP, Routing Information Protocol),
- Protocolo de enrutamiento de gateway interior mejorado EIGRP
- Open Shortest Path First OSPF
- —> En este punto es también muy importante conocer el concepto de Gateway (Puerta de Enlace), o Gateway por defecto.



Enrutamiento Dinámico

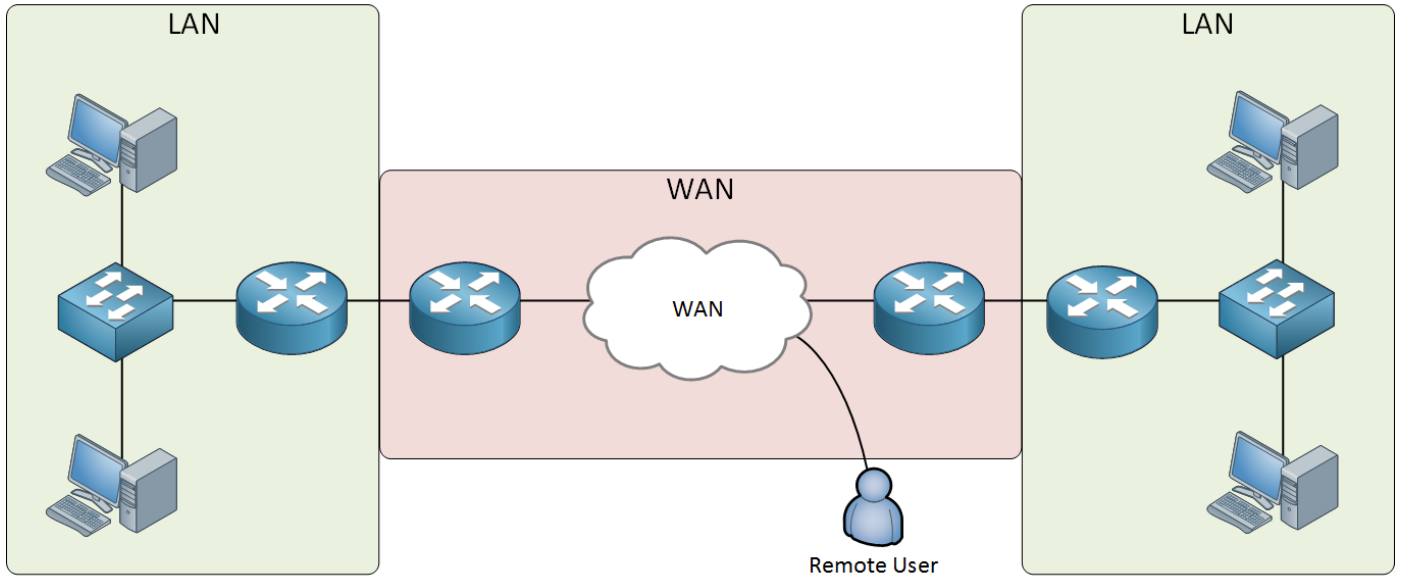
- **Direcciones con clase.** Son direcciones de red que dentro de la topologia tienen la misma mascara de red y no pueden subdividirse (FLSM).
- **Direcciones sin clase**. Son direcciones de red que permiten tener diferentes mascaras de subred en un una topología (VLSM).
- **Vector-Distancia**. Los routers se comunican con sus vecinos para pasar las tablas de enrutamiento y usar un algoritmode métrica el cual cuenta el número de saltos.
- **Estado-Enlace**. Los routers transmiten sus rutas a una BD de un router el cual concentrará la información, para despues hacer la actualización a los demás routers.
- **Convergencia**. Es cuando todos los routers manejan las tablas de ruteo de acuerdo a la topologia que existe.
- **Métrica.** Es la forma que tiene un protocolo de ruteo para medir la mejor ruta a un destino.
- **Distancia Administrativa (DA):** nos indica la preferencia para seleccionar una ruta y contemplarla en la tabla de ruteo.



Taller de caracterización de un router empresarial.

Se pide:

- Organizar grupos de trabajo de 3 o 4 estudiantes (máximo). No existen grupos iguales o menores de 2)
- Investigar las características de los routers empresariales.
  - Arquitectura interna (Dimensiones de CPU, RAM, ROM, FLASH, NVRAM)
  - Arquitectura externa (Tipos de interfaces, velocidades, alcance)
  - Multi-acceso, servicios, formas de configuración
- Elabore un informe abierto, tuneado, con marcas, costos, características, que de respuesta a este taller.
- Una presentación en power point de 5 minutos.
- Favor subirlo a la carpeta compartida en Drive



Routing Information Protocol (RIP)

Essentials of RIP:

- Is a **dynamic routing protocol** which uses hop count as a routing metric to find the best path between the source and the destination network.
- It is **a distance vector routing protocol** which has AD value 120 and works on the application layer of OSI model.
- RIP uses **port number** 520.
- Hop Count **is the number of routers** occurring in between the source and destination network.
- The path with the **lowest hop count** is considered as the best route to reach a network and therefore placed in the routing table.
- The **maximum hop count allowed for RIP is 15** and hop count of 16 is considered as network unreachable. The **maximum hop count allowed for RIP version 2 is 30.**

Features of RIP :

1. Updates of the network are exchanged periodically;
2. Updates (routing information) are always broadcast;
3. Full routing tables are sent in updates;
4. Routers always trust on routing information received from neighbor routers.

RIP versions :

There are three versions of routing information protocol:

- **RIP Version1**;
- **RIP Version2** and
- **RIPng with IPV6**.

Routing Information Protocol (RIP)

RIP Routing protocol configuration commands summary

Command	Description
Router(config)#router rip	Enable RIP routing protocol
Router(config-router)#network a.b.c.d	Add a.b.c.d network in RIP routing advertisement
Router(config-router)#no network a.b.c.d	Remove a.b.c.d network from RIP routing advertisement
Router(config-router)#version 1	Enable RIP routing protocol version one (default)
Router(config-router)#version 2	Enable RIP routing protocol version two

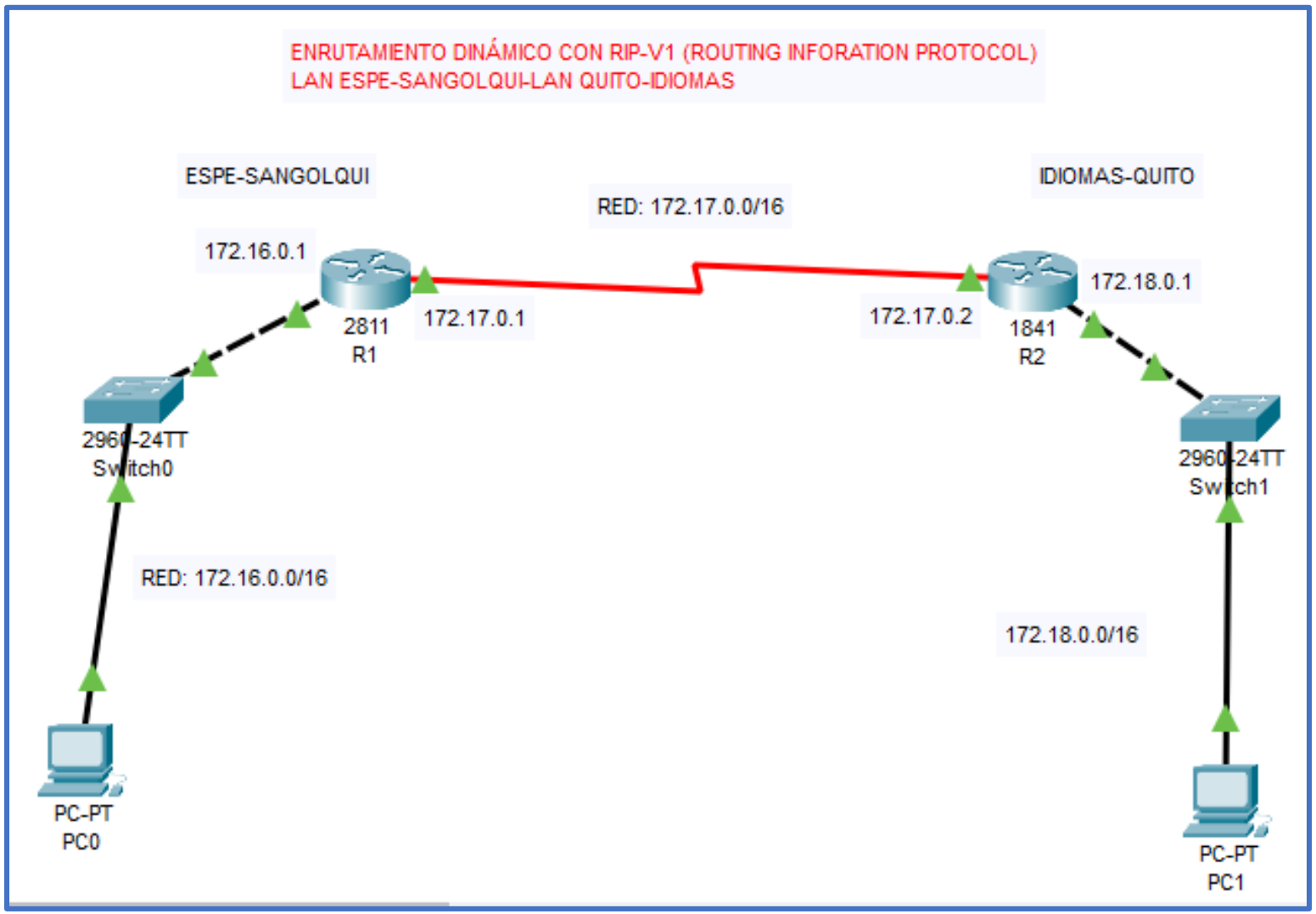
>> Use this command to show all routes configured in router, say for router R1 :

```
R1# show ip route
```

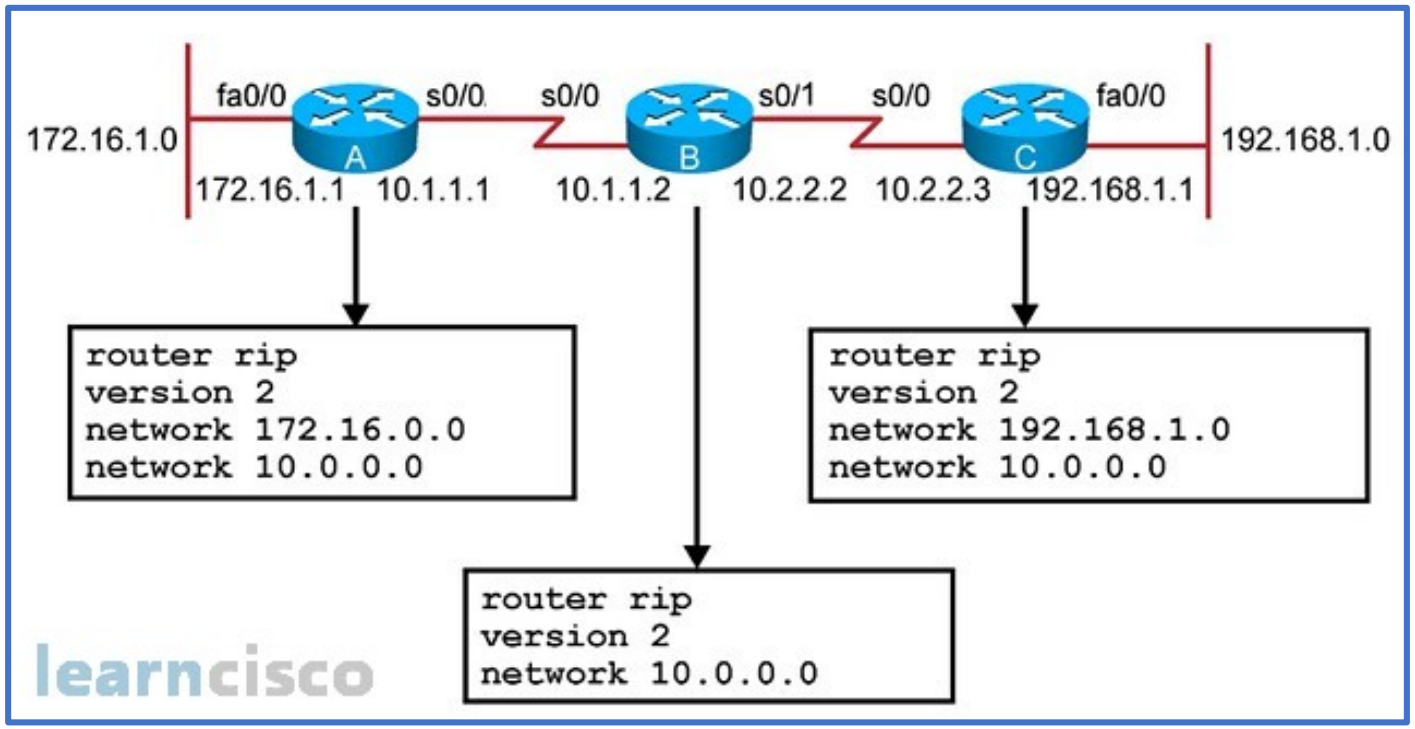
```
R1(config)# router rip
R1(config-router)# network 192.168.20.0
R1(config-router)# network 172.16.10.4
```

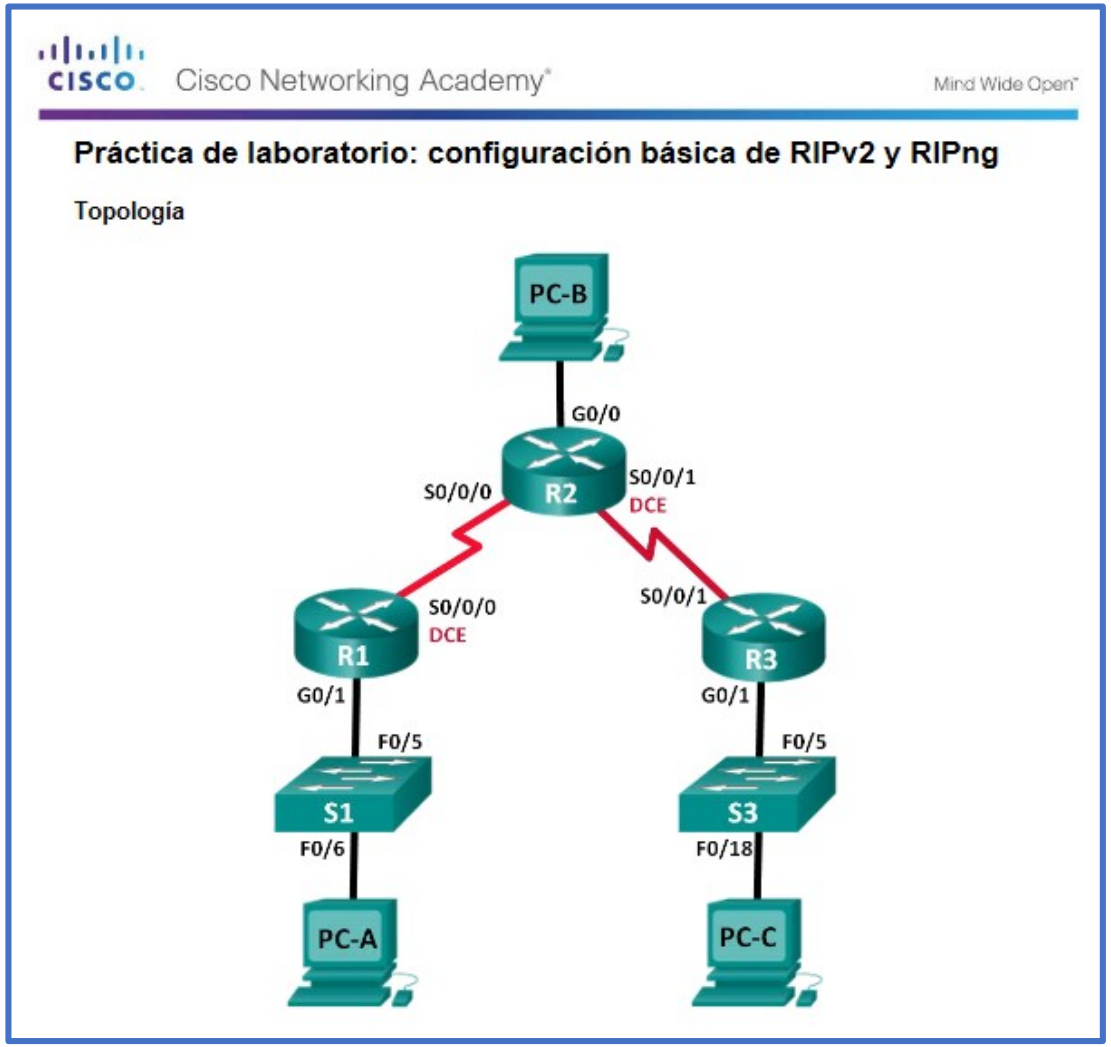
RIP v1	RIP v2
Sends update as broadcast	Sends update as multicast
Broadcast at 255.255.255.255	Multicast at 224.0.0.9
Doesn't support authentication of update messages	Supports authentication of RIPv2 update messages
Classful routing protocol	Classless protocol, supports classful

RIP V1, Exercices:



RIP V2, Homework:





Open Shortest Path First (OSPF) protocol

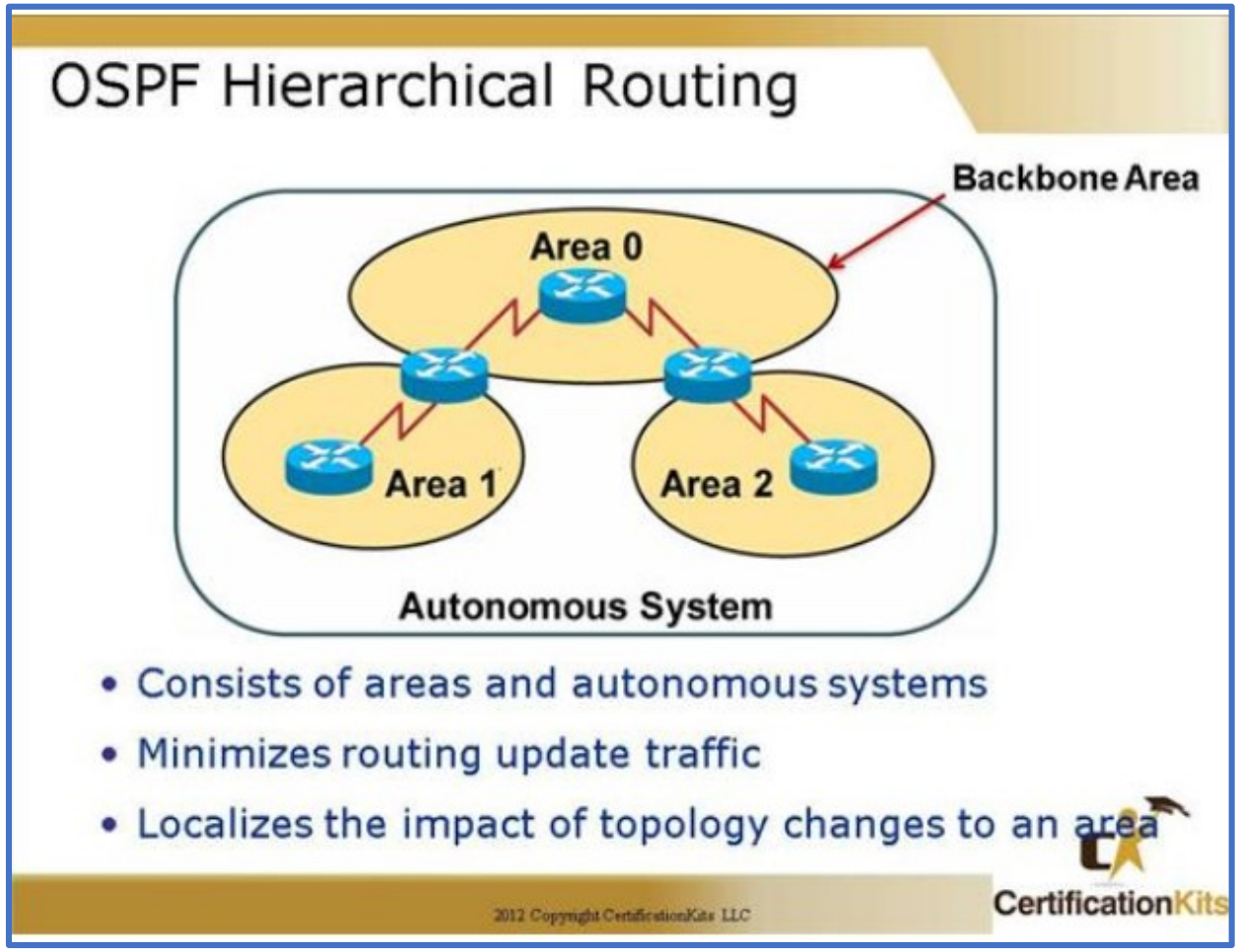
Essentials of OSPF

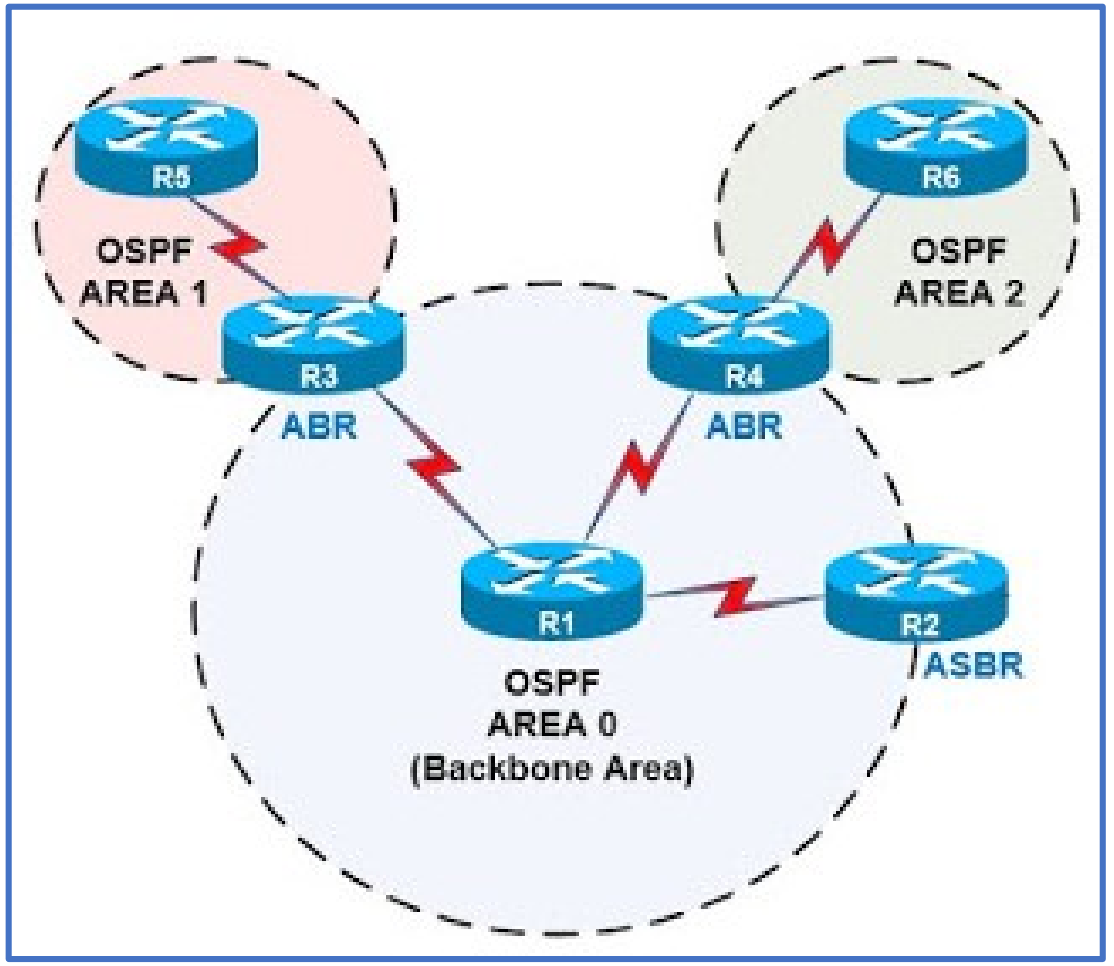
- It is defined in RFC 2328 leavingcisco.com.
- It is an Interior Gateway Protocol used to distribute routing information within a single Autonomous System.
- The OSPF protocol is based on link-state technology.
- OSPF has introduced new concepts such as authentication of routing updates, Variable Length Subnet Masks (VLSM), route summarization, and Autonomous System and Areas.

Features of OSPF

- With OSPF, there is no limitation on the hop count.
- The intelligent use of VLSM is very useful in IP address allocation.
- OSPF uses IP multicast to send link-state updates.
- OSPF ensures a better use of bandwidth.
- OSPF has better convergence than RIP.
- OSPF allows for a logical definition of networks where routers can be divided into areas.
- OSPF allows for routing authentication by using different methods of password authentication.
- OSPF allows for the transfer and tagging of external routes injected into an Autonomous System.

Autonomous Systems and Areas





OSPF-Wildcards

- Una máscara **Wildcard Cisco**, es una máscara de bits que indica qué partes de una dirección de IP son relevantes para la ejecución de una determinada acción.
- Otra forma de decirlo es que el Wilcard es la representación de bits significativos (generalmente los bist de red) y no significativos (generalmente los bits de host), se escribe exactamente al contrario de una máscara de subred.
- Usos principales
  - Indicar el tamaño de una red o subred para algunos protocolos de enrutamiento, como OSPF.
  - Indicar qué direcciones IP tendrían que ser permitidas o denegadas en las listas de control del acceso (ACLs).

Ejemplo 1: El Wildcard para la máscara de red 255.255.255.0

	255	255	255	255
—	255	255	255	0
				255

Wildcard: 0.0.0.255

Ejemplo 2: El Wildcard para la máscara de red 255.255.255.240

	255	255	255	255
—	255	255	255	240
				15

Wildcard: 0.0.0.15

Fuente: Qué es Wildcard-Cisco, URL: https://eclassvirtual.com/que-es-el-wildcard-cisco/

OSPF main Configurations Commands

Table 1
OSPF Basic Configuration

1	Enter global configuration mode.	router#configure terminal
2	Create an OSPF routing process and enter router configuration mode.	router(config)#**router ospf** *process-id*
3	Configure the interfaces that OSPF will be enabled on.	router(config-router)#**network** *network wildcard-mask* **area** *area-id*

OSPF Basic Configuration— Individual network statements

1	Enter global configuration mode.	router#configure terminal
2	Enter EIGRP router configuration mode.	router(config)#**router ospf** 10
3	Configure a network statement for the F0/0 interface.	router(config-router)#**network** 172.16.100.0 0.0.1.255 **area** 0
4	Configure a network statement for the F0/1 interface.	router(config-router)#**network** 172.16.50.128 0.0.0.127 **area** 0
5	Configure a network statement for the F0/2 interface.	router(config-router)#**network** 172.16.1.0 0.0.0.255 **area** 0

Práctica de laboratorio: OSPFv2 básico de área única Topología

Topología

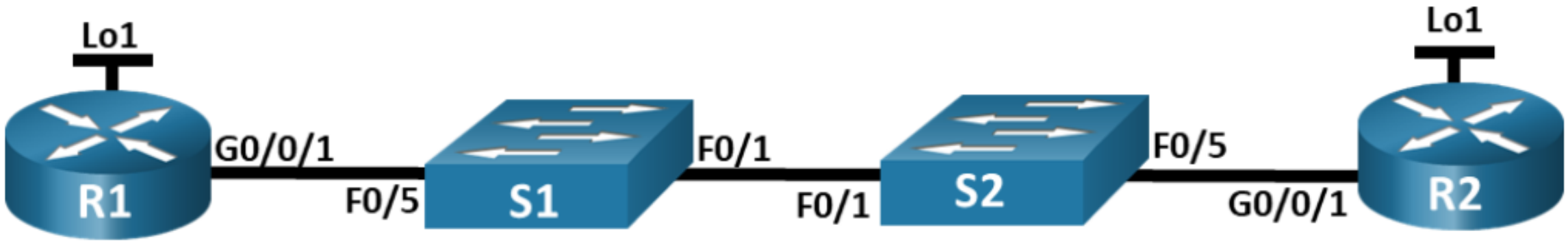


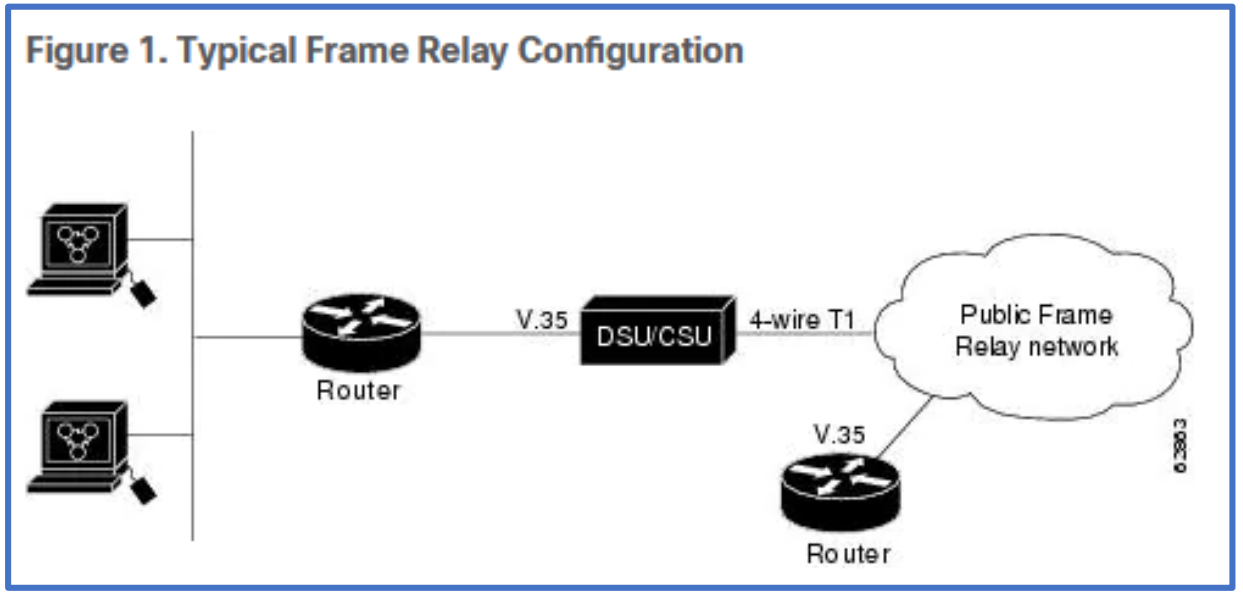
Tabla de asignación de direcciones

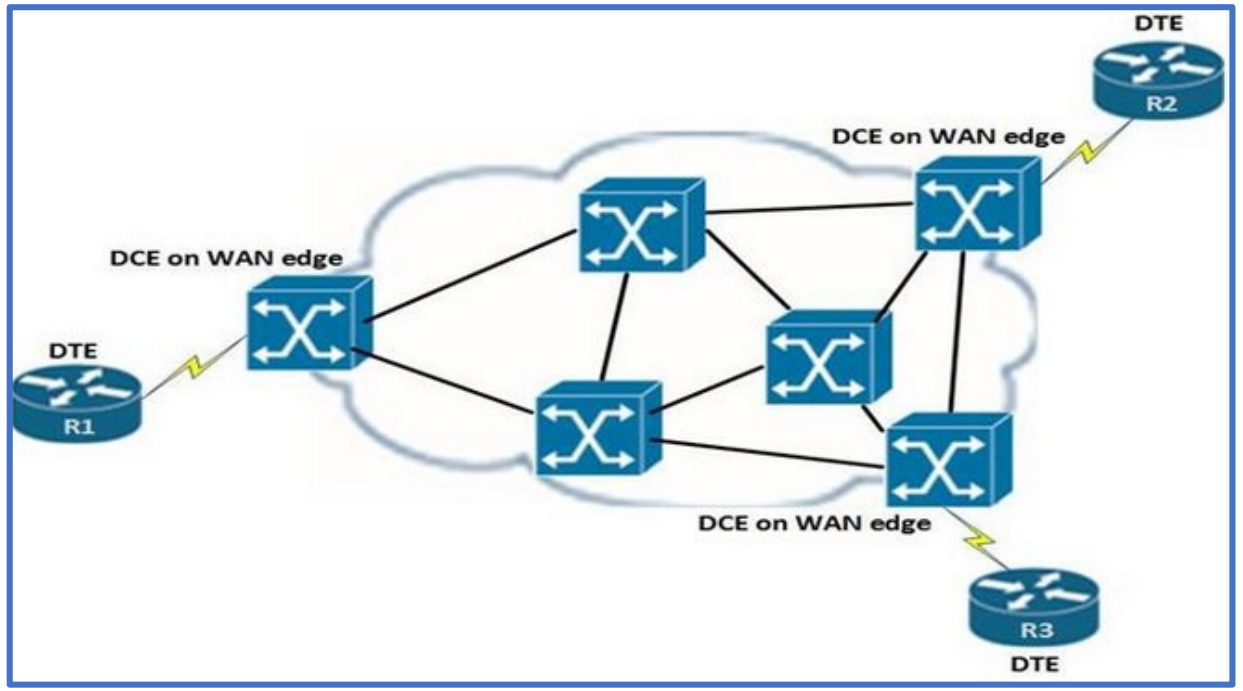
Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/0/1	10.53.0.1	255.255.255.0
	Loopback1	172.16.1.1	255.255.255.0
R2	G0/0/1	10.53.0.2	255.255.255.0
	Loopback1	192.168.1.1	255.255.255.0

Frame Relay

Introduction

- Frame Relay is **WAN protocol** with high performance operating at layer 1 and layer 2 of the OSI model.
- In frame relay, **costs are reduced** by using less equipment, easy implementation and reduced complexity.
- Despite this, it is possible for a customer to get **high bandwidth, reliability** and more resilience as compared to leased connections.
- In frame relay, the **connection from DTE to the DCE** devices (switches), is made up of both physical layer components as well as data link layer components.
- In frame relay, the **routers connected** to remote networks are usually the DTE devices while the **frame relay switch** is usually the DCE device.





Frame Relay

Virtual Circuits

- In frame relay, the connection between the two remote DTE devices is known as a (VC) virtual circuit.
- Unlike direct connections such as PPP and HDLC, there is no physical connection between the host and destination networks between the frame relay networks.
- The Virtual Circuits are used as a path for bidirectional communication between the source and destination devices.
- They are identified by addresses known as **DLCIs** which are usually given out by the WAN service provider.

High-Level Data Link Control (HDLC) is a group of data link (Layer 2) protocols **used to** transmit synchronous data packets between point-to-point nodes. Data is organized into addressable frames. This format has been **used for** other multipoint-to-multipoint protocols, and inspired the **HDLC**-like framing protocol described in RFC 1662.

A **data link connection identifier** (DLCI) is a Frame Relay 10-bit-wide link-local virtual circuit identifier used to assign frames to a specific PVC or SVC. Frame Relay networks use DLCIs to statistically multiplex frames.

LMI Local Management Interface

The LMI is a mechanism that provides information on the status of a frame relay connection between a DTE and a DCE device.

There are several LMI types, and they are incompatible with others, the LMI configured must match the LMI on the service provider.

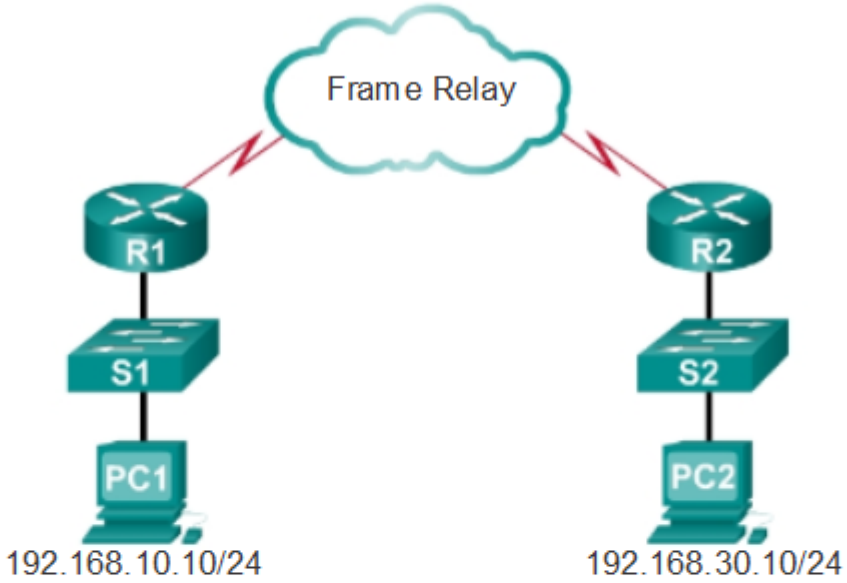
Frame Relay

Basic frame relay configuration

- ❖Paso 1. Establezca la dirección IP en la interfaz;
- ❖Paso 2. Configure la encapsulación;
- ❖Paso 3. Establezca el ancho de banda;
- ❖Paso 4. Establezca el tipo de LMI (optativo).

```
R1(config)#
R1(config)#interface serial0/0/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#no shutdown

R2(config)#
R2(config)#interface serial0/0/0
R2(config-if)#encapsulation frame-relay
R2(config-if)#no shutdown
```

Tareas de configuración de Frame Relay

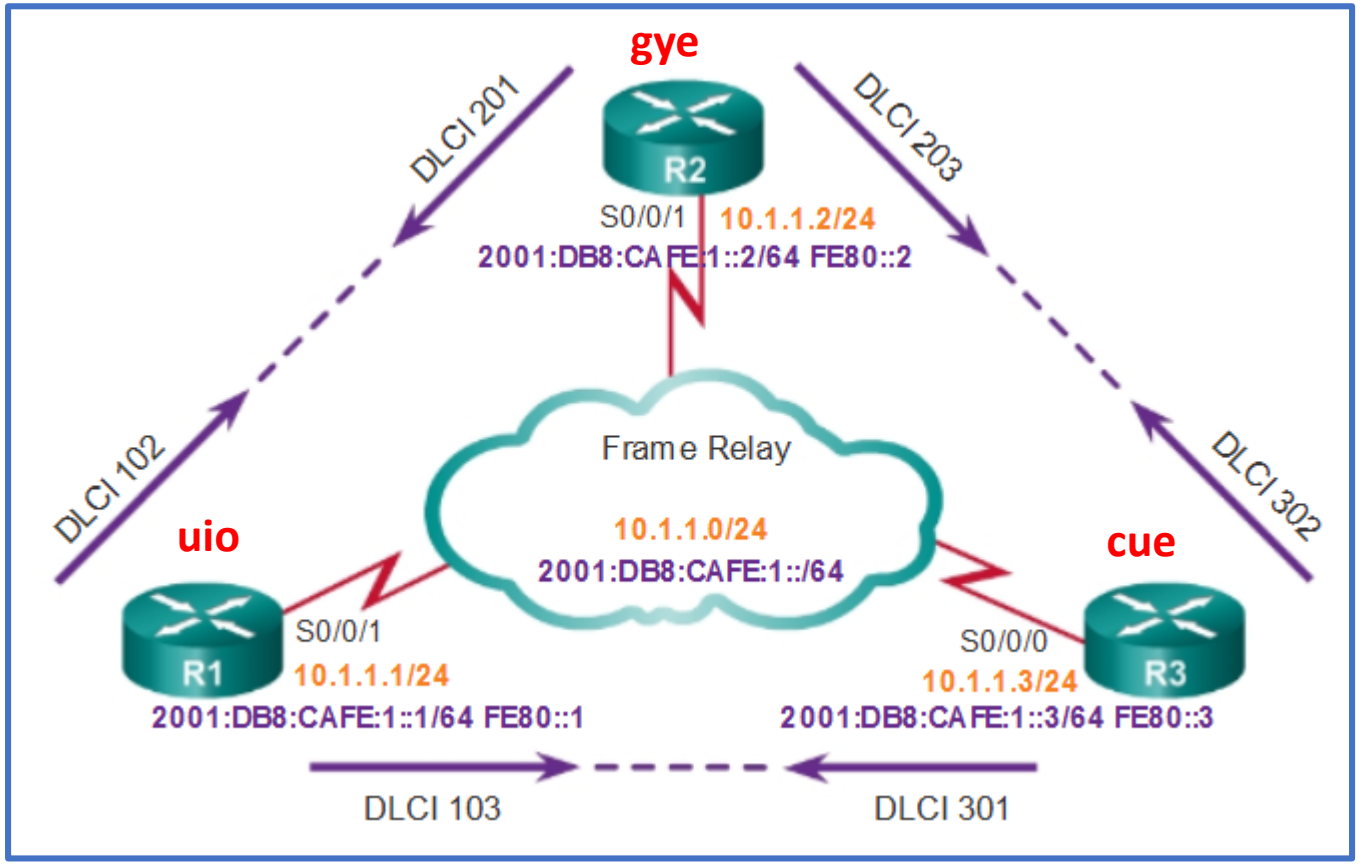


Tareas requeridas	Tareas opcionales
Habilitar la encapsulación de Frame Relay en una interfaz.	Configurar la LMI.
Configurar la asignación de direcciones dinámica o estática.	Configurar SVC de Frame Relay.
	Configurar el modelado del tráfico de Frame Relay.
	Personalizar Frame Relay para la red.
	Controlar y mantener las conexiones de Frame Relay.

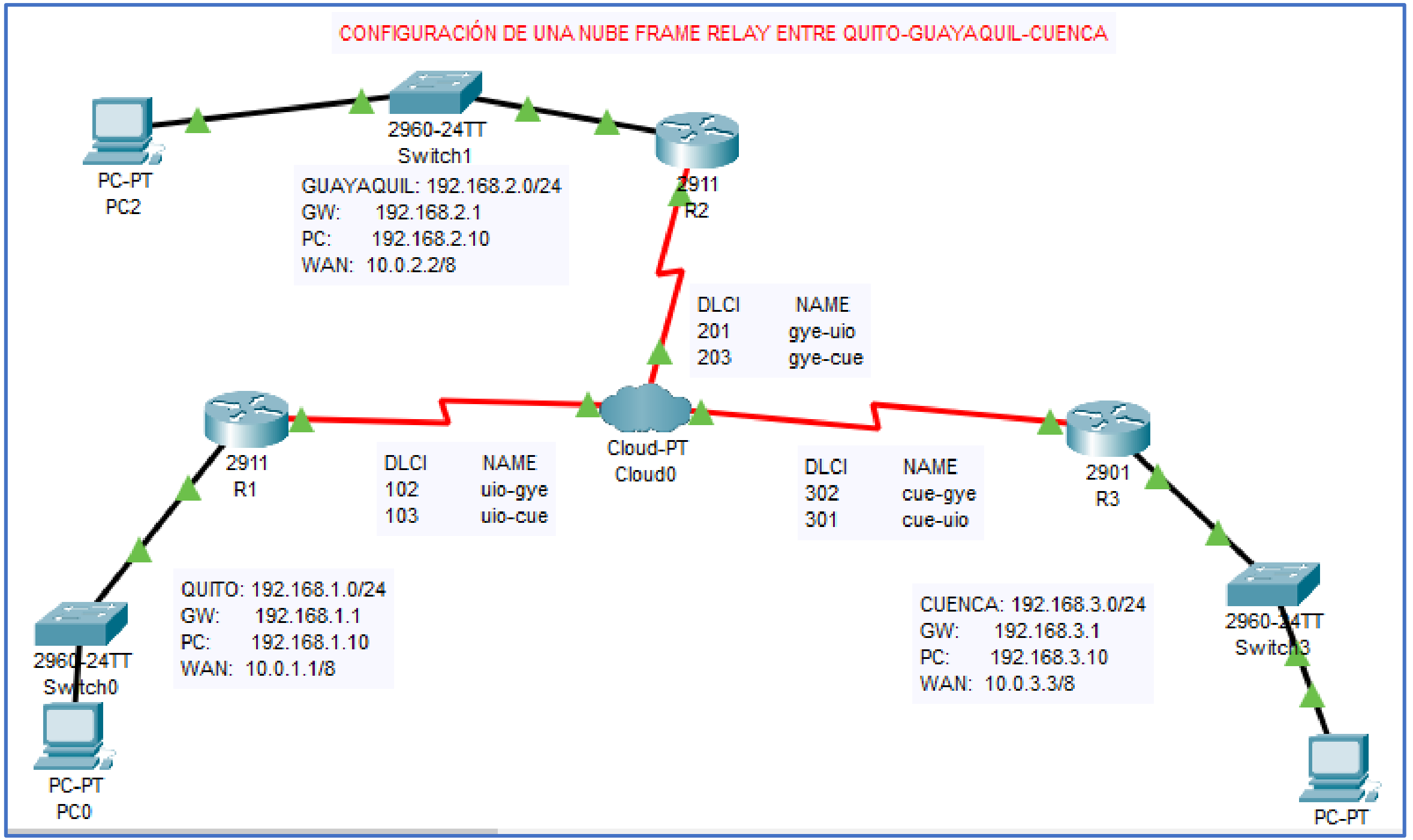
Frame Relay: Example

Connect three cities in a frame relay cloud: Quito (uio), Guayaquil (gye) and Cuenca (cue):

- Physically design the WAN;
- Program the cloud: Configure DLCIs on the serial interfaces of the cloud;
- Connect the circuits in the Frame Relay cloud;
- Configure static routing on each router;
- Configure Frame Relay encapsulation on each serial interface of the routers;
- Check connectivity.



CONFIGURACIÓN DE UNA NUBE FRAME RELAY ENTRE QUITO-GUAYAQUIL-CUENCA



NAT: NETWORK ADDRES TRANSLATION