

Manual de configuración de Redes Telemáticas de mediana y gran envergadura con equipos **CISCO**

Tutorizado por: Moisés Pérez Delgado

Edición Febrero 2019

CFGS Sistemas de Telecomunicaciones e Informáticos

Sergio Martín González
Isaac Martín Mendoza
Abisai Plasencia Fleitas
Daniel Plasencia Hernández



Javier Acosta González
Arai Cabrera González
Victor Carrero León
Jose Domínguez Darias

Índice

[Plantilla para nuevas páginas](#)

[Modelo OSI](#)

[Trabajo 1.1. Diseño y simulación de una red de datos elemental. Primeros pasos con PT](#)

[Trabajo 1.2. Red de Hubs interconectados](#)

[Trabajo 1.3. Red de hubs interconectados mediante un bridge](#)

[Trabajo 1.4. Red de ordenadores conectados mediante un switch](#)

[Trabajo 1.5. Instalación y operación básica de switches](#)

[Trabajo 1.6. Seguridad básica. VLAN y trunking](#)

[Trabajo 2.1. Subnetting: Cálculo y diseño](#)

[Trabajo 2.2. VLSM: Diseño y pruebas DHCP y BOOTP RIP v2](#)

[Trabajo 2.3. Subnetting: Cálculo](#)

[Trabajo 2.4. Cisco Lab 2: Configurando Interfaces](#)

[Trabajo 3.1. Enrutamiento estático en routers corporativos](#)

[Trabajo 3.2. InterVLAN routing: router on a stick](#)

[Trabajo 3.3. VTP: VLAN Trunking Protocol. Cisco Lab 3](#)

[Trabajo 3.4. Configuración básica sobre equipos reales: switch 2950-12 \(I\)](#)

[Trabajo 3.5. Routers Cisco de 3ª Generación: Serie 4000](#)

[Trabajo 4.1. Creación de una conexión WAN por xDSL](#)

[Trabajo 4.2. Simulación de conexión ISP - cable y xDSL](#)

[Trabajo 4.3. Simulación de conexión ISP - cable y xDSL utilizando NAT](#)

[Trabajo 5.1. Puesta en servicio de redes. Protocolos dinámicos](#)

[Anexo I](#)

[Anexo I. BOOTP](#)

[Anexo I. CIDR](#)

[Anexo I. Beneficios de las mejoras en 3ª Generación. Routers Cisco Serie 4000](#)

[Anexo I. Glosario de comandos](#)

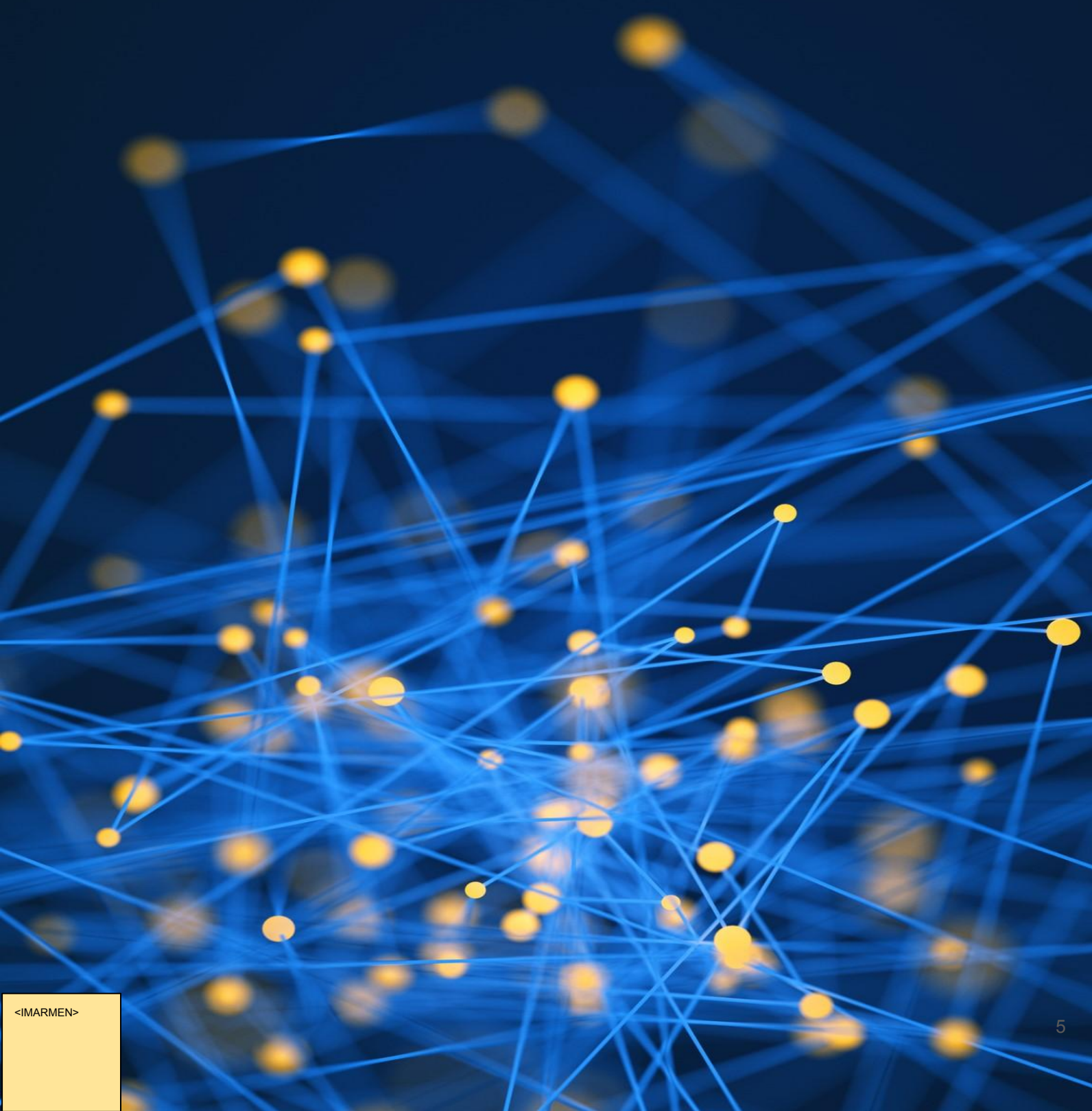
Historial de versiones

Versión	Descripción	1.5Aportaciones	
v1 Inicio: 18 Septiembre Fin: 25 Septiembre	Explicación detallada de los campos Ejercicio 1.1: Víctor e Isaac Ejercicio 1.2: Javier y Abisay Ejercicio 1.3: Sergio y Jose Ejercicio 1.4: Aray y Daniel	IMARMEN: 9 ACABGON: 7 DPLAHER: 7 VCARLEO: 7	JDOMDAR: 6 SMARGON: 6 APLAFLE: 5 JACOGON: 5
v2 Inicio: 27 Septiembre Fin: 2 Octubre	Ejercicio 1.5 Isaac y Javier: Portada y apartados 4, 8 Daniel y Sergio: apartados 1, 5, 9 Víctor y Jose: apartados 2, 6, 10 Aray y Abisay: apartados 3, 7	JACOGON: 16 (21) IMARMEN: 13 (22) APLAFLE: 7 (12) VCARLEO: 7 (14)	ACABGON: 6 (13) JDOMDAR: 5 (11) DPLAHER: 3 (10) SMARGON: 3 (9)
v3 Inicio: 3 Octubre Fin: 9 Octubre	Ejercicio 1.6 Javi y Jose: Apartados 1, 5, 9, 13, Isaac y Abisai: Apartados 2, 6, 10, 14 Víctor y Sergio: Apartados 3, 7, 11, poner imagen de fondo TF y GC. Aray y Dani: Apartados 4, 8, 12, explicar conexión ssh	JACOGON: 15 (36) JDOMDAR: 12 (22) IMARMEN: 11 (33) SMARGON: 10 (19)	VCARLEO: 8 (22) APLAFLE: 8 (20) ACABGON: 7 (20) DPLAHER: 5 (15)
v4 Inicio: 31 Octubre Fin: 6 Noviembre	Adecuación y homogeneización de la memoria al estándar de estilos Javi: Marcador lateral con nº de trabajo (ok) Jose: Pie de figura (ok) Isaac: Separadores de trabajo (ok) Sergio: Enunciados completos de trabajo (ok) Víctor: Resaltar secuencias de código en cuadro gris y letra Courier (ok) Daniel: Hipervínculos x3 (ok) Abisai: Resaltar comandos entre explicación con resalte gris y letra courier (ok) Arai: Repetir enunciados parciales de apartado (###) Todos: Corregir márgenes y tipo de letra (según hoja de estilos) Todos: Sello de autoría (ok)	IMARMEN: 10 (43) JDOMDAR: 10 (32) APLAFLE: 10 (30) SMARGON: 10 (29)	DPLAHER: 4 (19) JACOGON: 2 (38) VCARLEO: 2 (24) ACABGON: 0 (19)
v5 Inicio: 7 Noviembre Fin: 14 Noviembre	Trabajo 2.1: FLSM. Isaac Trabajo 2.3: FLSM. José Trabajo 2.2.1: fase 1. Arai Trabajo 2.2.2: fase 1b. Javi Trabajo 2.2.3: fase 2. Víctor Trabajo 2.2.4: fase 3. Daniel Trabajo 2.2.5: fase 4. Abisai Trabajo 2.4: Cisco LAB 2. Sergio	DPLAHER: 16 (35) JACOGON: 13 (51) IMARMEN: 9 (52) VCARLEO: 7 (31)	JDOMDAR: 6 (38) APLAFLE: 6 (36) SMARGON: 5 (34) ACABONG: 5 (24)
v6 Inicio: 28 Noviembre Fin: 18 Diciembre	Víctor: 3.1.1, 3.1.9, 3.3.2, 3.3.Añadido5, 3.5.5 Isaac: 3.1.2, 3.1.10, 3.3.3, 3.3.Añadido6 Javi: 3.1.3, 3.1.11, 3.3.4, 3.3.Añadido7 Abisai: 3.1.4, 3.1.12, 3.3.5, 3.3.Añadido8 Sergio: 3.1.5, 3.1.Añadido1, 3.3.Añadido1, 3.5.1 Jose: 3.1.6, 3.1.Añadido2, 3.3.Añadido2, 3.5.2 Arai: 3.1.7, 3.3.Intro VTP, 3.3.Añadido3, 3.5.3 Dani: 3.1.8, 3.3.1, 3.3.Añadido4, 3.5.4	DPLAHER: 31 (66) IMARMEN: 28 (80) JDOMDAR: 23 (61) SMARGON: 21 (55)	JACOGON: 20 (71) VCARLEO: 20 (51) APLAFLE: 14 (50) ACABGON: 1 (25)

Historial de versiones

Versión	Descripción	1.5Aportaciones	
v7 Inicio: 15 Enero Fin: 22 Enero	Trabajo 3.2 Router on Stick Trabajo 3.4: 8 apartados Grupo 1, Isaac y Abisay: trabajo 3.2, 3.4.1 Grupo 2, Jose y Víctor: 3.4.3, 3.4.5 Grupo 3, Sergio y Javi: 3.4.2, 3.4.6, 3.4.7 Grupo 4, Dani: 3.4.4, 3.4.8	JACOGON: 17 (88) DPLAHER: 17 (83) SMARGON: 15 (70) IMARMEN: 6 (86) APLAFLE: 6 (56) JDOMDAR: 4 (65) VCARLEO: 3 (57)	
v8 Inicio: 5 Febrero Fin: 12 Febrero	Sergio: Trabajo 4.1 Javi e Isaac: Trabajo 5.1 Dani y Jose: Trabajo 4.3 Víctor y Abisai: Trabajo 4.2	JACOGON: 28 (116) IMARMEN: 28 (114) JDOMDAR: 15 (80) APLAFLE: 13 (69) DPLAHER: 9 (92) VCARLEO: 9 (66) SMARGON: 3 (73)	

Modelo OSI
Capa 2: Capa de red
Capa 3: Capa de enlace de datos



Definiciones de campos de paquete de red

En este trabajo tomaremos un paquete de datos ICMP y estudiaremos uno por uno todos los campos de los que se compone en las capas de Enlace de datos (capa 2) y capa de Red (capa 3).

Explicación DSCP, Type y CHKSUM.

DSCP: Siglas de Differentiated Services Code Point. Se trata del segundo byte en la cabecera de los paquetes IP. Se utiliza para diferenciar la calidad en la comunicación que requieren los datos que son transportados, como por ejemplo un video en streaming.

DSCP Class Selector Names	Binary DSCP Values	IPP Binary Values	IPP Names
Default/CS0*	000000	000	Routine
CS1	001000	001	Priority
CS2	010000	010	Immediate
CS3	011000	011	Flash
CS4	100000	100	Flash Override
CS5	101000	101	Critical
CS6	110000	110	Internet Control
CS7	111000	111	Network Control

Figura 1.0.A. Muestra y significado de los valores del DSCP.

CHKSUM: En realidad quiere decir "Checksum" (también es llamado suma de verificación o suma de chequeo). Es una función resumen que se propone detectar algún cambio que pueda ocurrir en una secuencia de datos, comprobando que todo se encuentra tal cual cuando ha terminado la transmisión de datos. Su funcionamiento es que se transmite el dato con el valor resumen, de esta forma el receptor calcula ese valor y lo compara con el valor resumen recibido. En caso de que haya discrepancia se puede pedir una retransmisión o se puede producir un rechazo de los datos.

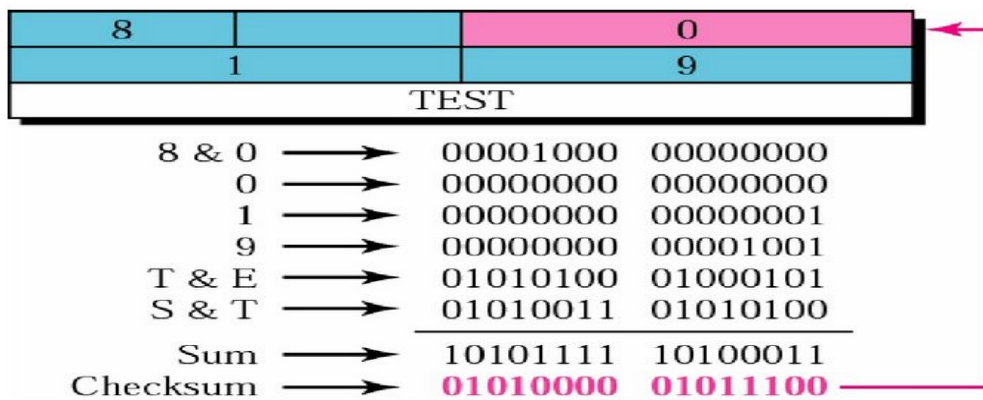


Figura 1.0.B. Representación de la función de CHKSUM.

Type: Este campo indica en las tramas de Ethernet II al Sistema Operativo que tipo de paquete lleva. Por ejemplo -0x0800 quiere decir que esa trama lleva un paquete IPV4. En esta [TABLA](#) encontramos todas las opciones posibles.

TYPE: es el campo que se encarga de decirle al sistema operativo qué tipo de datos son los que lleva el paquete. En nuestro caso es TYPE: 0x0800, que quiere decir que el frame tiene un paquete IPv4. Existen muchos otros protocolos que van a través de Ethernet, es por eso que este campo es tan necesario.

Aquí un enlace de los diferentes EtherType: <https://en.wikipedia.org/wiki/EtherType>

FLAGS: son los encargados de indicar la finalidad del paquete (para iniciar o finalizar una conexión, para transmitir datos, etc). Estos se encuentran dentro de la cabecera TCP y están formados por 9 bits:

- **NS (1 bit):** ECN-nonce concealment protection. Para proteger frente a paquetes accidentales o maliciosos que se aprovechan del control de congestión para ganar ancho de banda de la red.
- **CWR (1 bit):** Congestion Window Reduced. El flag se activa por el host emisor para indicar que ha recibido un segmento TCP con el flag ECE activado y ha respondido con el mecanismo de control de congestión.
- **ECE (1 bit):** Para dar indicaciones sobre congestión.
- **URG (1 bit):** Indica que el campo del puntero urgente es válido.
- **ACK (1 bit):** Indica que el campo de asentimiento es válido. Todos los paquetes enviados después del paquete SYN inicial deben tener activo este flag.
- **PSH (1 bit):** Push. El receptor debe pasar los datos a la aplicación tan pronto como sea posible, no teniendo que esperar a recibir más datos.
- **RST (1 bit):** Reset. Reinicia la conexión, cuando falla un intento de conexión, o al rechazar paquetes no válidos.
- **SYN (1 bit):** Synchronice. Sincroniza los números de secuencia para iniciar la conexión.
- **FIN (1 bit):** Para que el emisor (del paquete) solicite la liberación de la conexión.

OPT: [Opciones](#) es un campo que apenas se utiliza y este muestra un número el cual indicará el tipo de opción. Entre ellos se puede distinguir opciones de seguridad, ruta de registro, marca de tiempo o el indicador de flujo.

A continuación se explica que designa cada dígito:

- FC: Flag copy indica si se debe copiar este campo: 0 no 1 sí.
- Clase: es un entero de 2 bits que indica: 0 control de red o datagrama, 1 reservado para uso futuro, 2 depuración y medición y 3 reservado para uso futuro.
- Option number: es un entero de 5 bits que indica el número de opción dentro de cada clase

Tamaño de la cabecera(IHL):

La longitud de la cabecera no es constante, por eso se por ello incluye un campo en la cabecera **IHL** para indicar la longitud en palabras de 32 bits,es decir, es la cantidad de palabras de 32 bits que componen el encabezado.

Su valor mínimo es de 5 palabras ($5 \times 32 = 160$ bits, 20 bytes) para una cabecera correcta, y el máximo de 15 palabras ($15 \times 32 = 480$ bits, 60 bytes).

Identificador(ID):

Se utilizará, en caso de que el datagrama debe ser fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro. El originador del datagrama debe asegurar un valor único para la pareja origen-destino y el tipo de protocolo durante el tiempo que el datagrama pueda estar activo en la red.

Es un valor de identificación asignado por el remitente como ayuda en el ensamblaje de fragmentos de un datagrama.

Al enviar un datagrama, el emisor lo divide en fragmentos, asignándole un ID a cada uno de ellos para que el receptor pueda montar el datagrama de nuevo en el orden correcto.

Protocolo(PRO):

El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino.

En este URL está la tabla completa generada por IANA,organismo encargado de la asignación de estos protocolos.

https://es.wikipedia.org/wiki/Anexo:N%C3%BAmeros_de_protocolo_IP

Valor	Comentario
0	Reservado
1	Internet Control Message Protocol (ICMP)
2	Internet Group Management Protocol (IGMP)
3	Gateway-to-Gateway Protocol (GGP)
4	IP (IP encapsulation)
5	Stream
6	Transmission Control (TCP)
8	Exterior Gateway Protocol (EGP)
9	Private Interior Routing Protocol
17	User Datagram (UDP)
89	Open Shortest Path First

Figura 1.0.B. Tabla generada por IANA.

El **TTL (Tiempo De Vida)** forma parte de la cabecera IP (protocolo IP) con un tamaño de 8 bits. El valor se inicializa en el emisor y tiene la función de ir descontando de un contador una unidad según el datagrama IP viaje de un nodo a otro, por lo que debe de ser recalculado en cada salto. Si dicho contador llega a cero, descarta el paquete recibido y lo reenvía al destino del que proviene en vez de difundirlo. Este campo de la cabecera IP impide la congestión o sobrecarga en las colas de las líneas de transmisión, ya que si un paquete está en la cola, el TTL se decrementa también si pasa un largo periodo.

SFD (Start Frame Delimiter), es un delimitador de comienzo de marco y sus dos últimos bits están en 0000011, indicando el inicio del frame.



• SFD = Start of Frame Delimiter

Figura 1.0.C. Ejemplo de una trama Ethernet.

Los **Flags** son los encargados de indicar la finalidad del paquete (para iniciar o finalizar una conexión, para transmitir datos, etc). Estos se encuentran dentro de la cabecera TCP y están formados por 9 bits:

- **NS (1 bit):** ECN-nonce concealment protection. Para proteger frente a paquetes accidentales o maliciosos que se aprovechan del control de congestión para ganar ancho de banda de la red.
- **CWR (1 bit):** Congestion Window Reduced. El flag se activa por el host emisor para indicar que ha recibido un segmento TCP con el flag ECE activado y ha respondido con el mecanismo de control de congestión.
- **ECE (1 bit):** Para dar indicaciones sobre congestión.
- **URG (1 bit):** Indica que el campo del puntero urgente es válido.
- **ACK (1 bit):** Indica que el campo de asentimiento es válido. Todos los paquetes enviados después del paquete SYN inicial deben tener activo este flag.
- **PSH (1 bit):** Push. El receptor debe pasar los datos a la aplicación tan pronto como sea posible, no teniendo que esperar a recibir más datos.
- **RST (1 bit):** Reset. Reinicia la conexión, cuando falla un intento de conexión, o al rechazar paquetes no válidos.
- **SYN (1 bit):** Synchronise. Sincroniza los números de secuencia para iniciar la conexión.
- **FIN (1 bit):** Para que el emisor (del paquete) solicite la liberación de la conexión.

FCS: *Frame Check Sequence* se refiere al conjunto de bits adjuntos al final de la trama Ethernet utilizado para verificar la integridad de la información recibida mediante un método de verificación de trama, como puede ser el *checksum*. Así, el receptor comparará el FCS emitido en la trama con el calculado. Si son coincidentes, los datos recibidos son correctos, de lo contrario, habrá ocurrido un error en la trama y se descarta. El FCS solo proporciona detección de errores.

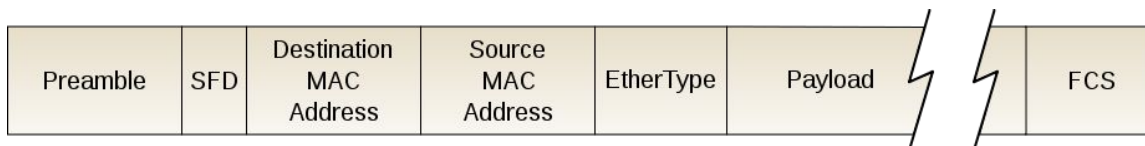


Figura 1.0.D. Ubicación de los bits de FCS en una trama Ethernet.

CHKSUM: Una suma de verificación (*checksum*) es un método de verificación que pretende comprobar cambios en una secuencia de datos: para ello, el emisor transmite los datos junto a una función *hash* de éstos; el receptor realiza el mismo proceso, calcula la función *hash* de los datos recibidos y compara el *hash* recibido con el *hash* calculado. Si los *hash* son diferentes, no se pueden verificar los datos recibidos y se rechazan o se pide una retransmisión.



Figura 1.0.E. Proceso de codificación mediante la función HASH.

Una función hash, es una función computable mediante un algoritmo que convierte un conjunto de datos en un rango de salida finito (cadena de longitud fija). Se dice que estas funciones resumen datos del conjunto dominio.

En el siguiente enlace se explica perfectamente ###:

<https://www.rfc-es.org/rfc/rfc0791-es.txt>

Tamaño de la Cabecera (IHL).

El campo IHL (Internet Header length) es al ancho de la cabecera, esta tiene un formato de palabras de 32 bits, este campo nos permite distinguir donde la cabecera de la IP finaliza y donde los datos o carga comienzan. Su valor mínimo es de 5.

(5* 32 bits = 160 bits o 20 octetos [bytes]).

Este campo es útil conocerlo debido a que las cabeceras de las direcciones IPV4 pueden contener un número variable de opciones, debido a esto, Este campo nos ayuda a poder especificar el tamaño de la cabecera.

Tiempo de Vida (TTL).

El campo TTL (Time to live) es otro de los componentes de la cabecera IPV4 y tiene un tamaño de 8 bits, este campo indica el máximo número de saltos que el paquete podrá realizar dentro de un router antes de ser desechado o ser devuelto al destino de donde proviene, el host que genera el paquete le asignará un valor determinado. Por ejemplo windows como norma general suele establecer un valor de 128. Este número será disminuido cada vez que el paquete sea redirigido.

Este campo dentro de la cabecera IPV4 sirve para evitar formar congestiones o sobrecargas en las colas de las líneas de transmisión.

Tamaño Total (TL).

El campo TL (Total Length) forma parte de la cabecera IPV4 y tiene un tamaño de 16 bits, tiene la función de, como su propio nombre indica, decirnos el tamaño total del paquete incluyendo la cabecera IPV4 y los datos del paquete. El tamaño mínimo de el TL es de 20 bytes (cabecera sin datos) y tiene un tamaño máximo de 65535 bytes.

IPv4 Header Format																																	
Offsets	Octet	0				1				2				3																			
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP				ECN				Total Length															
4	32	Identification								Flags				Fragment Offset																			
8	64	Time To Live				Protocol				Header Checksum																							
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

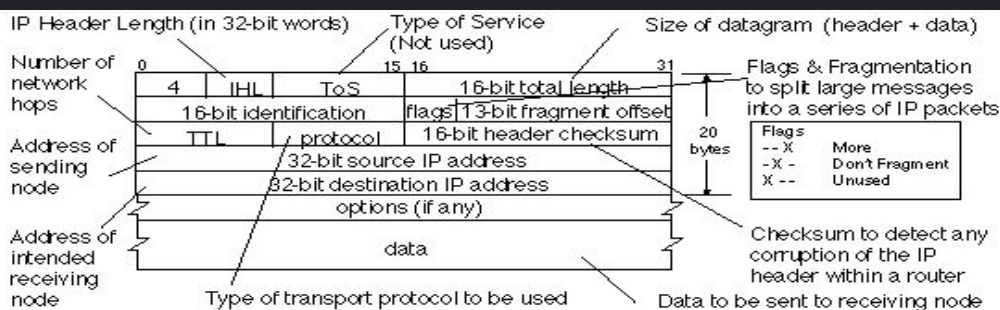


Figura 1.0.F. Cabecera IPv4 explicada.

Conceptos FCS, TL y OPT

FCS

Campo Secuencia de verificación de trama (Frame Check Sequence, 4 bytes). Tiene la función de detectar errores al momento de enviar información, errores en la trama. Es un conjunto de bits adjuntos al final de la trama que utiliza la CRC (comprobación cíclica de redundancia).

Por un lado el elemento emisor incluye los datos de CRC en este campo de la trama. Y el receptor recibe dicha trama y genera una CRC para detectar errores. Se comparan los resultados de ambos CRC y si coinciden significa que no hay error. En caso de error se descarta la trama.

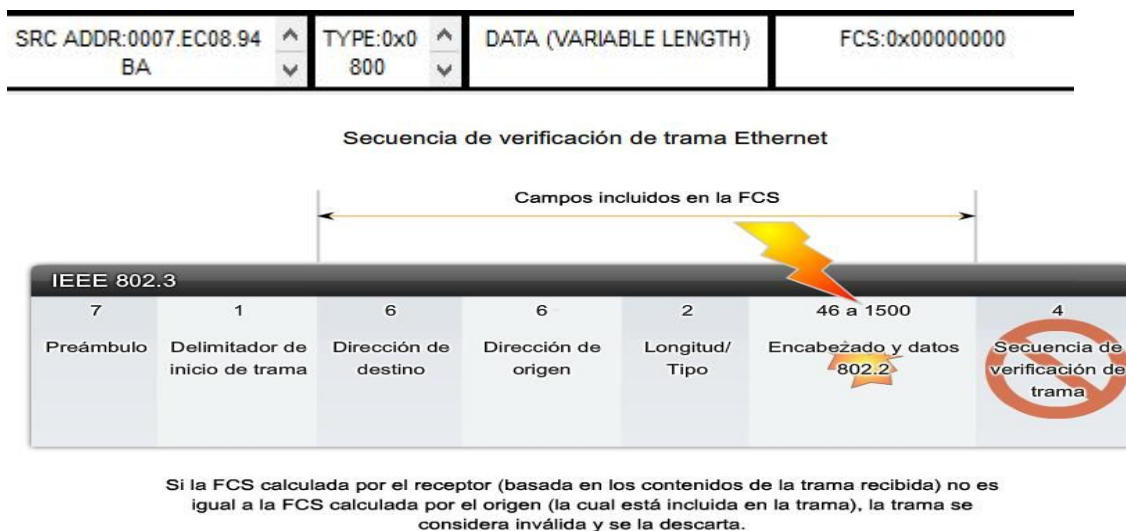


Figura 1.0.G. Secuencia de verificación de trama Ethernet..

TL

Longitud total de paquete (16 bits) incluye todo el datagrama: tanto la cabecera como los datos. La longitud máxima es de 65535 bytes, pero la carga útil será menor, porque hay que descontar lo que ocupa la propia cabecera. El tamaño mínimo de los datagramas usados normalmente es de 576 octetos (64 de cabeceras y 512 de datos). El campo identificación es necesario para que el host destino determine a qué datagrama pertenece un fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación.

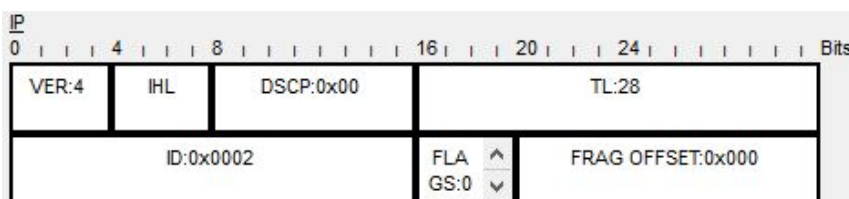


Figura 1.0.H. Cabecera de trama Ethernet.

OPT

Opciones es un campo que apenas se utiliza y este muestra un número el cual indicará el tipo de opción. Entre ellos se puede distinguir opciones de seguridad, ruta de registro, marca de tiempo o el indicador de flujo.



Figura 1.0.I. Campo OPT.

A continuación se explica que designa cada dígito:

- FC: Flag copy indica si se debe copiar este campo: 0 no 1 sí.
- Clase: es un entero de 2 bits que indica: 0 control de red o datagrama, 1 reservado para uso futuro, 2 depuración y medición y 3 reservado para uso futuro.
- Option number: es un entero de 5 bits que indica el número de opción dentro de cada clase

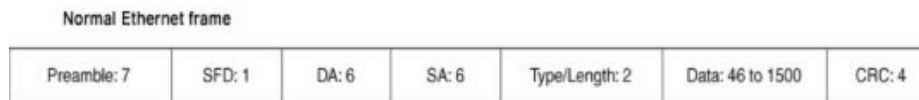
FC	Clase	Option number
0	1 2	3 4 5 6 7

Clase	Número	Tamaño	Descripción
0	0	-	Final de lista de opciones. Formato simple.
0	1	-	Ninguna operación (NOP). Formato simple.
0	2	11	Seguridad.
0	3	variable	Enrutado desde el Origen, abierto (Loose Source Routing).
0	9	variable	Enrutado desde el Origen, estricto (Strict Source Routing).
0	7	variable	Registro de Ruta (Record Route).
0	8	4	Identificador de flujo (Stream ID).
2	4	variable	Marca de tiempo (Internet Timestamping).

Figura 1.0.J. Tabla de significado de los dígitos de OPT.

Campos SFD, DSCP y PRO

SFD: Se le denomina delimitador de inicio de trama y es la principal diferencia entre los dos tipos de trama Ethernet (el IEEE 802.3 original y el IEEE 802.3 revisado Ethernet), también es conocido como Inicio de trama (1 byte). Este campo junto con el Preámbulo (7 bytes) se utilizan para la sincronización entre los dispositivos emisores y receptores. Estos 8 primeros bytes de la trama captan la atención de los nodos receptores. Dicho de otro modo, los primeros bytes le indican al receptor que se prepare para recibir una trama nueva.



- SFD = Start of Frame Delimiter

Figura 1.0.K. Muestra de los campos de una trama Ethernet.

PRO: Campo protocolo especifica qué protocolo está encapsulado dentro del datagrama IP, es decir, qué protocolo hay por encima del nivel IP.

Valor	Comentario
0	Reservado
1	Internet Control Message Protocol (ICMP)
2	Internet Group Management Protocol (IGMP)
3	Gateway-to-Gateway Protocol (GGP)
4	IP (IP encapsulation)
5	Stream
6	Transmission Control (TCP)
8	Exterior Gateway Protocol (EGP)
9	Private Interior Routing Protocol
17	User Datagram (UDP)
89	Open Shortest Path First

Figura 1.0.L. Tabla de valores del campo PRO.

DSCP: De sus siglas en inglés Differentiated Services Code Point, hace referencia al segundo byte en la cabecera de los paquetes IP que se utiliza para diferenciar la calidad en la comunicación que quieren los datos que se transportan. Como por ejemplo los vídeos en streaming o una videollamada.

DSCP Class Selector Names	Binary DSCP Values	IPP Binary Values	IPP Names
Default/CS0*	000000	000	Routine
CS1	001000	001	Priority
CS2	010000	010	Immediate
CS3	011000	011	Flash
CS4	100000	100	Flash Override
CS5	101000	101	Critical
CS6	110000	110	Internetwork Control
CS7	111000	111	Network Control

Figura 1.0.M. Tabla de valores del DSCP.

Trabajo 1.1

Diseño y simulación de una red de datos elemental



Enunciado 1

Diseño y simulación de una red de datos elemental. **Primeros pasos con PT.**

En este primer trabajo vamos a realizar la primera toma de contacto con el simulador de redes de datos Cisco Packet Tracer (a partir de ahora PT).

Utiliza dicha herramienta para implementar una red formada por un hub y 4 PCs interconectados. El nombre de los ordenadores debe ser exactamente PC01, PC02, PC03 y PC04.

Comprueba utilizando la herramienta de envío de paquetes básicos que hay conectividad entre dos equipos.

Realiza la simulación paso a paso de esta conexión y explica lo que ocurre en cada caso.

Abre un paquete de datos y explica el contenido de los campos de las capas 2 y 3.

COLISIONES:

Provoca una colisión en la red de datos y fíjate cómo la representa PT. Comenta también esto en tu memoria.

EXTRA: Realiza un vídeo en el que se vea esta primera red en funcionamiento así como los pasos para llevarlo a cabo. Incluye en tu memoria un código QR que dirija directamente al vídeo que has elaborado. Sería bueno realizar el vídeo a partir de la grabación de lo que ocurre en la pantalla.

Durante el curso vamos a elaborar una memoria que llamaremos Redes telemáticas. En este primer trabajo rellenamos el primer apartado de esta memoria. Al finalizar el curso tendremos un manual completo de redes telemáticas.

En este primer trabajo debes explicar cómo se han utilizado las herramientas de PT que has necesitado para llevar a cabo el diseño y la simulación de la red.

1- Primero entramos en el packet tracer y seleccionamos los dispositivos necesarios para la práctica que serán: el Hub genérico y los cuatro ordenadores (Pondremos en cada PC su nombre correspondiente del PC01 al PC04 como nos indica el ejercicio).

-Como nos muestra el siguiente gif, pinchamos en Network Devices (se puede usar el atajo Ctrl+Alt+R) y seleccionamos un Hub genérico.

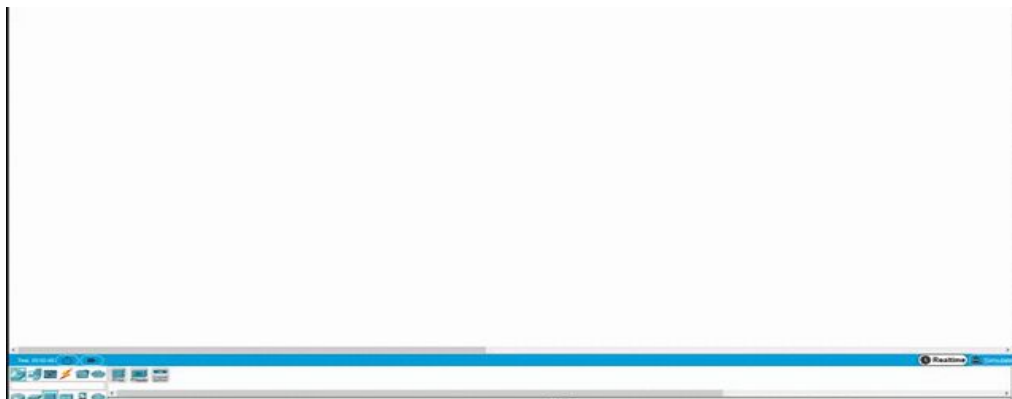


Figura 1.1.A. Proceso de selección de un Hub genérico.

-Luego vamos a End Devices and seleccionamos un PC-PT



Figura 1.1.B. Selección de un PC.

-Hacemos click en los PC vamos a config y le asignamos sus respectivos nombres (PC01, PC02, PC03 Y PC04).

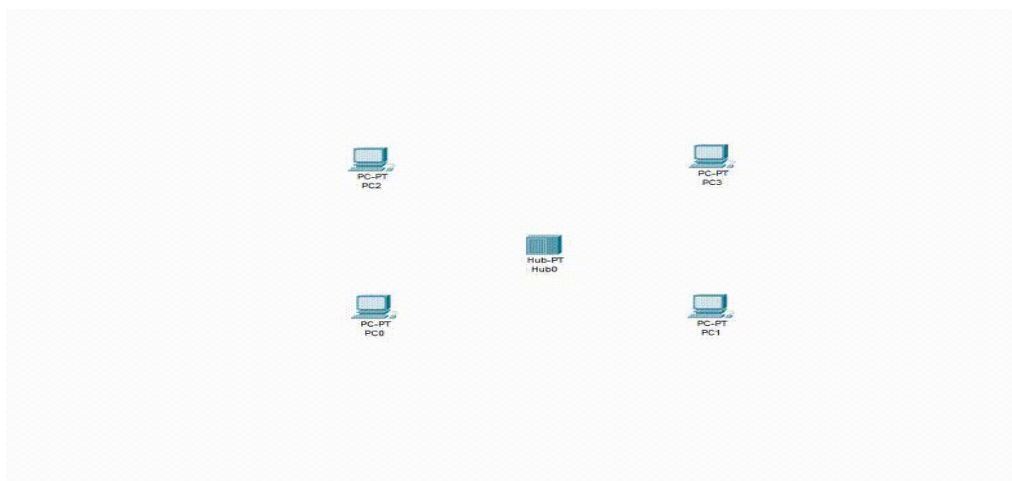


Figura 1.1.C. Proceso de configuración de nombres a los PC.

2- Una vez seleccionados los elementos por medio de los conectores los PC irán conectados al Hub. Además, le asignaremos a cada ordenador una IP distinta.

-Para conectar los PC al Hub pinchamos en  o también podemos seleccionar el cable de cobre  que será el que se pondrá automáticamente.

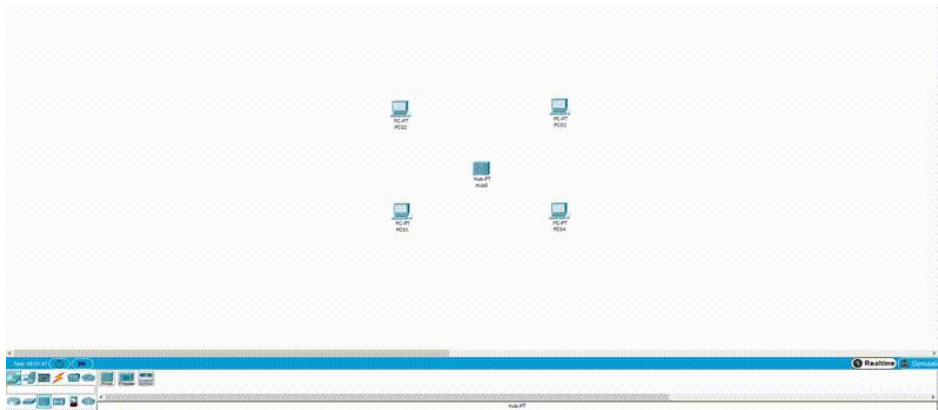


Figura 1.1.D. Conexión de los PC al Hub mediante cable.

-Y conectamos los ordenadores a los puertos del Hub.

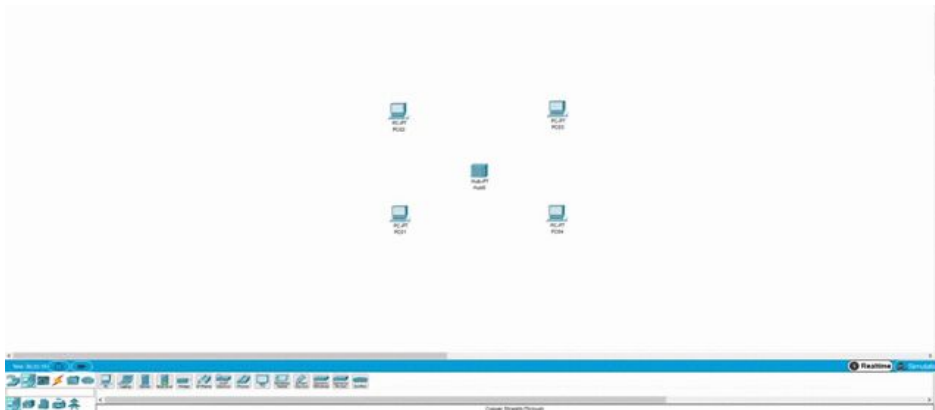


Figura 1.1.E. Selección del puerto de conexión al Hub

-Una vez conectados, pinchamos en los PC, vamos a config, entramos en el apartado FastEthernet0 en la configuración de IP y le asignamos una IP distinta a cada PC, encontrándose todas en el mismo rango.

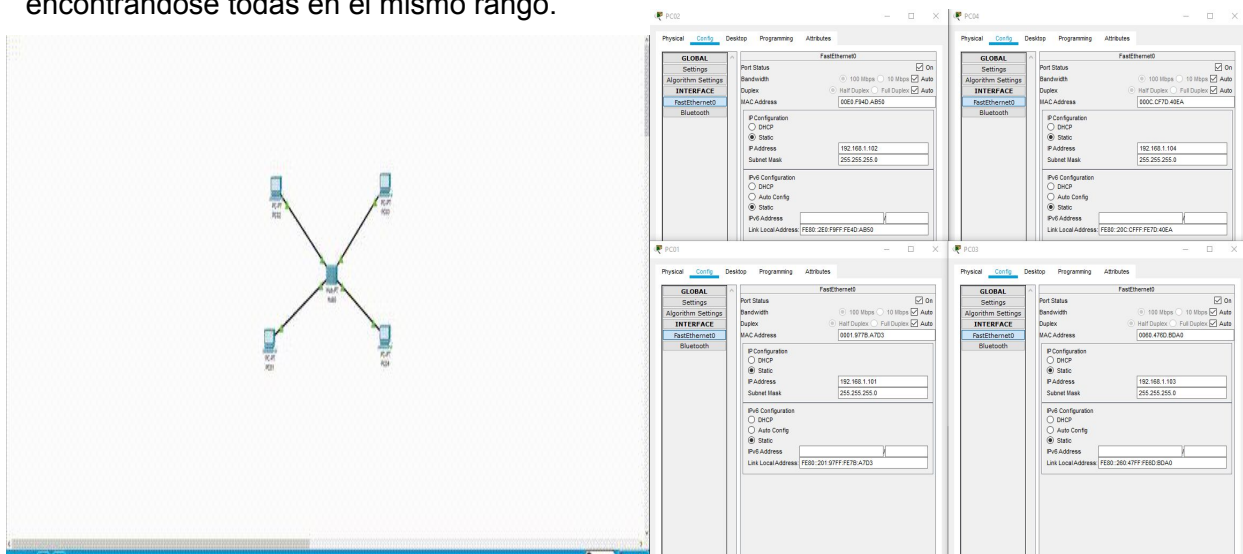



Figura 1.1.F. Asignación de IPs.

3- Al enviar un paquete de un PC a otro el Hub solo lo enviará a uno ya que está, por así decirlo, limitado a una red o dominio.

-Pulsamos en el icono 

- Hacemos click en un PC y en otro (nuestro caso PC01 y PC02).

-Abrimos el panel de simulación  y seleccionamos el botón de play.

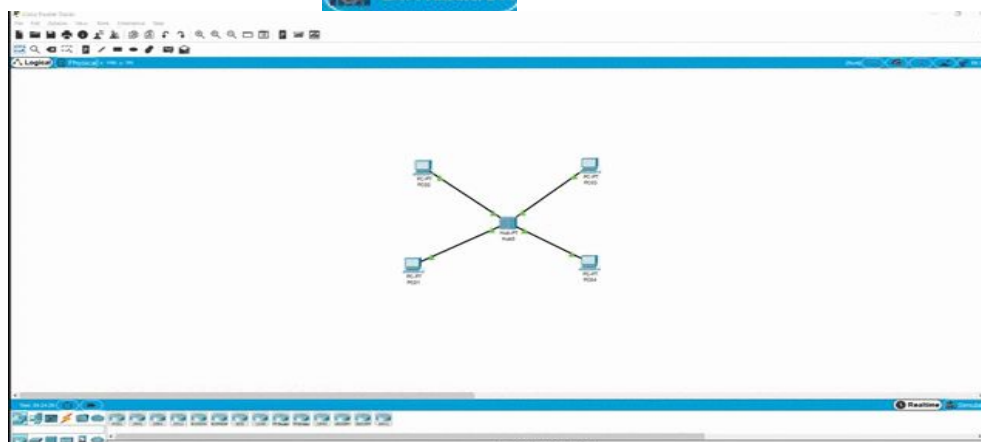


Figura 1.1.G. Inicio del proceso de simulación de ping.

-El paquete recorre el cable y llega al Hub.

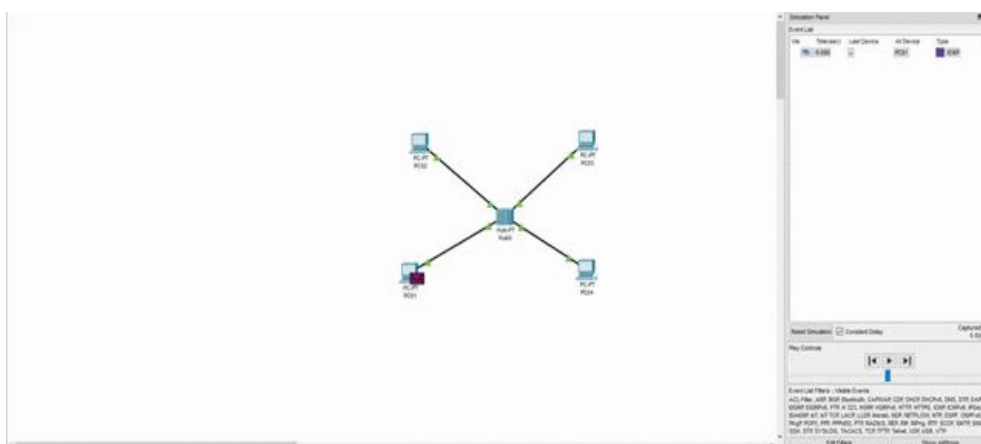


Figura 1.1.H. Salida del paquete desde el PC emisor.

-Luego el Hub envía el paquete a todos los demás PC que se encuentran conectados, diciéndole los PC03 y PC04 que ese no es su destino, además de recibir el PC02 el paquete que le ha enviado el PC01.

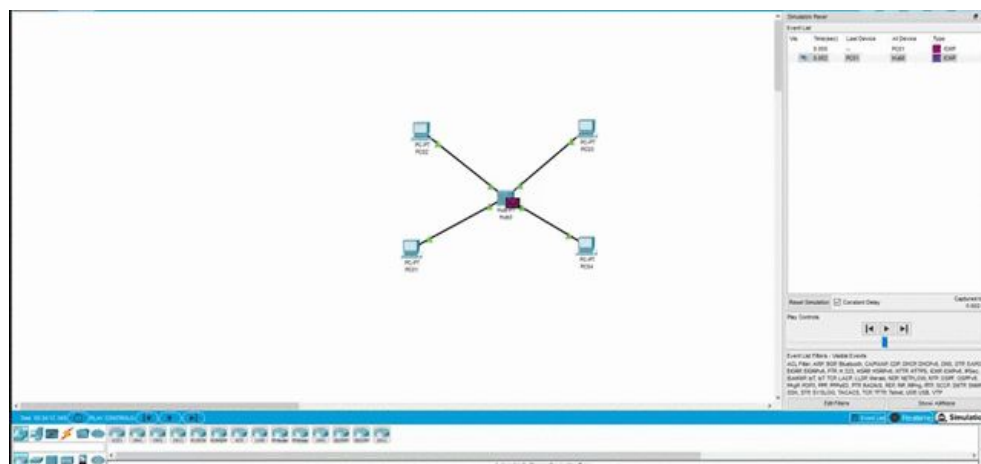


Figura 1.1.I. Reenvío broadcast del hub a todos los posibles PC receptores.

-Cuando el paquete llega a su destino (PC02) le envía una respuesta al Hub.

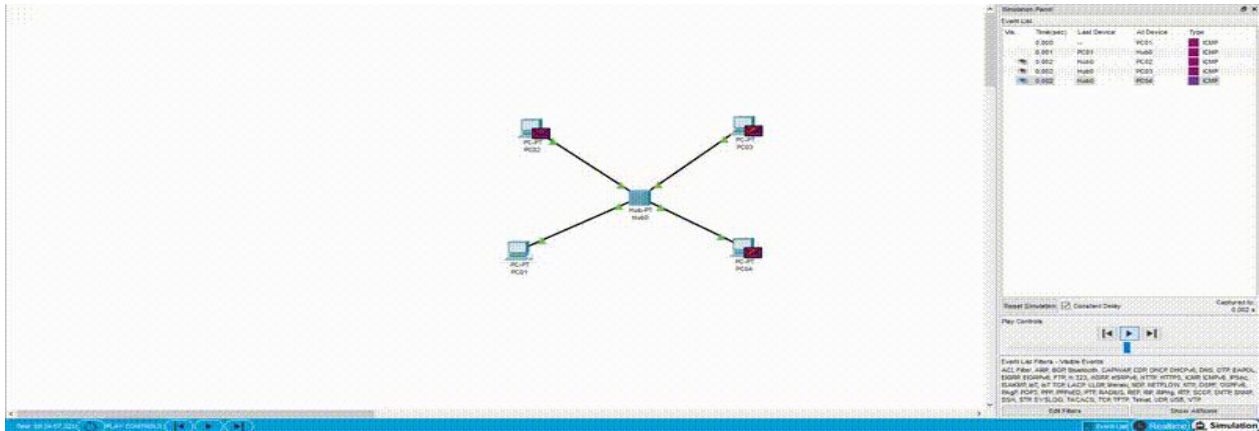


Figura 1.1.J. Respuesta del PC receptor.

-Luego vuelve a mandar el paquete al resto de PC diciéndole tanto el PC03 y PC04 que ese no es su destino y llegando finalmente la respuesta al PC de inicio (PC01).

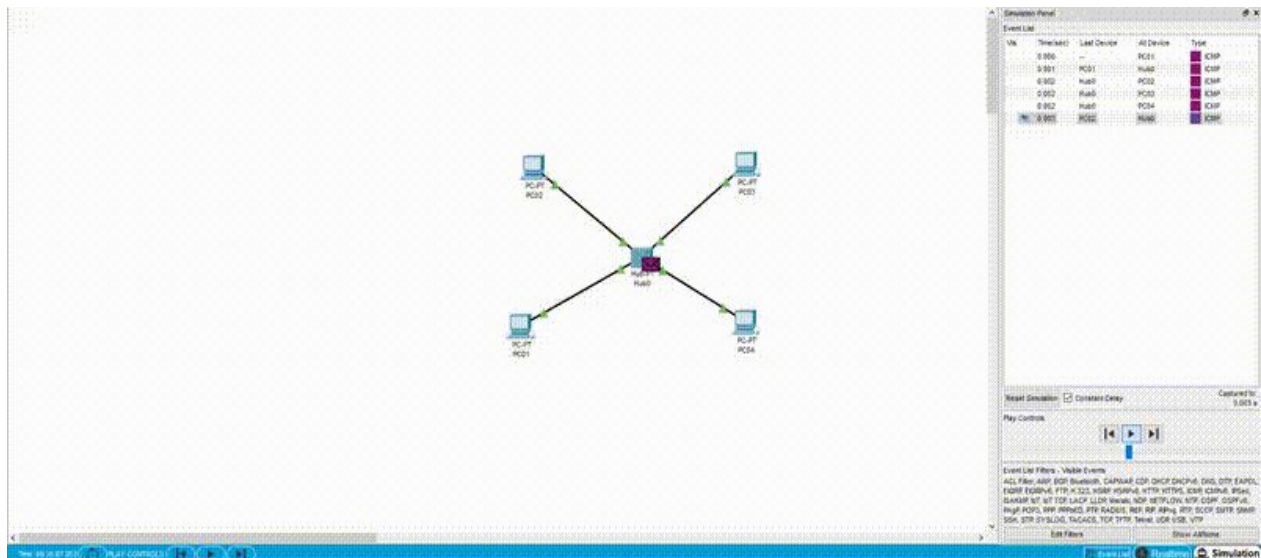


Figura 1.1.K. Envío en broadcast del Hub.

-A continuación, en el panel de simulación nos mostrarán los tipos de paquete que mandamos, como muestra el gif, hacemos click en el tipo de paquete ICMP para ver su contenido.

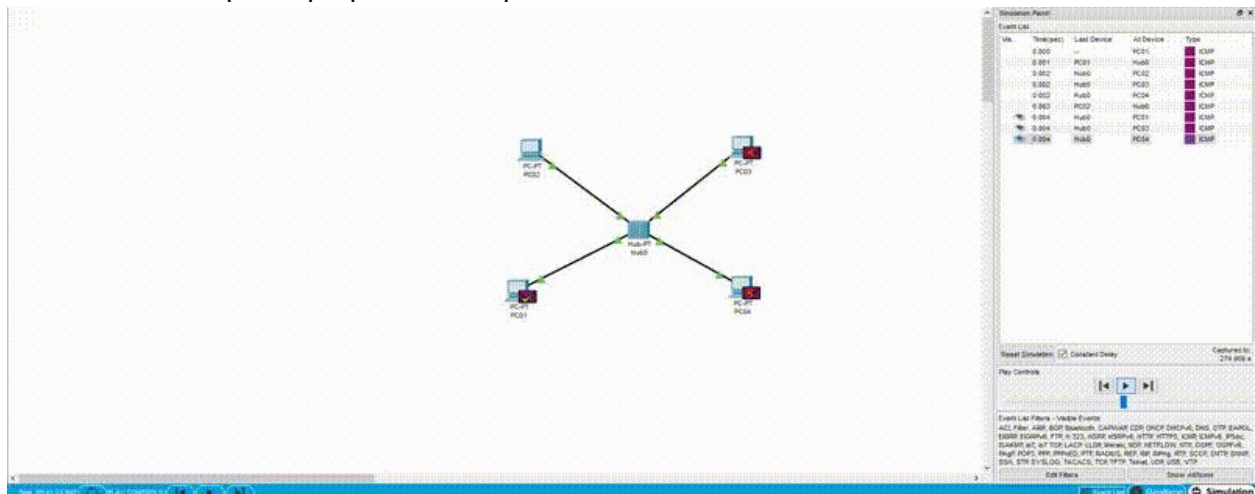


Figura 1.1.L. Proceso de muestra del contenido del paquete elegido.

<IMARMEN>
<VCARLEO>

CAPAS 2 Y 3.

Una vez abierto el contenido de la trama definiremos la capa 2 y 3 como nos indica el ejercicio.

CAPA 2: Capa de enlace de datos - Esta capa se ocupa del direccionamiento físico, del acceso al medio, detectar errores, distribuir ordenadamente las tramas y controlar el flujo. En este caso crea los protocolos básicos para regular la forma conexión entre ordenadores, es decir, la dirección IP o MAC.

CAPA 3: Capa de red - Se encarga de identificar el enrutamiento existente entre una o más redes. Aquí se indica la dirección IP del emisor y la del receptor, a parte de decirnos el tipo de mensaje que se está enviando.

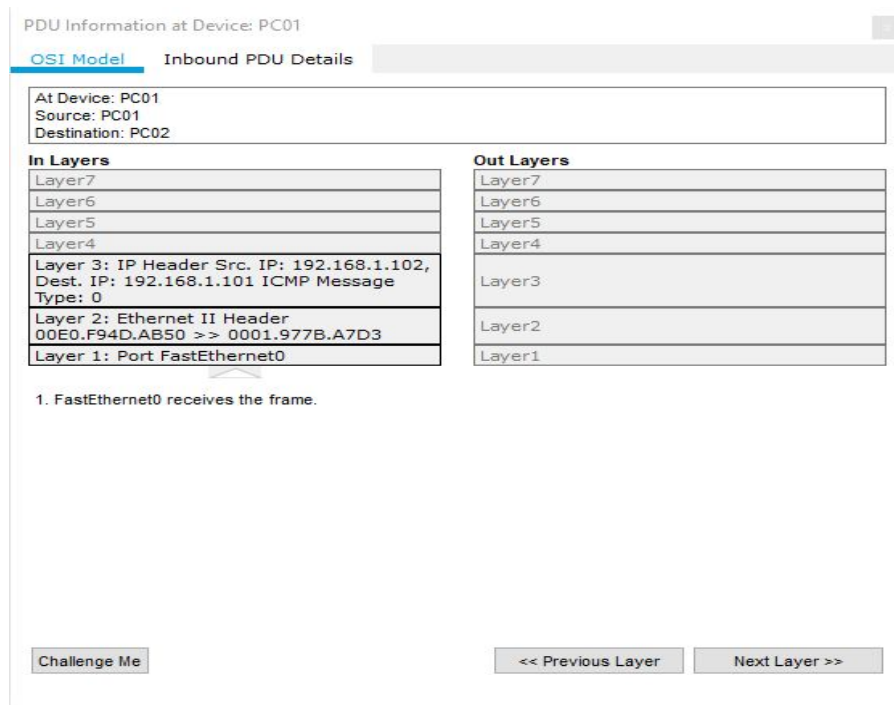


Figura 1.1.M. Contenido del paquete seleccionado.

COLISIONES.

En el caso del Hub como sus puertos están en el mismo dominio de colisión, como se ve en las siguientes imágenes dos PC enviarán una trama a otro PC a la vez por lo que se producirá una colisión ya que, como hemos mencionado antes, los puertos del Hub pertenecen al mismo dominio.

-Para provocar la colisión enviaremos dos paquetes simultáneamente desde el PC01 y el PC04 al PC03.

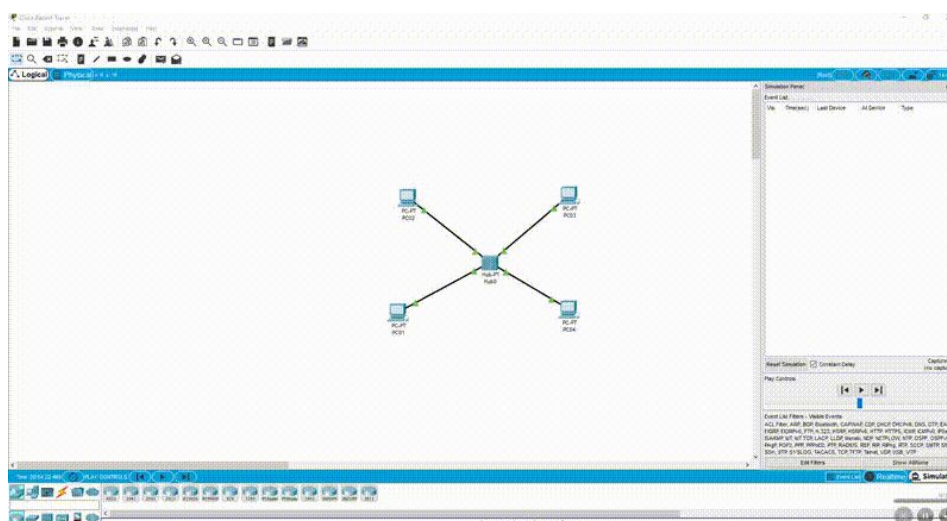


Figura 1.1.N. Proceso para provocar una colisión.

-Los dos paquetes van hacia el Hub y colisionan como nos hub indican las llamas con el icono

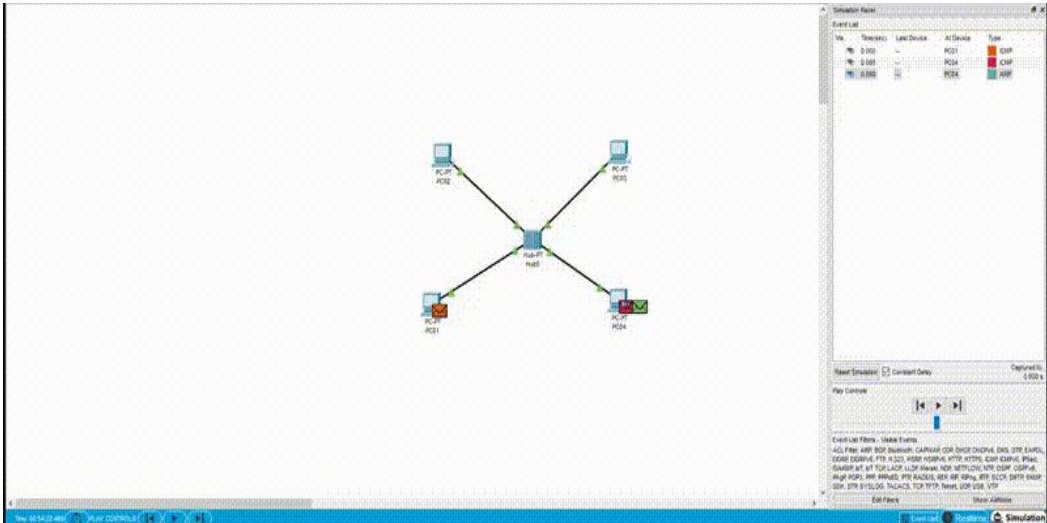


Figura 1.1.N. Colisión de dos paquetes.

- Debido a las colisiones las tramas no llegan correctamente por lo que al volver al PC04 nos muestra el error.

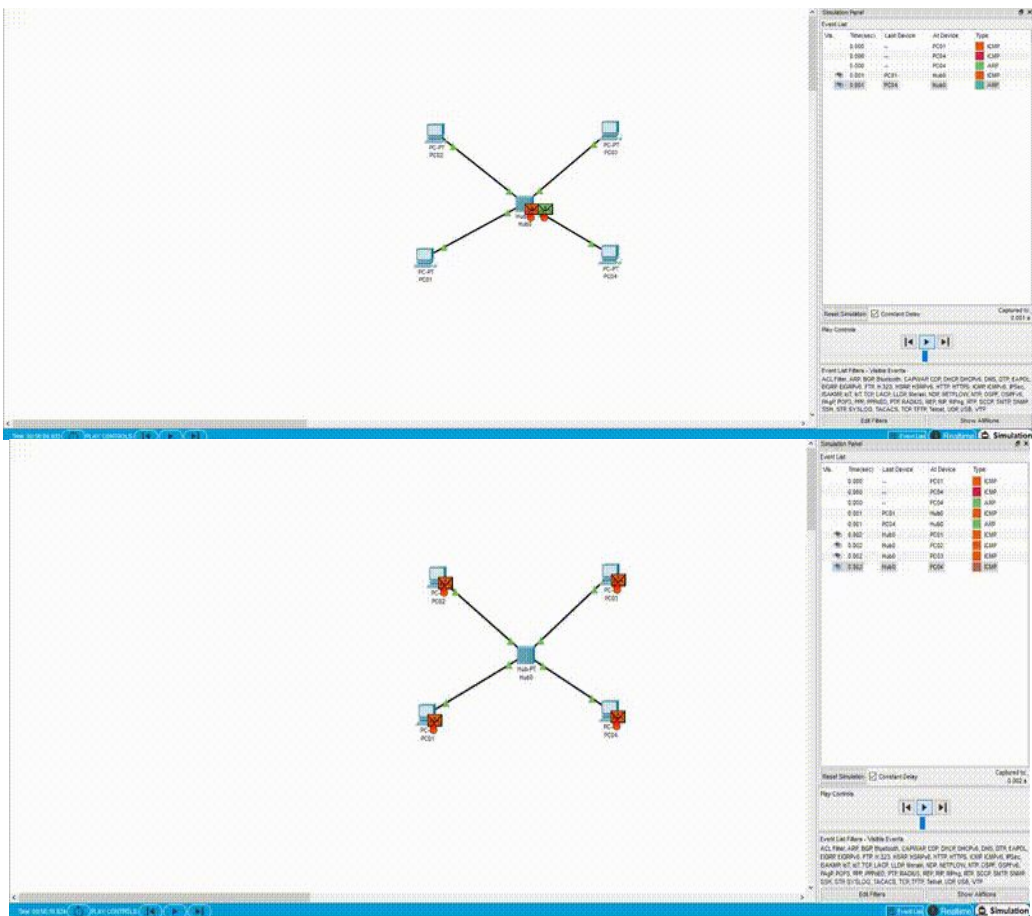


Figura 1.1.O. Muestra de los efectos de una colisión.

<IMARMEN>
<VCARLEO>

Resumen:

- 1-** Primero entramos en el packet tracer y seleccionamos los dispositivos necesarios para la práctica que en este caso serán: un Hub genérico y cuatro ordenadores (Pondremos en cada PC su nombre correspondiente del PC01 al PC04 como nos indica el ejercicio).
- 2-** Una vez seleccionados los elementos por medio de los conectores los PC irán conectados al Hub. Además, le asignaremos a cada ordenador una IP distinta.
- 3-** Al enviar un paquete de un PC a otro, el Hub repetirá la señal recibida por todos sus puertos, enviándolo así a toda la red que tenga conectada.

Trabajo 1.2

Red de hubs interconectados



Trabajo 1.2: Red de Hubs Interconectados


1. Utilizando la herramienta PT crea una red de 8 ordenadores que incluya 2 hubs conectados entre sí. Cada hub tendrá asociados 4 PCs.
2. Llama a los ordenadores de la siguiente manera: PC11, PC12, PC13 y PC14 para el primer hub y PC21, PC22, PC23 y PC24 para el segundo.
3. Prueba que puedes realizar un ping entre dos equipos bajo el mismo hub.
4. Prueba que puedes realizar un ping entre dos equipos conectados a diferentes hubs.
5. Utilizando las herramientas de dibujo que incluye PT representa una red como si fuera un dominio de Secretaría y la otra como si fuera un dominio de Dirección.
6. Completa la memoria de Redes telemáticas incluyendo este segundo diseño y explica de forma sencilla y gráfica cómo has utilizado las herramientas de dibujo que incluye PT.
7. Explica también de forma razonada los dos tipos de cableado que se han utilizado en el diseño.


COLISIONES:


Demuestra que un envío en la red de Secretaría y otro envío paralelamente la red de Dirección provoca una colisión en el sistema. Indica este aspecto en tu memoria.

1./2.

Para crear la red debemos seleccionar los elementos y arrastrar a la zona de trabajo.

El símbolo  representa a los pc por lo que arrastraremos tantos como deseemos.(8)Este se encuentra en la pestaña "End devices".

El símbolo  representa a los HUB por lo que arrastraremos tantos como deseamos. (2)Este se encuentra en la pestaña "Network Devices".

Para interconectar los elementos usaremos los "cables" cuyo símbolo  .Al seleccionarlo clicamos sobre uno de los elementos y después al que queremos conectarlo y se crearía la conexión.

Por último paso antes de realizar pruebas será darle un IP a cada PC. Para ello clicamos sobre un PC, elegimos la pestaña "Config" ,FastEthernet0 y en el campo IP escribimos la IP. Esto se realiza con todos los PC.

Trabajo 1.2: Red de Hubs Interconectados

1.2. Diseño de la red

1.2

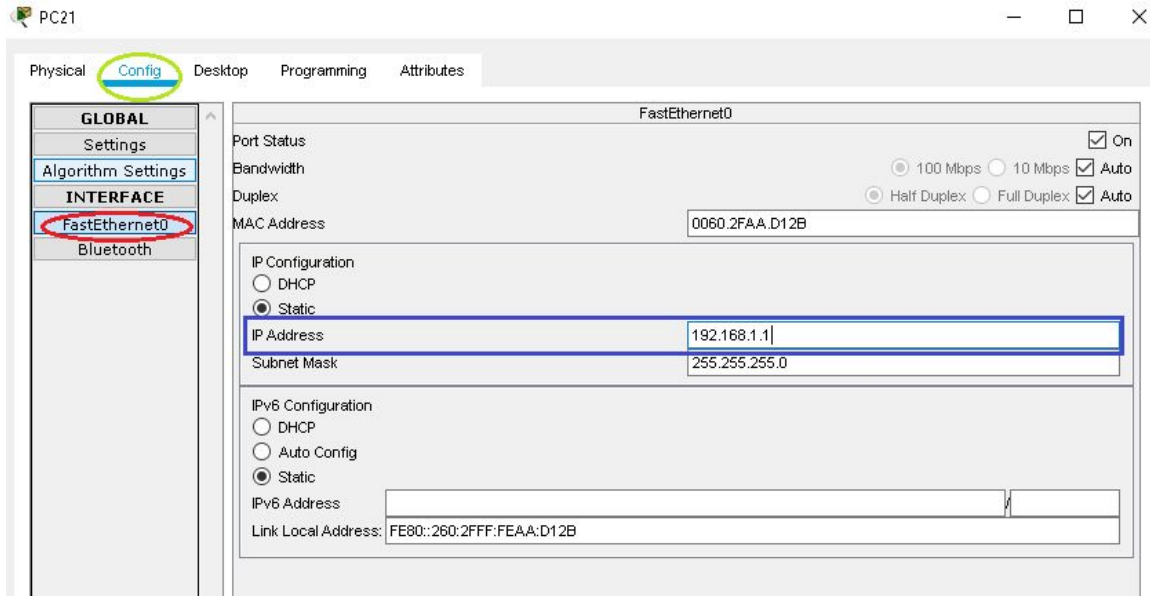


Figura 1.2.A. Pestaña de asignación de IP.

Así podría quedar:

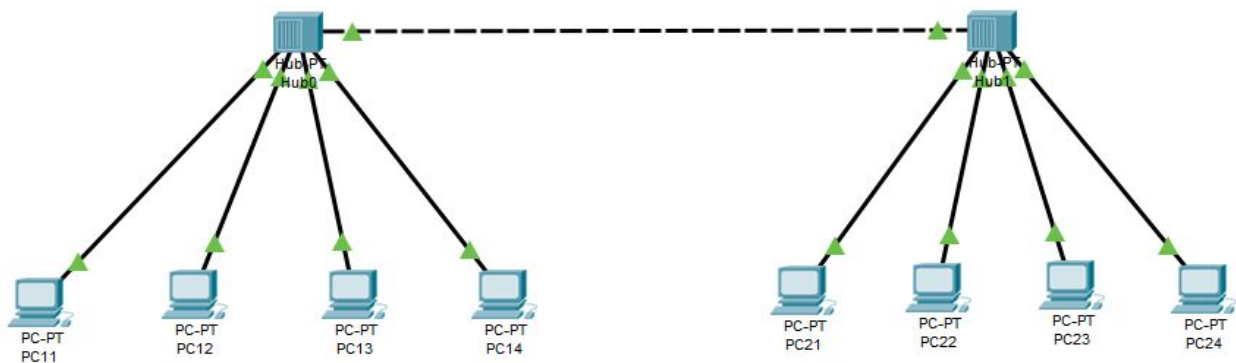


Figura 1.2.B. Diseño de la red.

Trabajo 1.2: Red de Hubs Interconectados

3. Ping mismo HUB: Se realiza el envío y solo responde el PC destinatario.

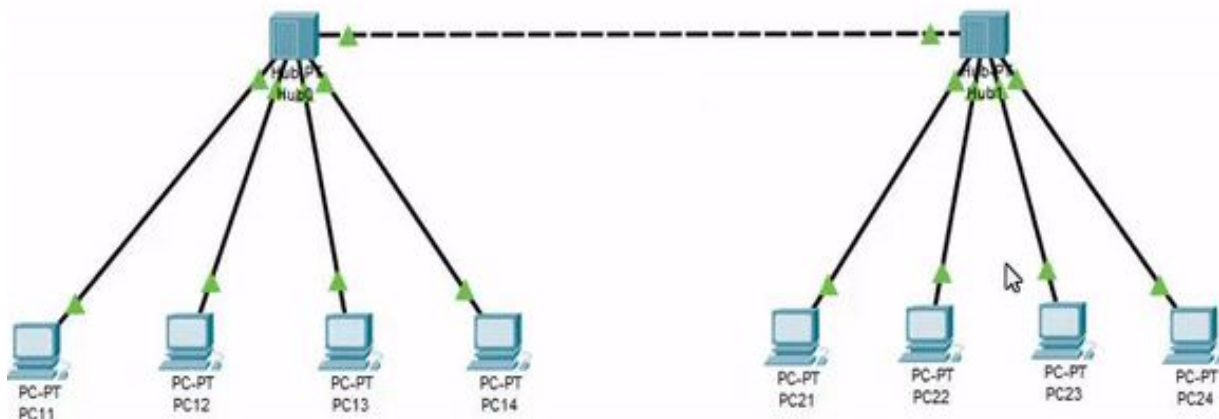


Figura 1.2.C. Ping entre dos PC del mismo Hub.

4. Ping PC distinto HUB: Se realiza el envío y solo responde el PC destinatario.

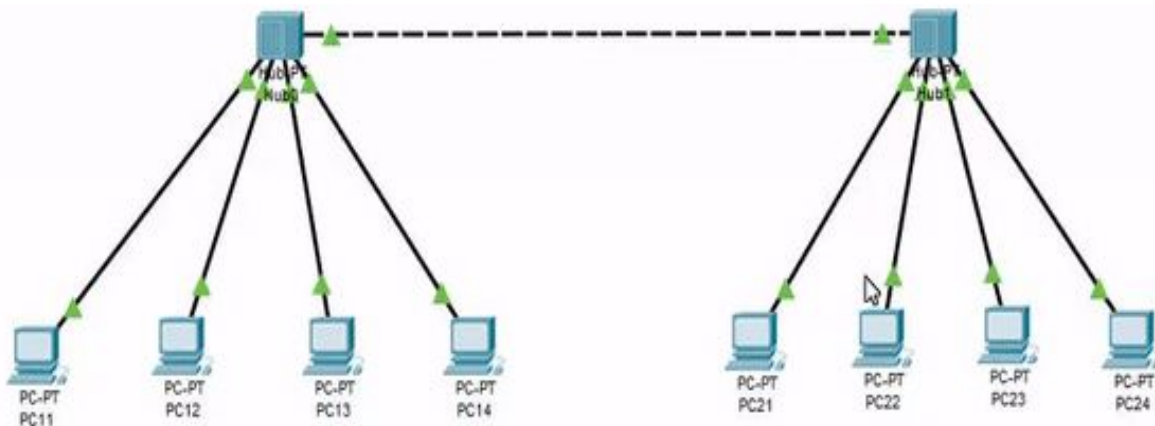



Figura 1.2.D. Colisión

Para realizar esto debemos clicar en el símbolo  y seleccionar primero el PC emisor y después el receptor. Para simular el envío iríamos al apartado siguiente:

En este tenemos la opción de dejar que simule automáticamente o manual. Automático le damos al símbolo Play, y en caso de manual tendríamos backwards o forward.

Vis.	Time(sec)	Last Device	At Device
	0.003	Hub1	PC22
	0.003	Hub1	PC23
	0.003	Hub1	PC24
	0.004	PC21	Hub1
	0.005	Hub1	PC22
	0.005	Hub1	PC23
	0.005	Hub1	PC24
	0.005	Hub1	Hub0
	0.006	Hub0	PC11
	0.006	Hub0	PC12
	0.006	Hub0	PC13
	0.006	Hub0	PC14

Figura 1.2.E. Apartado de simulación.

Trabajo 1.2: Red de Hubs Interconectados

5-6 Herramienta de dibujo

Para poder utilizar las herramientas de dibujo de packet tracer deberemos acceder a la pestaña de herramientas y luego seleccionar drawing palette, también se puede acceder a ella directamente mediante el comando Ctrl+D.

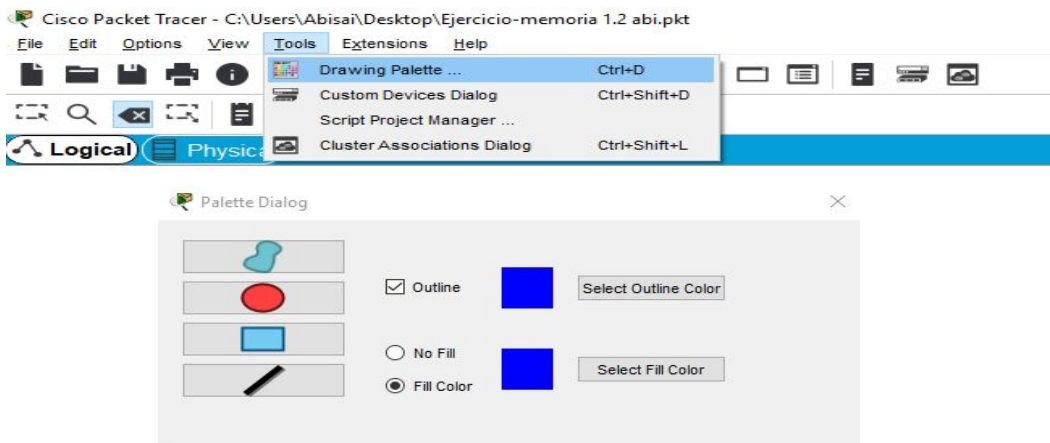


Figura 1.2.F. Pestaña y herramienta de dibujo.

Después de acceder a las herramientas tendremos la opciones de dibujar en diferentes formas y diferentes colores. Las pestañas con las formas geométricas indican las formas en las que podemos dibujar, círculo, línea, rectángulo, etc.

La pestaña select outline color nos permite cambiar el color del contorno, y la pestaña de select fill color nos permitirá cambiar el color del fondo.

El cuadro seleccionable que pone outline, nos permite elegir si queremos contornos o no; y los círculos seleccionables de fill color y no fill, nos permitirá decidir si queremos un color de fondo o no.

Como se nos pide que creamos dos zonas, una de secretaría y otra de dirección, el resultado final será el siguiente:

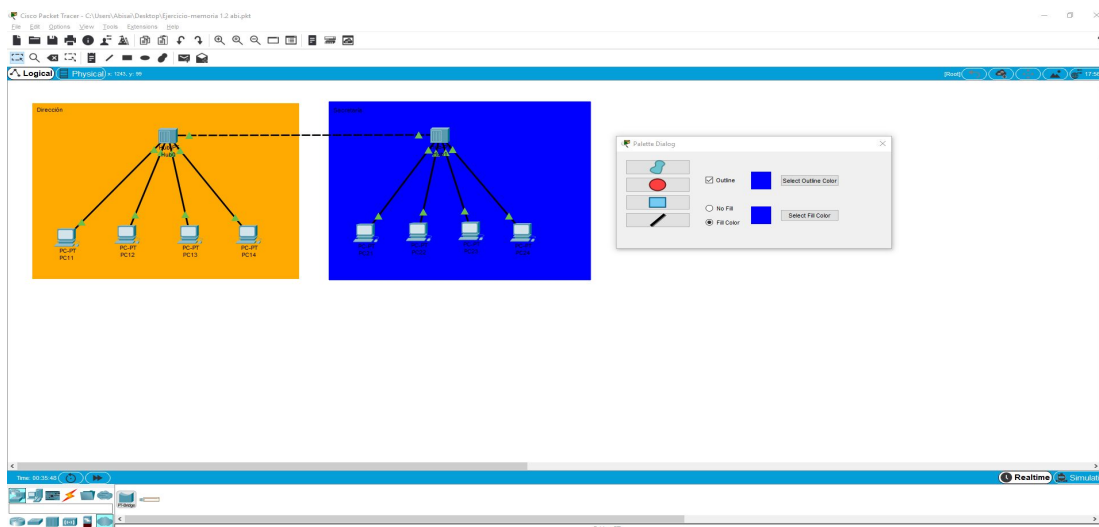


Figura 1.2.G. Diseño de la red con dos áreas bien diferenciadas.

Trabajo 1.2: Red de Hubs Interconectados

1.2

7. Explica también de forma razonada los dos tipos de cableado que se han utilizado en el diseño.

Las dos representaciones de los cables que aparecen en esta imagen es porque el cable que es continuo indica que la conexión de los dispositivos es directa, y el cable discontinuo representa una conexión cruzada.

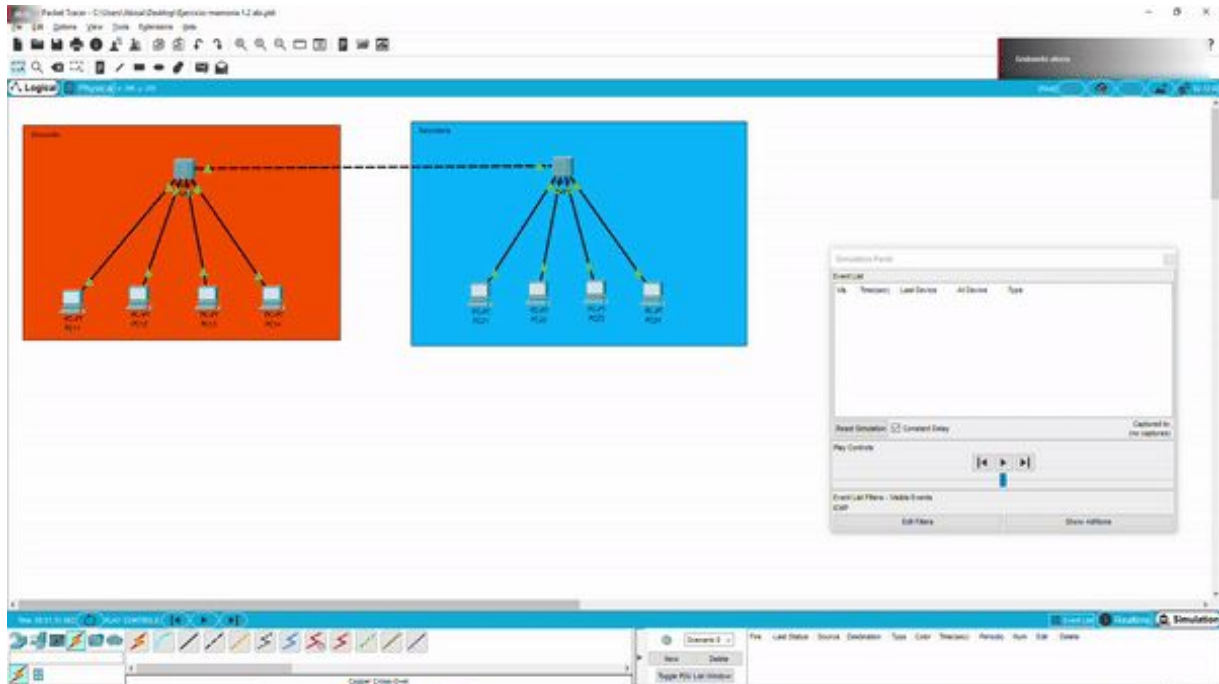
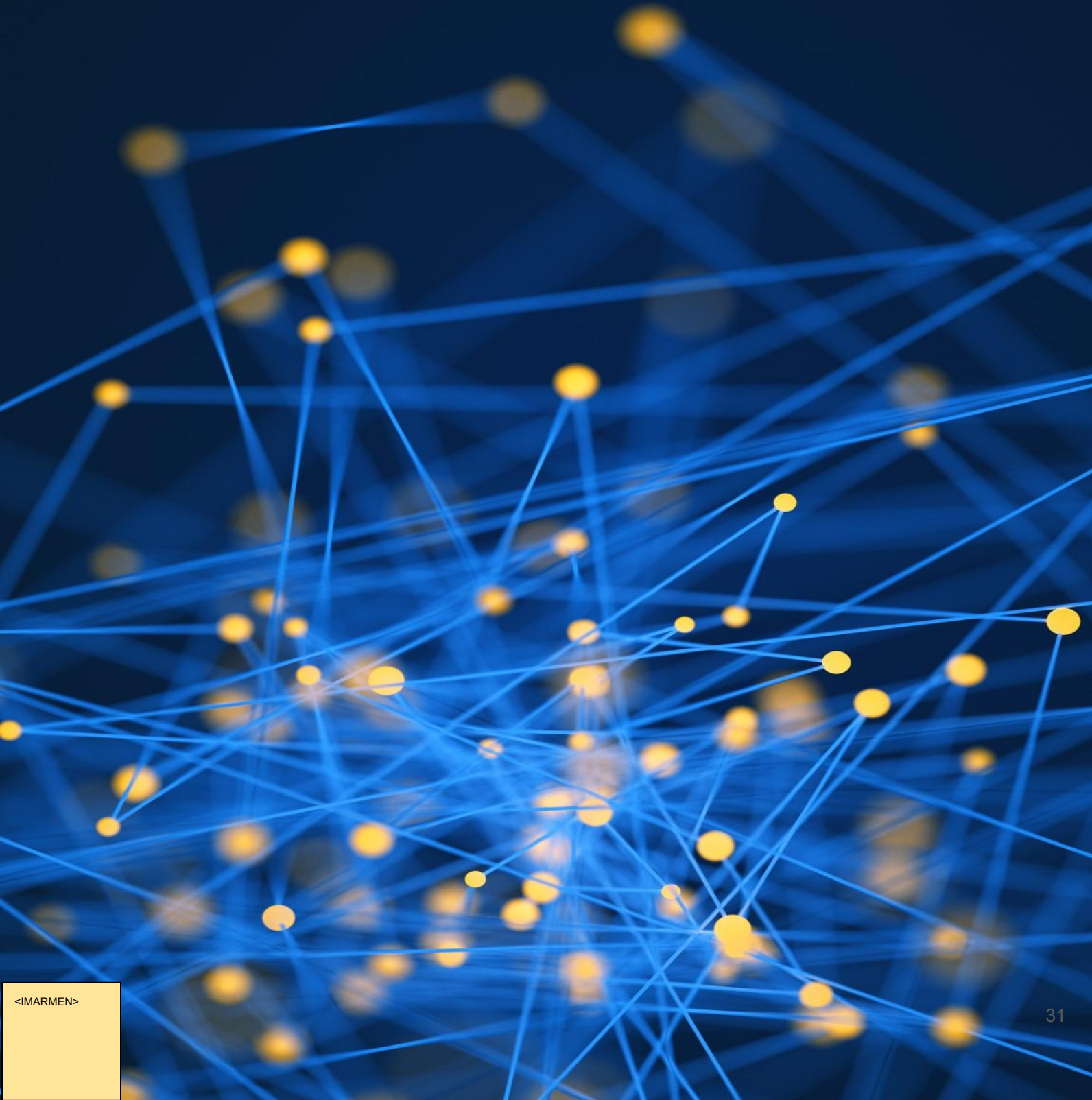


Figura 1.2.H. Colisión de dos paquetes en un envío a través de un Hub.

Por último como podemos observar en este GIF, si hacemos un envío de paquetes simultáneamente de un equipo de secretaría a un equipo de dirección y de un equipo de dirección a uno de secretaría estos dos envíos de paquetes causarían una colisión en la red debido a que los dos paquetes chocarían y tendrían una colisión en el hub.

Trabajo 1.3

Red de hubs interconectados mediante un bridge



Enunciado 1.3

Amplía la red del trabajo 2 y sustituye la conexión directa que hay entre los dos hubs por una conexión a través de un bridge.

Prueba que puedes realizar un ping entre dos equipos bajo el mismo hub y entre dos equipos conectados a diferentes hubs. Explica cómo fluye un paquete de datos en el primer caso y en el segundo y aclara de qué manera contribuye el bridge a mejorar la confidencialidad y el rendimiento entre las 2 redes.

COLISIONES:

Comprueba ahora que se puede realizar un envío interno dentro de la red de Secretaría a la vez que un envío interno dentro de la red de Dirección.

¿Qué manera contribuye el bridge a mejorar la confidencialidad y el rendimiento entre las 2 redes?

- Confidencialidad: con el bridge se conseguirá formar dos dominios, es decir, dos subredes “aisladas”. Así, lo que se envía desde una red no llegará a la otra, mejorando así la confidencialidad (privacidad) de los datos e información de cada red.
- Rendimiento: con un bridge se consigue regular el tráfico de los paquetes de dos dominios, evitando colisiones debido a que posee un buffer que almacena los paquetes hasta ser enviados secuencialmente.

1.3 Red de hubs interconectados mediante un bridge

1.3

Para realizar este tipo de red, necesitaremos seleccionar un bridge. Para ello deberemos clicar en el icono 'Switches' de la esquina inferior derecha de la pantalla inicial (o presionar Ctrl+Alt+S) y seleccionar el PT-Bridge



Luego habría que seleccionar un 'PT-Hub' (Ctrl+Alt+U), cablear cada uno al bridge (Ctrl+Alt+O y el icono del relámpago), y asignar mediante cableado cuatro PC (Ctrl+Alt+V) a cada Hub.

Nos quedaría:

Hub1 - PC11 + PC12 + PC13 + PC14 | Hub2 - PC21 + PC22 + PC23 + PC24.

Para finalizar, deberemos asignar una IP a cada ordenador. Para ello clicamos en el icono del PC a configurar, seleccionamos la pestaña 'Config', y en 'FastEthernet0', escribiremos la IP en IP Address (dejaremos la Subnet Mask que se creará por defecto).

Los PC de la Red 1 (Secretaría) irán desde 192.168.1.101 hasta 192.168.1.104, y los de la Red 2 (Dirección), desde 192.168.1.121 hasta 192.168.1.124.

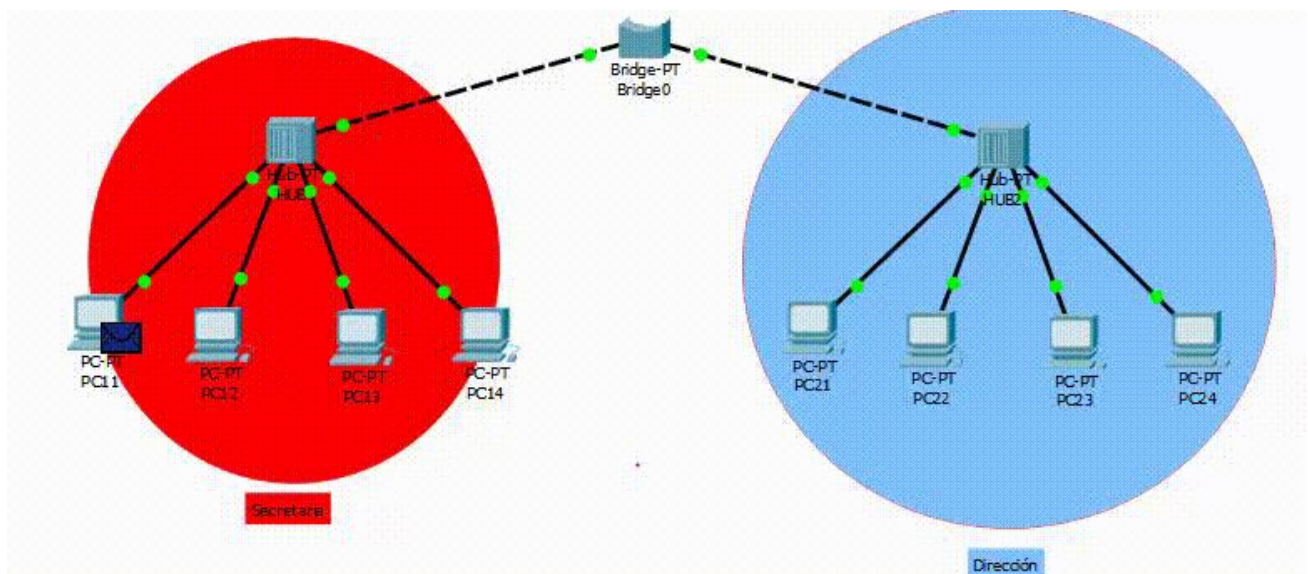
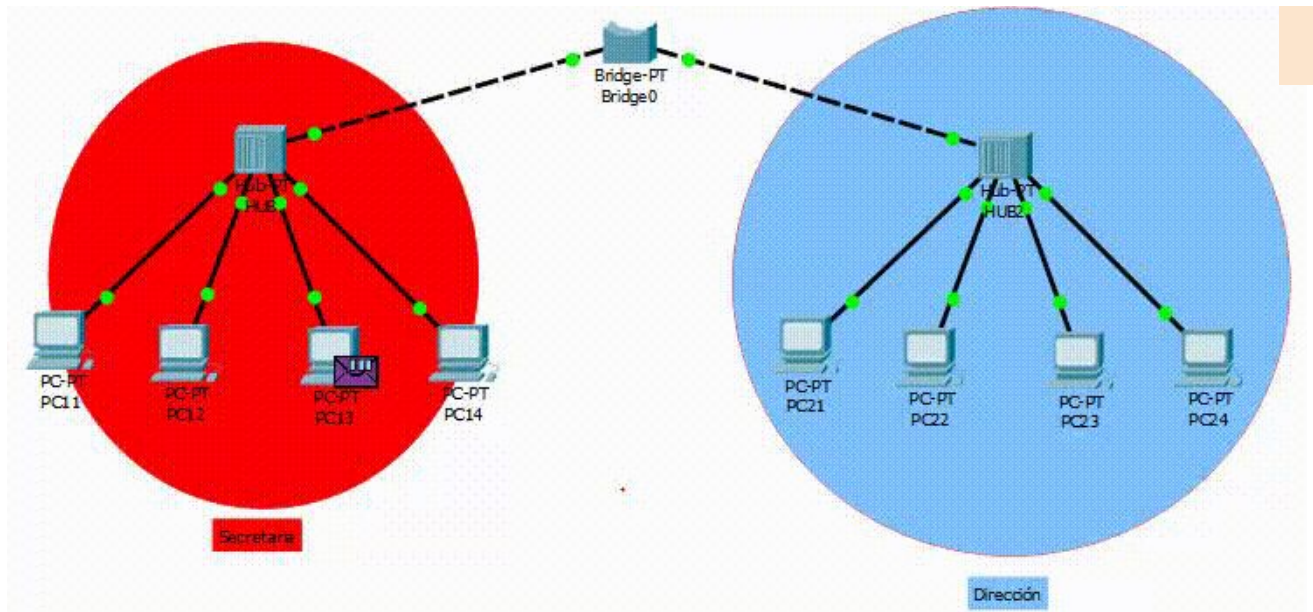


Figura 1.3.A. Paquete enviado entre dos ordenadores (PC11->PC13) en un mismo hub.

Como podemos observar, el envío se realizará sin problemas entre la red de secretaría sin afectar a la red de dirección, pues el bridge se encarga de parar el envío hacia esta segunda red. El paquete sale del PC11 hacia el Hub1, éste lo distribuye hacia el resto de PC de la red de secretaría (detectándolo el PC13), y al bridge, el cual para el envío hacia la red de dirección. Tras haber llegado así el paquete al PC 13, éste responde con un paquete hacia el Hub, el cual se lo distribuye al resto de PC de la red 1 y de nuevo al bridge, parando otra vez el envío hacia la red 2 y detectando el PC11 el paquete de respuesta.

1.3 Red de hubs interconectados mediante un bridge



1.3

Figura 1.3.B. Paquete enviado entre dos ordenadores en distinto hub (PC13->PC23).

Aquí podemos ver cómo el bridge detecta que el envío del PC13 va hacia el PC23, y deja pasar el paquete desde la Red 1 a la Red 2.

El paquete sale del PC13 hacia el Hub1, éste lo distribuye hacia el resto de PC de la red de secretaría, y al bridge, el cual detecta que el envío es para el PC23 de la red 2 y permite el paso hacia dicha red. Así, el paquete va hacia el Hub2, que distribuye el paquete hacia todos los PC de la red de dirección. El PC23 detectará entonces el paquete y mandará su respuesta hacia el Hub2, repitiéndose el proceso pero a la inversa.

1.3 Red de hubs interconectados mediante un bridge

Aquí tenemos los ping enviados entre dos PC:

- PC en el mismo Hub desde 192.168.1.101 (PC11) a 192.168.1.102 (PC12):

```
C:\>ping 192.168.1.102

Pinging 192.168.1.102 with 32 bytes of data:

Reply from 192.168.1.102: bytes=32 time=8ms TTL=128
Reply from 192.168.1.102: bytes=32 time=4ms TTL=128
Reply from 192.168.1.102: bytes=32 time=4ms TTL=128
Reply from 192.168.1.102: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms
```

Figura 1.3.C. Representación del ping enviado desde PC11 a PC12.

- PC en distinto Hub desde 192.168.1.101 (PC11) a 192.168.1.122 (PC22):

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.122

Pinging 192.168.1.122 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.122: bytes=32 time=12ms TTL=128
Reply from 192.168.1.122: bytes=32 time=6ms TTL=128
Reply from 192.168.1.122: bytes=32 time=6ms TTL=128

Ping statistics for 192.168.1.122:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 12ms, Average = 8ms
```

Figura 1.3.D. Representación del ping enviado desde PC11 a PC22.

1.3 Red de hubs interconectados mediante un bridge

Colisiones:

Aquí tenemos un envío interno dentro de la red de Secretaría a la vez que un envío interno dentro de la red de Dirección.

1.3

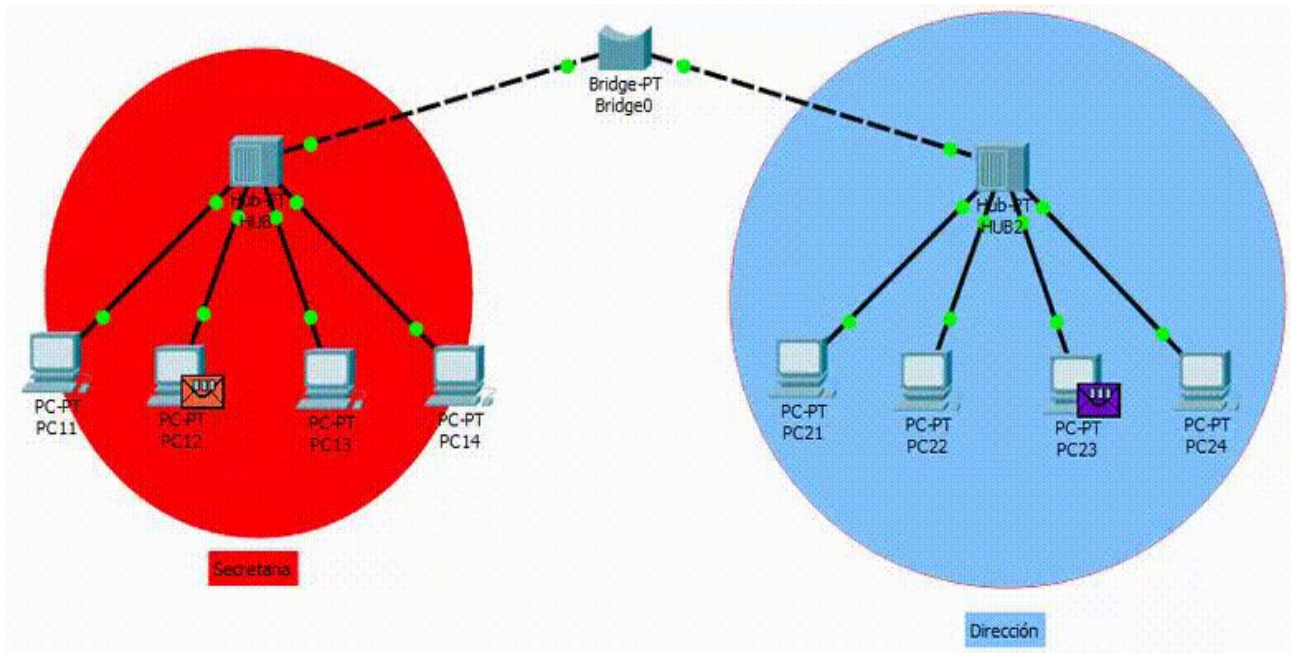


Figura 1.3.E. Simulación con colisión.

Como observamos, el primer paquete enviado internamente desde secretaria se envía correctamente hasta llegar al Hub de secretaria, que lo distribuye a todos los ordenadores, inclusive lo envía al Bridge; y el que es enviado desde dirección también es distribuido a todos los ordenadores inclusive al Bridge, que es aquí donde se realiza la colisión.

*** En la simulación hecha por JDOMDAR, no hubo colisión. La colisión se da porque no se le da dado el tiempo necesario al bridge para que complete su proceso de reconocimiento de la red.**

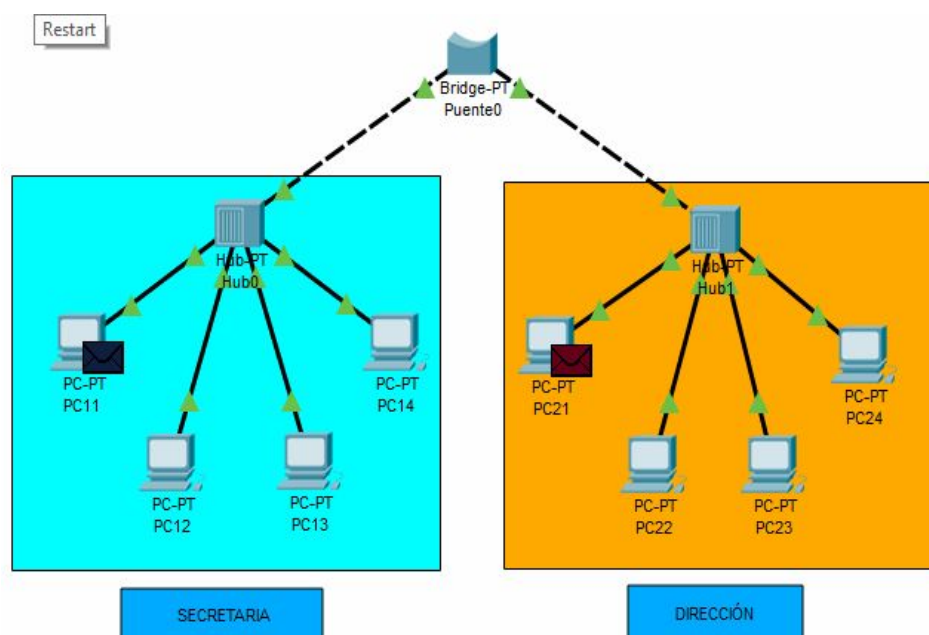
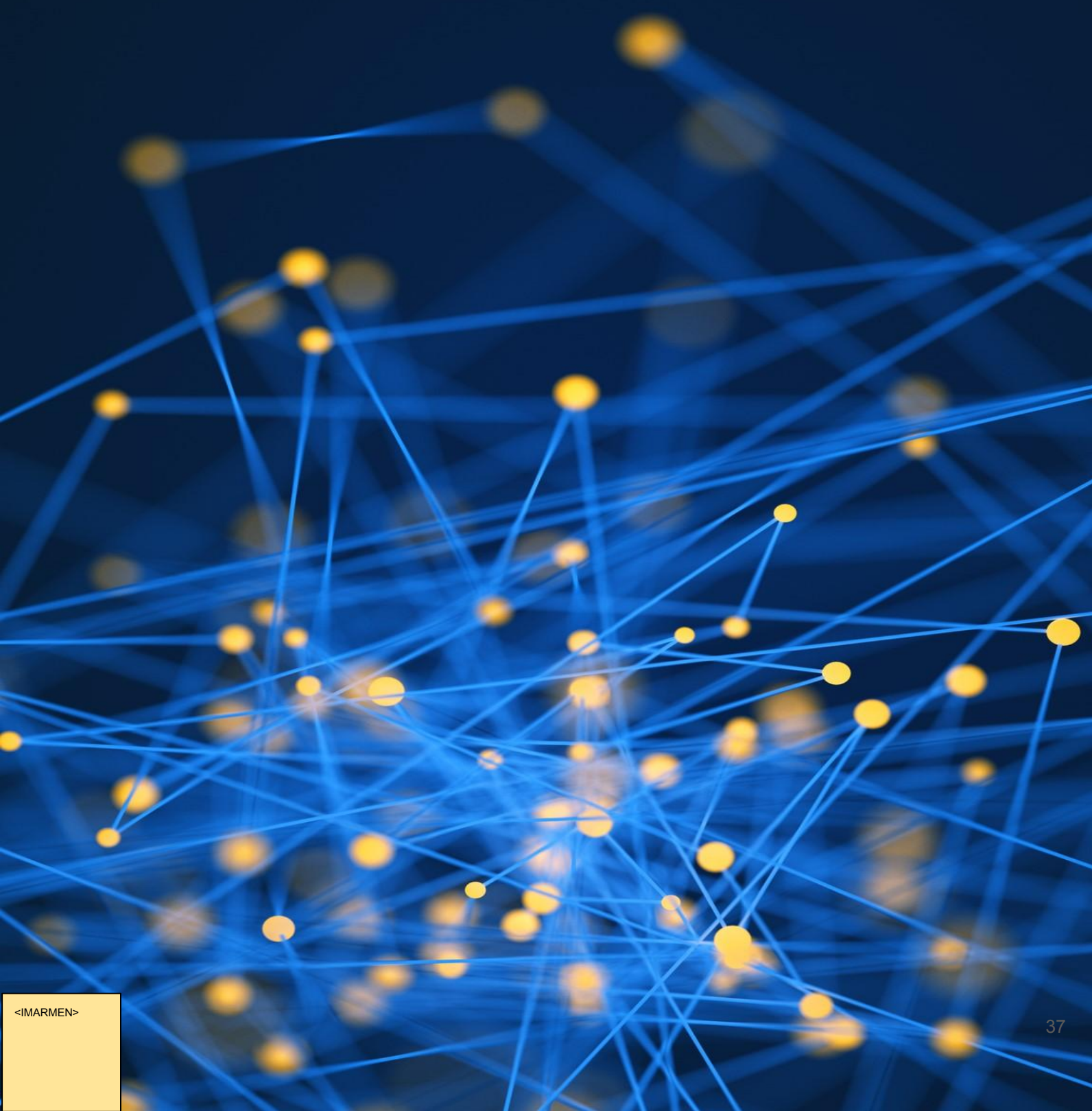


Figura 1.3.F. Simulación sin colisión.

<SMARGON>
<JDOMDAR>

Trabajo 1.4

Red de ordenadores conectados mediante un switch



Enunciado 1.4

Red de ordenadores conectados mediante un switch

Vamos ahora a conectar 4 PCs mediante un switch genérico. Cuando hayas realizado la conexión, prueba a realizar un ping entre cualquier par de equipos y prueba que funciona.

Fíjate que ahora, además de los paquetes ICMP, aparece un nuevo tipo de paquete que es ARP.

Destaca esta novedad en tu memoria y explica de forma sencilla qué utilidad tiene este protocolo.

Explica también por qué cuando hemos utilizado el hub como elemento de interconexión NO se envían paquetes ARP.

Resalta en tu memoria como, tras el primer envío, los siguientes envíos entre cada par de PCs no vuelven a requerir broadcasting.

COLISIONES:

Prueba que en esta red se pueden realizar dos envíos simultáneos sin que se provoquen colisiones.

Comenta esto en tu memoria.

BUFFERING:

Prueba que el switch realiza tareas de buffering. Comenta esto en tu memoria.

IMPORTANTE: De momento NO vamos a ver la tabla de forwarding del switch ni como resetearla.

1.4 Red de ordenadores conectados mediante un switch

Para crear la red debemos seleccionar los elementos en el Packet Tracer y arrastrar a la zona de trabajo.

1º Lo primero que debemos seleccionar es un switch genérico (Switch-PT), el cual se encuentra en el apartado Network Devices - Switches - Switch-PT como se observa en el gif.

1.4

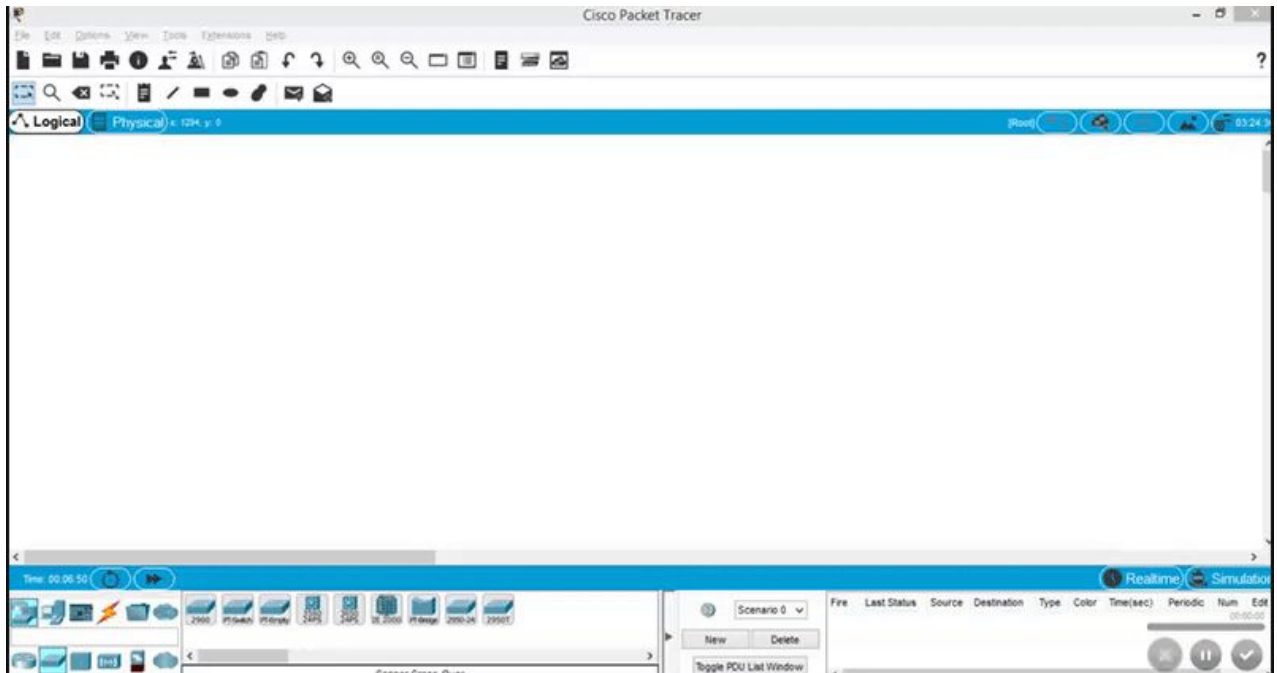


Figura 1.4.A. Proceso de selección del switch genérico **Switch-PT**.

2º Lo segundo que debemos seleccionar, son los 4 PCs, los cuales se encuentran en End Devices, y seleccionamos un PC-PT tal y como sale en el gif.

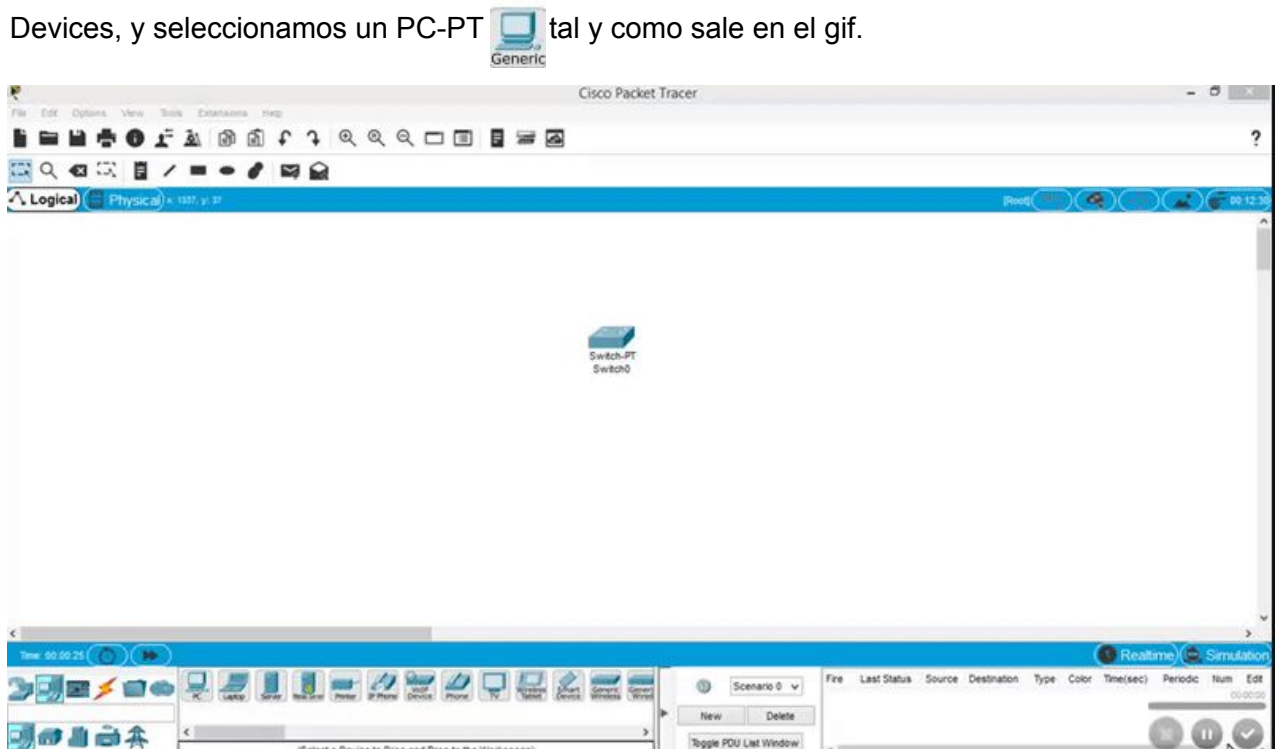


Figura 1.4.B. Selección de cada PC.

1.4 Red de ordenadores conectados mediante un switch

Para crear la red debemos seleccionar los elementos en el Packet Tracer y arrastrar a la zona de trabajo.

3º Lo tercero que debemos hacer es clicar sobre cada PC y en el apartado de Settings aplicarle un nombre a cada uno de los 4 PC's como se explica en el gif. Los nombres serán PC1,PC2, PC3 y PC4.

1.4

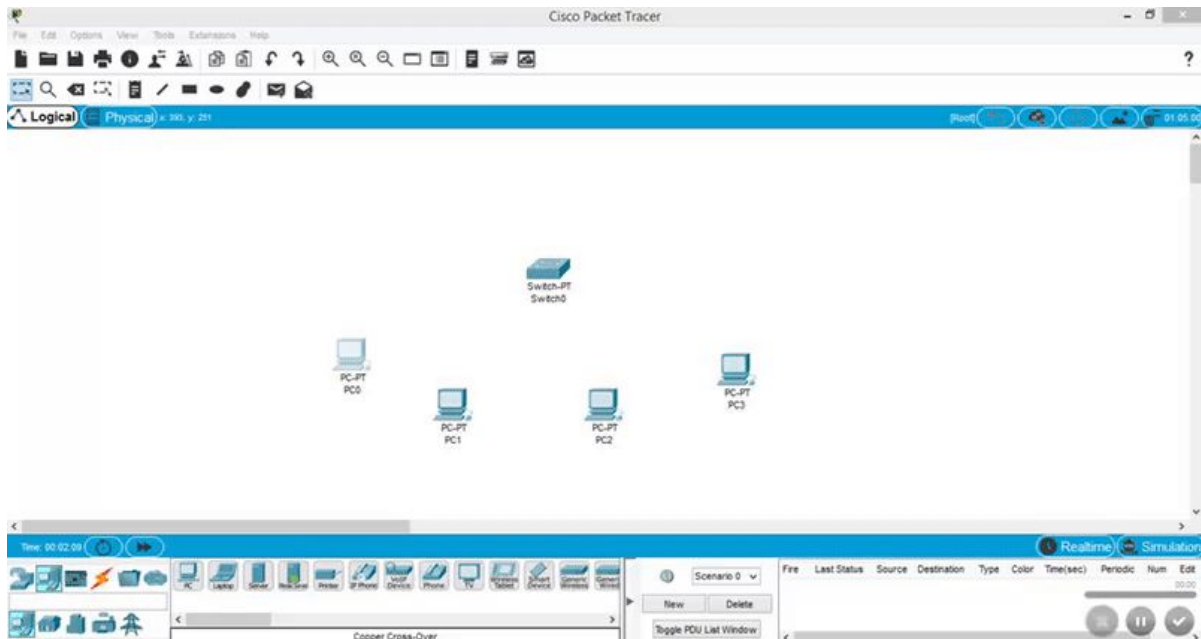



Figura 1.4.C. Asignación de nombre al PC.

4º Para interconectar los elementos usaremos los “cables” cuyo símbolo es .Al seleccionarlo clicamos sobre uno de los elementos y después al que queremos conectarlo y se crearía la conexión.

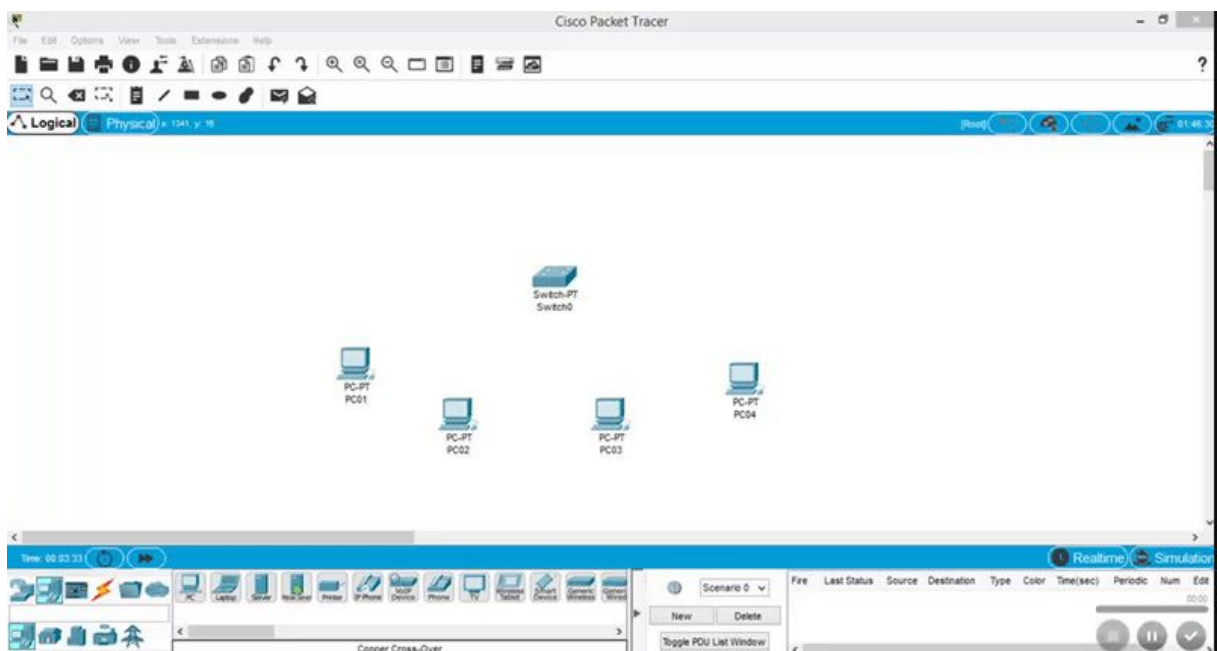


Figura 1.4.D. Conexión mediante cable de los disti

1.4 Red de ordenadores conectados mediante un switch

5º Lo quinto que debemos hacer es asignar una dirección IP a cada uno de los 4 PCs. Para ello hacemos clics sobre cada uno, nos dirigimos a la pestaña llamada Config, después nos dirigimos a la barra de la izquierda llamada FastEthernet0 y donde pone IP Address le colocamos una IP. Las IPs utilizadas son por orden: 192.168.1.1 hasta la 192.168.1.4

1.4

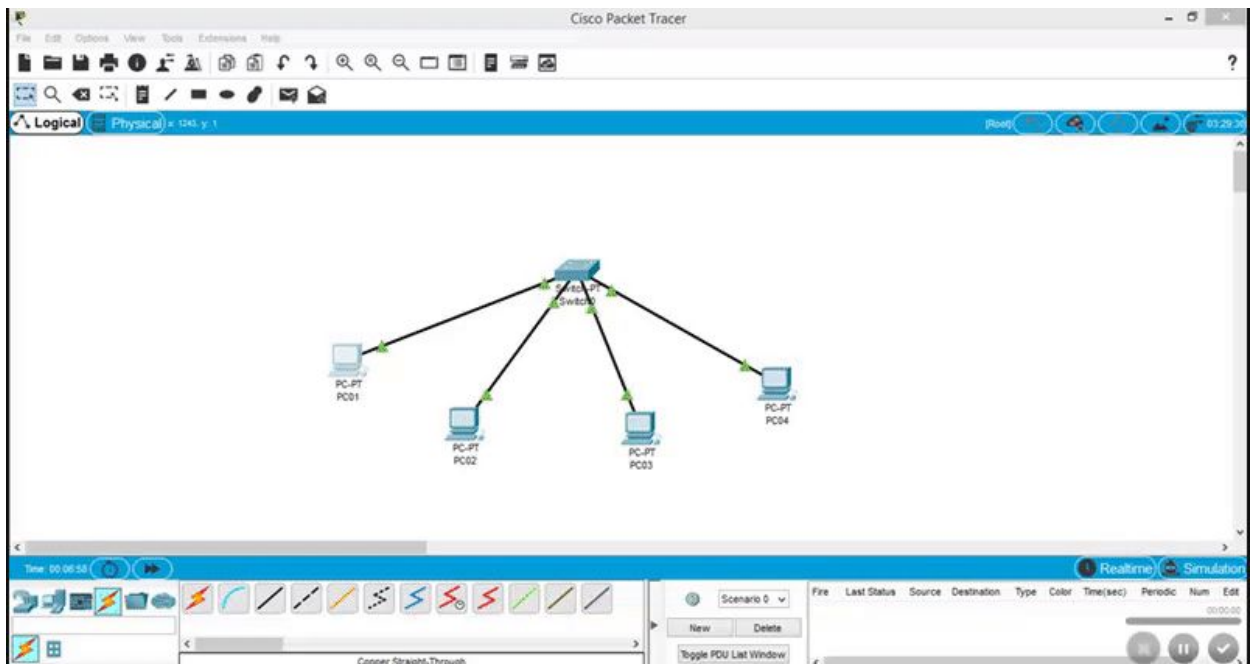



Figura 1.4.E. Asignación de IP a cada PC.

6º Para realizar esto debemos clicar en el símbolo  y seleccionar primero el PC emisor y después el receptor. Para simular el envío iríamos al apartado Simulation:

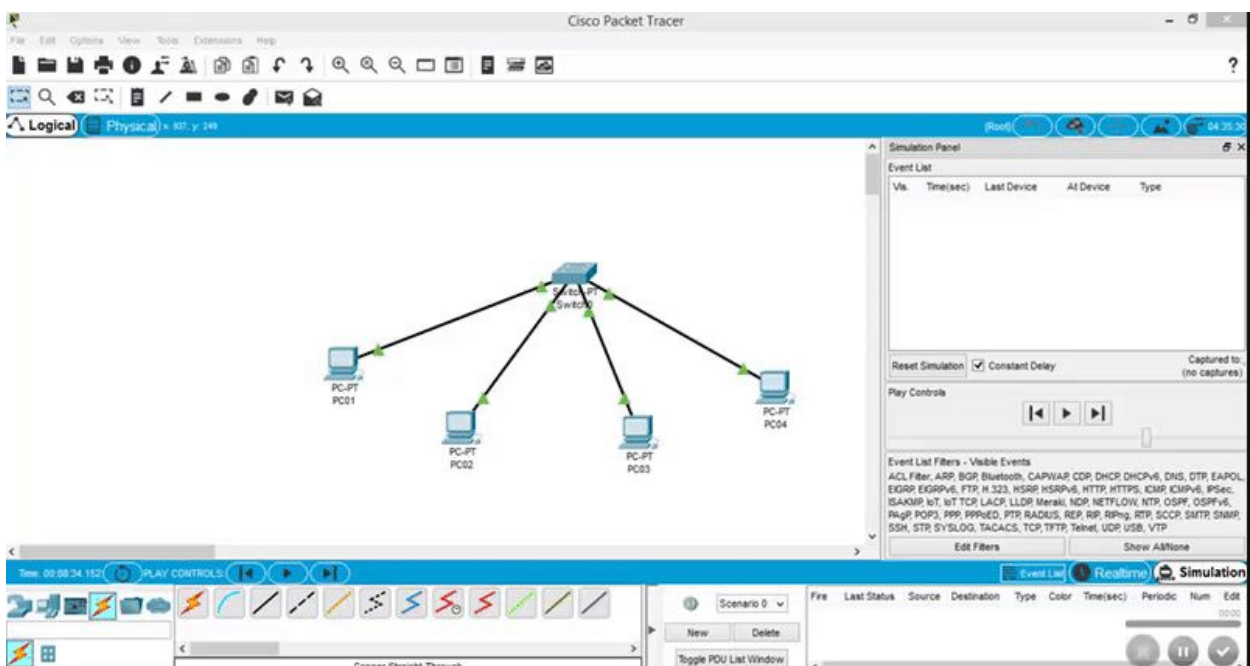


Figura 1.4.F. Muestra del inicio del envío de un ping.

1.4 Red de ordenadores conectados mediante un switch

Como podemos observar, cuando hacemos un envío de un paquete, a parte del paquete ICMP se crea un paquete llamado ARP.

1.4



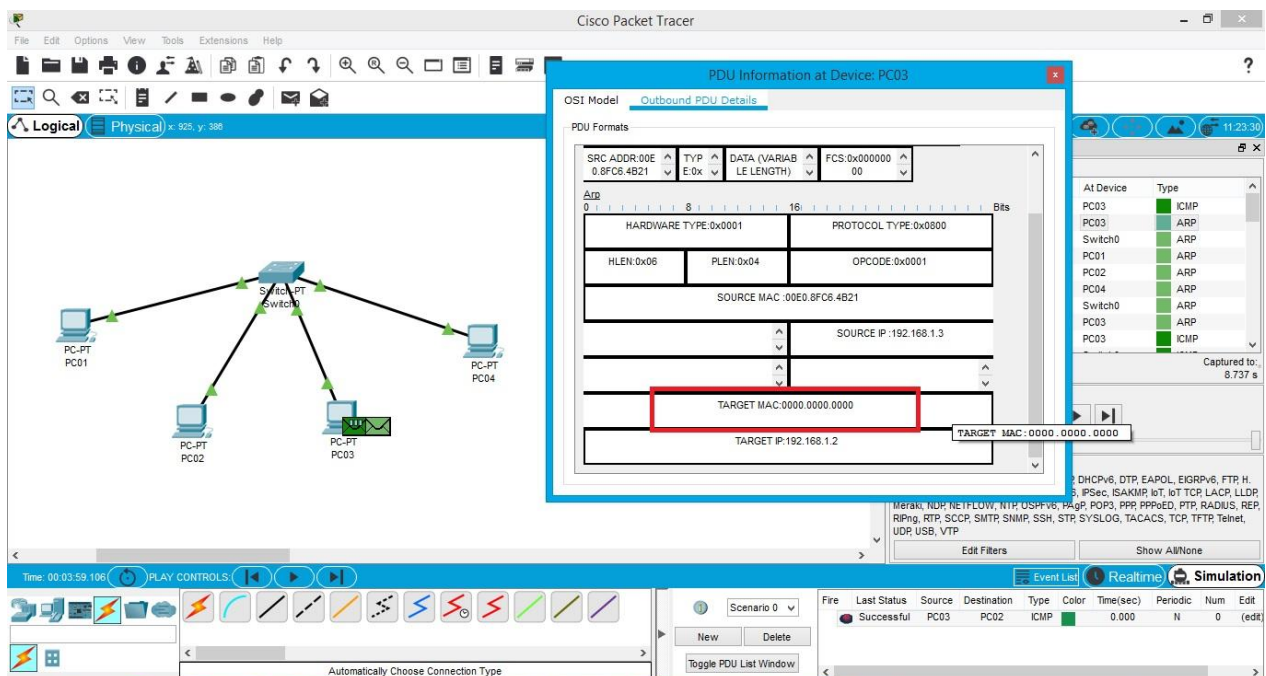
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC01	ICMP
	0.000	--	PC01	ARP
	0.001	PC01	Switch0	ARP

Figura 1.4.G. Muestra del paquete ARP creado.

¿Qué es el protocolo ARP?

Como ya sabemos, cada paquete que enviamos a una dirección pasa por los diferentes dispositivos que tenemos en la red (switch, router...) y para realizar este proceso utiliza las direcciones MAC. Básicamente de lo que se encarga el protocolo ARP es de realizar una traducción entre la dirección MAC y la IP. Cada host y cada router tienen un módulo ARP.

El módulo ARP que tenemos en cada PC mantiene una tabla (tabla ARP), la cual contiene la traducción de las direcciones IP a direcciones MAC. Pero ¿qué pasa si esta tabla está vacía? Para ello el emisor construye un paquete ARP, el cual contiene las direcciones IP y MAC de envío y recepción. Al hacer una captura en PT podemos ver que nos falta un campo, y este es el de la dirección MAC de destino. El PC emisor envía un paquete ARP a todos los ordenadores de la red con el fin de buscar el destinatario, del cual desconocemos su dirección MAC. El paquete ARP contiene tanto la dirección IP de origen como la de destino, entonces cuando el PC cuya IP coincida con la IP de destino del paquete, le enviará un paquete ARP de respuesta con la traducción deseada.



The image shows the Cisco Packet Tracer interface. On the left, a network diagram displays a central switch connected to four PCs (PC01, PC02, PC03, PC04). On the right, a 'PDU Information at Device: PC03' window is open, showing the details of an outgoing ARP packet. The packet structure is as follows:

Field	Value	
SRC_ADDR:00E	0.8FC6.4B21	
TYP	E:0x	
DATA (VARIABLE LENGTH)	FCS:0x00000000	
ARP		
HARDWARE TYPE:0x0001	PROTOCOL TYPE:0x0800	
HLEN:0x06	PLEN:0x04	OPCODE:0x0001
SOURCE MAC:00E0.8FC6.4B21		
SOURCE IP:192.168.1.3		
TARGET MAC:0000.0000.0000		
TARGET IP:192.168.1.2		

Below the packet details, an event list shows a successful ARP request from PC03 to PC02 via the switch at 0.000 seconds.

Figura 1.4.H. Detalles del paquete ARP formado.

<ACABGON>
<DPLAHER>

1.4 Red de ordenadores conectados mediante un switch

¿Por qué no se envían paquetes ARP cuando utilizamos un HUB?

Porque, los hubs solo trabajan en la capa física, mientras que un switch también trabaja en la capa de enlace (MAC) y la capa de red, que se encarga del direccionamiento IP.

1.4

Al contrario que ocurre con los hubs, cuando utilizamos un switch, tras el primer envío, los siguientes envíos no requieren broadcasting. Esto ocurre ya que el switch va creando una tabla dinámica con las direcciones IP y MAC, ayudándose de los paquete ARP de cada dispositivo, de modo que el paquete enviado por el emisor ya irá con su destino bien fijado, pasa por el switch y sale directo por el puerto correspondiente.

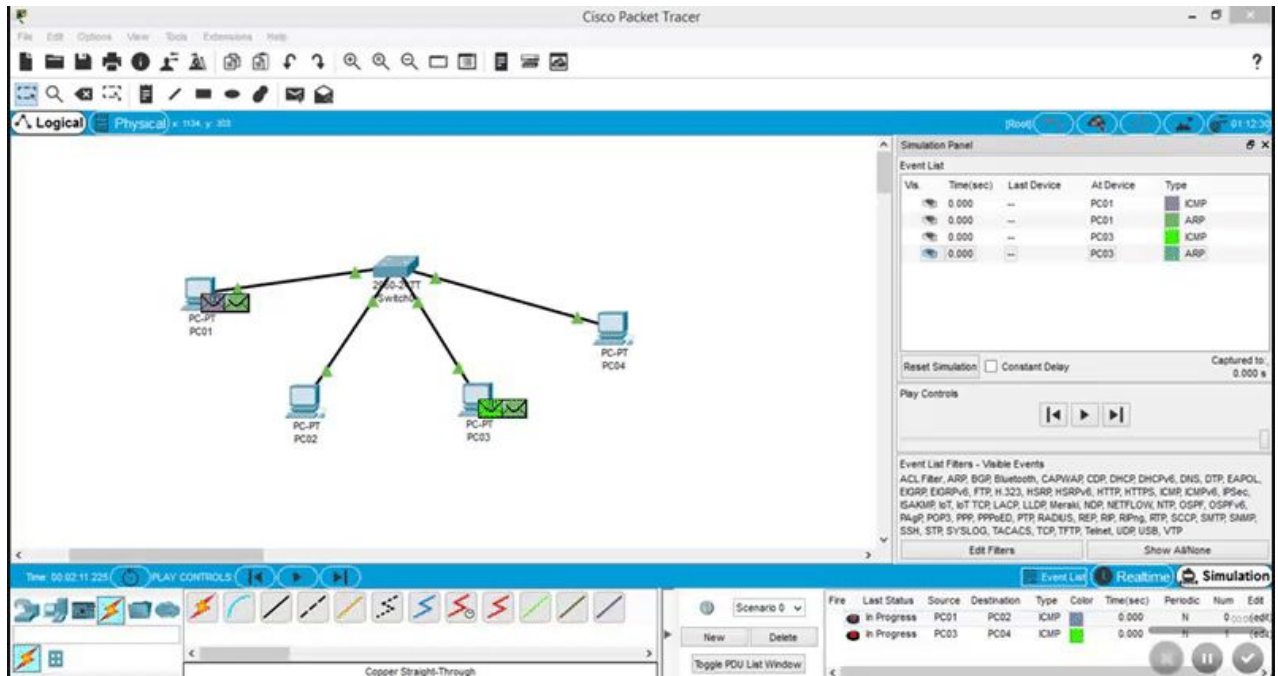


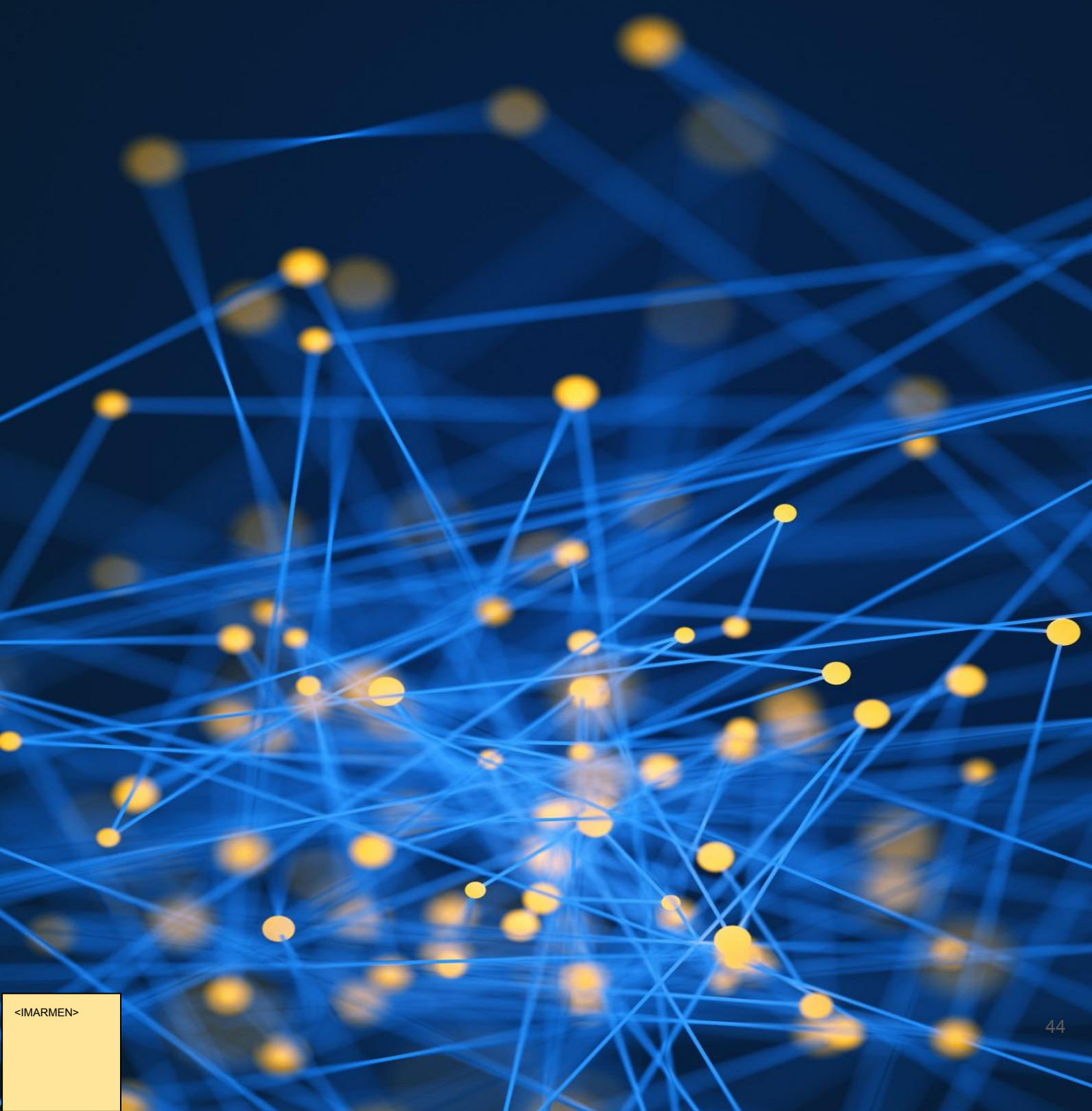
Figura 1.4.I. Intercambio de paquetes en un envío a través de switch.

Buffering:

Como se puede observar en el gif anterior, cuando enviamos más de un paquete a través de la red estos se “ponen en cola” en el switch, esto es a lo que llamamos buffering.

Trabajo 1.5

Instalación y operación básica de switches



Trabajo 1.5. Instalación y operación básica de switches.

1.5

1. Acceso al modo usuario y administrador. Abre la CLI y entra en modo usuario. Accede entonces al modo administrador. Vuelve al modo usuario. **(Daniel y Sergio)**

2. Reinicio de IOS. Reinicia el sistema operativo del switch. **(Jose y Victor)**

3. Desactivar Translating “xyz”. Los switches por defecto, cuando insertamos un comando no conocido busca por la red un host con ese nombre, lo cual provoca un tiempo de espera que se vuelve altamente improductivo, máxime si estamos iniciándonos en la operación de estos dispositivos. Prueba a desactivar este comportamiento en un switch y demuestra que funciona. **(Abisai y Aray)**

4. Comando show. Utilizando este comando, recupera la siguiente información del sistema: a **Javier e Isaac**

- a. Hora del sistema
- b. Tabla de forwarding (mac-table)
- c. Configuración que está ejecutando actualmente
- d. Configuración actual del STP. Para ello, crear una red de varios switches y varios Pcs y espera a que se configure STP. Muestra de un switch su configuración STP. Explica cómo representa los puertos bloqueados. Explica cómo representa los puertos raíz
- e. Procesos en ejecución
- f. Número del modelo del switch: WS-C2960-24TT

5. Cambiar el nombre del switch. Utilizando el comando hostname modifica el nombre del switch. Demuestra que efectivamente ha sido así tanto en la consola como en la GUI. **(Daniel y Sergio)**

6. Clave de acceso a la consola. Modifica la configuración del switch de modo que incluya una clave de configuración para la consola de configuración **(Jose y Victor)**

7. Acceso a la consola desde hyperterminal. Utilizando PT, accede a la consola de configuración de un switch usando la utilidad de escritorio de un PC **(Abisay y Aray)**

8. Cambiar la configuración de un puerto (o boca). Desde la consola de un PC, modifica la configuración del puerto F0/1 a 10Mbps y half-dúplex. **Javier e Isaac**

9. Habilitar conexión de administrador vía telnet. (Daniel y Sergio)

Configuramos las sesiones telnet:

- configure terminal
- line vty 0 15
- no login
- login local
- username moi password moi
- username moi privilege 15

Establecemos IP para el switch

- configure terminal
- interface vlan 1
- ip address 192.168.1.3 255.255.255.0
- no shutdown

10. Accede desde un PC a la configuración del switch vía telnet. Prueba que efectivamente ha funcionado tu configuración telnet del switch. **(Jose y Victor)**

Actividad 1.5

Apartado 1

1. Acceso al modo usuario y administrador. Abre la CLI y entra en modo usuario. Accede entonces al modo administrador. Vuelve al modo usuario.

1.5.1

Para entrar en el modo usuario, simplemente abrimos con doble click el switch el cual queremos usar y entramos en la CLI, y seguidamente pulsamos RETURN(tecla ENTER). Se puede observar como el carácter a la derecha del hostname (nombre del switch) cambia y encontramos el símbolo mayor '>'.</p></div>
<div data-bbox="118 201 909 249" data-label="Text">
<p>Para entrar en el modo administrador, estando en la CLI, tecleamos **enable** y presionamos ENTER. Podremos observar como el carácter a la derecha del hostname del switch cambia al símbolo almohadilla '#'.</p></div>
<div data-bbox="118 265 909 313" data-label="Text">
<p>Para salir del modo administrador, estando en la CLI, tecleamos **disable** y presionamos ENTER. Esta vez observaremos como el carácter de la derecha del hostname del switch vuelve a cambiar de '#' al símbolo mayor '>'.</p></div>
<div data-bbox="219 326 771 629" data-label="Diagram">

 El diagrama muestra una configuración de red básica. En el centro superior hay un icono de un switch etiquetado como '2950-24TT'. Dos líneas de conexión lo vinculan a dos iconos de PC situados a la izquierda y a la derecha. El PC a la izquierda está etiquetado como 'PC-PT PC0' y el PC a la derecha como 'PC-PT PC1'. Las conexiones se representan por líneas rectas que terminan en pequeños círculos verdes, indicando un enlace físico o lógico entre los dispositivos.
</div>
<div data-bbox="282 631 746 646" data-label="Caption">
<p>Figura 1.5.1. Acceso y salida del modo administrador en la consola.</p></div>
<div data-bbox="9 927 67 944" data-label="Page-Footer">
<p></p></div>
<div data-bbox="955 934 986 949" data-label="Page-Footer">
<p>46</p></div>

2. Reinicio de IOS

Reinicia el sistema operativo del switch.

Estando en la consola de comandos CLI del switch como administrador, procederemos a aplicar el comando `reload` para reiniciar el sistema operativo del switch:

1.5.2

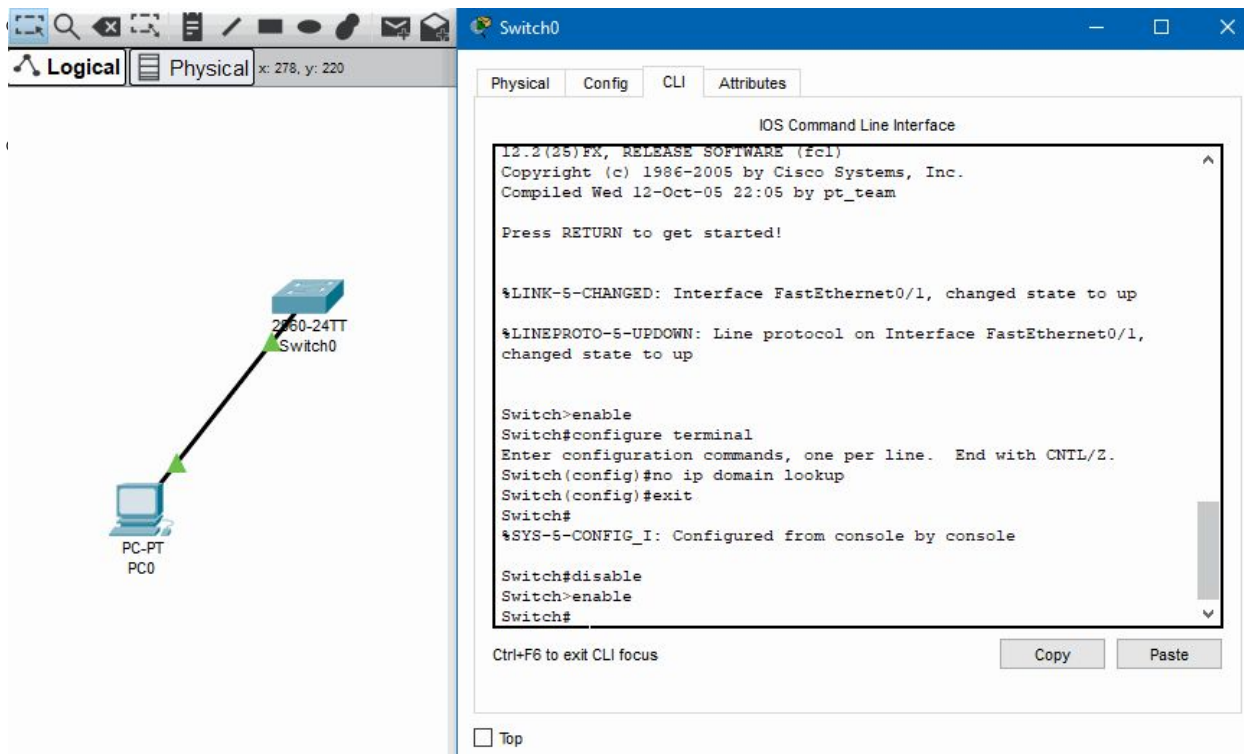


Figura 1.5.2. Reinicio del SO del switch.

Apartado 3. Desactivar Traslating XYZ

3. Desactivar Translating “xyz”. Los switches por defecto, cuando insertamos un comando desconocido busca por la red un host con ese nombre, lo cual provoca un tiempo de espera que se vuelve altamente improductivo, máxime si estamos iniciándonos en la operación de estos dispositivos. Prueba a desactivar este comportamiento en un switch y demuestra que funciona.

Esto es lo que ocurre cuando introducimos un comando desconocido:

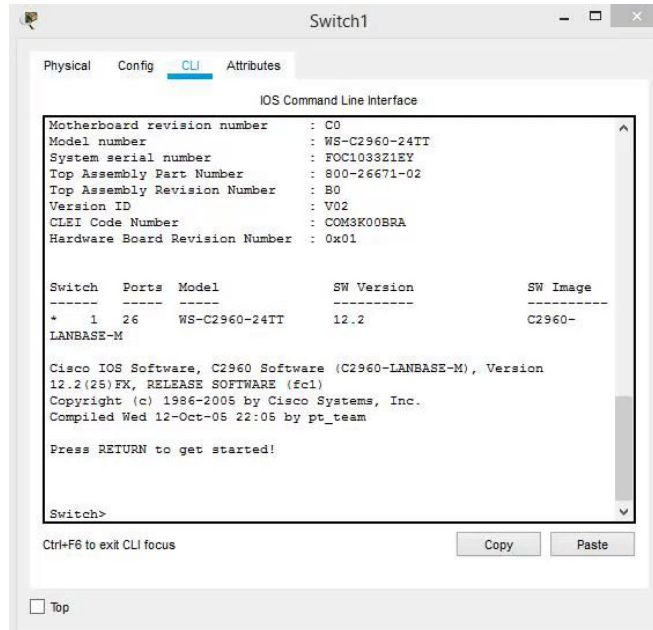


Figura 1.5.3.A. Introducción de un comando desconocido.

Lo primero que hay que hacer es entrar al CLI del switch y activar el “Modo configuración”, para ello utilizaremos el comando `“configure terminal”`.

- **Modo usuario:**

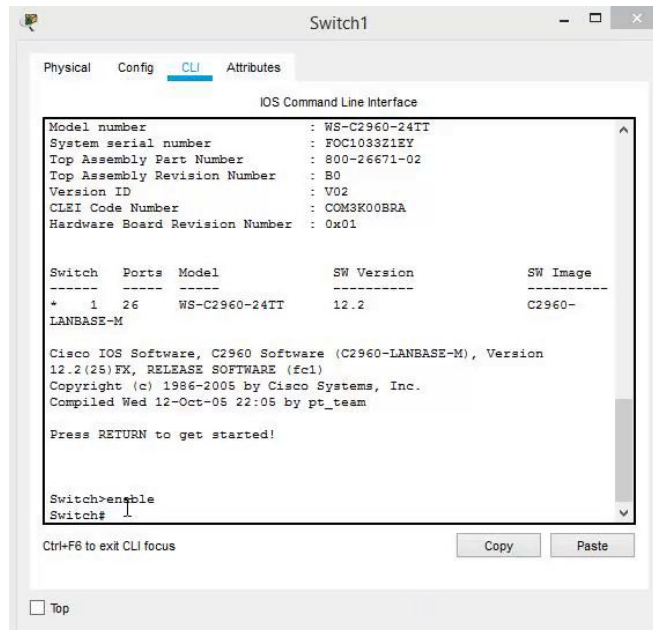
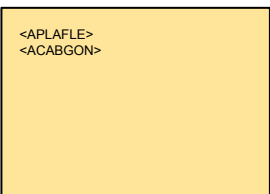


Figura 1.5.3.B. Introducción del comando `configure terminal`.

Como se aprecia en el GIF, cuando introducimos el comando en el modo usuario el dispositivo no lo reconoce.



Apartado 3. Desactivar Traslating XYZ

- **Modo administrador:**

Ahora lo que haremos será entrar en el modo administrador y volvemos a introducir el comando

`"configure terminal"`.

1.5.3

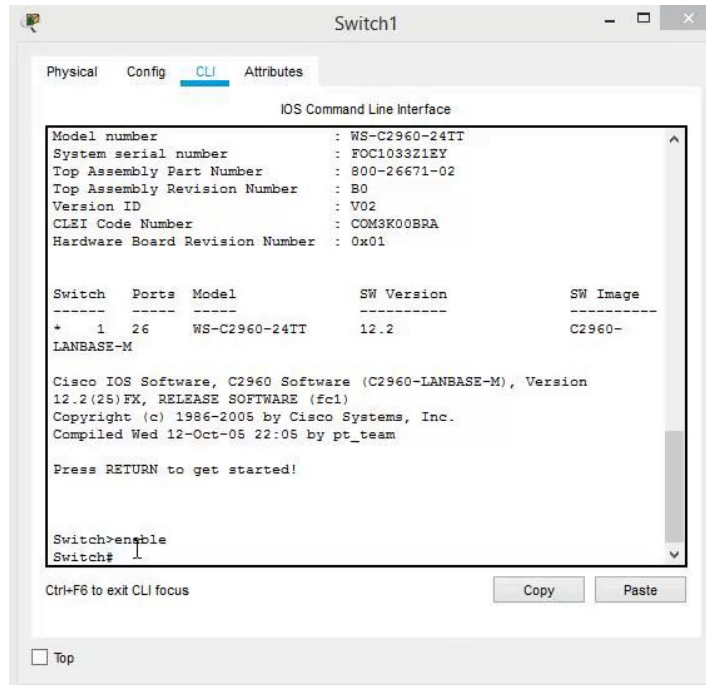


Figura 1.5.3.D. Ejecución del comando `configure terminal`.

Como se puede observar, cuando introducimos el comando en el modo de usuario el dispositivo si lo acepta.

Una vez hemos entrado en el **“Modo configuración”** tenemos que introducir el comando `"no ip domain-lookup"` cuyo fin es evitar los tiempos de espera que se producen cuando introducimos un comando y nos equivocamos al teclear.

- **Modo configuración:**

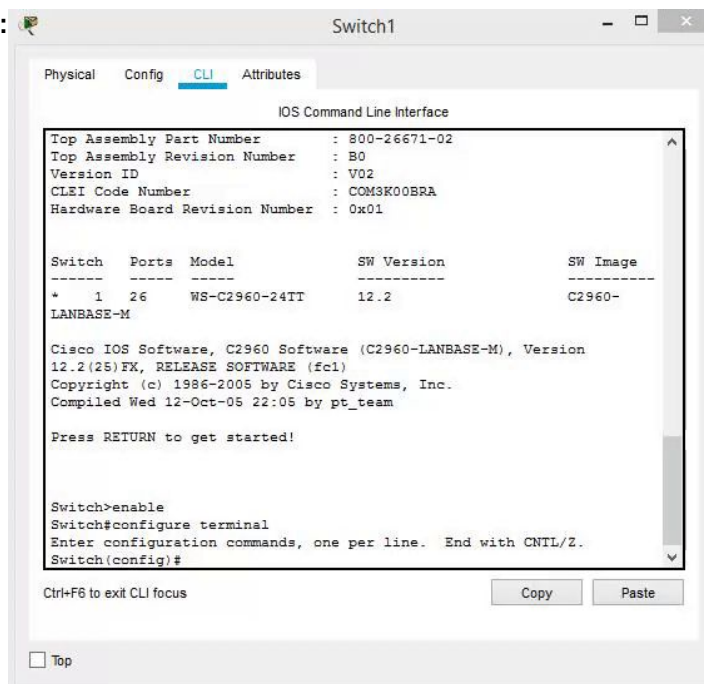


Figura 1.5.3.E.

<APLAFLE>
<ACABGON>

Apartado 3. Desactivar Traslating XYZ

Ahora que hemos activado el comando "no ip domain-lookup", probaremos a introducir un comando desconocido para demostrar que funciona.

1.5.3

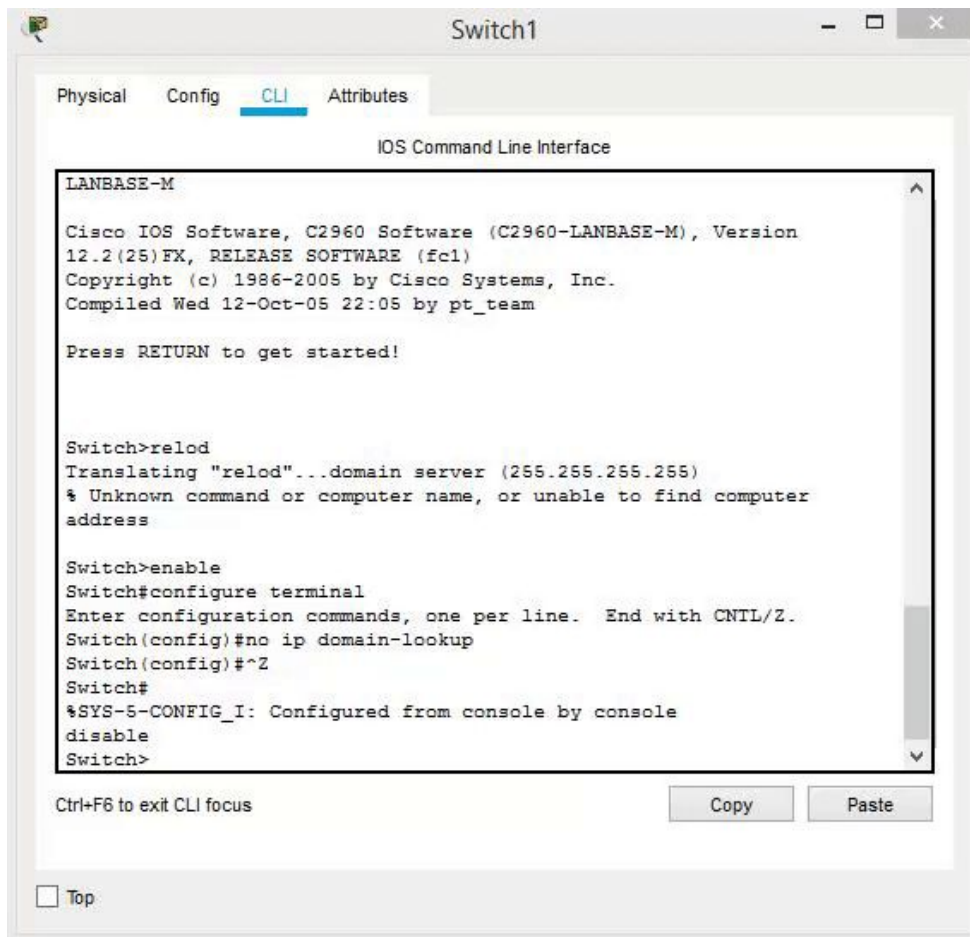


Figura 1.5.3.C. Funcionamiento correcto tras introducir un comando incorrecto.

<APLAFLE>
<ACABGON>

Apartado 4. Comando show ?

Primero mostramos los comandos posibles con el comando `show ?`

```
Switch#show ?
  access-lists      List access lists
  arp                Arp table
  boot              show boot attributes
  cdp               CDP information
  clock             Display the system clock
  crypto            Encryption module
  dhcp              Dynamic Host Configuration Protocol status
  dtp               DTP information
  etherchannel      EtherChannel information
  flash:            display information about flash: file syste
  history           Display the session command history
  hosts             IP domain-name, lookup style, nameservers,
  interfaces        Interface status and configuration
  ip                IP information
  lldp              LLDP information
  logging           Show the contents of logging buffers
  mac               MAC configuration
  mac-address-table MAC forwarding table
  mls               Show MultiLayer Switching information
  monitor           SPAN information and configuration
  ntp               Network time protocol
  port-security     Show secure port information
--More-- |
```

1.5.4

Figura 1.5.4.A. Información extraída mediante el comando `show ?`

Para ver todos los comando pulsamos “enter” varias veces o “espacio” para saltar una página directamente.

```
Switch#show ?
  access-lists      List access lists
  arp                Arp table
  boot              show boot attributes
  cdp               CDP information
  clock             Display the system clock
  crypto            Encryption module
  dhcp              Dynamic Host Configuration Protocol status
  dtp               DTP information
  etherchannel      EtherChannel information
  flash:            display information about flash: file system
  history           Display the session command history
  hosts             IP domain-name, lookup style, nameservers, and host table
  interfaces        Interface status and configuration
  ip                IP information
  lldp              LLDP information
  logging           Show the contents of logging buffers
  mac               MAC configuration
  mac-address-table MAC forwarding table
  mls               Show MultiLayer Switching information
  monitor           SPAN information and configuration
  ntp               Network time protocol
  port-security     Show secure port information
  privilege         Show current privilege level
  processes         Active process statistics
  running-config    Current operating configuration
  sdm               Switch database management
  sessions          Information about Telnet connections
  snmp              snmp statistics
  spanning-tree     Spanning tree topology
  ssh               Status of SSH server connections
  startup-config    Contents of startup configuration
  storm-control     Show storm control configuration
  tcp               Status of TCP connections
  tech-support      Show system information for Tech-Support
  terminal          Display terminal configuration parameters
  users             Display information about terminal lines
  version           System hardware and software status
  vlan              VTP VLAN status
  vtp               VTP information
Switch#show |
```

Figura 1.5.4.B. Uso de la tecla “enter”/“espacio” en la consola de comandos.

Apartado 4

Apartado A. Hora del sistema

Para ver la hora el comando será `show clock`

```
Switch#show clock
*0:4:18.345 UTC Mon Mar 1 1993
Switch#
```

1.5.4

Apartado B. Tabla de forwarding (mac-table)

Se trata de una tabla en la que el switch guarda las direcciones MAC de todos los dispositivos que se ha encontrado.

Tenemos esta configuración.

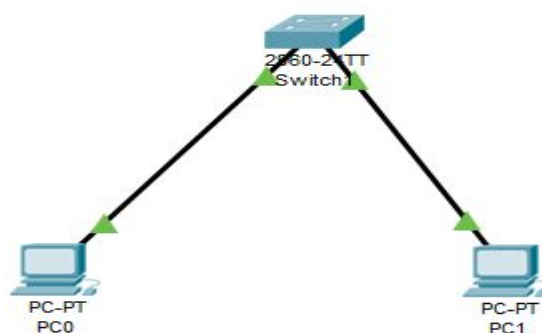


Figura 1.5.4.C. Red de dos PC y un switch.

Comprobamos la tabla Mac con el comando `show mac-address-table`

La imagen muestra una interfaz de usuario de un switch con una ventana de CLI abierta. A la izquierda, se repite el diagrama de la red con el switch y los dos PCs. La ventana de CLI muestra el siguiente texto:

```
IOS Command Line Interface
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up

Switch>enable
Switch#show mac-
Switch#show mac-address-table
      Mac Address Table
-----
Vlan  Mac Address      Type    Ports
-----
Switch#
Switch#
```

Figura 1.5.4.D. Uso del comando `show mac-address-table`

No se ha realizado ningún proceso, por ejemplo un “ping”, por lo que el switch no tiene reconocidas las Mac de los PC.

Apartado 4. A y B

Apartado A. Hora del sistema

Realizamos un ping para que reconozca las Mac.

1.5.4

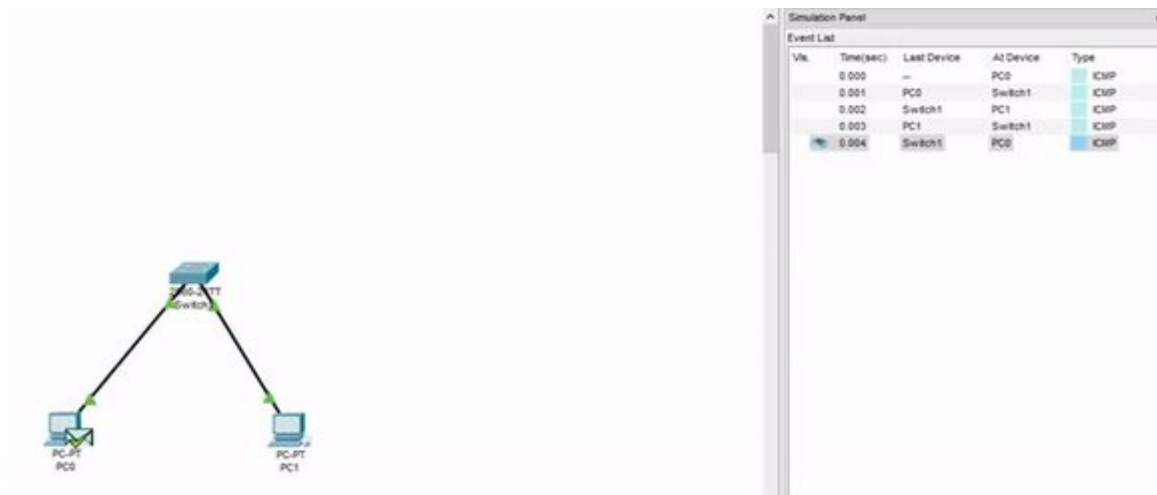


Figura 1.5.4.E. Realización de un ping.

Comprobamos la tabla mac de nuevo. Ahora sí podemos distinguir las dos Mac.

```
Switch#show mac-address-table
      Mac Address Table
-----
Vlan  Mac Address      Type      Ports
----  -
1     000b.be19.4caa    DYNAMIC   Fa0/2
1     00e0.8fld.655d    DYNAMIC   Fa0/1
Switch#
```

Figura 1.5.4.F. Tabla de MACs del switch.

Apartado 4. B

Comprobamos que las Mac corresponden con los dos PC.

PC0

1.5.4

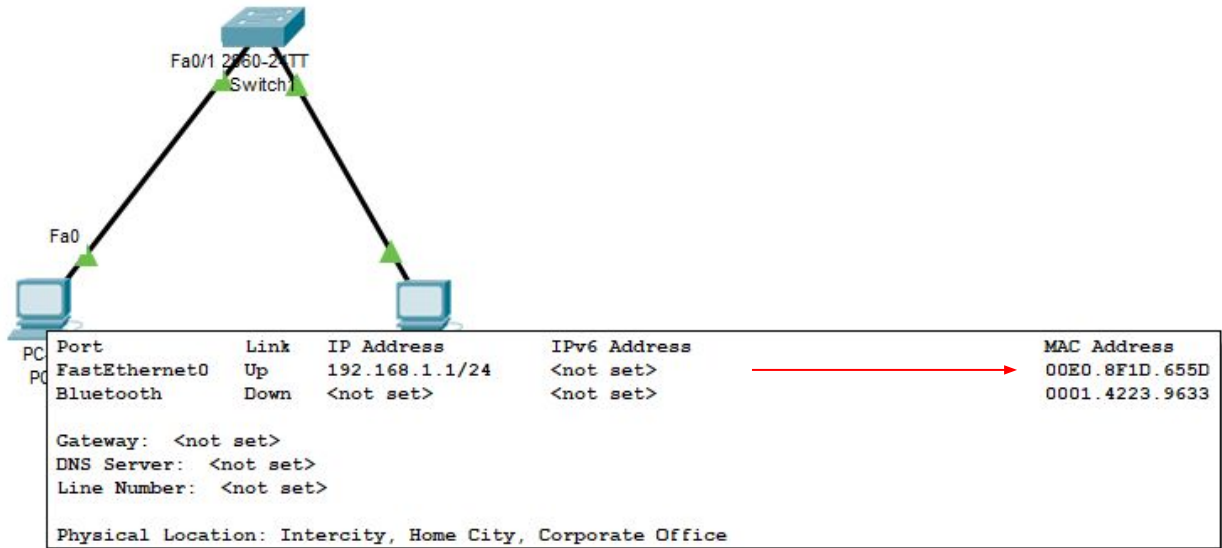


Figura 1.5.4.G. Comprobación de la MAC del PC0.

PC1

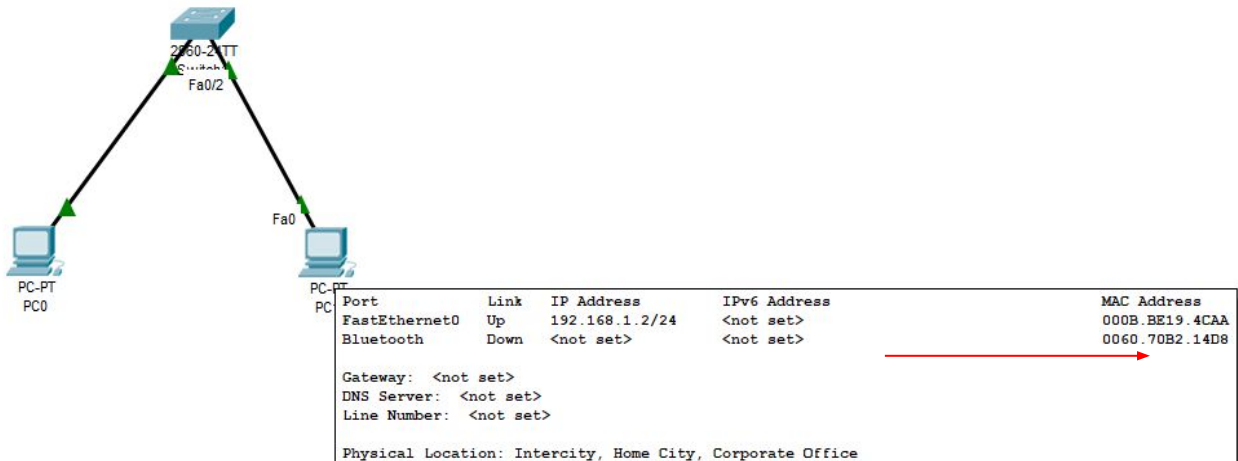


Figura 1.5.4.H. Comprobación de la MAC del PC1.

Apartado 4. C

Apartado C. Configuración que está ejecutando actualmente

Comprobamos el estado con el comando `show running-configuration`

1.5.4

```
Switch#show running-config
Building configuration...

Current configuration : 1078 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
--More-- |
```

Figura 1.5.4.I. Muestra de la configuración actual mediante `show running-configuration`

Como ya hemos visto la información, si pulsamos la tecla “Q”, o usamos “Ctrl+C” dejaría de seguir mostrando el resto de datos.

```
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
end

Switch#|
```

Figura 1.5.4.J. Finalización de la muestra de información tras ejecutar “Ctrl+C” o pulsar la tecla Q.

Apartado 4. D

Apartado D. Configuración actual del STP. Para ello, crear una red de varios switches y varios Pcs y espera a que se configure STP. Muestra de un switch su configuración STP. Explica cómo representa los puertos bloqueados. Explica cómo representa los puertos raíz.

Montamos una red y mostramos la configuración STP del Switch 1

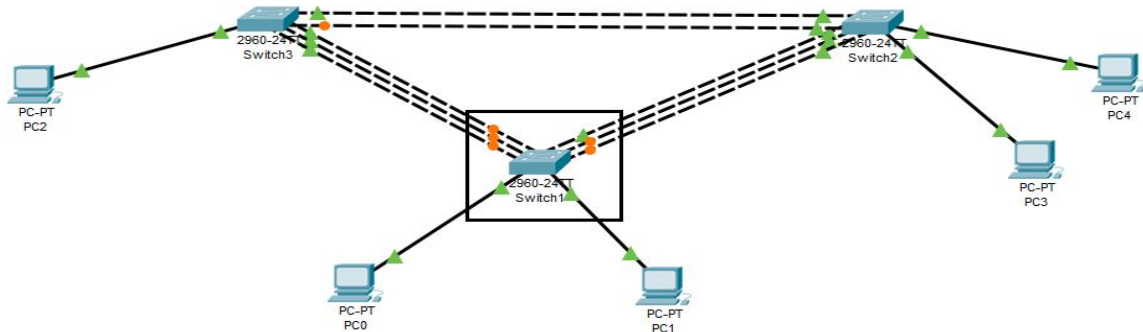


Figura 1.5.4.K. Diseño de una red para comprobar STP.

STP: Spanning Tree Protocol. Su utilidad es que no se generen bucles en la red.

Para ello usamos el comando `show spanning-tree`

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address     0002.1797.21B2
            Cost        19
            Port        4 (FastEthernet0/4)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address     0060.5C76.CCE0
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/9        Altn BLK 19        128.9   P2p
Fa0/2        Desg FWD 19        128.2   P2p
Fa0/3        Altn BLK 19        128.3   P2p
Fa0/4        Root FWD 19        128.4   P2p
Fa0/5        Altn BLK 19        128.5   P2p
Fa0/8        Altn BLK 19        128.8   P2p
Fa0/6        Altn BLK 19        128.6   P2p
Fa0/1        Desg FWD 19        128.1   P2p

Switch#
```

Figura 1.5.4.L. Muestra de la configuración activa del STP.

Como se ve en la configuración, hay bocas bloqueadas BLK que en la imagen se muestran como puntos naranjas, y bocas activas FWD como triángulos verdes.

Tendríamos 2 rectángulos en la imagen anterior: en verde la boca activa (FWD) y en naranja la boca bloqueada(BLK).

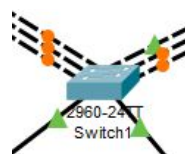


Figura 1.5.4.M. Muestra gráfica del estado de los puertos.

Apartado 4. D y E

El puerto raíz lo muestra en la columna Role - Root

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/9	Altn	BLK	19	128.9	P2p
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/3	Altn	BLK	19	128.3	P2p
Fa0/4	Root	FWD	19	128.4	P2p
Fa0/5	Altn	BLK	19	128.5	P2p
Fa0/8	Altn	BLK	19	128.8	P2p
Fa0/6	Altn	BLK	19	128.6	P2p
Fa0/1	Desg	FWD	19	128.1	P2p

Figura 1.5.4.N. Muestra del puerto raíz resaltado.

Apartado E. Procesos en ejecución

En la lista de comandos encontramos processes para ver todos los procesos en ejecución. Por lo tanto escribimos dicho comando: `show processes.`

```
Switch#show processes
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID QTY PC Runtime (ms) Invoked uSecs Stacks TTY Process
 1 Csp 602F3AF0 0 1627 0 2600/3000 0 Load Meter
 2 Lwe 60CSBE00 4 136 29 5572/6000 0 CEF Scanner
 3 Lst 602D90F8 1676 837 2002 5740/6000 0 Check heaps
 4 Cwe 602D08F8 0 1 0 5568/6000 0 Chunk Manager
 5 Cwe 602DF0E8 0 1 0 5592/6000 0 Pool Manager
 6 Mst 602S1E38 0 2 0 5560/6000 0 Timers
 7 Mwe 600D4940 0 2 0 5568/6000 0 Serial Backgrou
 8 Mwe 6034B718 0 1 0 2584/3000 0 OIR Handler
 9 Mwe 603FA3C8 0 1 0 5612/6000 0 IPC Zone Manage
10 Mwe 603FA1A0 0 8124 0 5488/6000 0 IPC Periodic Ti
11 Mwe 603FA220 0 9 0 4884/6000 0 IPC Seat Manage
12 Lwe 60406818 124 2003 61 5300/6000 0 ARP Input
13 Mwe 60581638 0 1 0 5760/6000 0 HC Counter Time
14 Mwe 605E3D00 0 2 0 5564/6000 0 DDR Timers
15 Msp 80164A38 0 79543 0 5608/6000 0 GraphIt
16 Mwe 802DB0FC 0 2 011576/12000 0 Dialer event
17 Cwe 801E74BC 0 1 0 5808/6000 0 Critical Bkgnd
18 Mwe 80194D20 4 9549 010428/12000 0 Net Background
19 Lwe 8011E9CC 0 20 011096/12000 0 Logger
20 Mwe 80140160 8 79539 0 5108/6000 0 TTY Background
21 Msp 80194114 0 95409 0 8680/9000 0 Per-Second Job
22 Mwe 8047E960 0 2 0 5544/6000 0 dotltx
23 Mwe 80222C8C 4 2 2000 5360/6000 0 DHCPD Receive
24 Mwe 800844A0 0 1 0 5796/6000 0 HTTP Timer
25 Mwe 80099378 0 1 0 5612/6000 0 RARP Input
26 Mst 8022F178 0 1 011796/12000 0 TCP Timer
27 Lwe 802344C8 0 1 011804/12000 0 TCP Protocols
28 Hwe 802870E8 0 1 0 5784/6000 0 Socket Timers
29 Mwe 80426048 64 3 21333 4488/6000 0 L2MM
30 Mwe 80420010 4 1 4000 5592/6000 0 MRD
31 Mwe 8041E570 0 1 0 5584/6000 0 IGMPSN
32 Hwe 80429B40 0 1 0 2604/3000 0 IGMP Snooping P
33 Mwe 804F43B0 0 5 0 5472/6000 0 Cluster L2
34 Mwe 804F18D0 0 17 0 5520/6000 0 Cluster RARP
35 Mwe 804EA650 0 23 0 5440/6000 0 Cluster Base
36 Lwe 802A1158 4 1 4000 5592/6000 0 Router Autoconf
37 Mwe 80022058 0 1 0 5624/6000 0 Syslog Traps
38 Mwe 8031CE88 0 1 0 5788/6000 0 AggMgr Process
39 Mwe 8035EF88 0 407 0 5592/6000 0 PM Callback
40 Mwe 80437B58 0 3 0 5556/6000 0 VTP Trap Proces
41 Mwe 80027D40 0 2 0 5676/6000 0 DHCPD Timer
42 Mwe 8040D3B0 0 2 0 2560/3000 0 STP STACK TOPOL
43 Hwe 8040E338 0 2 0 2560/3000 0 STP FAST TRANSI
Switch#
```

Figura 1.5.4.Ñ. Muestra de los procesos en ejecución.

Apartado 4. F

Apartado F. Número del modelo del switch: WS-C2960-24TT

Podemos comprobarlo con varios comandos como: `show tech-support` o `show version`

1.5.4

• `show tech-support`

```
Switch#show tech-support
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.

24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0060.5C76.CCE0
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC103321EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01
```

Figura 1.5.4.O. Muestra del modelo del switch a través de `show tech-support`

• `show version`

```
Switch#
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.

24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0060.5C76.CCE0
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC103321EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01

Switch  Ports  Model                SW Version          SW Image
-----  ----  -
*      1    26    WS-C2960-24TT      12.2                C2960-LANBASE-M

Configuration register is 0xF

Switch#
```

Figura 1.5.4.P. Muestra del modelo del switch a través de `show version`

Apartado 4. Video Explicativo

<https://www.youtube.com/watch?v=isaFNGIj4No&feature=youtu.be>

QR del vídeo:

1.5.4



Apartado 5

5. Cambiar el nombre del switch. Utilizando el comando `hostname` modifica el nombre del switch. Demuestra que efectivamente ha sido así tanto en la consola como en la GUI.

1.5.5

Para cambiar el nombre al switch entramos en la CLI del switch haciendo doble click, y seguidamente pulsamos RETURN. A continuación, entramos en el modo administrador usando el comando `'enable'` como se explicó anteriormente en el apartado 1.

Seguidamente, introducimos dentro del modo administrador el comando `'configure terminal'`, para entrar en el modo configuración del switch, y presionamos ENTER.

A continuación, dentro del modo configuración del switch introducimos el comando `'hostname'`, presionamos la tecla espacio del teclado y escribimos el nuevo nombre que le queremos poner al switch que como se puede observar en el gif en este caso es 'Ejercicio', seguidamente presionamos ENTER.

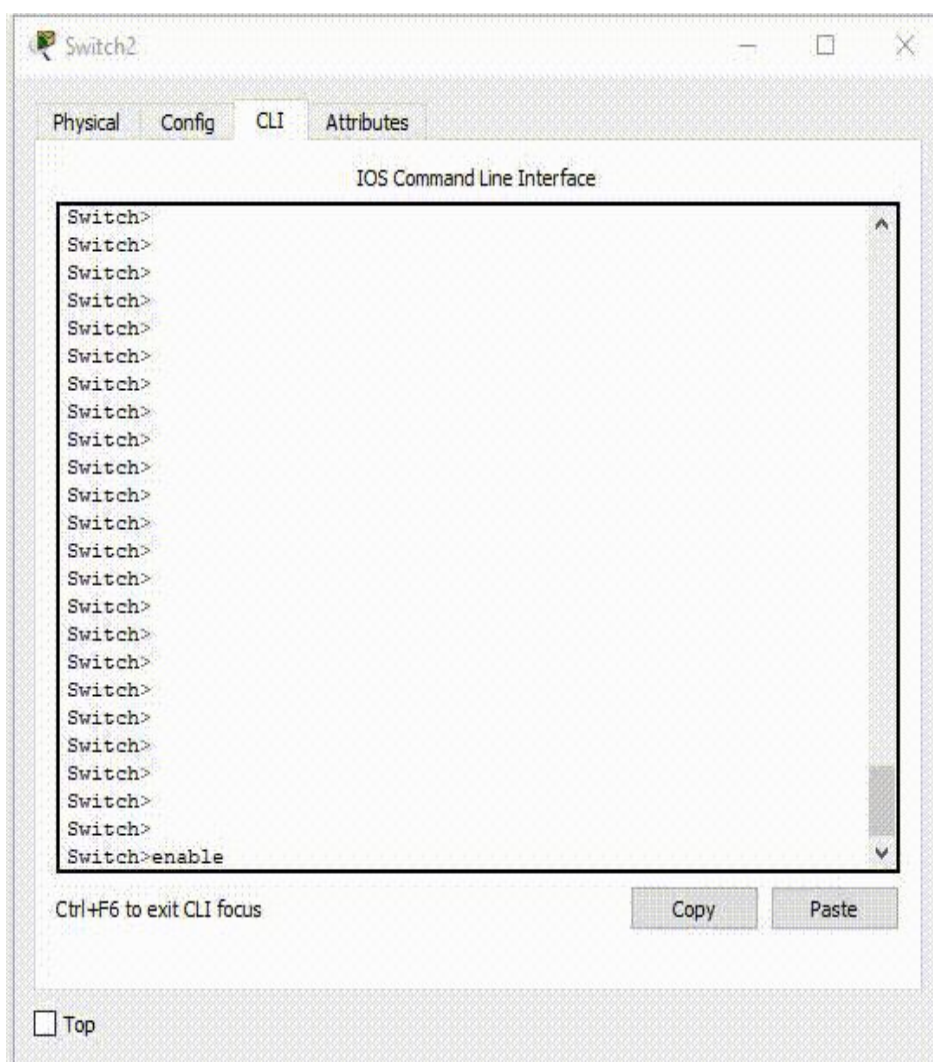


Figura 1.5.5.A. Proceso para cambiarle el nombre al switch.

Apartado 5

A la izquierda del carácter almohadilla '#' se encuentra el nuevo nombre del switch, como podemos observar como se cambia el nombre del Switch por Ejercicio al poner el comando `hostname Ejercicio`.

1.5.5

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one
Switch(config)#hostname Ejercicio
Ejercicio(config)#
```

Figura 1.5.5.B. Nuevo nombre del switch resaltado.

6. Clave de acceso a la consola

Modifica la configuración del switch de modo que incluya una clave de configuración para la consola de configuración.

1.5.6

Estando en la consola de comandos CLI del switch como administrador, procederemos a configurar una contraseña para poder entrar a la consola de comandos de la siguiente manera:

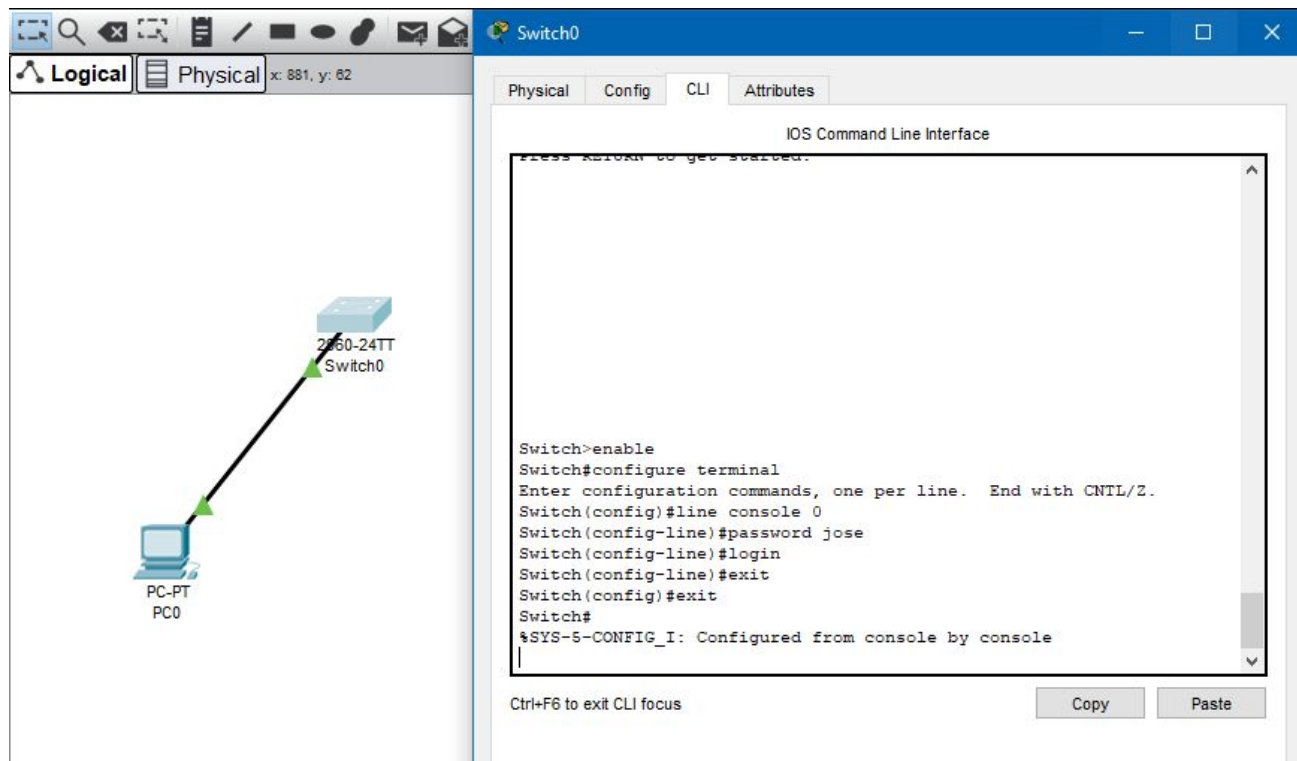


Figura 1.5.6.A. Creación de contraseña para la consola de configuración.

Tras aplicar el comando *configure terminal*, (estando en modo administrador), añadiremos los siguientes comandos:

Line console 0

password X (sustituyendo X por la contraseña, en mi caso jose).

login

Con el comando **login**, lo que conseguiremos es que se nos pida la contraseña, puesto que si sólo aplicásemos el comando **password + clave**, únicamente habremos establecido la contraseña, pero no tendríamos la petición para introducirla al entrar en la consola.

En el gif de la **figura 1.5.6.B**, se puede apreciar cómo se nos pide la contraseña para acceder a la consola de comandos, y tras haber fallado tres veces con ésta, terminamos accediendo a ella escribiendo bien la clave de acceso.

Para desactivar la contraseña, bastará con repetir el proceso hasta el comando **line console 0**, tras el que aplicaremos el comando **no password**.

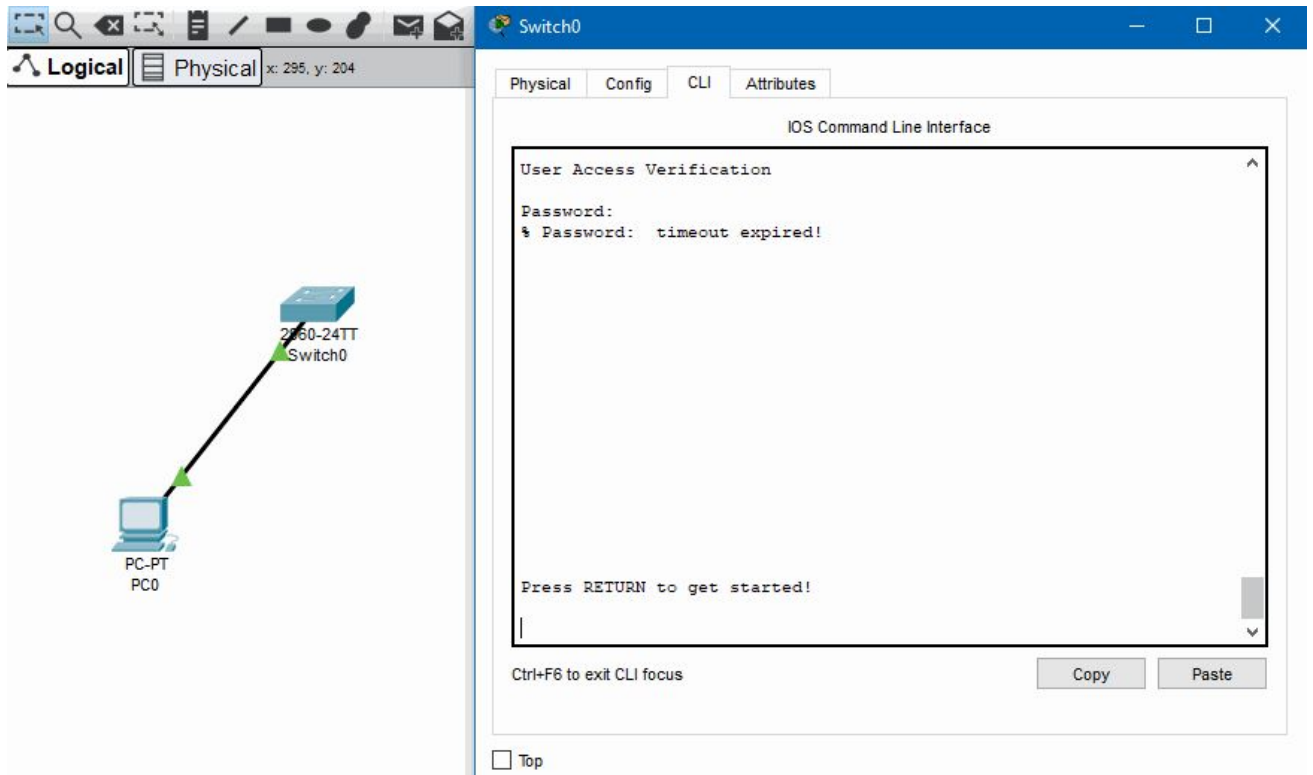


Figura 1.5.6.B. Petición de contraseña para entrar a la consola de configuración.

Plantilla para crear nuevas páginas

Para comprobar la conectividad, pinchamos en el PC, vamos a la pestaña Desktop y pinchamos en Command Prompt:

1.5.6

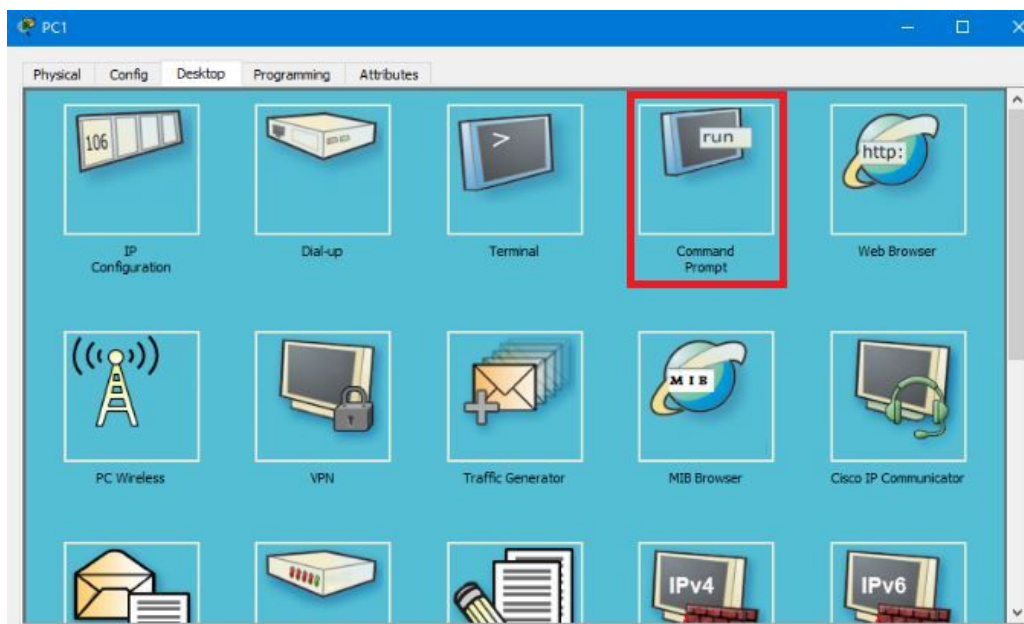


Figura 1.5.6.C. Ubicación de Command Prompt en Packet Tracer.

Hecho esto, estaremos dentro de la consola del PC y podremos comprobar si hay conexión entre ambos dispositivos:

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<lms TTL=255
Reply from 192.168.1.3: bytes=32 time<lms TTL=255
Reply from 192.168.1.3: bytes=32 time<lms TTL=255
Reply from 192.168.1.3: bytes=32 time<lms TTL=255

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 1.5.6.D. Ping satisfactorio entre PC y switch.

Como hemos podido observar se ha aplicado el ping correctamente, por lo que hay conexión. Así que realizamos la conexión por telnet desde el PC hasta el switch con el comando telnet + la IP del switch, a lo que nos pedirá el nombre de usuario y la contraseña que le hayamos puesto. Hecho esto estaremos dentro de la consola del switch en modo admin.

```
C:\>telnet 192.168.1.3
Trying 192.168.1.3 ...Open

User Access Verification




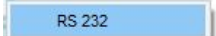
Username: moi

Password:
Switch#
```

Figura 1.5.6.E. Pantalla del acceso vía telnet.

Apartado 7: Acceder a terminal desde un PC

7. Acceso a la consola desde hyperterminal. Utilizando PT, accede a la consola de configuración de un switch usando la utilidad de escritorio de un PC

Para realizar la siguiente actividad necesitaremos en PT poner un Switch y un ordenador, luego de poner estos dos elementos, pincharemos en el apartado de conexiones  y seleccionaremos el cable de consola  conectaremos en puerto de consola del switch  con el puerto RS 232 del PC 

1.5.7

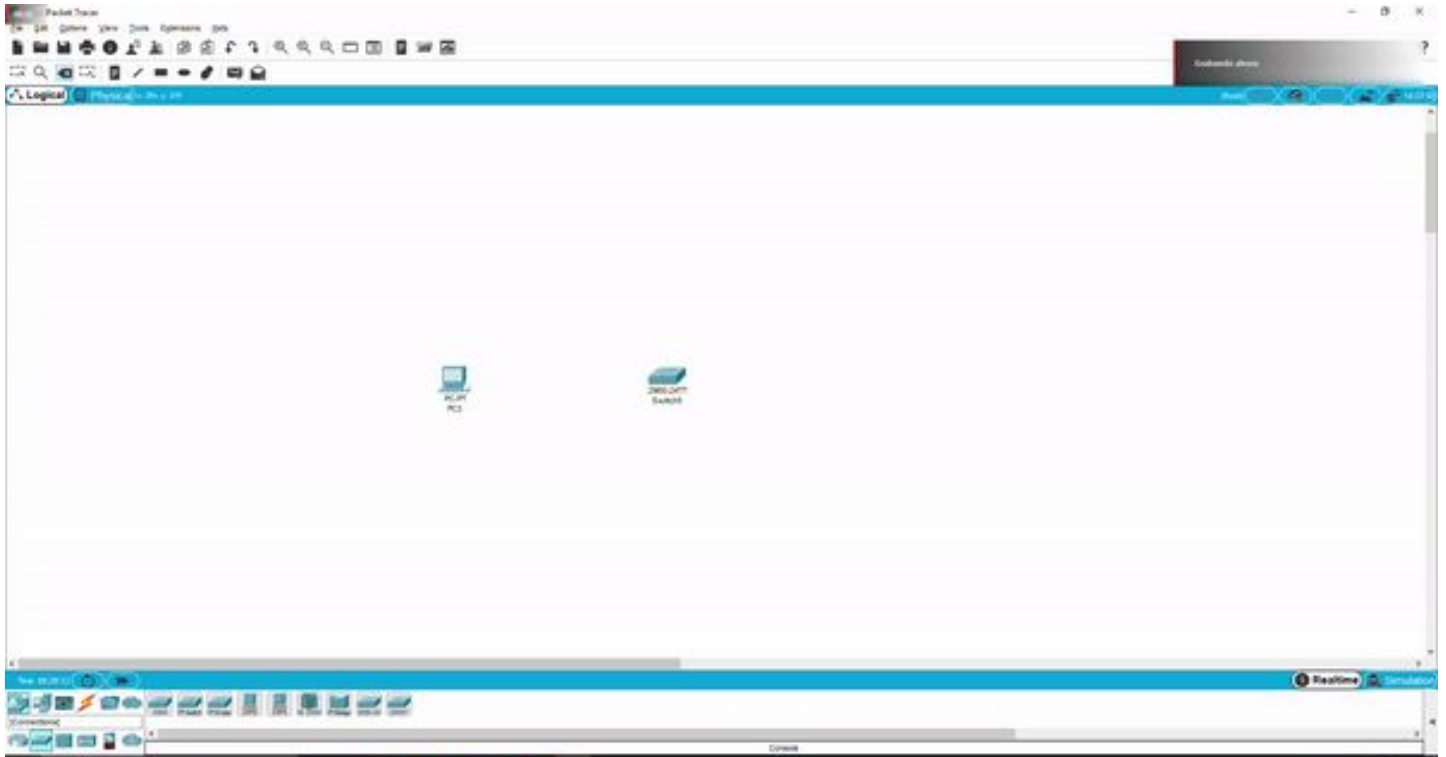


Figura 1.5.7.A. Acceso a la consola del switch desde hyperterminal.

El puerto RS 232 es también denominado el puerto serie es un puerto de comunicaciones que transmite bit por bit, enviando un bit cada vez suele estar situado en la parte trasera del PC y tiene este aspecto:



Figura 1.5.7.B. Muestra de un puerto RS 232

El cable de consola se conecta en el puerto de consola de los distintos aparatos de Cisco tanto routers, switches y otra electrónica de red y va conectado al puerto RS 232 o puerto serie de un ordenador, este cable sirve para conectar los ordenadores con los distintos aparatos de electrónica de red.



Figura 1.5.7.C. Muestra de un cable de consola de Cisco.

<APLAFLE>
<ACABGON>

Apartado 7: Acceder a terminal desde un PC

A continuación haciendo doble click al pc nos saldrá una ventana en la cual debemos seleccionar la opción que pone desktop.

1.5.7

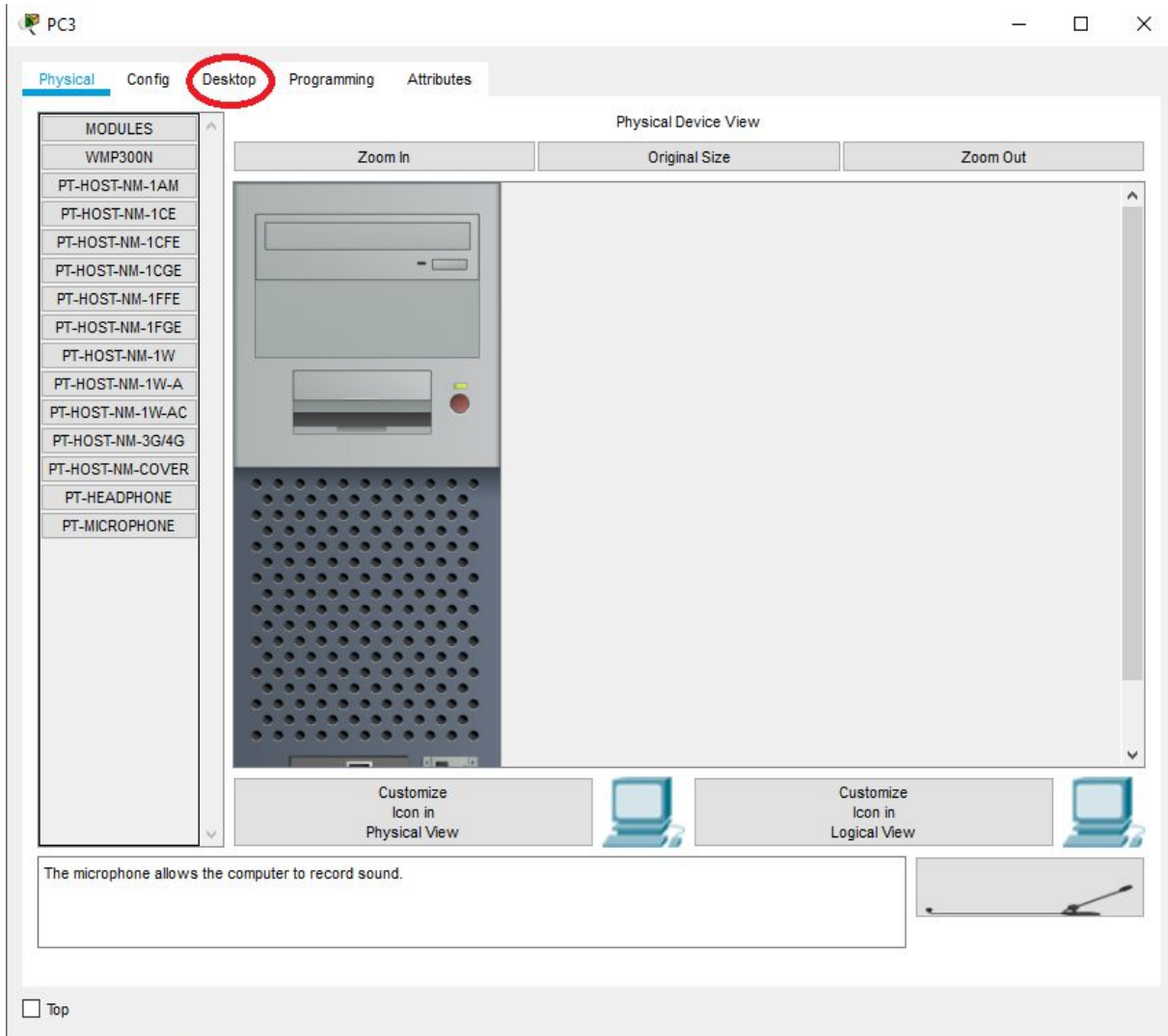


Figura 1.5.7.D. Elección de la pestaña Desktop desde un PC para acceder a terminal.

<APLAFLE>
<ACABGON>

Apartado 7: Acceder a terminal desde un PC

Al hacerlo nos encontraremos con la siguiente ventana, en ella debemos seleccionar el apartado llamado terminal.

1.5.7

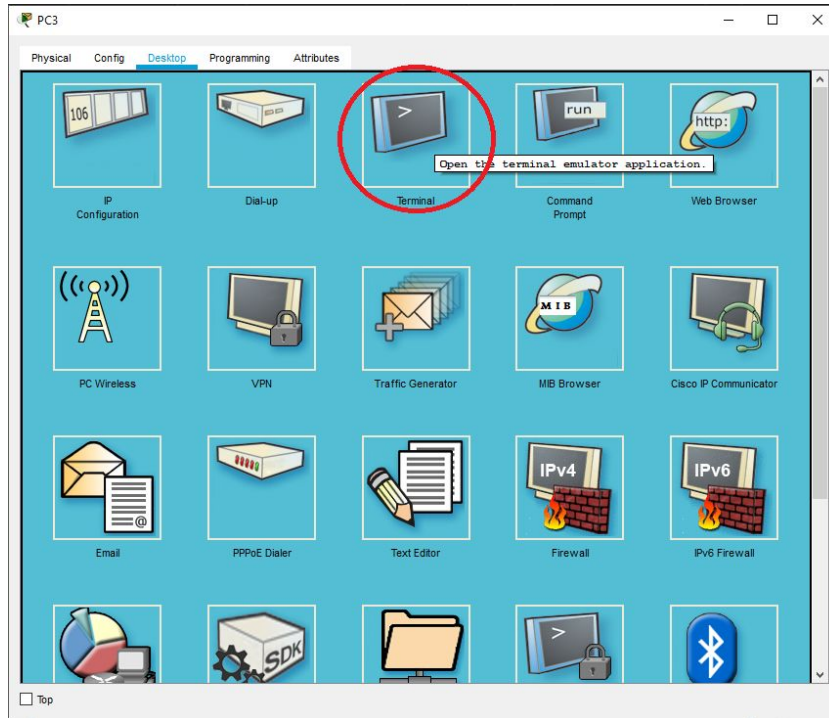


Figura 1.5.7.E. Muestra del apartado terminal.

Una vez dentro de este apartado nos encontraremos con la siguiente ventana, por el momento no necesitamos cambiar ninguno de los parámetros que está en esa ventana, nos limitaremos a hacer click en OK.

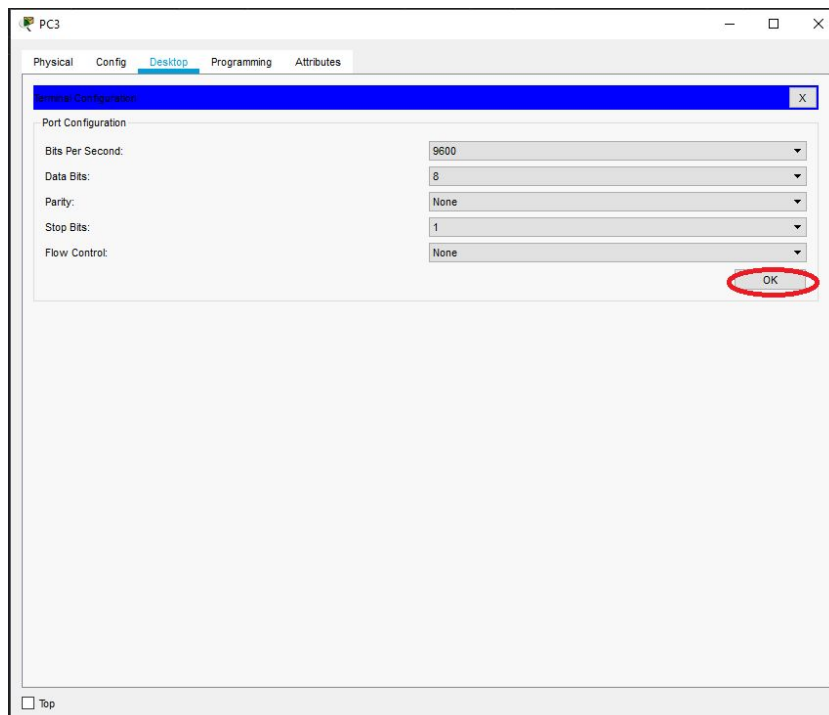


Figura 1.5.7.F. Ventana de configuración del apartado terminal.

<APLAFLE>
<ACABGON>

Apartado 7: Acceder a terminal desde un PC

Una vez hecho click en OK si todos los pasos se han seguido correctamente deberemos entrar a IOS del switch desde la consola de terminal del PC.

1.5.7

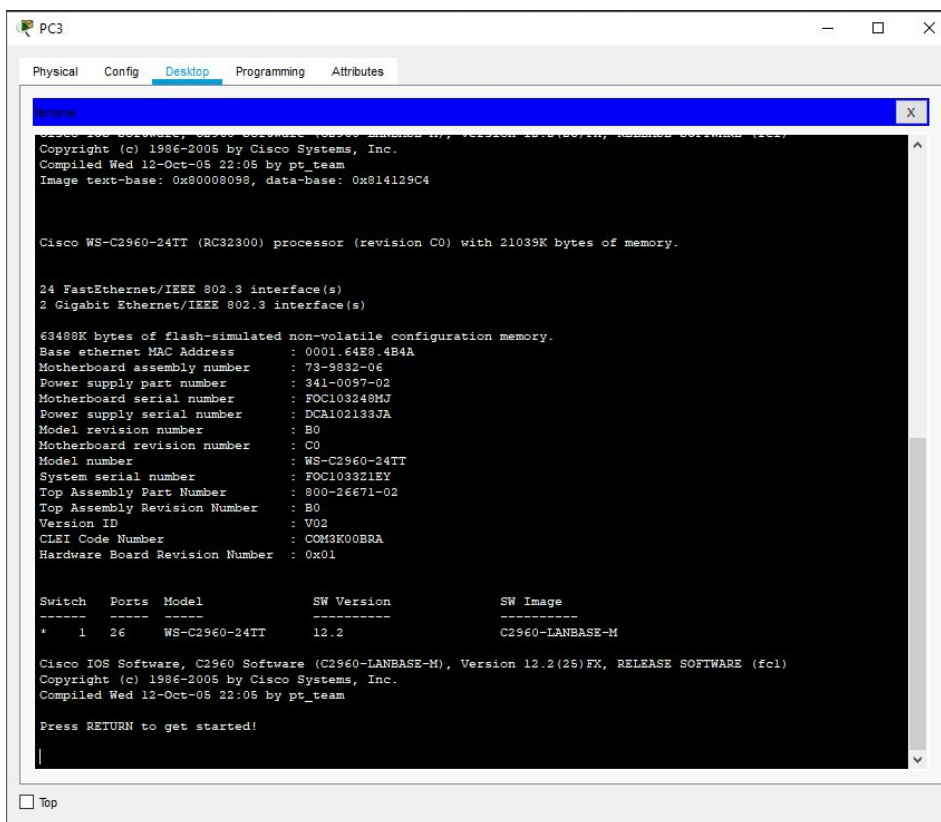


Figura 1.5.7.G. Muestra de la ventana terminal.

A continuación se mostrará un GIF en el cual estará el proceso descrito anteriormente realizado paso a paso.

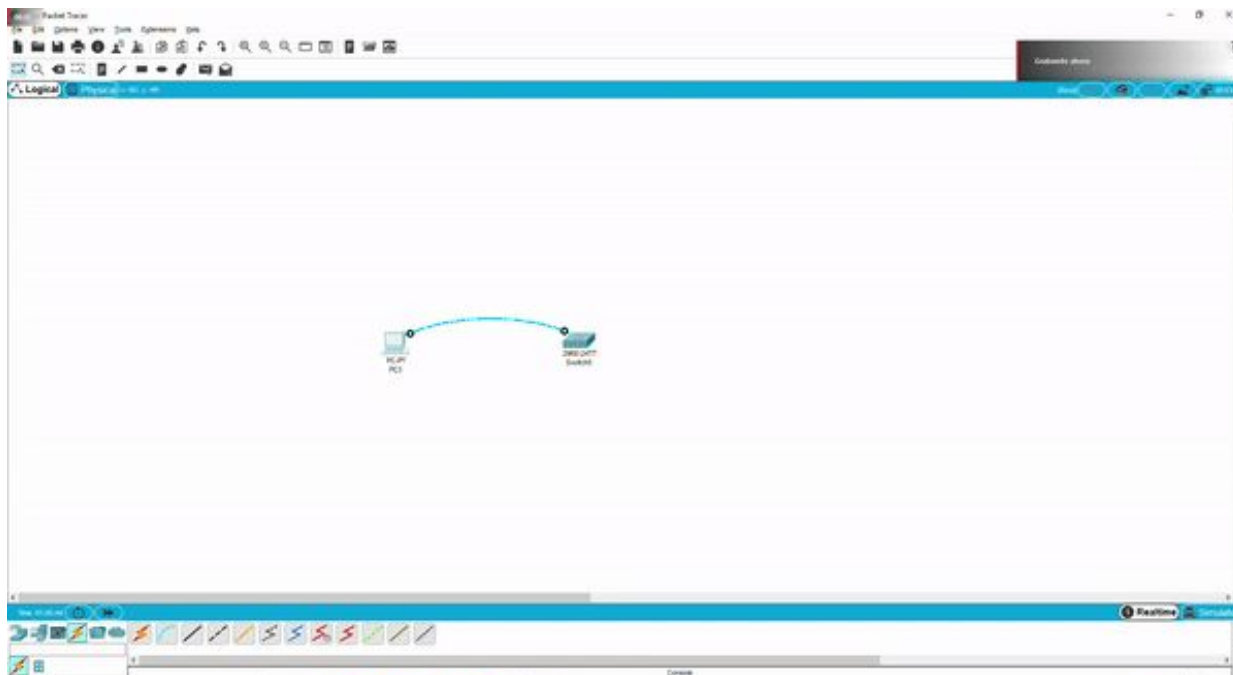


Figura 1.5.7.H. Proceso de acceso al terminal.

<APLAFLE>
<ACABGON>

Apartado 8. Conexión por cable de consola

- Cambiar la configuración de un puerto (o boca). Desde la consola de un PC, modifica la configuración del puerto F0/1 a 10Mbps y half-dúplex.

1.5.8

Lo primero será conectar un pc desde su puerto serie a la consola del switch con el cable azul el cual es el cable de consola.

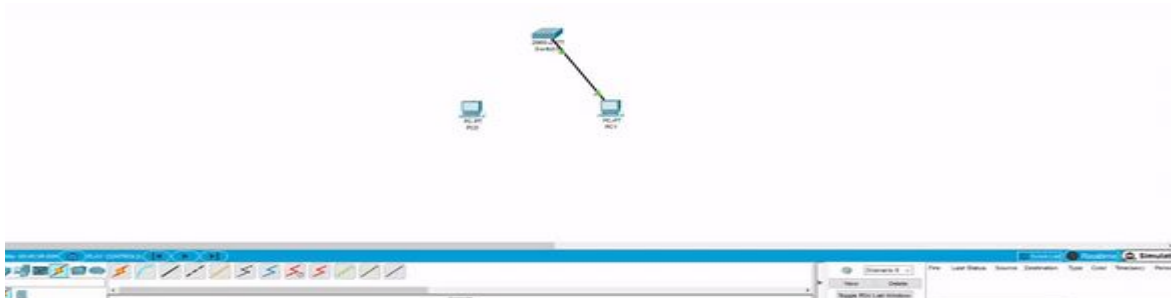


Figura 1.5.8.A. Conexión por cable de consola.

Conectamos el PC1 a la boca fa0/1.

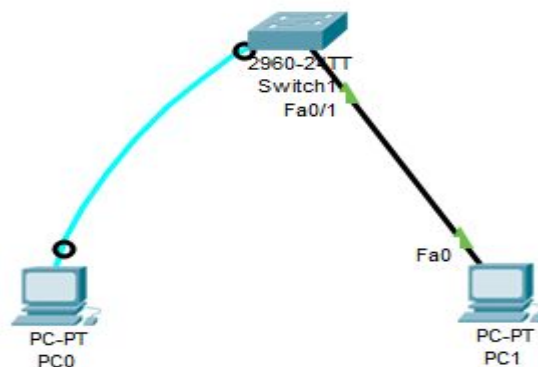


Figura 1.5.8.B. Conexión del PC1 a la boca Fa0/1 del switch.

Entramos en el terminal PC0 una vez haya cargado, configuración y terminal.

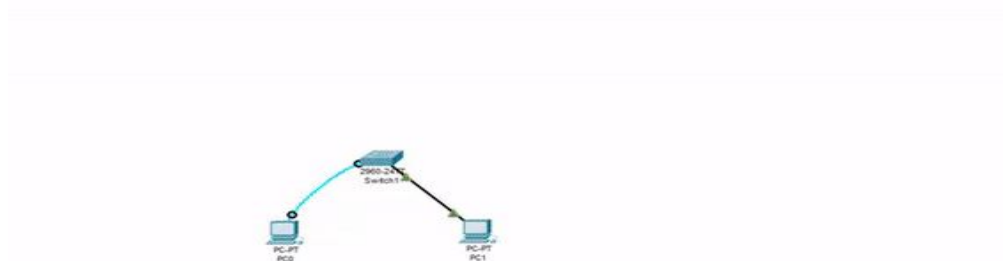


Figura 1.5.8.C. Entrada al terminal del PC0.

Apartado 8. Conexión por cable de consola

A continuación entramos en el modo configuración, luego `interface fastEthernet 0/1`

Modo configuración de esa boca

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#
```

1.5.8

Para ver los posibles comandos ponemos `?`

```
Switch(config-if)#?
cdp          Global CDP configuration subcommands
channel-group Etherchannel/port bundling configuration
channel-protocol Select the channel protocol (LACP, PAgP)
description  Interface specific description
duplex       Configure duplex operation.
exit         Exit from interface configuration mode
ip           Interface Internet Protocol config commands
lldp        LLDP interface subcommands
mdi         Set Media Dependent Interface with Crossover
mls         mls interface commands
no          Negate a command or set its defaults
shutdown    Shutdown the selected interface
spanning-tree Spanning Tree Subsystem
speed       Configure speed operation.
storm-control storm configuration
switchport  Set switching mode characteristics
tx-ring-limit Configure PA level transmit ring limit
Switch(config-if)#
```

Figura 1.5.8.D. Muestra de posibles comandos del modo `config-if` a través de `?`

Queremos dar una velocidad de 10 Mbps y half duplex por lo que escribimos el comando `duplex half`.

```
Switch(config-if)#duplex half
```

Y cambiamos la velocidad con: `speed 10`

```
Switch(config-if)#speed 10
```

Comprobamos en el switch si el cambio surtió efecto, para ello entramos en modo desarrollador y escribimos el comando `show running-config`

```
Switch#show running-config
Building configuration...

Current configuration : 1101 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 duplex half
 speed 10
!
```

Figura 1.5.8.E. Comprobación del estado del switch.

Apartado 8. Video Explicativo

<https://www.youtube.com/watch?v=tsiFCamgluE&feature=youtu.be>

QR del vídeo:

1.5.8



Apartado 9

9. Habilitar conexión de administrador vía telnet.

Telnet es un protocolo que sirve para emular una terminal remota, lo que significa que se puede utilizar para ejecutar comandos introducidos con un teclado en un equipo remoto.

1.5.9

Para habilitar la conexión vía Telnet tenemos que introducir una serie de comandos.

Los comandos son estos:

Primero deberemos acceder como modo administrador poniendo el comando **enable**.

Configuramos las sesiones telnet:

```
configure terminal
line vty 0 15
no login
login local
username moi password moi
username moi privilege 15
```

Establecemos IP para el switch

```
configure terminal
interface vlan 1
ip address 192.168.1.3 255.255.255.0
no shutdown
```

VÍDEO EXPLICATIVO:

<https://www.youtube.com/watch?v=S5NOnJ3rpsY&feature=youtu.be>


QR del vídeo:



10. Accede al switch vía telnet.

Prueba que efectivamente ha funcionado tu configuración telnet del switch.

Vamos a acceder desde un PC a la configuración del switch via Telnet.

Primero abrimos el packet tracer, pinchamos en Networks Devices y seleccionamos un switch 2960. Luego seleccionamos un PC genérico y lo conectamos al switch pinchando en 

1.5.10

Nos quedaría de esta forma:

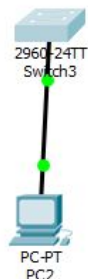


Figura 1.5.10.A. Conexión de un PC + switch en Packet Tracer.

Le asignamos una IP al PC:

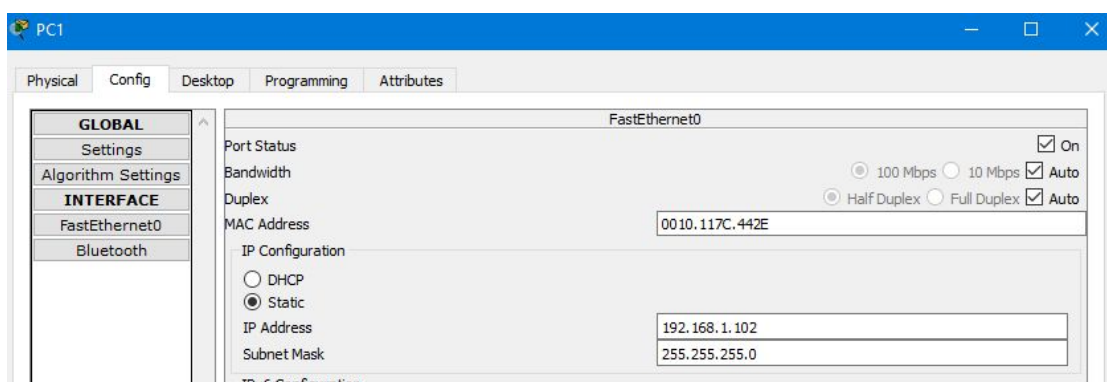
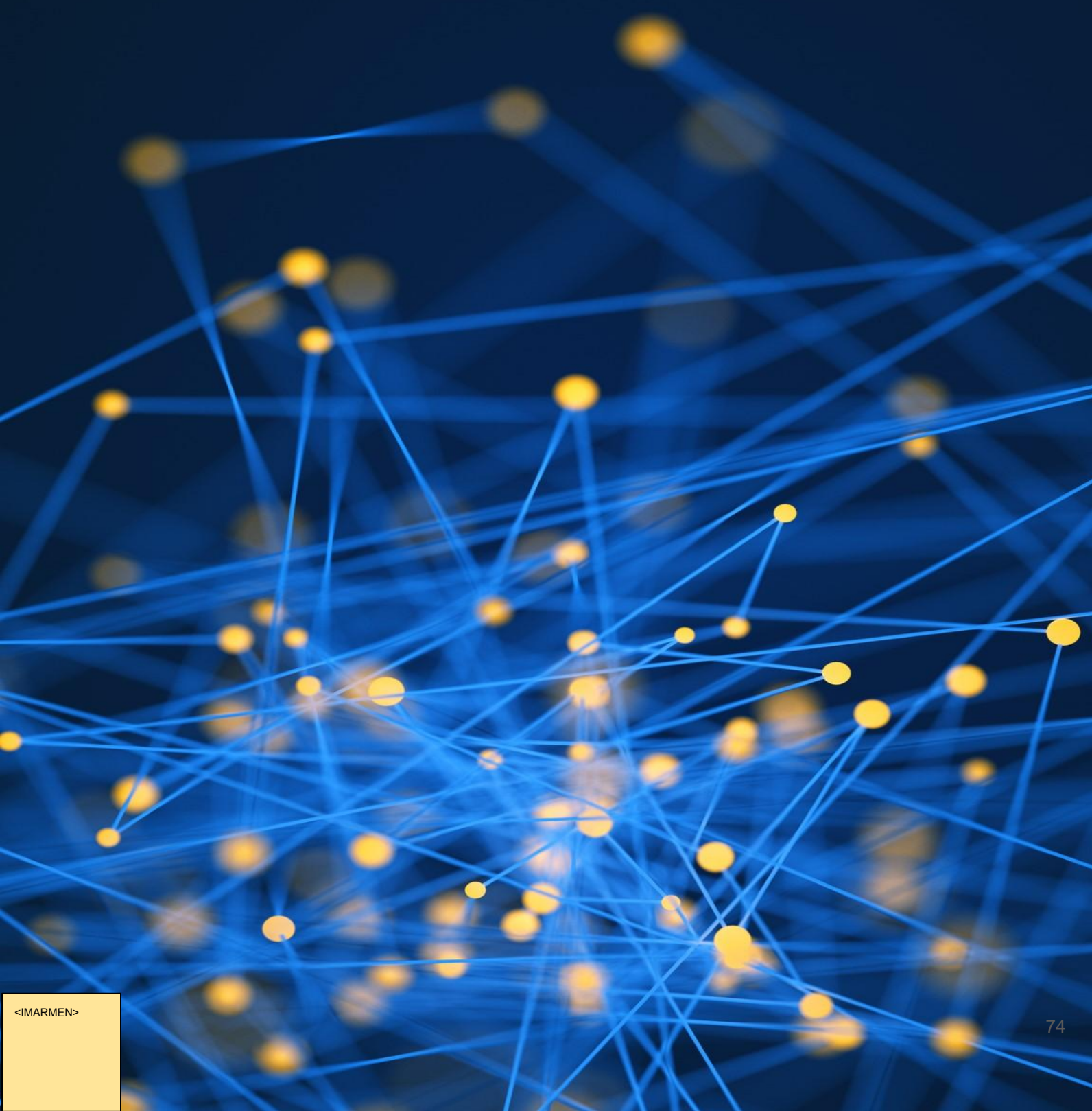


Figura 1.5.10.B. Asignación de IP a un PC.

Una vez habilitada la conexión vía telnet y se le haya establecido otra IP al switch (este procedimiento se explicó en el apartado 9), comprobaremos la conectividad con el comando ping desde el PC hasta el switch.

Trabajo 1.6

Seguridad básica VLAN y trunking



Tema 1.6. Seguridad básica. VLAN y trunking

1. Asegurando el acceso al modo administrador

En clase hemos visto múltiples formas de proteger la seguridad de nuestros equipos de red.

En este apartado, explica de forma clara y precisa e incluye evidencias de su correcto funcionamiento sobre la creación de credenciales de acceso al modo administrador tanto cifrada como sin cifrar.

Recuerda: enable password y enable secret

Explica también cómo desactivar/eliminar esa clave.

2. Modifica la configuración del switch para que incluya un banner de tipo MOTD

3. Configuración de los puertos del switch

Modifica la boca 1 e incluye una descripción

Modifica el rango de bocas 11 ~ 20 e incluye una descripción

4. Bloquear un puerto del switch

Explica de forma clara e incluye evidencias de su correcto funcionamiento sobre cómo bloquear a nivel lógico (desactivar) un puerto del switch.

5. Creación básica de VLANs

- Crea una red con un switch y 6 PCs
- Configura dos VLAN en el switch
- Establece que los puertos 1 – 10 pertenecen a la VLAN 1 y los puertos 11 – 20 a la vlan2 y 21-24 a la Vlan3
- Ponle un nombre simbólico a cada VLAN
- Muestra la configuración vlan del switch para comprobar que se han creado bien las vlan
- Comprueba que efectivamente hay comunicación interna entre los equipos la VLAN1 y de la VLAN2
- Comprueba que un equipo de la VLAN1 NO tiene comunicación con otro de la VLAN2

6. VLAN multiswitch con enlaces dedicados

- Ampliar el diseño anterior de tal manera que nuestra red tenga 2 switches
- Crea un enlace por cada vlan que una los dos switches
- Comprueba que hay conectividad entre dos Pcs de una misma vlan de switches diferentes

Tema 1.6. Seguridad básica. VLAN y trunking

1.6

7. VLAN multiswitch con enlace compartido (trunking)

Diseño de la red

- Sobre el ejemplo anterior,
 - eliminar los dos enlaces
 - poner uno solo, el que voy a usar como trunk
 - IMPORTANTE: De puerto Gigabit a puerto Gigabit

8. VLAN multiswitch con enlace compartido (trunking)

Mostrar el estado inicial del puerto G1/1

- Directamente, tras añadir el enlace que hará de trunk de switch a switch usa el comando:
 - `show interface gigabitethernet 1/1 switchport`
- Administrative mode: dynamic auto
- ¿Qué quiere decir?
- Dynamic auto es el valor por defecto → el otro switch estará igual → ninguno de los dos inicia la negociación
- Operational mode: static access
- ¿Qué quiere decir?
- Acceso estático, sin trunking
- Administrative Trunking encapsulation: dot1q
- ¿Qué quiere decir?
- Este switch sólo soporta 802.1Q para trunking

9. VLAN multiswitch con enlace compartido (trunking)

Comprobar que inicialmente no hay ningún puerto para trunking

- Show interfaces trunk
- Muestra los puertos configurados para trunking
- NO sale nada porque ahora mismo NO tenemos ninguno configurado para tal

10. VLAN multiswitch con enlace compartido (trunking)

NO existe conectividad

Probar a hacer un ping entre dos máquinas conectadas a diferente switch

Tema 1.6. Seguridad básica. VLAN y trunking

1.6

11. VLAN multiswitch con enlace compartido (trunking)

Habilitar el trunking

- ¿Cómo lo podemos hacer?
- En uno de los dos switch → habilitamos dynamic desirable → ese switch inicia las negociaciones para trunking
- Cambiamos la configuración → se desactiva el puerto → se vuelve a activar → tarda un tiempo en estar operativo → está negociando

12. VLAN multiswitch con enlace compartido (trunking)

Mostrar el estado del puerto tras habilitar el trunking

- Show interface gigabitethernet 1/1 switchport

13. VLAN multiswitch con enlace compartido (trunking)

Mostrar los puertos de trunking que existen

- Show interfaces trunk
- Ahora sí que vemos que G1/1 está habilitado para trunking

NOTA: prune = podar

14. VLAN multiswitch con enlace compartido (trunking)

Existe conectividad

- Probar a hacer un ping entre dos máquinas conectadas a diferente switch y ver que efectivamente hay conectividad
- Lógicamente entre diferentes VLAN sigue sin haber conectividad

Apartado 1

1.6.1

1. Asegurando el acceso al modo administrador

En clase hemos visto múltiples formas de proteger la seguridad de nuestros equipos de red.

En este apartado, explica de forma clara y precisa e incluye evidencias de su correcto funcionamiento sobre la creación de credenciales de acceso al modo administrador tanto cifrada como sin cifrar.

Recuerda: enable password y enable secret

Explica también cómo desactivar/eliminar esa clave.

- **Para crear una contraseña para la CLI debemos:**

- a) Entrar en modo administrador y a la configuración del switch.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

- b) Buscamos en los posibles comandos dentro de la configuración y encontramos **enable**.

```
Switch(config)#?
Configure commands:
  access-list      Add an access list entry
  banner           Define a login banner
  boot             Boot Commands
  cdp              Global CDP configuration subcommands
  clock            Configure time-of-day clock
  crypto           Encryption module
  default          Set a command to its defaults
  do               To run exec commands in config mode
  enable           Modify enable password parameters
  end              Exit from configure mode
  exit            Exit from configure mode
```

- c) Dentro de este comando nos dan dos opciones: **password o secret**.

En la primera opción la clave no será cifrada (password) y en la segunda sí (secret).

```
Switch(config)#enable ?
  password  Assign the privileged level password
  secret    Assign the privileged level secret
```

- **Primera opción "password" sin cifrar**

- a) Introducimos el comando **enable password** y a continuación la contraseña deseada. Y volvemos al inicio con **end** y salimos del modo administrador **disable**.

```
Switch(config)#enable password JJ
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#disable
```


Apartado 1

- b) Comprobamos que al entrar al modo administrador nos pide la contraseña.

```
Switch#disable
Switch>enable
Password:
Switch#
```

1.6.1

- c) Ahora quitamos la contraseña utilizando el mismo comando que usamos para crearla con un **no** antes y volvemos a comprobar:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no enable password
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#disable
Switch>enable
Switch#
```

- d) Este sería el resultado total:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable password JJ
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#disable
Switch>enable
Password:
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no enable password
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#disable
Switch>enable
Switch#
```

```
enable
configure terminal
enable password JJ
end

no enable password
end
```

Apartado 1

- Segunda opción “secret” con cifrado

1.6.1

- a) Introducimos el comando `enable secret` y a continuación la contraseña deseada. Volvemos al inicio con `end` y salimos del modo administrador `disable`.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable secret JJ
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#disable
```

- b) Comprobamos que al entrar al modo administrador nos pide la contraseña.

```
Switch>enable
Password:
Switch#
```

- c) Ahora quitamos la contraseña utilizando el mismo comando que usamos para crearla con un `no` antes y volvemos a comprobar.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no enable secret
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#disable
Switch>enable
Switch#
```

- d) Este sería el resultado total:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable secret JJ
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#disable
Switch>enable
Password:
Switch#
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no enable secret
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#disable
Switch>enable
Switch#
```

```
enable
configure terminal
enable secret JJ
end

no enable secret
end
```

Apartado 2. Escribir mensaje

2. Modifica la configuración del switch para que incluya un banner de tipo MOTD.

Este comando sirve para que al iniciar el switch se muestre el mensaje que quieras escribir. (MOTD son las siglas de “Message of the day”)

1.6.2

Al iniciar el switch como hacemos siempre, vemos que no aparece ningún mensaje.

```
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0090.21E7.6A32
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number       : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC103321EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01

Switch  Ports  Model                SW Version          SW Image
-----  ----  -----
* 1      26      WS-C2960-24TT      12.2                C2960-LANBASE-M

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fcl)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!

Switch>
```

Figura 1.6.2.A. Muestra de la ausencia de un MOTD.

Entramos en el modo desarrollador y posteriormente en el modo configuración. Dentro del modo configuración, escribimos el siguiente comando:

```
banner motd
```

El último carácter quiere decir que finalizará el texto una vez se escriba ese carácter. (Puede ser cualquier carácter, nosotros usamos “@” simplemente como ejemplo.)

En siguiente lugar escribiremos el mensaje que queremos que aparezca al iniciar el switch, escribimos el carácter para terminar y pulsamos la tecla “Enter”. Quedando en pantalla algo tal que así:

```
Enter TEXT message. End with the character '@'.
FELICIDADES                               :)
@
Switch(config)#
```

Apartado 2. Mostrar mensaje

Ahora tenemos que salir del modo configuración y reiniciar el switch. Una vez hecho esto, al pulsar la tecla "Enter" y poder comenzar a escribir, nos mostrará justo encima el mensaje que hemos escrito anteriormente.

1.6.2

```
Press RETURN to get started!
```

```
FELICIDADES :)
```

```
Switch>|
```

Figura 1.6.2.B. Muestra del MOTD al iniciar el switch.

Aquí se encuentra un vídeo explicativo:

https://www.youtube.com/watch?v=x_KaK9ltn-g&feature=youtu.be

QR del vídeo:



Apartado 3. Configuración de los puertos del switch

3. Configuración de los puertos del switch

-Modifica la boca 1 e incluye una descripción

Las descripciones nos ayudan y nos permiten trabajar con más velocidad y eficiencia debido a que al tener una explicación detallada de para qué sirven o para qué se están usando las bocas del switch.

1.6.3

Primero debemos entrar como **modo administrador**, luego **configure terminal** y dentro de la configuración de la terminal debemos situarnos en la boca que vamos a poner la descripción y luego usar el comando **description**.

```
enable
configure terminal
interface fastEthernet 0/1
description " Internet para
clase"
```

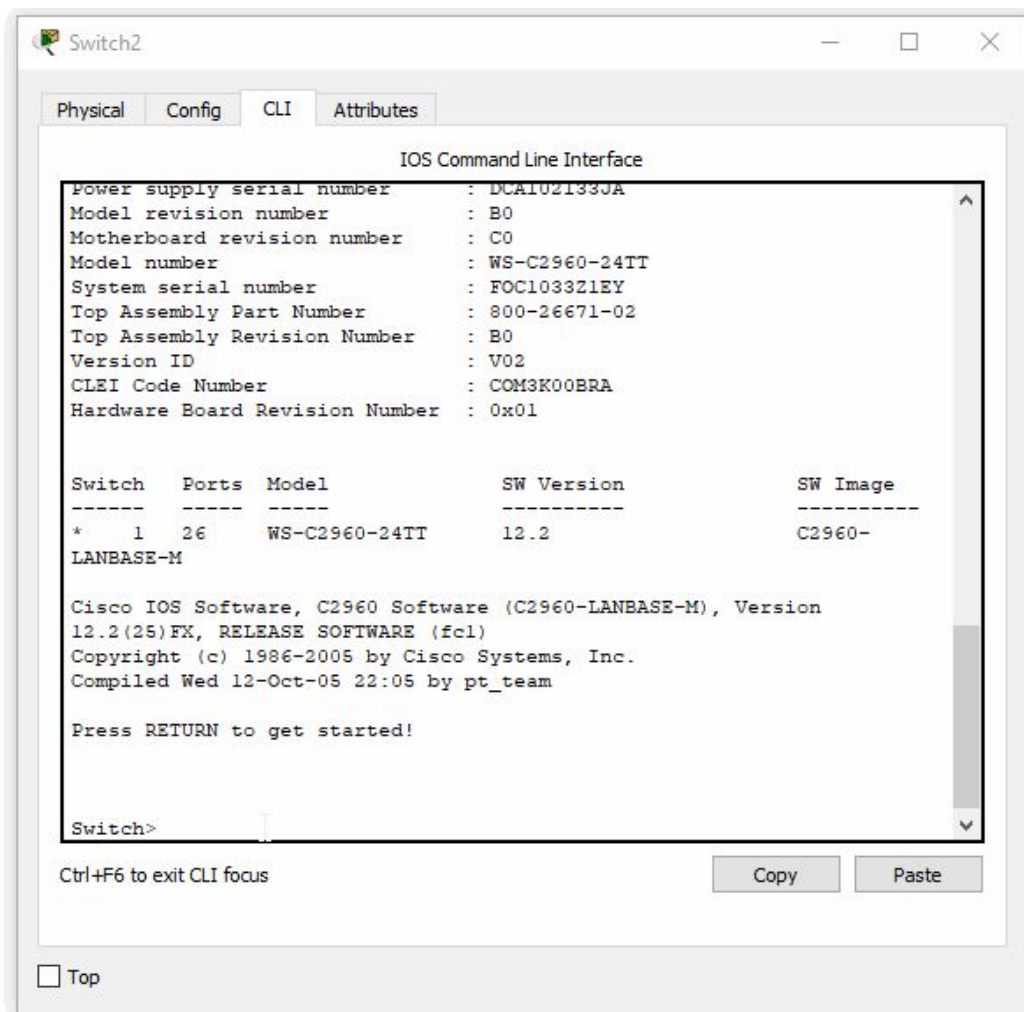


Figura 1.6.3.A. Muestra del proceso de creación de una descripción.

Apartado 3. Configuración de los puertos del switch

3. Configuración de los puertos del switch

-Modifica la boca 1 para incluir una descripción

-Después de ejecutar este comando :

```
Switch(config-if)#description " Internet para Clase "
```

-Podemos observar los cambios en la boca fastethernet 0 / 1 usando el comando:

```
Switch#show running-config
!
interface FastEthernet0/1
  description " Internet para Clase "
!
```

Para modificar la velocidad y su comunicación necesitamos realizar los pasos anteriores hasta situarnos en la boca del switch que queremos modificar, en este caso la fastEthernet 0 / 1

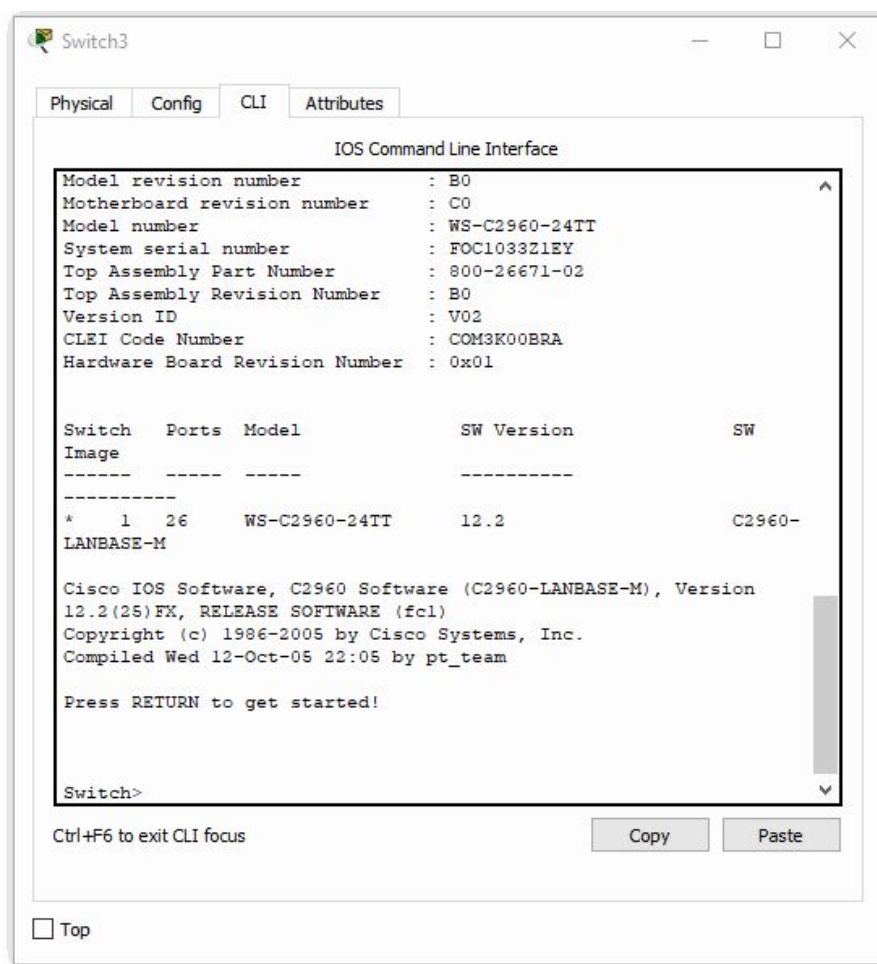


Figura 1.6.3.B. Muestra de modificación de los parámetros de un puerto.

```
speed 10
duplex full
exit
```

1.6.3

Apartado 3. Configuración de los puertos del switch

1.6.3

-Para observar los cambios realizados a la boca y comprobar que se han hecho correctamente , volvemos a realizar el comando `show running-config`

```
Switch#show running-config
```

-Podemos ver como en la boca FastEthernet 0/1 se nos muestran los cambios realizados.

```
interface FastEthernet0/1
description " Internet para Clase "
duplex full
speed 10
```

Si hablamos del tipo de comunicación que se puede establecer sabemos que se divide en tres:

Simplex: La transmisión simplex o unidireccional es aquella que ocurre en una dirección solamente, deshabilitando al receptor de responder al transmisor.

Duplex: La transmisión half-duplex permite transmitir en ambas direcciones; sin embargo, la transmisión puede ocurrir solamente en una dirección a la vez. Tanto transmisor y receptor comparten una sola frecuencia.

Full-Duplex: La transmisión full-duplex (fdx) permite transmitir en ambas dirección, pero simultáneamente por el mismo canal. Existen dos frecuencias una para transmitir y otra para recibir.

Apartado 3. Configuración de los puertos del switch

-Modifica el rango de bocas 11 ~ 20 e incluye una descripción

Para realizar modificaciones a más de una boca simultáneamente debemos seguir estos pasos :

1.6.3

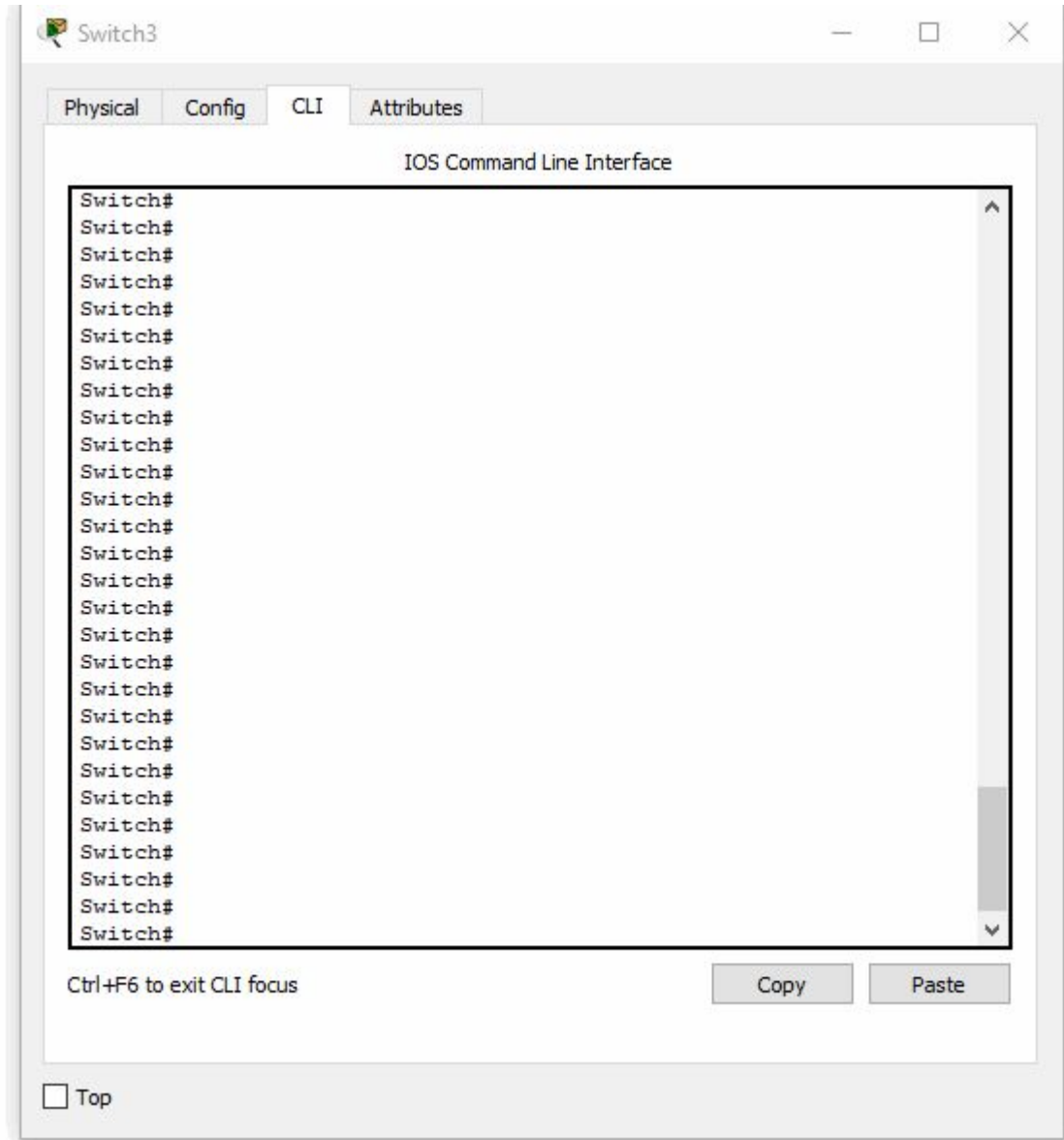


Figura 1.6.3.C. Selección de un rango de bocas.

Una vez entramos como administrador (**enable**), luego **configure terminal** y por último introducimos el comando **interface range FastEthernet 0/11 - 20**, el cual nos hace modificar las bocas desde la 11 hasta la 20.

Luego podemos observar con el comando **show running-config** como se muestran los cambios, en este caso hemos

Apartado 3. Configuración de los puertos del switch

-Modifica el rango de bocas 11 ~ 20 e incluye una descripción

Una vez entramos como administrador (**enable**), luego **configure terminal** y por último introducimos el comando **interface range FastEthernet 0/11 - 20**, el cual nos hace modificar las bocas desde la 11 hasta la 20.

Luego podemos observar con el comando **show running-config** como se muestran los cambios, en este caso hemos modificado la velocidad a 100 Mbps y la comunicación a half duplex.

```
interface FastEthernet0/11
  duplex half
  speed 100
!
interface FastEthernet0/12
  duplex half
  speed 100
!
interface FastEthernet0/13
  duplex half
  speed 100
!
interface FastEthernet0/14
  duplex half
  speed 100
!
interface FastEthernet0/15
  duplex half
  speed 100
!
interface FastEthernet0/16
  duplex half
  speed 100
!
interface FastEthernet0/17
  duplex half
  speed 100
!
interface FastEthernet0/18
  duplex half
  speed 100
!
interface FastEthernet0/19
  duplex half
  speed 100
!
interface FastEthernet0/20
  duplex half
  speed 100
```

Figura 1.6.3.D. Muestra de los parámetros actuales de los puertos.

Apartado 3. Configuración de los puertos del switch

-Para poner un fondo de pantalla en Cisco Packet Tracer:

Situado en la parte superior o en la parte superior derecha en los nuevos modelos de Cisco Packet Tracer debemos buscar



1.6.3

-Luego podemos buscar la imagen pulsando el botón Browse y una vez seleccionada la imagen podemos elegir dos opciones :

Use Original Image: La cual usa la imagen con su tamaño.

Display Tiled Background Image: En esta la imagen si el tamaño es menor al del fondo se repite hasta completar las partes vacías.

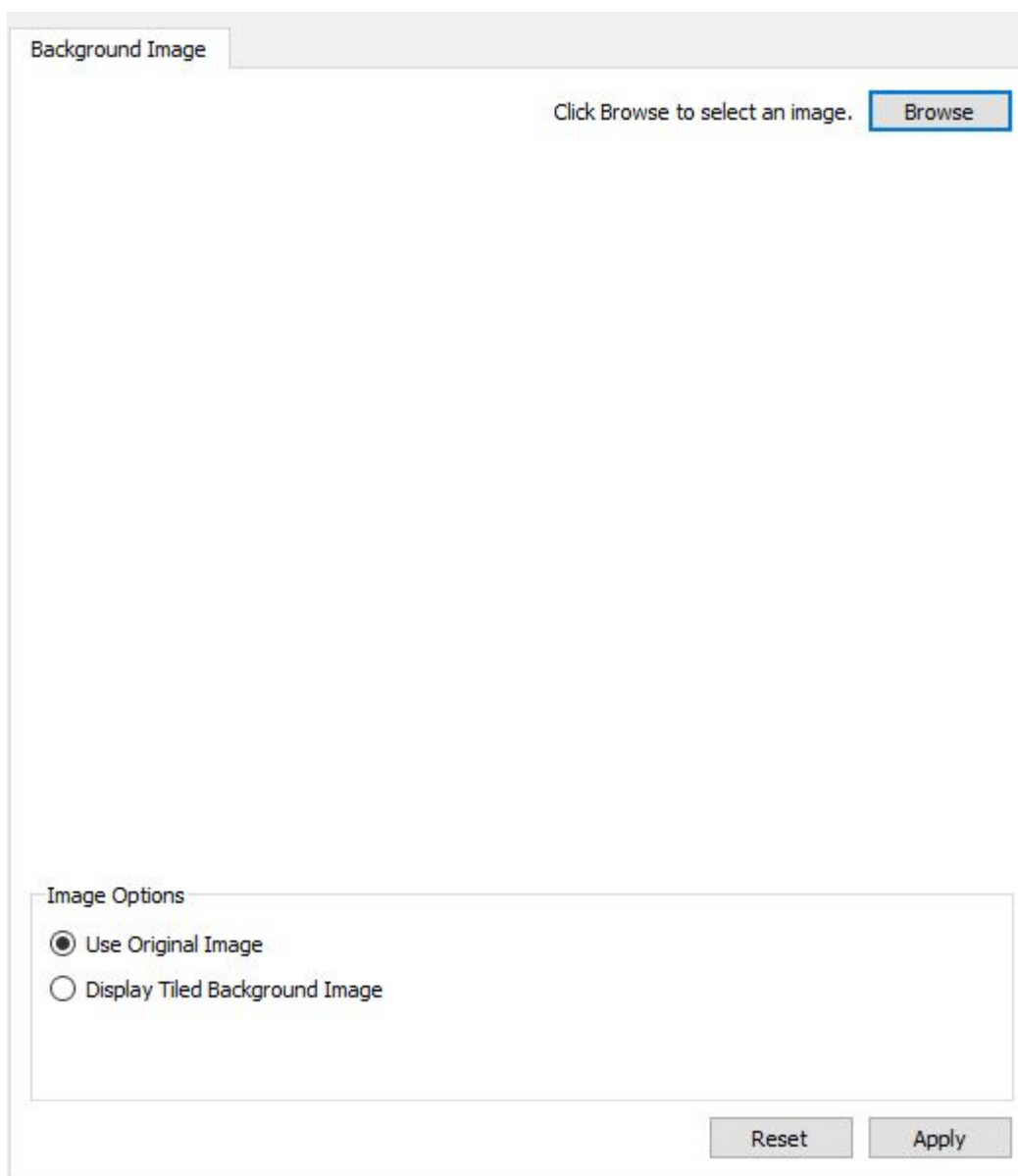


Figura 1.6.3.E. Pantalla de selección de imagen como fondo de pantalla.

Apartado 4. Bloquear puertos

4. Bloquear un puerto del switch

Explica de forma clara e incluye evidencias de su correcto funcionamiento sobre cómo bloquear a nivel lógico (desactivar) un puerto del switch.

1.6.4

Para realizar este apartado vamos a crear una red de 3 PCs conectados a 1 switch como se muestra en la imagen:

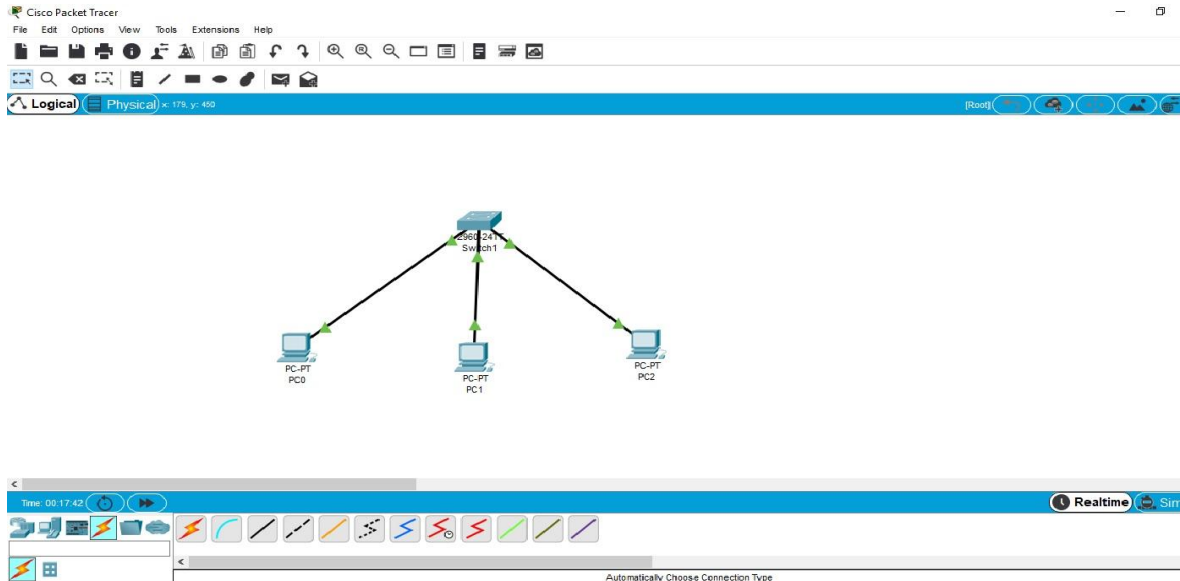


Figura 1.6.4.A. Red de tres PCs conectados a un switch.

A continuación, le asignamos una IP a cada uno de los 3 PCs desde la configuración de FastEthernet las cuales serán:

- PC-0: 192.168.1.1
- PC-1: 192.168.1.2
- PC-2: 192.168.1.3

La máscara siempre será en los tres PCs 255.255.255.0

La conexión entre los 3 PCs es correcta.

Para saber qué boca del switch vamos a desactivar conectaremos los 3 PCs a las bocas FastEthernet0/1, FastEthernet0/2 y FastEthernet0/3, respectivamente como se muestra en la siguiente foto:

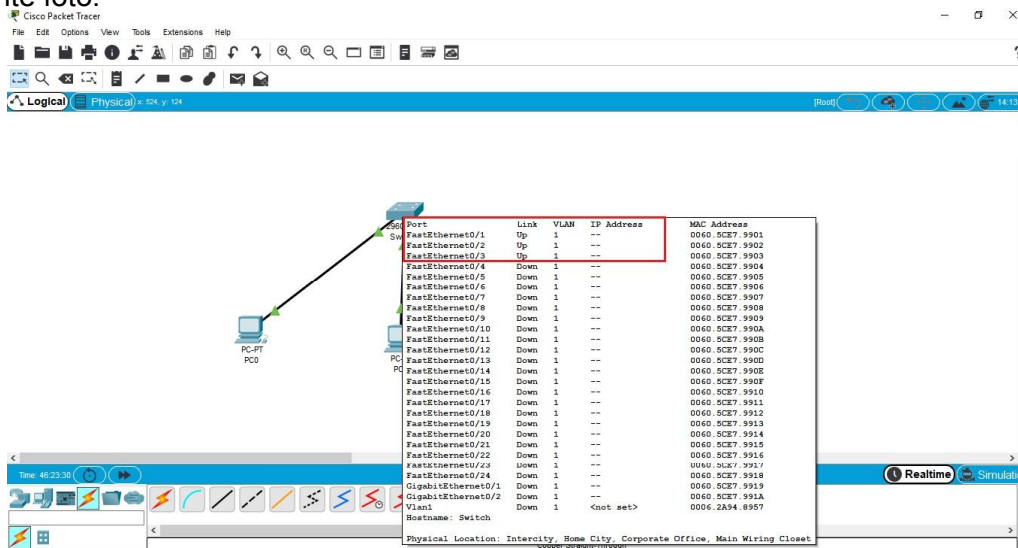


Figura 1.6.4.B. Muestra de conexionado de los PCs a los puertos del switch.

Apartado 4. Bloquear puertos

Ahora vamos a proceder a desactivar, por ejemplo, la boca 3 del switch. Para ello haciendo click con el botón izquierdo del ratón sobre el switch y accedemos a la pestaña CLI. Allí vamos a aprender a usar el comando `'shutdown'`, como se observa en la imagen. Los comandos que utilizaremos en este caso serán los siguientes:

1.6.4

```
enable - configure terminal - interface fastEthernet 0/3 - shutdown - exit
```

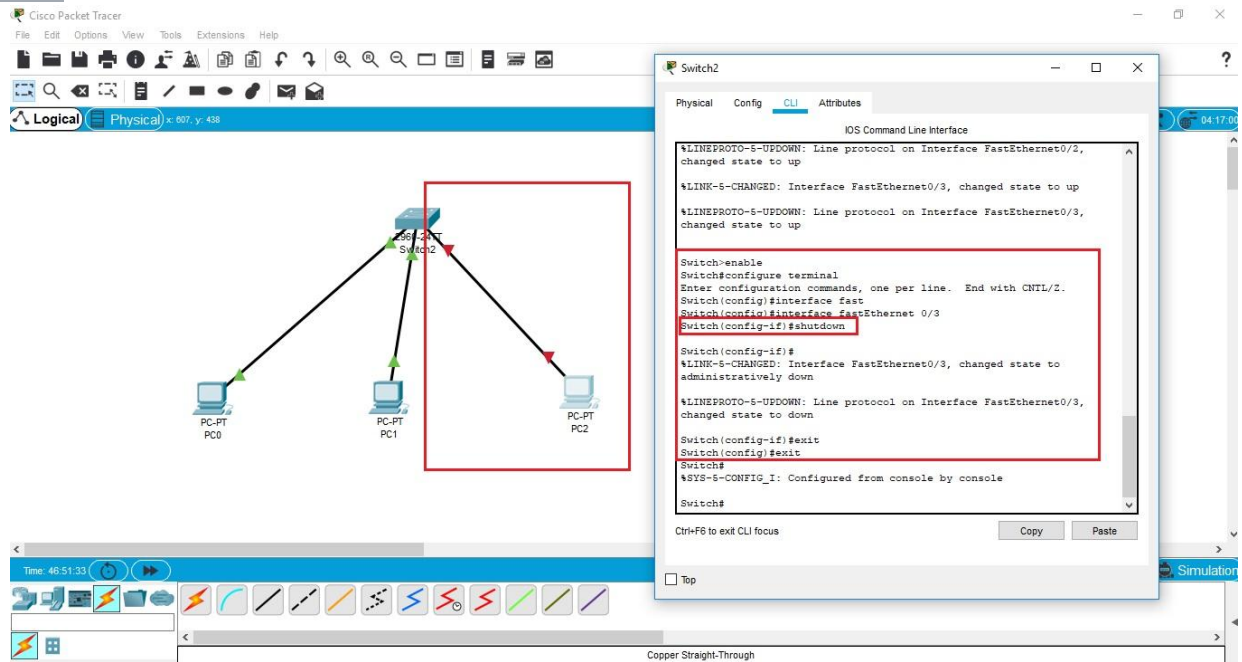


Figura 1.6.4.C. Bloqueo de un puerto del switch.

En esta imagen se puede observar como se ha hecho uso del comando `'shutdown'` para deshabilitar en este caso la boca fastEthernet 0/3 desde CLI del switch, y a la izquierda de la imagen se observa como esta boca se encuentra deshabilitada de forma gráfica debido a que sale un indicador en forma de triángulo de color rojo.

Apartado 5

5. Creación básica de VLANs

1.6.5

- Crea una red con un switch y 6 PCs
- Configura dos VLAN en el switch
- Establece que los puertos 1 – 10 pertenecen a la VLAN 1 y los puertos 11 – 20 a la vlan2 y 21-24 a la Vlan3
- Ponle un nombre simbólico a cada VLAN
- Muestra la configuración vlan del switch para comprobar que se han creado bien las vlan
- Comprueba que efectivamente hay comunicación interna entre los equipos la VLAN1 y de la VLAN2
- Comprueba que un equipo de la VLAN1 NO tiene comunicación con otro de la VLAN2

a) **Montamos la red y configuramos las IP para los PC.**

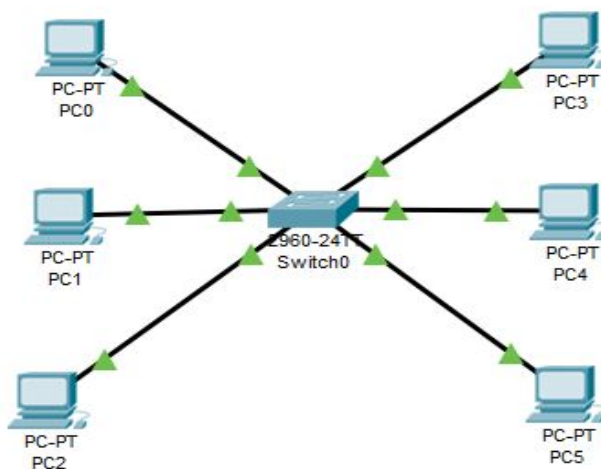


Figura 1.6.5.A. Montaje de la red de seis PC y un switch.

b) y d) **Configuramos las Vlan y les asignamos un nombre.**

- Para configurar las VLAN debemos entrar a la configuración del switch.

```
Switch>enable  
Switch#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#
```
- Miramos en los comandos dentro de config y vemos uno llamado "**vlan**". Ponemos este comando y miramos las opciones que ofrece.

Apartado 5

- Continuación

```
Switch(config)#?
Configure commands:
  access-list      Add an access list entry
  banner           Define a login banner
  boot             Boot Commands
  cdp              Global CDP configuration subcommands
  clock            Configure time-of-day clock
  crypto           Encryption module
  default          Set a command to its defaults
  do               To run exec commands in config mode
  enable           Modify enable password parameters
  end              Exit from configure mode
  exit             Exit from configure mode
  hostname         Set system's network name
  interface        Select an interface to configure
  ip               Global IP configuration subcommands
  line             Configure a terminal line
  lldp             Global LLDP configuration subcommands
  logging          Modify message logging facilities
  mac              MAC configuration
  mac-address-table Configure the MAC address table
  mls              mls global commands
  monitor          SPAN information and configuration
  no               Negate a command or set its defaults
  ntp              Configure NTP
  port-channel     EtherChannel configuration
  privilege        Command privilege parameters
  sdm              Switch database management
  service          Modify use of network based services
  snmp-server      Modify SNMP engine parameters
  spanning-tree    Spanning Tree Subsystem
  username         Establish User Name Authentication
  vlan             Vlan commands
  vtp              Configure global VTP state
Switch(config)#vlan ?
<1-4094> ISL VLAN IDs 1-1005
Switch(config)#vlan |
```

1.6.5

- Como se nos indica debemos poner un numero para crear la vlan en este caso 2. Dentro de la vlan 2 miramos las opciones.

```
Switch(config)#vlan 2
Switch(config-vlan)#?
VLAN configuration commands:
  exit          Apply changes, bump revision number, and exit mode
  name          Ascii name of the VLAN
  no            Negate a command or set its defaults
  remote-span   Add the Remote Switched Port Analyzer (RSPAN) feature
to the VLAN
Switch(config-vlan)#|
```

- Debemos asignarle un nombre por lo que usamos el comando name y a continuación escribimos el nombre que queramos. Por último salimos de la vlan con el comando **exit** para crear la vlan 3.

```
Switch(config-vlan)#name Javi
Switch(config-vlan)#exit|
```

Apartado 5

- Repetimos el proceso anterior y creamos la Vlan 3 con el nombre Jose.

```
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name Jose
Switch(config-vlan)#exit
Switch(config)#
```

```
vlan 3
name Jose
exit
```

1.6.5

- c) Establece que los puertos 1-10 pertenecen a la VLAN 1 , puertos 11-20 a la VLAN2 y 21-24 a la Vlan3.

- Seguimos dentro de la configuración y volvemos a comprobar los comandos posibles. Entre ellos se encuentra “**interface**” el cual usaremos para asignar los puertos a las distintas VLAN.

```
Switch(config)#?
Configure commands:
access-list      Add an access list entry
banner          Define a login banner
boot            Boot Commands
cdp             Global CDP configuration subcommands
clock           Configure time-of-day clock
crypto          Encryption module
default         Set a command to its defaults
do             To run exec commands in config mode
enable         Modify enable password parameters
end            Exit from configure mode
exit           Exit from configure mode
hostname       Set system's network name
interface     Select an interface to configure
ip            Global IP configuration subcommands
line          Configure a terminal line
lldp         Global LLDP configuration subcommands
```

- Escribimos interface ? y nos muestra los comandos posibles.

```
Switch(config)#interface ?
Ethernet        IEEE 802.3
FastEthernet    FastEthernet IEEE 802.3
GigabitEthernet GigabitEthernet IEEE 802.3z
Port-channel    Ethernet Channel of interfaces
Vlan           Catalyst Vlans
range          interface range command
```

- Usaremos el comando “**range**” para seleccionar un rango de puertos y abrimos los posibles comandos.

```
Switch(config)#interface range ?
Ethernet        IEEE 802.3
FastEthernet    FastEthernet IEEE 802.3
GigabitEthernet GigabitEthernet IEEE 802.3z
Vlan           Vlan interface
```

- Vamos a configurar los puertos FastEthernet. Escribimos **FastEthernet** y a continuación el rango de puertos que queremos tal como **0/11 - 20**.

```
Switch(config)#interface range FastEthernet 0/11 - 20
Switch(config-if-range)#
```

- Tenemos seleccionado el rango y debemos asignarlos a una VLAN en este caso la nº2. Comprobamos los posibles comandos. Utilizaremos el comando “**switchport**”.

Apartado 5

1.6.5

- Continuación

```
Switch(config-if-range)#?  
cdp                Global CDP configuration subcommands  
channel-group      Etherchannel/port bundling configuration  
channel-protocol   Select the channel protocol (LACP, PAgP)  
description        Interface specific description  
duplex             Configure duplex operation.  
exit              Exit from interface configuration mode  
ip                Interface Internet Protocol config commands  
lldp              LLDP interface subcommands  
mdix              Set Media Dependent Interface with Crossover  
mls               mls interface commands  
no                Negate a command or set its defaults  
shutdown          Shutdown the selected interface  
spanning-tree     Spanning Tree Subsystem  
speed             Configure speed operation.  
storm-control      storm configuration  
switchport      Set switching mode characteristics  
tx-ring-limit     Configure PA level transmit ring limit
```

- Dentro de switchport comprobamos las distintas opciones. Utilizaremos “**access**”.

```
Switch(config-if-range)#switchport ?  
access          Set access mode characteristics of the interface  
mode             Set trunking mode of the interface  
nonegotiate      Device will not engage in negotiation protocol on  
this  
interface  
port-security    Security related command  
priority          Set appliance 802.1p priority  
protected        Configure an interface to be a protected port  
trunk             Set trunking characteristics of the interface  
voice            Voice appliance attributes
```

- Escribimos switchport access y el número de la vlan a la que asignamos el rango de bocas. Salimos con end para configurar asignar los puertos a la vlan 3.

```
Switch(config-if-range)#switchport access vlan 2  
Switch(config-if-range)#end  
Switch#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Switch#|
```

- Repetimos el proceso anterior para los puertos 21 - 24 para la VLAN 3.

```
Switch#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#interface range fastethernet 0/21 - 24  
Switch(config-if-range)#switchport access vlan 3  
Switch(config-if-range)#end  
Switch#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Switch#|
```

- e) Comprobamos que están asignados con el comando **show vlan brief**.

```
Switch#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, Gig0/1, Gig0/2
2 Javi	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20
3 Jose	active	Fa0/21, Fa0/22, Fa0/23, Fa0/24

Apartado 5

f) Comprueba que efectivamente hay comunicación interna entre los equipos la VLAN1 y de la VLAN2

1.6.5

La VLAN 1 está representada por los PC0 y PC1, la VLAN 2 (Javi) por PC2 y PC5 y la VLAN 3 (Jose) por PC3 y PC4.

- Para comprobar el correcto funcionamiento interno de cada VLAN haremos ping entre los equipos de la misma VLAN.

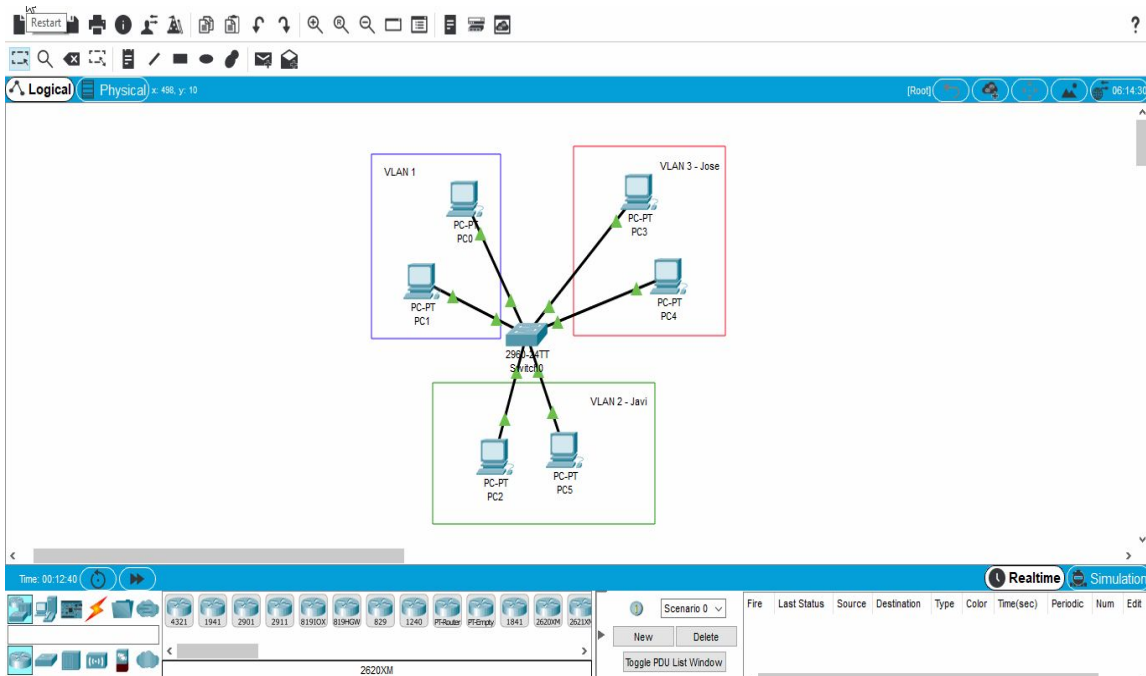


Figura 1.6.5.B. Comprobación satisfactorio de la red mediante ping.

g) Comprueba que un equipo de la VLAN1 NO tiene comunicación con otro de la VLAN2.

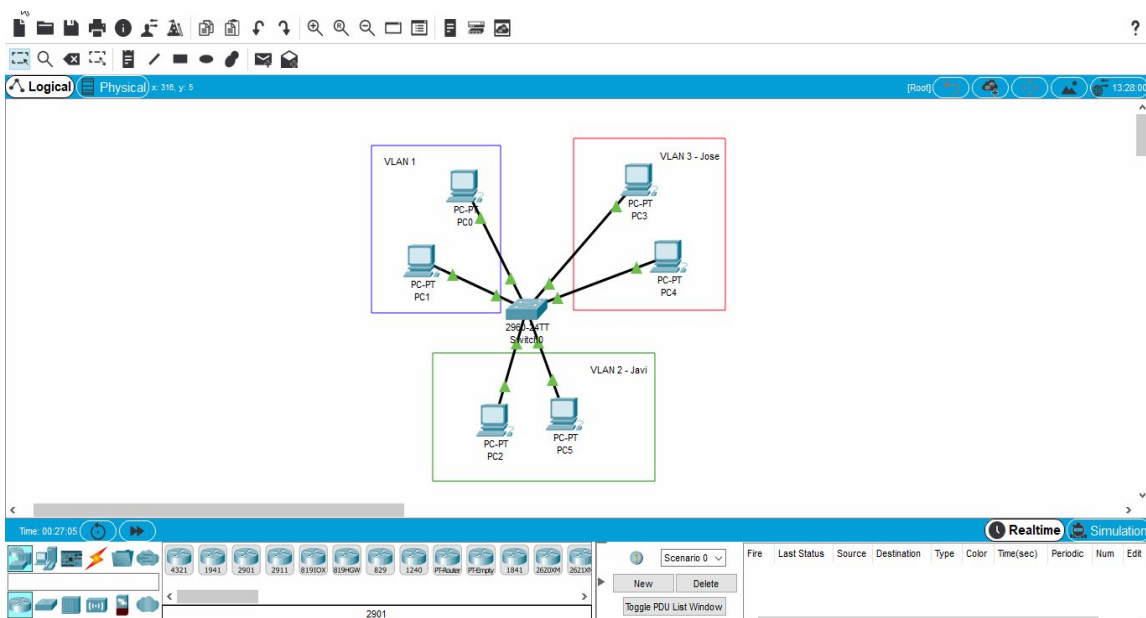


Figura 1.6.5.C. Comprobación de la independencia de la VLAN1 respecto a la VLAN2.

Apartado 6.2 Switches

6. VLAN multiswitch con enlaces dedicados

- Ampliar el diseño anterior de tal manera que nuestra red tenga 2 switches
- Crea un enlace por cada vlan que una los dos switches
- Comprueba que hay conectividad entre dos Pcs de una misma vlan de switches diferentes

1.6.6

En primer lugar pondremos 1 switch y 4 equipos informáticos más.

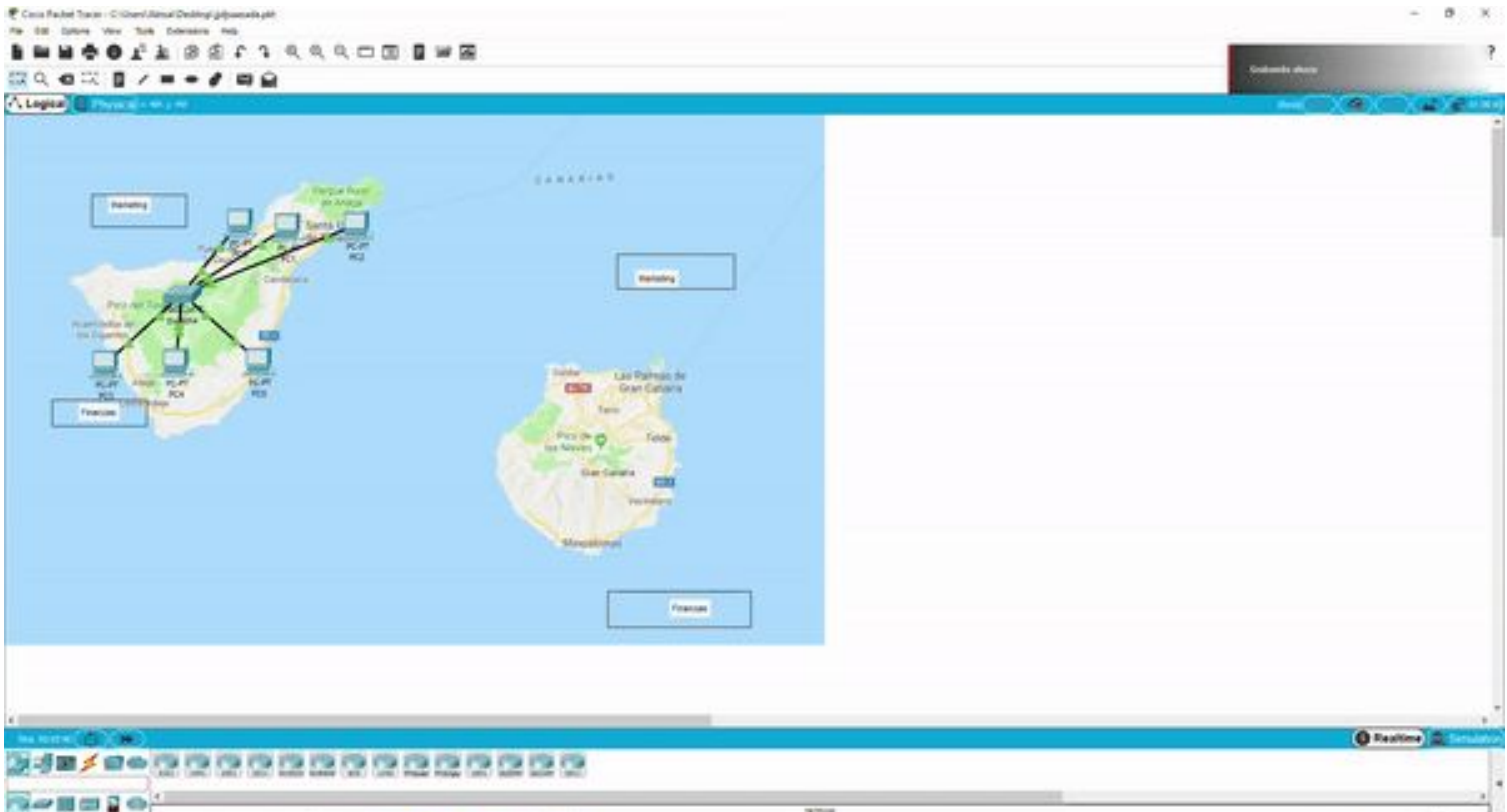


Figura 1.6.6.A. Creación de una red con dos switch.

Después de haber hecho esto tendremos que configurar las VLAN en ambos switches tal como se ha explicado en el apartado nº 5 de este manual, para poder empezar a hacer las conexiones que se nos piden en este apartado.

<IMARMEN>
<APLAFLE>

Apartado 6. Enlace

Después los enlazaremos entre sí por un puerto correspondiente a la vlan 1 y por un puerto correspondiente a la vlan 2 tanto en el primer como el segundo switch, en este caso utilizaremos el puerto n° 12 para la 1° vlan y el puerto n° 24 para la 2° vlan, como se muestra en el siguiente GIF.

1.6.6

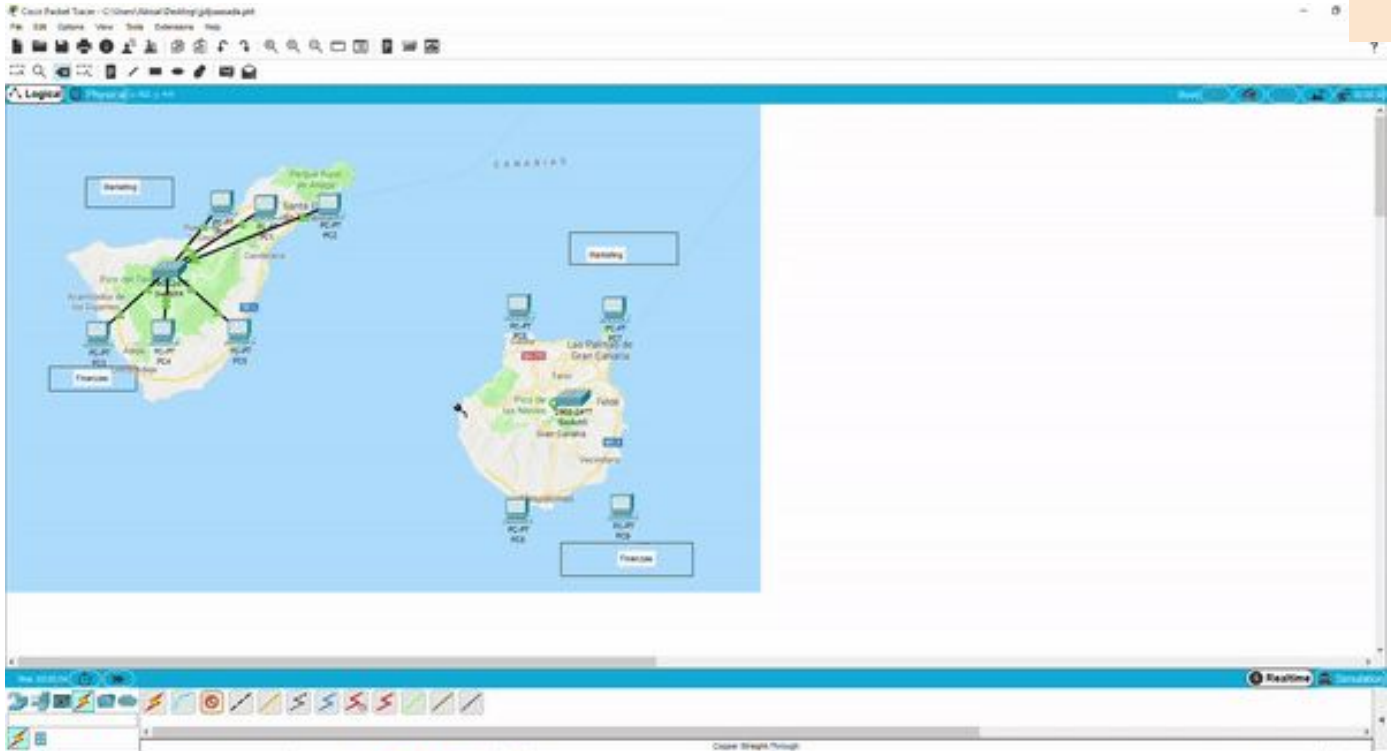


Figura 1.6.6.B. Conexionado del PC al puerto de su correspondiente VLAN.

Por último haremos dos ping entre los distintos switches de una misma VLAN uno en el departamento de marketing y otro en el departamento de finanzas como se muestra en el siguiente GIF.

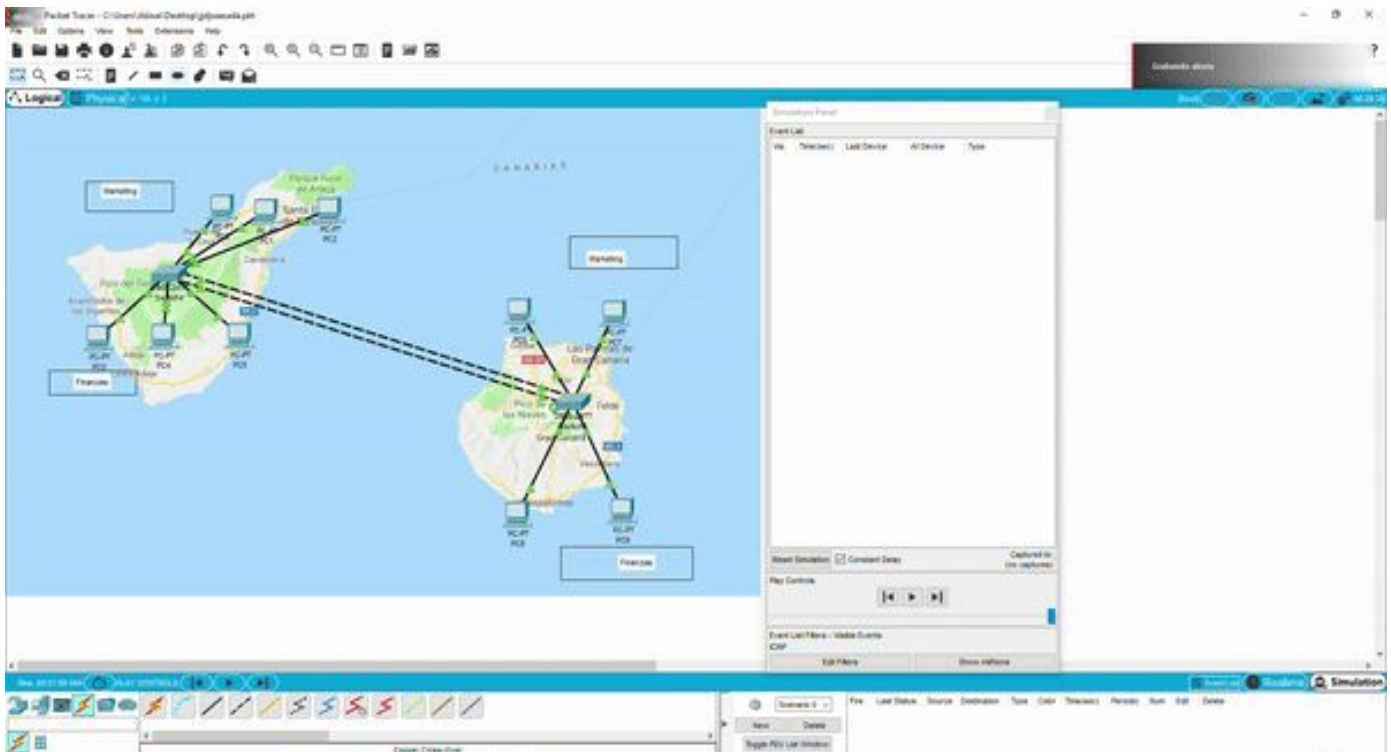


Figura 1.6.6.C. Realización de un ping entre PC de distinto switch pero de la misma VLAN

<IMARMEN>
<APLAFLE>

Apartado 6. Vídeo explicativo

https://www.youtube.com/watch?v=vgQZn3A_fXA&feature=youtu.be

QR del vídeo:



1.6.6

Apartado 7.

7. VLAN multiswitch con enlace compartido (trunking)

- Sobre el ejemplo anterior,
 - eliminar los dos enlaces
 - poner uno solo, el que voy a usar como trunkIMPORTANTE: De puerto Gigabit a puerto Gigabit

1.6.7

Del esquema del apartado 6 eliminaremos los dos enlaces y pondremos un solo cable para utilizarlo como trunk más adelante el esquema nos quedaría de esta forma:



Figura 1.6.7. Conexión de dos switch a través de un único enlace.

Importante tener en cuenta que el cable que une los switch debe ir conectado de puerto gigabit a puerto gigabit (el switch que utilizaremos tiene 2 puertos gigabit se puede usar cualquiera)



Apartado 8: Trunking

8. VLAN multiswitch con enlace compartido (trunking)

Mostrar el estado inicial del puerto G1/1

Directamente, tras añadir el enlace que hará de trunk de switch a switch usa el comando:

1.6.8

- `show interface gigabitethernet 0/1 switchport`

Tal y como dice el enunciado lo que hay que hacer es, según hemos conectado un switch con el otro a través del puerto Gigabitethernet, introduciremos el comando “show interface gigabitethernet 0/1 switchport” en la CLI del Switch de Tenerife.

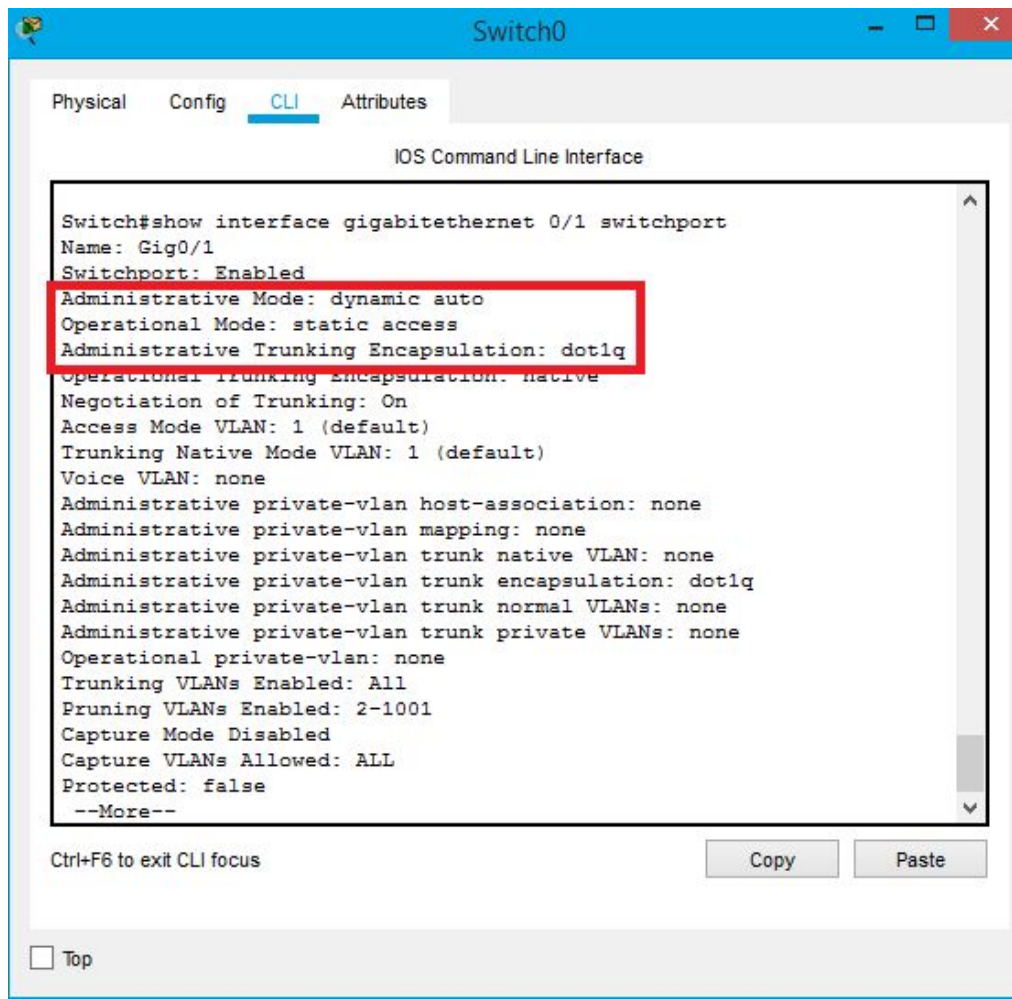


Figura 1.6.8. Muestra del estado del puerto GigabitEthernet 0/1.

Hemos resaltado esos 3 valores ya que son los que más nos interesan al utilizar este comando:

- Administrative mode: dynamic auto es el valor por defecto; el otro switch estará igual; ninguno de los dos inicia la negociación
- Operational mode: static access, acceso estático, sin trunking
- Administrative Trunking encapsulation: dot1q, es decir, que este switch sólo soporta 802.1Q para trunking

Apartado 9

9. VLAN multiswitch con enlace compartido (trunking)

Comprobar que inicialmente no hay ningún puerto para trunking

- `Show interfaces trunk`
- Muestra los puertos configurados para trunking
- NO sale nada porque ahora mismo NO tenemos ninguno configurado para tal

1.6.9

Para comprobar si hay o no puertos habilitados para **trunking**, estando en el modo administrador (**#**), aplicaremos el comando `show interfaces trunk:`

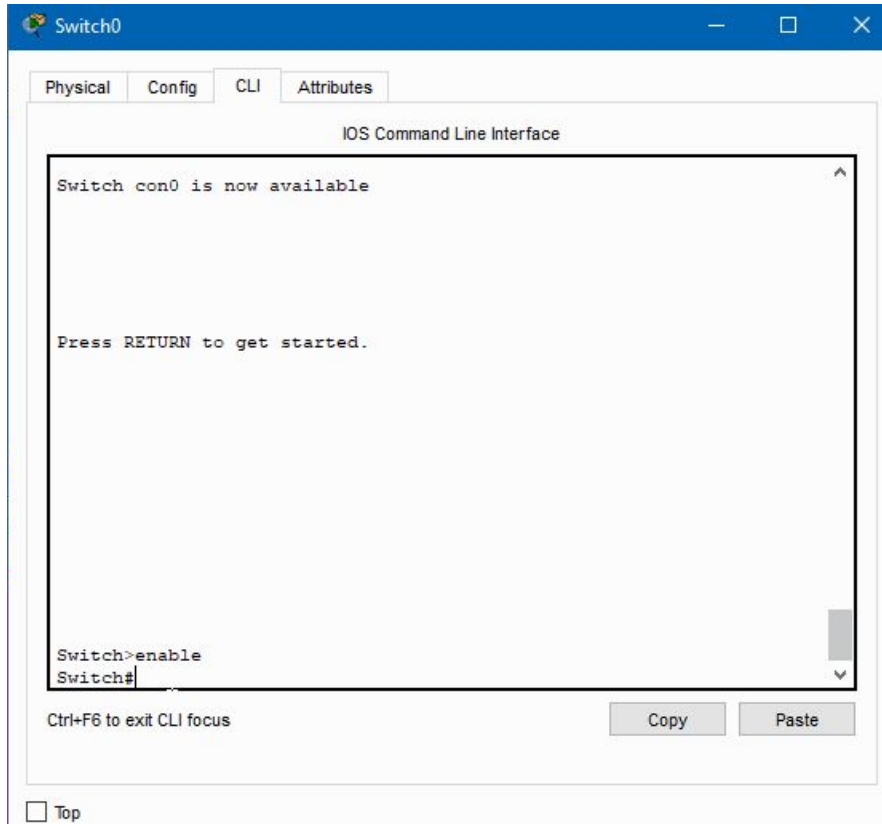


Figura 1.6.9. Muestra de la acción del comando `show interface trunk.`

Como se puede apreciar en la imagen anterior, la acción del comando `show interfaces trunk` no revela nada, pues todavía no se han configurado los puertos requeridos para la conexión troncal entre los dos switch.

Apartado 10. Comprobación

10. VLAN multiswitch con enlace compartido (trunking)

NO existe conectividad

Probar a hacer un ping entre dos máquinas conectadas a diferente switch

1.6.10

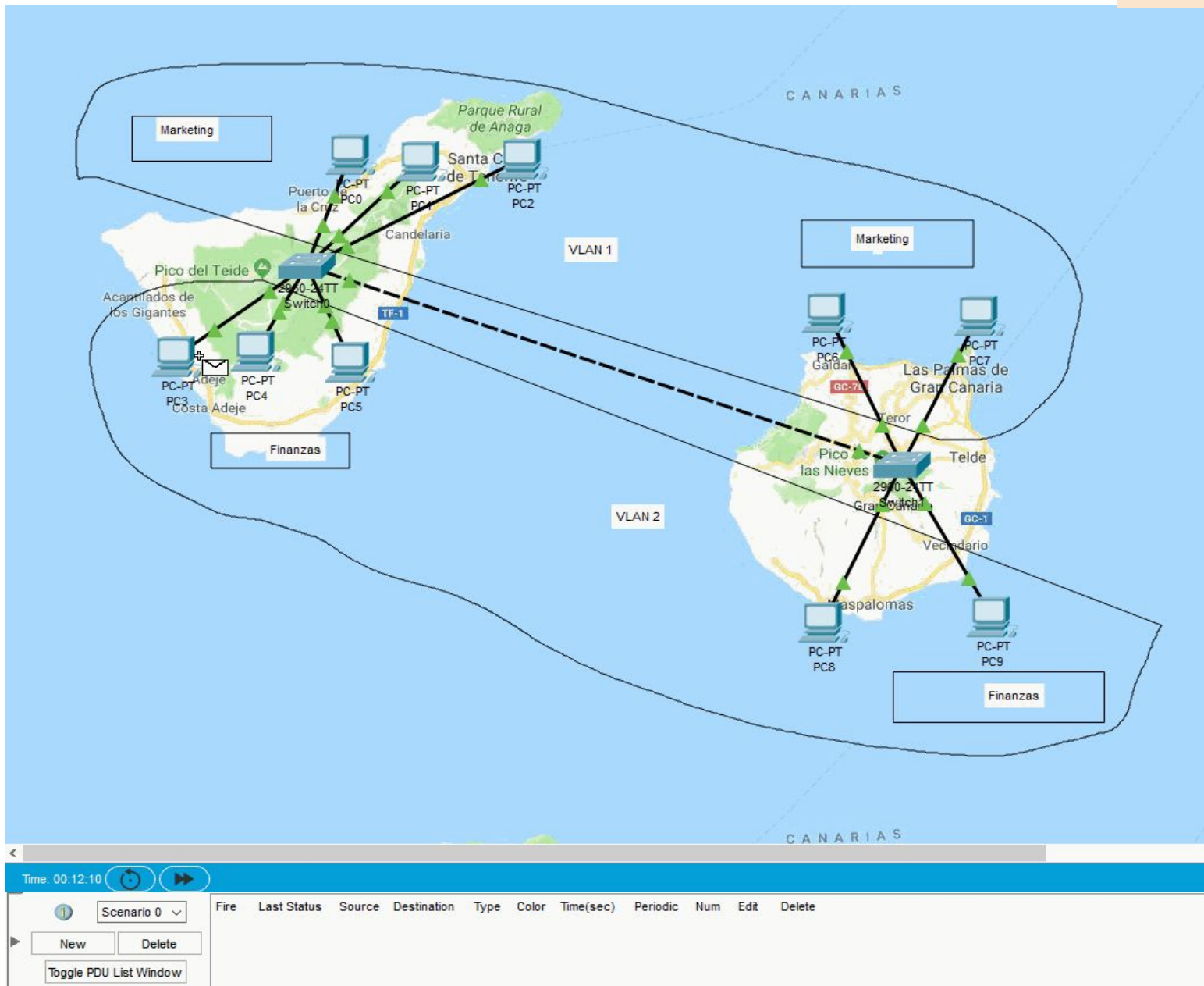


Figura 1.6.10. Ping entre dos PC conectados a distinto switch.

Al no tener configurados los switch para que las bocas en las que está conectado el cable que queremos como troncal, no va a funcionar como tal.

Vídeo explicativo:

https://www.youtube.com/watch?v=PlwDZ3rCy_8&feature=youtu.be



<IMARMEN>
<APLAFLE>

Apartado 11.

11. VLAN multiswitch con enlace compartido (trunking)

Habilitar el trunking

1.6.11

- ¿Cómo lo podemos hacer?
- En uno de los dos switch → habilitamos dynamic desirable → ese switch inicia las negociaciones para trunking
- Cambiamos la configuración → se desactiva el puerto → se vuelve a activar → tarda un tiempo en estar operativo → está negociando

Básicamente pinchamos en cualquiera de los dos switch entramos en `configure terminal` (recordemos que hay que entrar en modo admin así que antes le daremos a `enable`).

Luego, entramos en el puerto gigabitEthernet 0/2 y habilitamos el trunk con el comando `dynamic desirable`.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface giga
Switch(config)#interface gigabitEthernet 0/2
Switch(config-if)#swi
Switch(config-if)#switchport mode dynamic des
Switch(config-if)#switchport mode dynamic desirable
```

```
configure terminal
interface gigabitEthernet 0/2
switchport mode dynamic desirable
```


Apartado 12: Trunking

12. VLAN multiswitch con enlace compartido (trunking).

Mostrar el estado del puerto tras habilitar el trunking

Show interface gigabitethernet 1/1 switchport

1.6.12

Para poder llegar a observar el estado del switch debemos hacer uso del siguiente comando tras haber habilitado el trunking:

enable - show interface gigabitethernet 1/1 switchport

Y en la siguiente imagen se muestra la comprobación de dicho estado:



```
Switch1
Physical Config CLI Attributes
Switch>enable
Switch#show interface gigabitethernet 0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation:
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
```

Figura 1.6.12. Comprobación del estado del puerto G1/1.

En esta imagen se observa como haciendo uso del comando 'show interface gigabitethernet 1/1 switchport' dicho puerto se encuentra en modo trunking.

Apartado 13

13. VLAN multiswitch con enlace compartido (trunking)

Mostrar los puertos de trunking que existen

- Show interfaces trunk
- Ahora sí que vemos que G1/1 está habilitado para trunking

1.6.13

NOTA: prune = podar

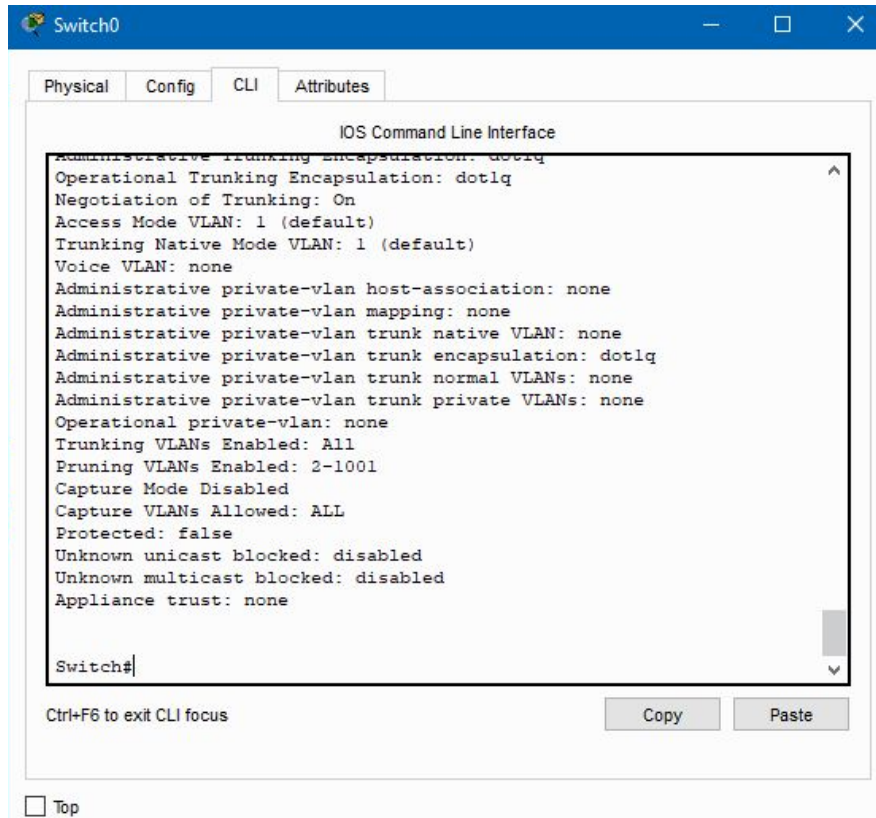


Figura 1.6.13. Muestra del resultado de la acción del comando `show interface trunk`.

En la imagen anterior, se puede comprobar cómo la acción del comando `show interface trunk` ahora sí nos informa de los puertos configurados con la función de `trunking` (en este caso el puerto GigabitEthernet 0/1), además de las VLAN permitidas, cuáles de ellas están activas...

Apartado 14. Comprobación

14. VLAN multiswitch con enlace compartido (trunking)

Existe conectividad

- Probar a hacer un ping entre dos máquinas conectadas a diferente switch y ver que efectivamente hay conectividad
- Lógicamente entre diferentes VLAN sigue sin haber conectividad

1.6.14

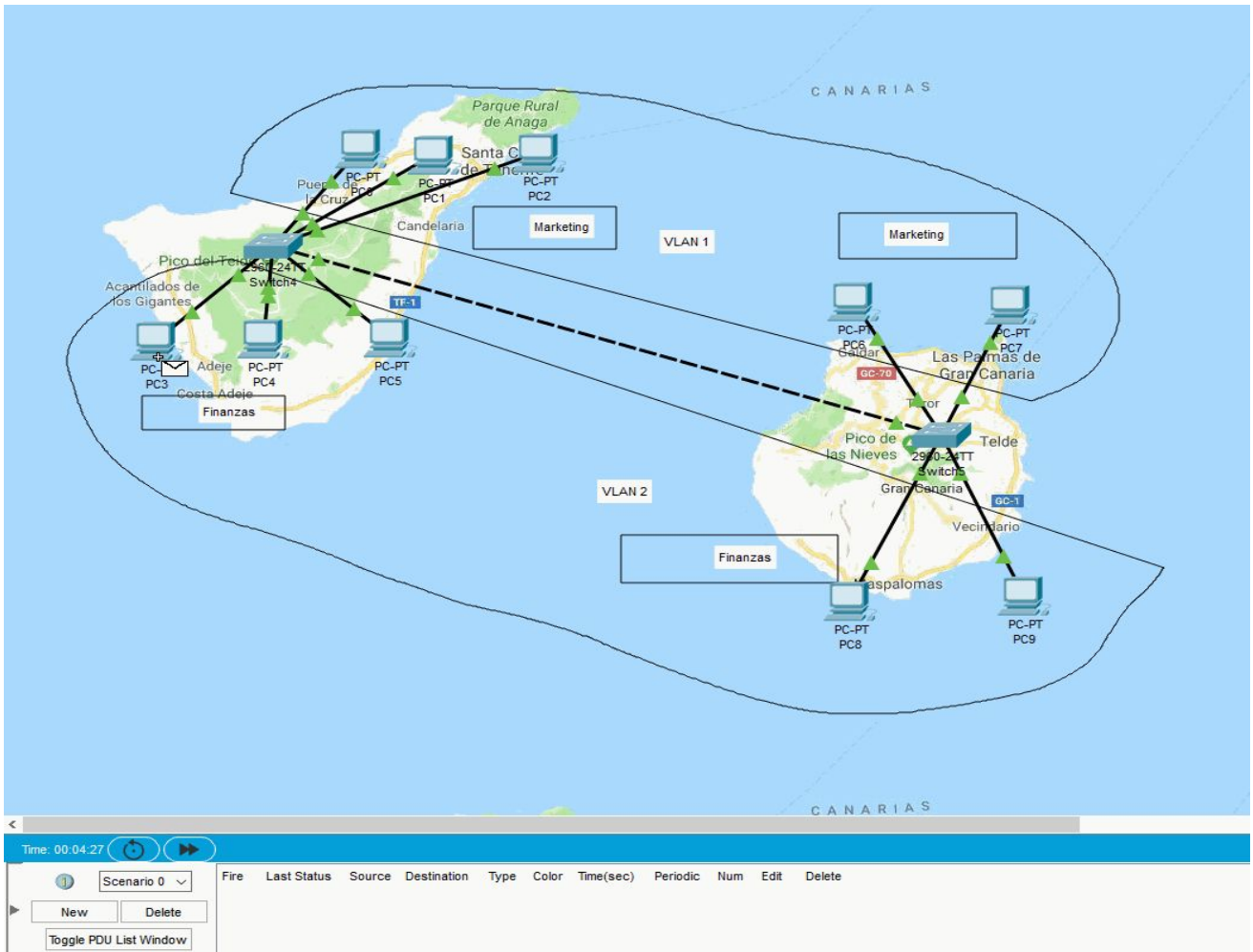


Figura 1.6.14. Comprobación de conectividad del enlace compartido (trunking).

VÍDEO EXPLICATIVO:

<https://www.youtube.com/watch?v=ZY9IDH-k8No&feature=youtu.be>

QR del vídeo:



Conexión SSH

- **¿Qué es?**

SSH o Secure SHell es un protocolo de seguridad que facilita las comunicaciones seguras entre dos sistemas empleando una estructura **cliente-servidor** y que permite a los usuarios conectarse a un host de forma remota. A diferencia de Telnet o FTP, SSH encripta la conexión, por lo que es imposible que alguien pueda obtener contraseñas no encriptadas.

1.6.ex

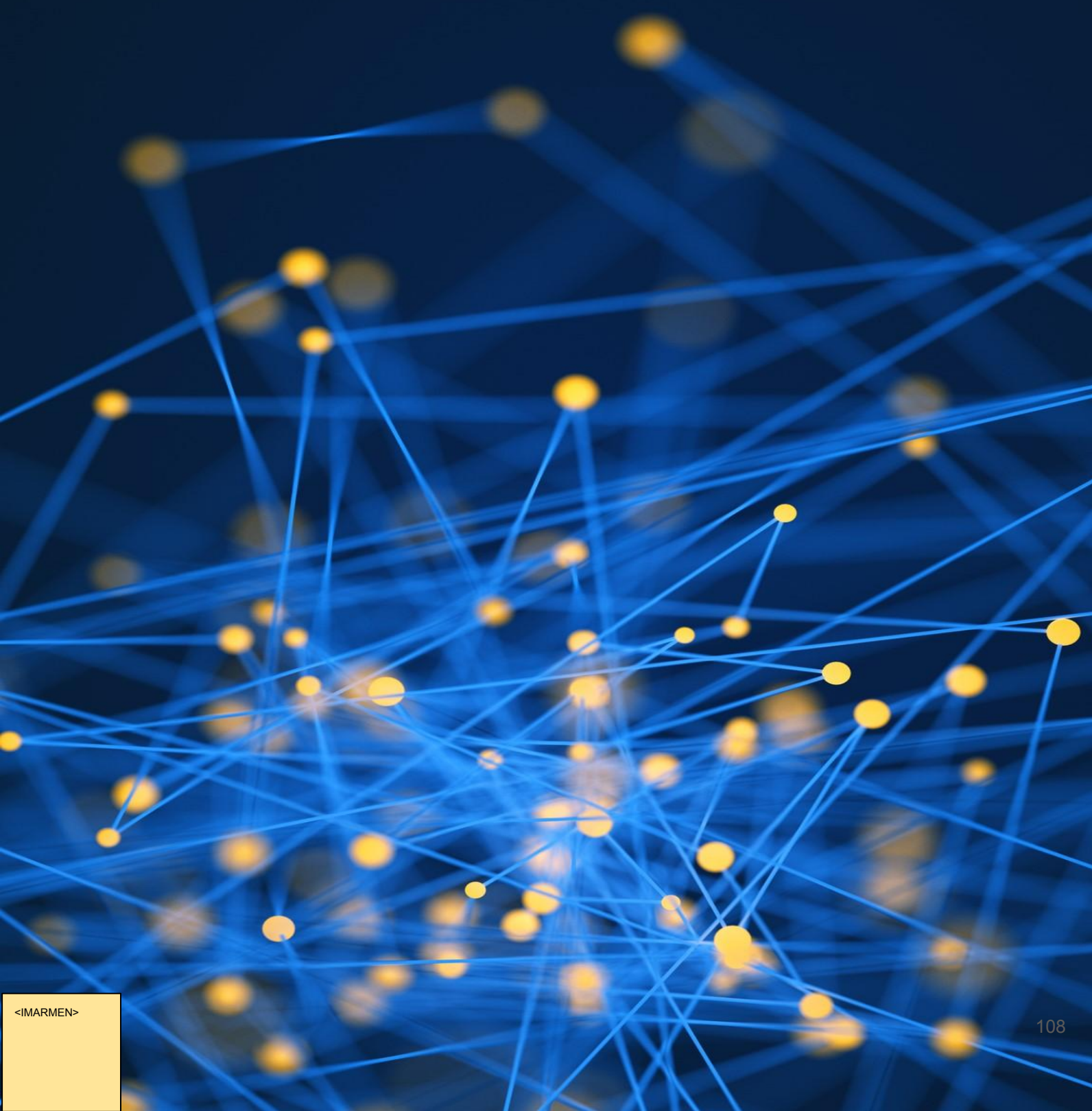
- **¿Qué proporciona SSH?**

- Tras la primera conexión, el cliente puede verificar que se está conectando al mismo servidor al cual se conectó anteriormente.
- El cliente transmite su información de autenticación al servidor usando una encriptación de 128 bits. De igual forma, todos los datos que se envían y se reciben durante la sesión se transfieren por medio de encriptación de 128 bits.

Trabajo 2.1

Subnetting

Cálculo y diseño



Trabajo 2.1. Subnetting: Cálculo y diseño

Dada la siguiente dirección IP **172.16.128.10/19** calcular:

1. Número de bits de red
2. Número de bits de subred
3. Número de bits de host
4. Indica cuántas subredes hay
5. ID de red de cada subred
6. Máscara de subred
7. Dirección IP de broadcast de cada subred
8. Dirección IP de 2 Pcs por subred: primero y último
9. Con todos los cálculos hechos, diseña esta red en PT utilizando como concentrador un switch
10. Comprueba que efectivamente hay conectividad dentro de los Pcs de cada subred
11. Comprueba que NO hay conectividad entre equipos de diferentes subredes
12. Contesta de forma razonada la/s diferencia/s que detectes de este diseño usando subnetting y VLAN

¿Qué es y cómo funciona Subnetting?

Conocimientos previos.

Definido de la forma más simple, el término subnetting hace referencia a la **subdivisión de una red en varias subredes**. El subneteo permite, por ejemplo, dividir una red empresarial en varias subredes sin hacerlo público en Internet. Esto se traduce en que el router que establece la conexión entre la red e Internet se especifica como dirección única, aunque puede que haya varios hosts ocultos. Así, el número de hosts que están a disposición del administrador aumenta considerablemente.

2.1

En el subnetting o subneteo se toman bits del ID del host “prestados” para crear una subred. Con solo un bit se tiene la posibilidad de generar dos subredes, puesto que solo se tiene en cuenta el 0 o el 1. Para un número mayor de subredes se tienen que liberar más bits, de modo que hay menos espacio para direcciones de hosts. Cabe remarcar en este caso que tanto las direcciones IP de una subred como aquellas que no forman parte de ninguna tienen la misma apariencia y los ordenadores tampoco encuentran ninguna diferencia, de ahí que se creen las llamadas **máscaras de subred**. Si se envían paquetes de datos de Internet a la propia red, el router es capaz de decidir mediante esta máscara en qué subred distribuye los datos.

Antes de empezar a hacer cálculos, debemos conocer varios datos.

Dirección de red:

Representa todos los bits en valor **cero** en la porción de host de la dirección. También va a ser siempre **la primera dirección** de la subred.

Dirección de broadcast:

Representa todos los bits en valor **uno** en la posición de host de la dirección. También será siempre **la última dirección** de la subred.

El rango de las diferentes clases de direcciones IP:

- **Clase A:** 0.0.0.0 - 127.255.255.255
- **Clase B:** 128.0.0.0 - 191.255.255.255
- **Clase C:** 192.0.0.0 - 223.255.255.255
- **Clase D:** 224.0.0.0 - 239.255.255.255
- **Clase E:** 240.0.0.0 - 255.255.255.255

Bits de red de cada clase:

- **Clase A:** 8 bits (Primer Octeto)
- **Clase B:** 16 bits (Primer + Segundo Octeto)
- **Clase C:** 24 bits (Primer + Segundo + Tercer Octeto)

Direcciones privadas (son las direcciones reservadas para LAN, es decir, la red que tendríamos en nuestra casa a partir del router):

- **Clase A:** 10.0.0.0 - 10.255.255.255
- **Clase B:** 172.16.0.0 - 172.31.255.255
- **Clase C:** 192.168.0.0 - 192.168.255.255

En este caso, no se trabajará con redes clase E y D, puesto que son para multicasting e investigación y desarrollo respectivamente, siendo algo que a nosotros no nos concierne.

En caso de no recordar la conversión de binario a decimal, se aconseja revisar el siguiente link.

https://www.quia.com/files/quia/users/istomar/DIPS/conversin_binario_a_decimal.html

Una vez se tengan estos conceptos claros, podremos proceder a realizar el siguiente ejercicio.

Apartados 1, 2, 3, 4 y 5.

172.16.128.10/19

1. Número de bits de red.

Representaremos este valor con la letra "N". Esto es sencillo de ver, simplemente tenemos que preguntarnos "**¿A qué clase pertenece esta red?**". Una vez tengamos la respuesta, tendremos el número de bits.

En este caso **N = 16 bits**, ya que, la red **172.16.128.10** se encuentra dentro de la **clase B**.

2.1

2. Número de bits de subred.

Representamos este valor con la letra "S". Tendremos que hacer una simple operación matemática, restar el número de bits a 1 de la máscara de subred al número de bits de red.

En este caso:

$$S = \text{Máscara de subred} - N \longrightarrow S = 19 - 16 \longrightarrow \mathbf{S = 3 \text{ bits.}}$$

3. Número de bits de host.

Representaremos este valor con la letra "H". ¿Sabemos que una dirección IPv4 tiene 4 octetos de 8 bits? O lo que es lo mismo, 32 bits. Esto será los bits que quedan por asignar, o de otra manera, restaremos a 32 el número de bits a 1 de la máscara de subred.

En este caso:

$$H = 32 - \text{Máscara de subred} \longrightarrow H = 32 - 19 \longrightarrow \mathbf{H = 13 \text{ bits.}}$$

4. Indica cuántas subredes hay.

Para esto necesitamos empezar a trabajar en binario, pero no es un cálculo para nada complejo. Necesitamos coger el número de bits de subred (S) y ponerlo en base 2. ¿Cómo se hace esto? Simple.

En este caso:

$$2^S = 2^3 = \mathbf{8 \text{ redes.}}$$

5. ID de cada subred.

$2^8 = 256$ bits. Si dividimos 256 entre el número de subredes, sabremos cuánto ocupará cada red. Para saber la ID de cada red tendremos que cambiar el primer octeto después del último de red, en este caso al ser **clase B**, sería el **tercer octeto**. En **clase A** sería el **segundo octeto** y en **clase C** el **cuarto octeto**.

Tendiendo que usar una fórmula así:

$$256 / \text{Número de subredes}$$

En este caso:

$$256 / \text{Número de subredes} \longrightarrow 256 / 8 = \mathbf{32.}$$

Con esto ahora simplemente tenemos que empezar desde la red 0, sumando 32 hasta llegar a la red 7. Recordar que a cada subred se le debe añadir 32 partiendo desde el 0.

Subred 0: 172.16.0.0

Subred 1: 172.16.32.0

Subred 2: 172.16.64.0

Subred 3: 172.16.96.0

Subred 4: 172.16.128.0

Subred 5: 172.16.160.0

Subred 6: 172.16.192.0

Subred 7: 172.16.224.0

Apartados 6 y 7.

172.16.128.10/19

6. Máscara de subred.

La máscara de subred siempre nos la tendrán que dar para poder realizar subnetting o subneteo, en caso de no la tengamos daremos por supuesto que es la máscara de red por defecto de cada red.

Hay varias representaciones para una máscara de subred en decimal, en binario o en versión natural. Serán expuestas en ese orden.

- **Clase A:** 255.0.0.0 11111111.00000000.00000000.00000000 /8
- **Clase B:** 255.255.0.0 11111111.11111111.00000000.00000000 /16
- **Clase C:** 255.255.255.0 11111111.11111111.11111111.00000000 /24

Ejemplo de representaciones con máscara de red.

Para este caso, nos han dado /19, por lo que tendremos que poner los 8 bits del primer octeto a 1, los 8 bits del segundo octeto a 1 y los 3 primeros bits del tercer octeto a 1. Es decir, poner los primeros 19 bits a 1.

1º Octeto: $11111111 = 2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0=128+64+32+16+8+4+2+1=255$

2º Octeto: $11111111 = 2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0=128+64+32+16+8+4+2+1=255$

3º Octeto: $11100000 = 2^7+2^6+2^5=128+64+32=224$.

Quedando así una máscara de subred tal que:

255.255.224.0

7. Dirección IP de broadcast de cada subred.

Como se explica en la primera página de este trabajo, la dirección IP de broadcast es la última de cada subred.

Una manera fácil de verlo, es coger la dirección de red de la siguiente subred y restar uno.

Ejemplo:

Subred 1 = 172.16.32.0

Subred 1 - 1 = 172.16.31.255

Para la última subred el resultado siempre será de 255 donde hayan bits de host. La dirección de broadcast siempre tendrá los octetos de host a 1, lo que en decimal sería el número 255. O también, poner todos los bits de host a 1.

Otra manera de verlo sería solo modificar el octeto de subred, mientras el resto será siempre igual.

Ejemplo:

172.16.x.255

x = Octeto de subred (en este caso)

255 se mantendrá siempre igual para todas las subredes (en este caso).

Para este caso quedaría tal que así:

Subred 0: 172.16.31.255

Subred 1: 172.16.63.255

Subred 2: 172.16.95.255

Subred 3: 172.16.127.255

Subred 4: 172.16.159.255

Subred 5: 172.16.191.255

Subred 6: 172.16.223.255

Subred 7: 172.16.255.255

2.1

Apartados 8 y 9 (I).

172.16.128.10/19

8. Dirección IP de 2 Pcs por subred: primero y último.

Representaremos el primer pc como **PC1** y el último como **PCn**. Para el **PC1** una manera sencilla de hacerlo sería **sumar uno** a la dirección de cada subred y para el **PCn** **restar uno** a la dirección de broadcast de cada subred.

Ejemplo:

Dirección de subred 0 = 172.16.0.0

PC1= 172.16.0.0 + 1 = 172.16.0.1

PCn= 172.16.31.255 - 1 = 172.16.31.254

Para este caso quedaría tal que así:

Subred 0: PC1=172.16.0.1	PCn=172.16.31.254
Subred 1: PC1=172.16.32.1	PCn=172.16.63.254
Subred 2: PC1=172.16.64.1	PCn=172.16.95.254
Subred 3: PC1=172.16.96.1	PCn=172.16.127.254
Subred 4: PC1=172.16.128.1	PCn=172.16.159.254
Subred 5: PC1=172.16.160.1	PCn=172.16.191.254
Subred 6: PC1=172.16.192.1	PCn=172.16.223.254
Subred 7: PC1=172.16.224.1	PCn=172.16.255.254

9. Con todos los cálculos hechos, diseña esta red en PT utilizando como concentrador un switch

En primer lugar tendremos que colocar 16 PCs y conectarlos al switch. Luego, debemos dividirlos en parejas y decir a qué subred pertenece cada uno, quedando algo parecido a esto:

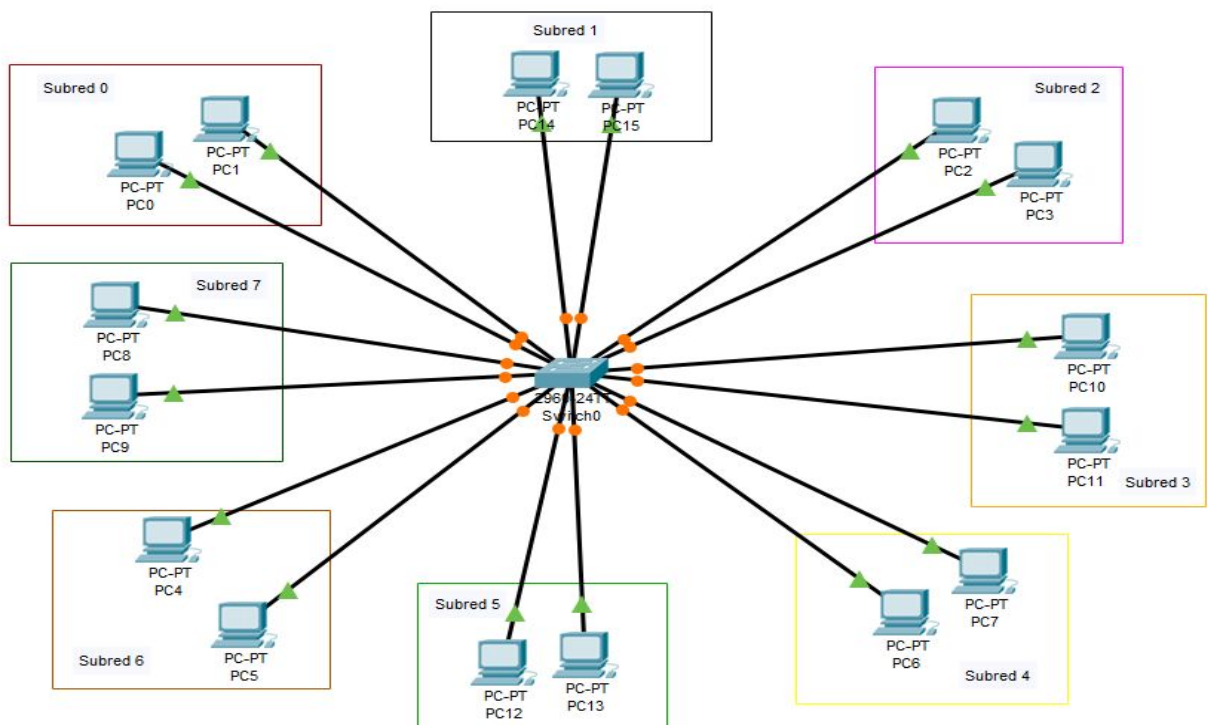
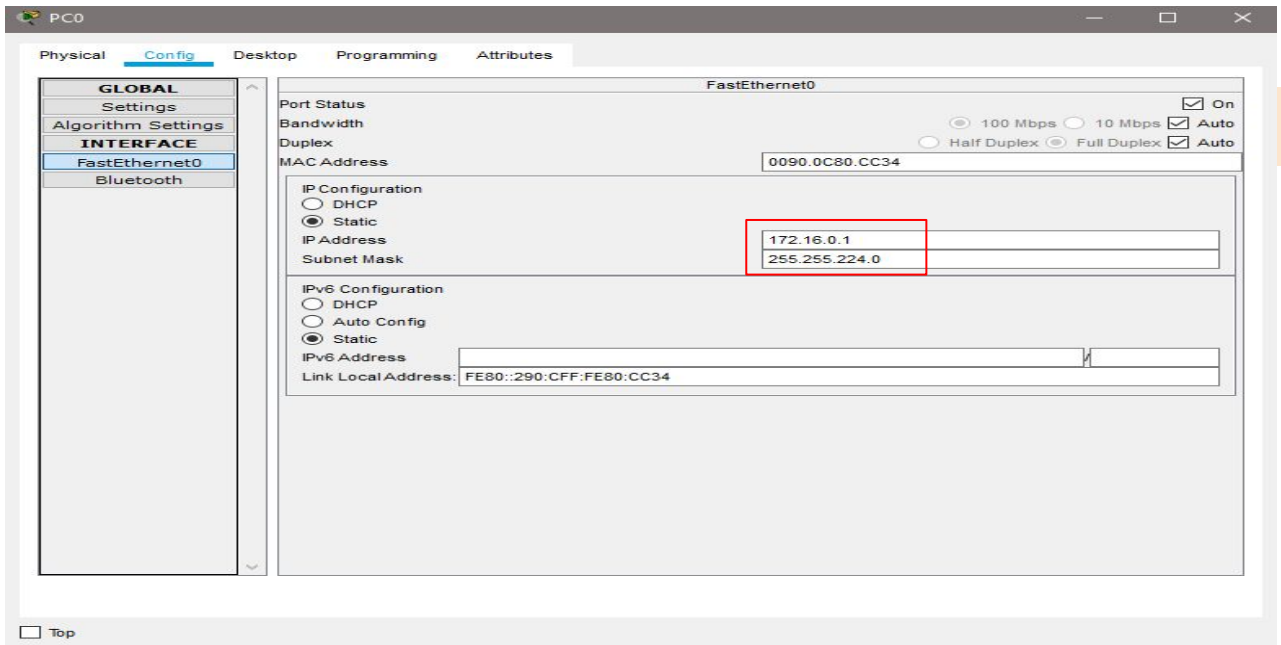


Figura 2.1.1. 8 Subredes en PT

Apartado 9 (II).

Una vez hecho esto, tendremos que poner las direcciones IP y la máscara de subred en todos los PCs, siendo uno el primer PC de la subred y el otro el último.



2.1

Figura 2.1.2. Ejemplo de configuración Subred 0 PC1.

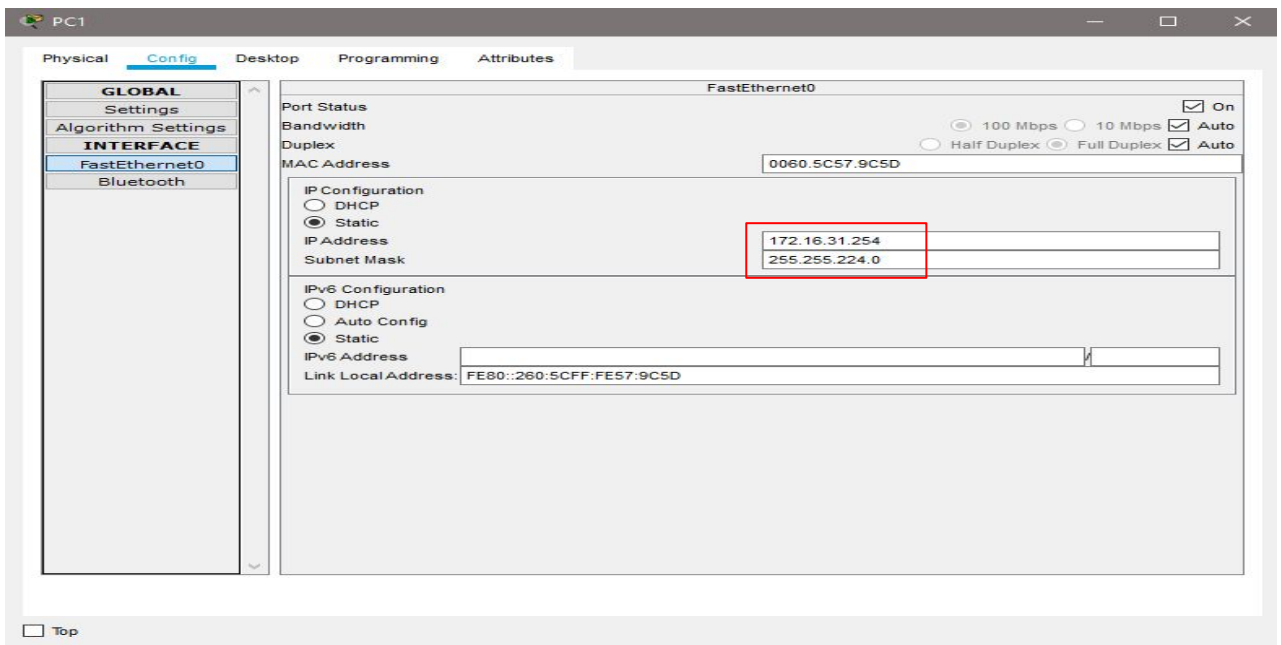


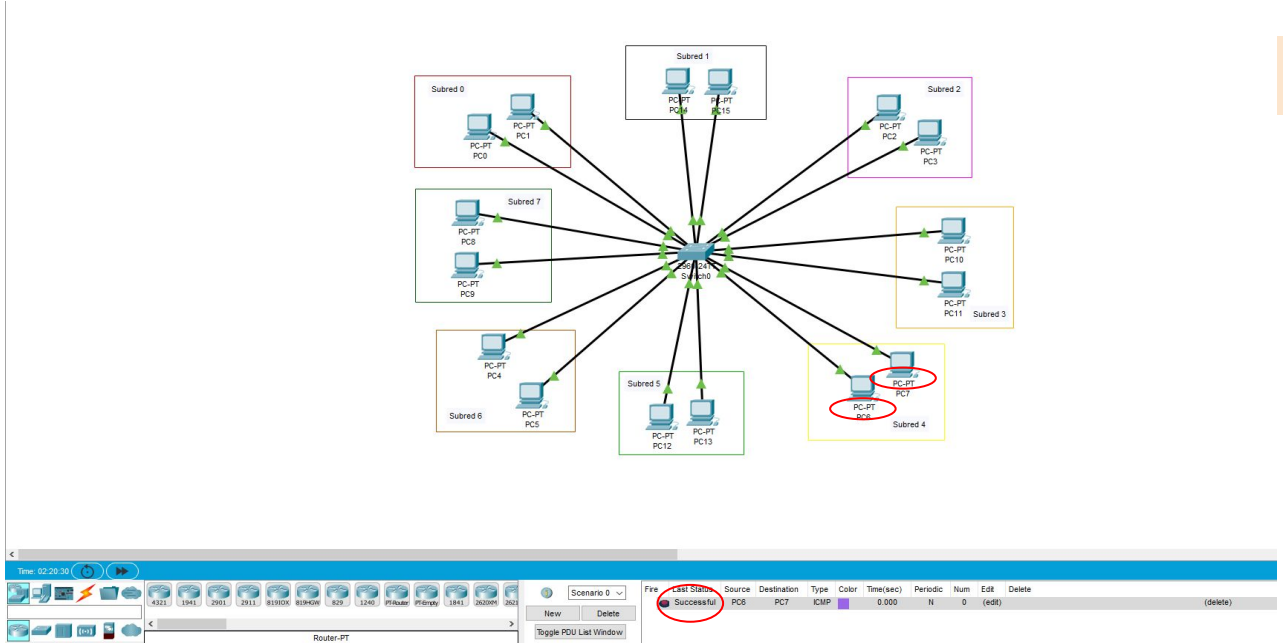
Figura 2.1.3. Ejemplo de configuración Subred 0 PCn.

Una vez realizada la configuración de cada PC, podremos proceder a realizar las pruebas.

Apartados 10 y 11.

10. Comprueba que efectivamente hay conectividad dentro de los Pcs de cada subred.

Para comprobarlo se enviará un ping entre, por ejemplo, el PC6 y PC7 pertenecientes a la Subred 4. Y efectivamente, hay conectividad.



2.1

Figura 2.1.4. Comprobación de conectividad en la misma subred.

11. Comprueba que NO hay conectividad entre equipos de diferentes subredes.

Para comprobarlo se enviará un paquete entre, por ejemplo, el PC15 perteneciente a la Subred 1 y el PC10 perteneciente a la Subred 3. Efectivamente no hay conexión entre estos dos ordenadores.

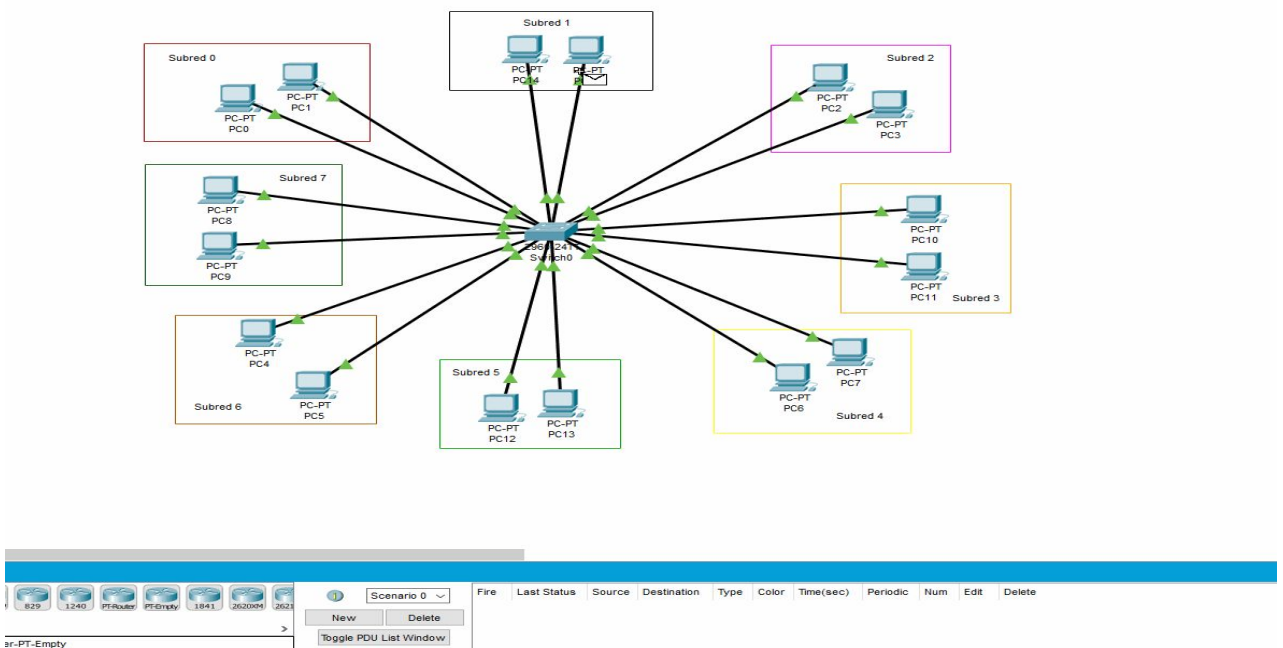


Figura 2.1.5. Comprobación de conectividad en distintas subredes.

Apartado 12 y vídeo explicativo.

12. Contesta de forma razonada la/s diferencia/s que detectes de este diseño usando subnetting y VLAN.

Mientras para hacer VLAN tendrías que trabajar sobre un Switch, haciendo subnetting o subneteo trabajas directamente con los PCs.

Es más pesado tener que ir PC por PC cambiando manualmente cada dirección IP y su máscara de subred, que asignar a cada puerto del Switch una VLAN.

2.1

Vídeo comprobación en Cisco Packet Tracer:

<https://youtu.be/9zxldsQ2Re4>



A background image showing a complex network of glowing blue lines connecting numerous yellow circular nodes, representing a network topology. The nodes and lines are scattered across the frame, with some appearing more prominent than others.

Trabajo 2.2

VLSM : diseño y pruebas DHCP y BOOTP RIP v2

Trabajo 2.2. VLSM: diseño y pruebas DCHP y BOOTP RIP v2.

Partiendo del ejemplo que hemos visto en clase de VLSM (192.168.1.0/24), diseña una red en PT en la que se plasmen exactamente los cálculos que ya hicimos.

2.2.1. Fase 1. Haz inicialmente un montaje en el que NO se usen routers

- conecta directamente los 3 switches de cada delegación entre sí
- Crea 2 hosts dentro de cada delegación, uno con la primera IP válida y otro con la última
- comprueba que hay sólo conectividad entre equipos del mismo departamento
- comprueba que NO hay conectividad entre equipos de diferente departamento

2.2.2. Fase 1b. Configuración VLSM aula de clase

- Para evitar cualquier tipo de interferencia, desconectar el aula de la red Medusa
- Seleccionar los grupos de PC del aula que representarán cada uno de los departamentos/delegaciones
- Configurar cada equipo con los parámetros de red propios del departamento al que pertenece
- Comprobar la conectividad dentro de cada departamento y la no conectividad con los equipos externos

2.2.3. Fase 2. Uso de routers

- Usa routers 2901
- Añade a cada router una tarjeta HWIC-2T
- Activa RIPv2 en todos los routers
- Indica en RIPv2 la dirección de red a la que están conectados.
- Configura la dirección IP y la máscara de subred de cada una de las bocas que tiene cada router
- Configura la dirección IP y la máscara de subred de cada uno de los enlaces WAN
- Asigna a cada uno de los PCs la dirección de su Gateway, que será la dirección IP del router que está conectado a la delegación
- Prueba que hay conectividad entre cualquier par de PCs de cualquier sede
- La dirección IP del puerto que gestiona la delegación debe ser la primera válida dentro de esa subred.
- Reasigna IPs a los PCs respetando que la 1ra IP es para el router.

Trabajo 2.2. VLSM: diseño y pruebas DCHP y BOOTP RIP v2.

2.2.4. Fase 3. Servidor de DHCP

- Instala ahora en cada delegación un servidor
- Asigne unos parámetros de red (IP, máscara,...) válidos dentro de la delegación
- Su IP debería ser la 2da válida dentro de la delegación
- Activa el servicio de DHCP de tal manera que entregue de forma automática unos parámetros de red válidos dentro de la delegación
- Asegúrate de que la 1ra IP que entregue no solape con el router ni con el propio servidor
- Asegúrate que el nº de IPs que asigna no sea superior al máximo que soporta la subred (según los cálculos que hemos hecho)
- RE-Asigna las IPs de los hosts de forma automática
- Comprueba el correcto funcionamiento de todo el montaje

IMPORTANTE:

- Representa gráficamente cada delegación
- Etiqueta convenientemente cada delegación con sus parámetros de red
- Etiqueta también los enlaces WAN incluyendo sus parámetros de red
- Etiqueta cada equipo con su IP y su máscara

2.2.5. Fase 4. BOOTP

- ¿Qué es BOOTP?
- ¿Para qué sirve?
- ¿Es anterior o posterior a DHCP?
- ¿Qué diferencias existen entre uno y otro?
- ¿Qué ventajas/desventajas incluye el uno frente al otro?
- ¿Cuál de los dos protocolos se usa en la actualidad?
- ...

Trabajo 2.2. VLSM: diseño y pruebas DCHP y BOOTP RIP v2.

Partiendo del ejemplo que hemos visto en clase de VLSM, diseña una red en PT en la que se plasmen exactamente los cálculos que ya hicimos.

Fase 1. Haz inicialmente un montaje en el que NO se usen routers 2.2.1

- conecta directamente los 3 switches de cada delegación entre sí
- Crea 2 hosts dentro de cada delegación, uno con la primera IP válida y otro con la última
- comprueba que hay sólo conectividad entre equipos del mismo departamento
- comprueba que NO hay conectividad entre equipos de diferente departamento

2.2.1

El ejercicio nos pide que a partir de la IP: 192.168.1.0/24 hagamos subneting con el fin de conseguir el número de hosts requeridos para cada departamento y, además, tiene que haber conectividad entre hosts del mismo departamento pero no puede haber conectividad entre hosts que se encuentren en departamentos distintos. En este caso tenemos 3 departamentos, **desarrollo**, **producción** y **administración**, y el número de host que nos pide cada departamento es 74, 52 y 28 respectivamente.

Como ya sabemos, la IP 192.168.1.0/24 es de **Clase C** cuya máscara de subred es 255.255.255.0.

Empezaremos con el departamento de **desarrollo** que nos pide que tengamos como mínimo 74 host. Para ello necesitaremos una subred cuyo tamaño sea mayor o igual que 74, y el tamaño que le hemos asignado es de 128. Para conseguir esto haremos subneting sobre la IP principal de forma que nos quedaría 192.168.1.0/25 lo que nos proporcionaría dos subredes de 128 cada una. Ahora tenemos dos subredes que son

- **Subred 1 (Desarrollo):** 192.168.1.0 - 192.168.1.127
 - **Subnet Mask:** 255.255.255.128

Ahora se nos pide que el departamento de **producción** tenga una capacidad de 52 hosts. Para conseguir esto haremos subnetting sobre la IP principal de forma que nos quedaría 192.168.1.0/26 lo que nos proporcionará cuatro subredes de 64 cada una, donde las 2 primeras subredes ya están asignadas al departamento de **desarrollo**.

- **Subred 1 (Desarrollo):** 192.168.1.0 - 192.168.1.127
 - **Subnet Mask:** 255.255.255.128
- **Subred 2 (Producción):** 192.168.1.128 - 192.168.1.191
 - **Subnet Mask:** 255.255.255.192

Por último, nos pide que el departamento de **administración** tenga una capacidad de 28 hosts. Repetiremos el procedimiento anterior con la diferencia que esta vez al hacer el subneting la red nos quedará 192.168.1.0/27 lo que nos proporcionará 8 subredes de 32 cada una, de las cuales una de ellas le pertenece al departamento de **administración**.

Trabajo 2.2. VLSM: diseño y pruebas DCHP y BOOTP RIP v2.

Una vez hemos hecho todos los cálculos de subnetting, el resultado final de la red será:

- **Subred 1 (Desarrollo):** 192.168.1.0 - 192.168.1.127
 - **Subnet Mask:** 255.255.255.128
 - **ID Subred:** 192.168.1.0
 - **Broadcast IP:** 192.168.1.127
 - **Host 1:** 192.168.1.1
 - **Último Host:** 192.168.1.126
- **Subred 2 (Producción):** 192.168.1.128 - 192.168.1.191
 - **Subnet Mask:** 255.255.255.192
 - **ID Subred:** 192.168.1.128
 - **Broadcast IP:** 192.168.1.191
 - **Host 1:** 192.168.1.129
 - **Último Host:** 192.168.1.190
- **Subred 3 (Administración):** 192.168.1.192 - 192.168.1.223
 - **Subnet Mask:** 255.255.255.224
 - **ID Subred:** 192.168.1.192
 - **Broadcast IP:** 192.168.1.223
 - **Host 1:** 192.168.1.193
 - **Último Host:** 192.168.1.222

2.2.1

Fase 1: Haz inicialmente un montaje en el que no se usen routers

- conecta directamente los 3 switches de cada delegación entre sí
- Crea 2 hosts dentro de cada delegación, uno con la primera IP válida y otro con la última

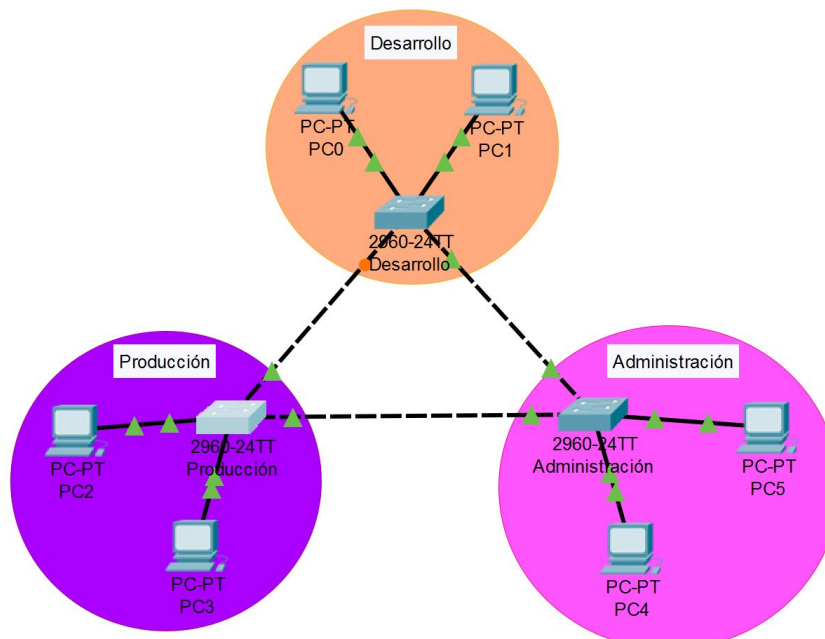
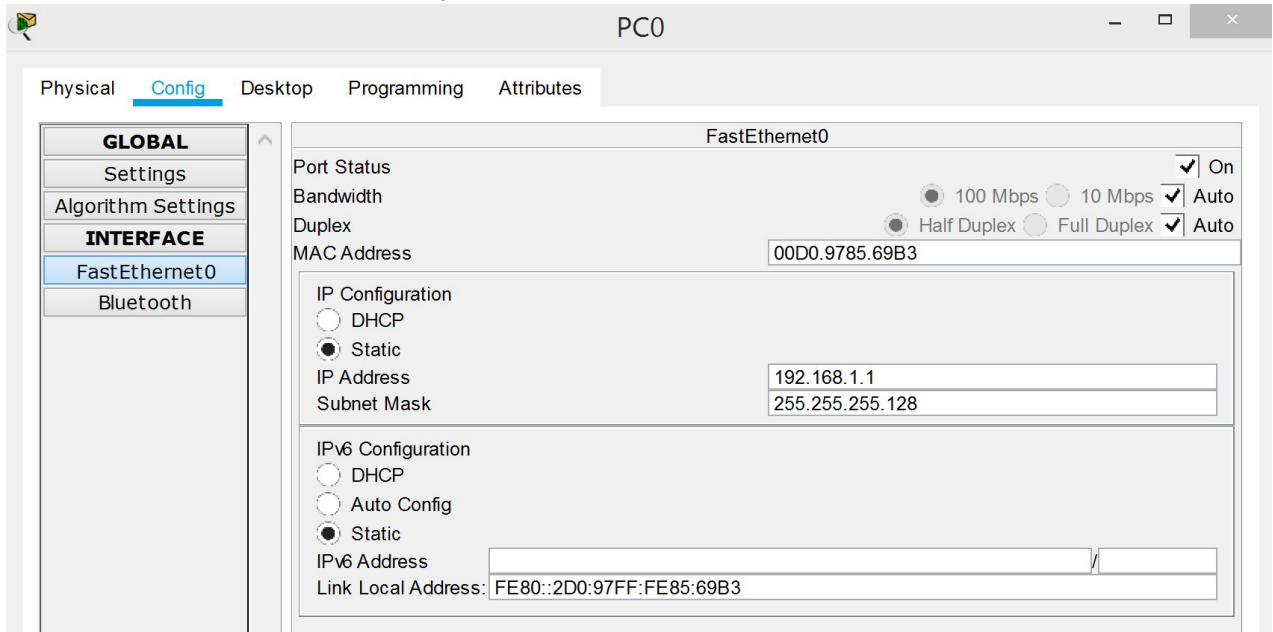


Fig. 2.2.1.a Montaje de la red

Trabajo 2.2. VLSM: diseño y pruebas DCHP y BOOTP RIP v2.

Crea 2 hosts dentro de cada delegación, uno con la primera IP y otro con la última

A continuación se adjuntan una serie de imágenes donde se muestra cada host de cada departamento con la primera IP y la última:



2.2.1

Fig. 2.2.1.b Host con la primera IP del departamento de Desarrollo

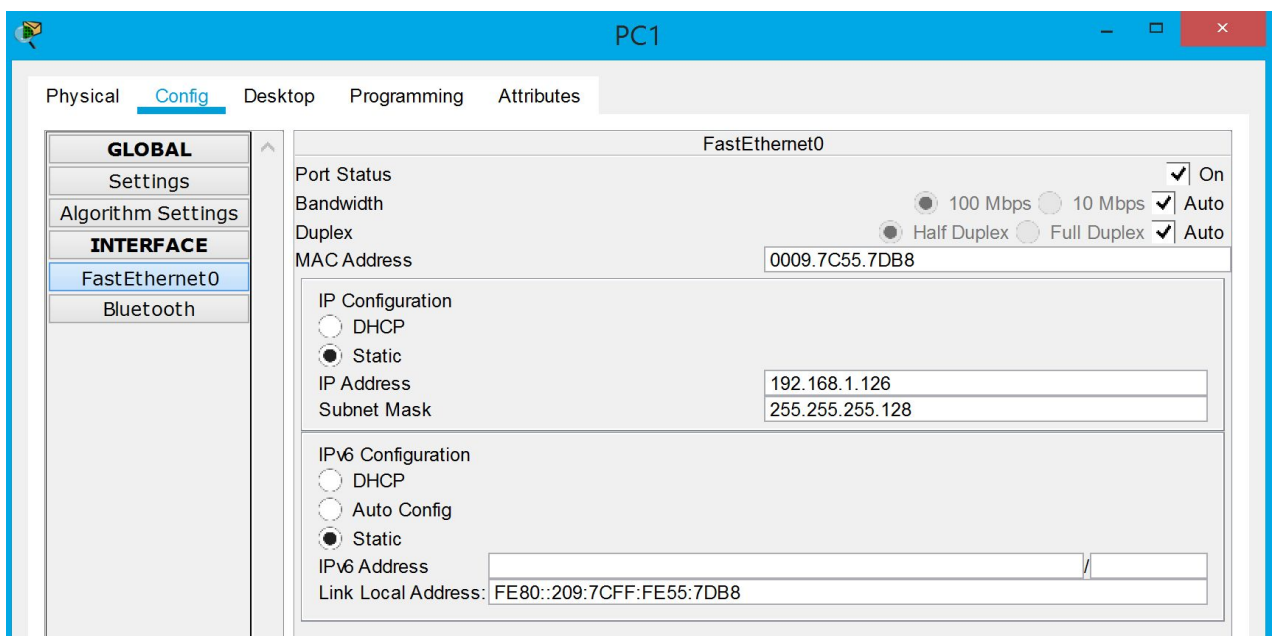
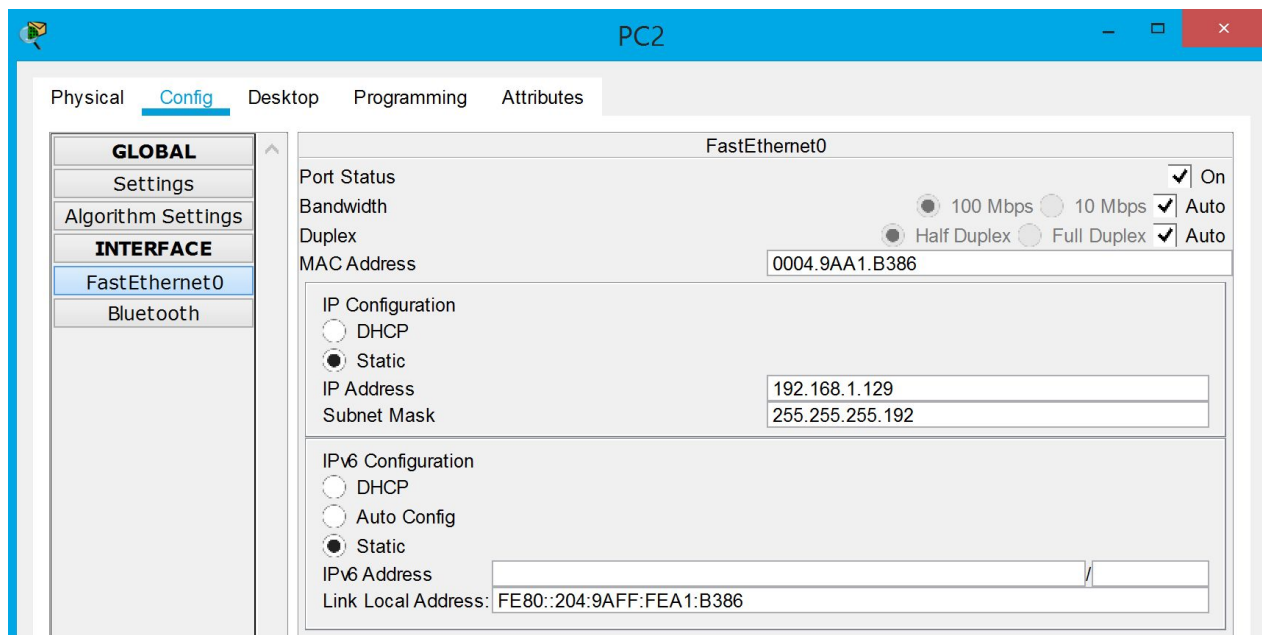


Fig. 2.2.1.c Host con la última IP del departamento de Desarrollo

Trabajo 2.2. VLSM: diseño y pruebas DCHP y BOOTP RIP v2.



2.2.1

Fig. 2.2.1.d Host con la primera IP del departamento de Producción

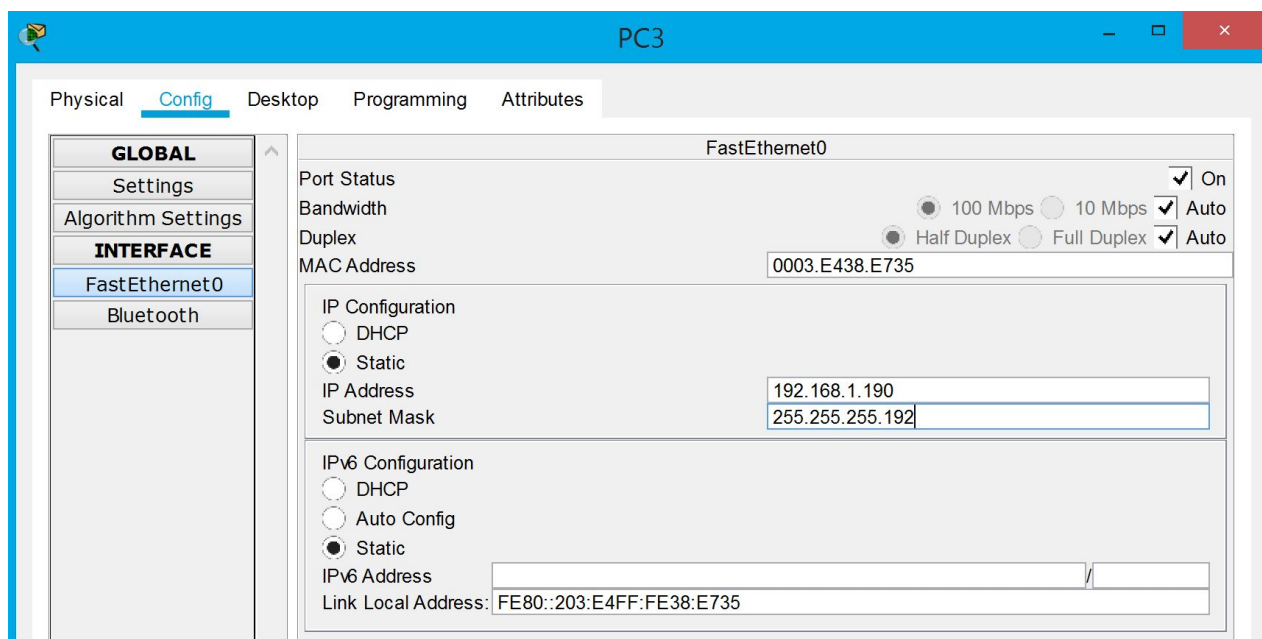


Fig. 2.2.1.e Host con la última Ip del departamento de Producción

Trabajo 2.2. VLSM: diseño y pruebas DCHP y BOOTP RIP v2.

Comprueba que hay sólo conectividad entre equipos del mismo departamento

2.2.1

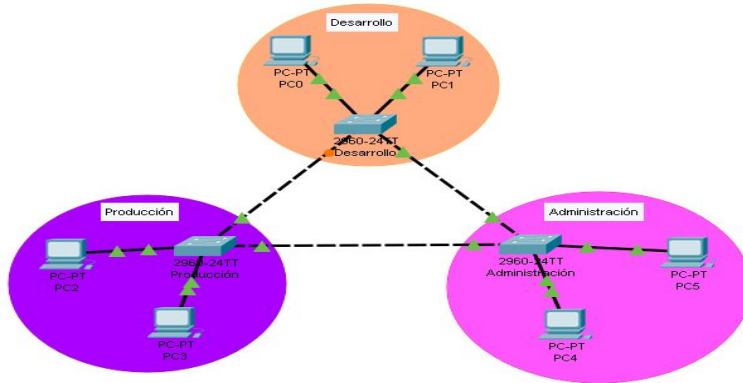


Fig. 2.2.1.f. Comprobación de conectividad

Comprueba que NO hay conectividad entre equipos de diferente departamento

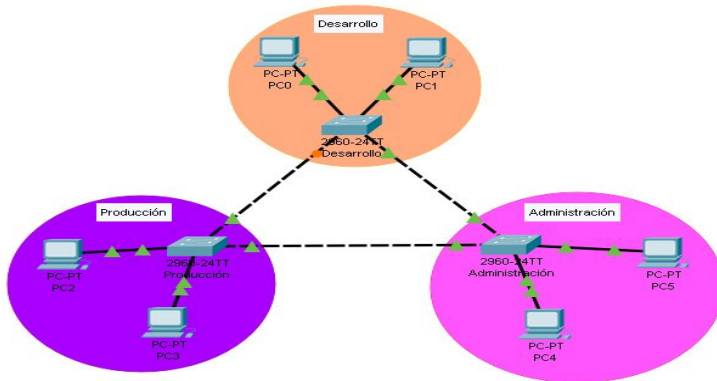


Fig. 2.2.1.g. Comprobación de no conectividad

Fase 1b. VLSM

- Configuración VLSM aula de clase
 1. Distribución del aula
 2. Desactivar Firewall
 3. Asignación de IP y máscara de subred a los PC
 4. Comprobar el correcto funcionamiento de la VLSM

2.2.2

1. Distribución del Aula

Para empezar debemos distribuir el aula en los tres sectores que se nos indica en el apartado anterior (**Desarrollo** **Producción** **Administración**). Véase **Figura 2.2.2.a**.



Figura 2.2.2.a Distribución del aula en sectores

A continuación para poder realizar las comprobaciones debemos desconectar todo el aula de la red medusa del centro (Circulo celeste **Figura 2.2.2.a**). Véase **Figura 2.2.2.b**.

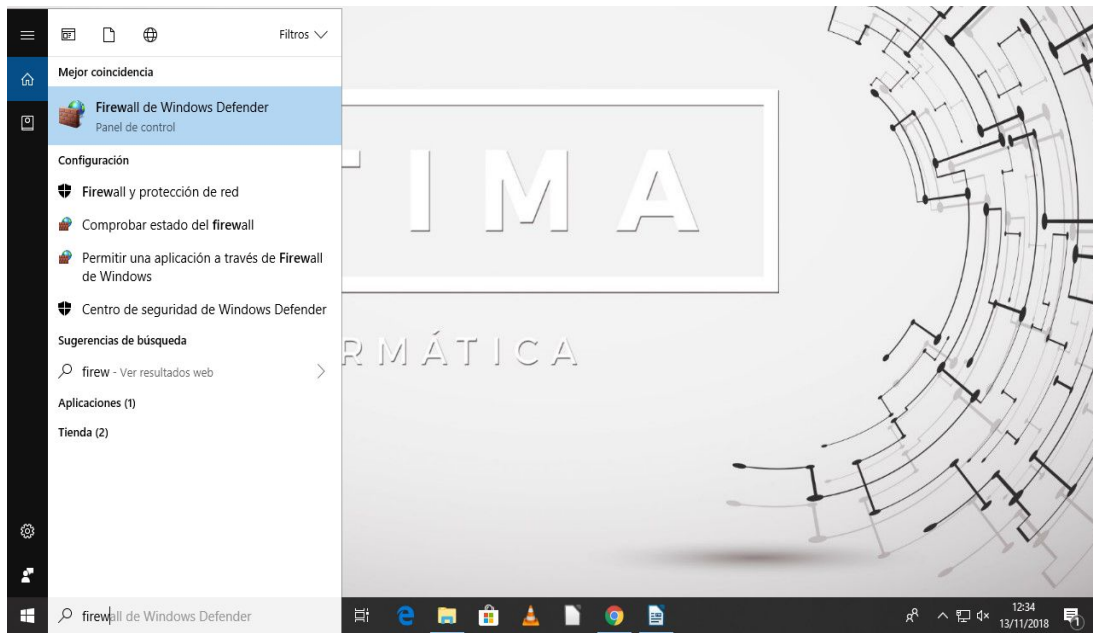


Figura 2.2.2.b Toma general Medusa en el aula

2. Desactivar el Firewall

Como último paso antes de comenzar las pruebas del correcto funcionamiento de la VLSM se debe desactivar el firewall de todos los PC que vayan a utilizarse para las comprobaciones. Este paso es imprescindible porque el firewall bloquea las comunicaciones con otros equipos.

Para ello debemos escribir en el explorador Firewall y nos aparecerá una opción llamada "Firewall de Windows Defender" y la seleccionamos. Véase **Figura 2.2.2.c**



2.2.2

Figura 2.2.2.c Buscando Firewall

Nos aparecerá la siguiente ventana y clicamos en Activar o desactivar el Firewall de Windows Defender: (**Figura 2.2.2.d**)

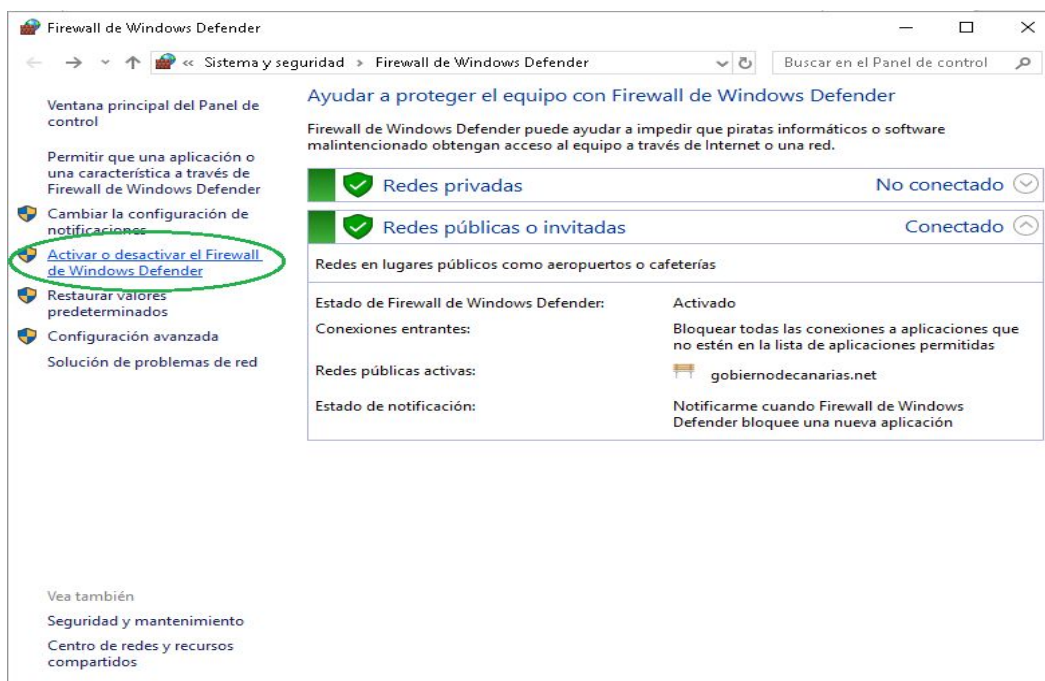


Figura 2.2.2.d Activar o desactivar el Firewall de Windows Defender

Aparecerá una ventana en la que se indica si el firewall se encuentra activado o no. En este caso está activo (indicado en color verde) por lo tanto hay que desactivarlo clickeando en las casillas indicadas en rojo en la **Figura 2.2.2.e**. Una vez realizado esto debe aparecer tal como la **Figura 2.2.2.f** y damos en “Aceptar”.

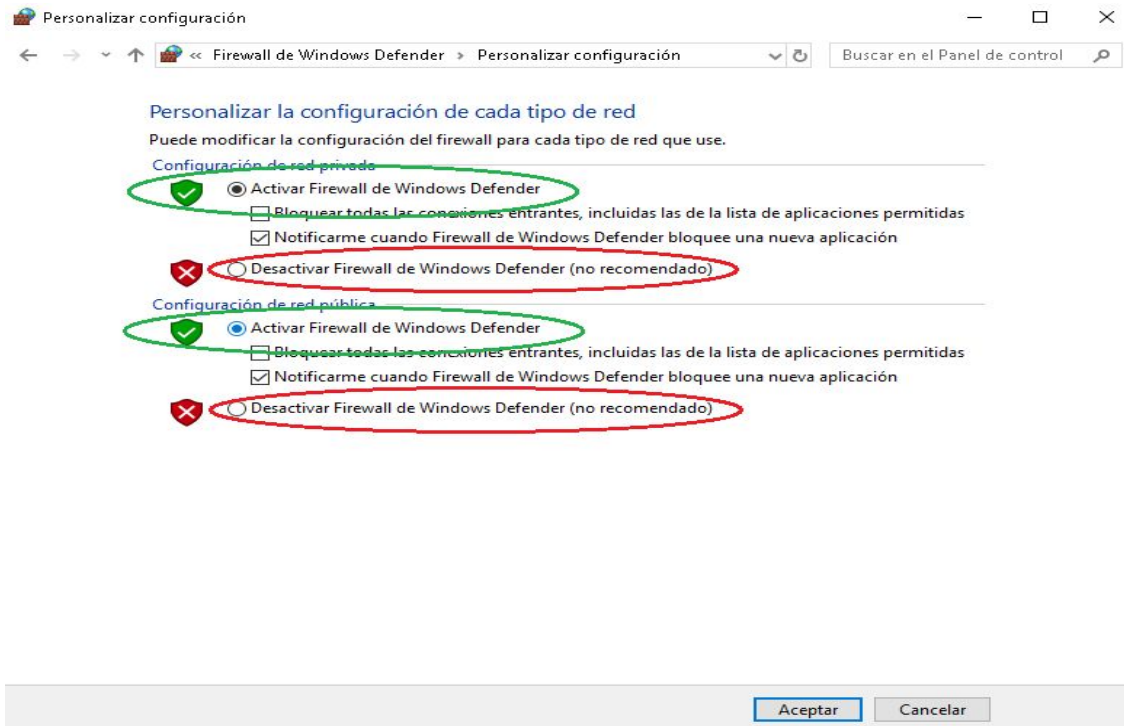


Figura 2.2.2.e Desactivar el Firewall de Windows Defender

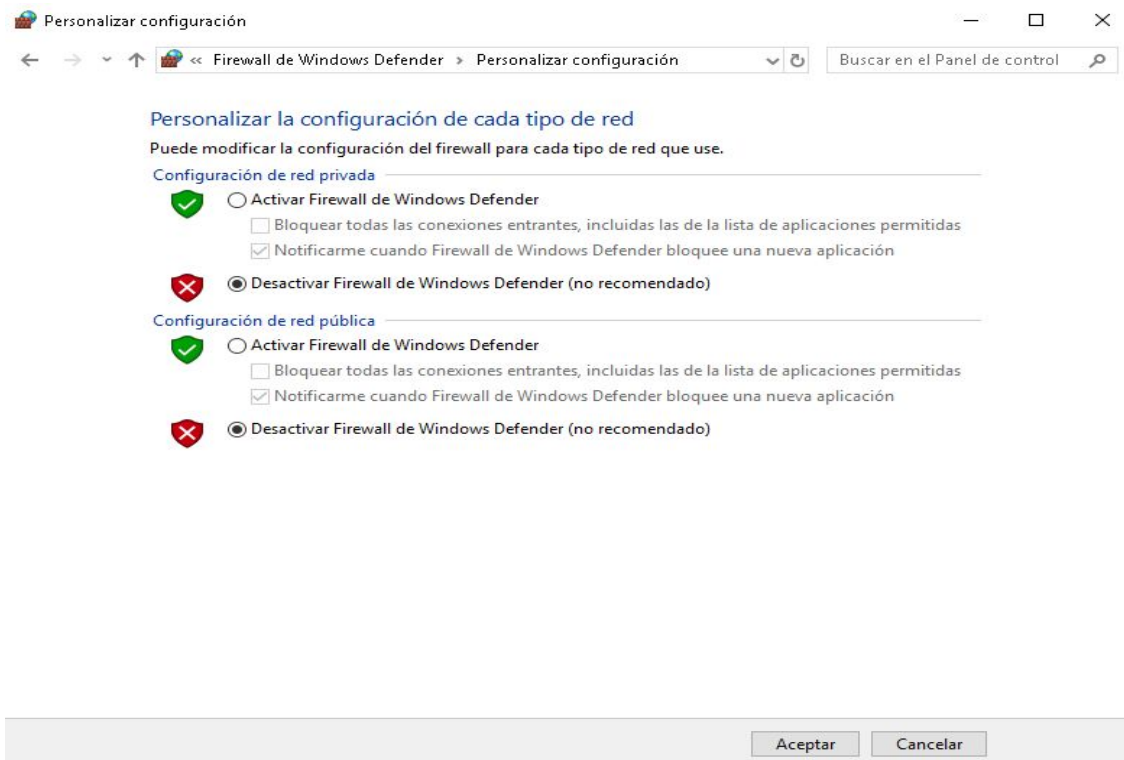


Figura 2.2.2.f Desactivado el Firewall de Windows Defender

3. Asignación de IP y máscara de subred a los PC

Los pasos para cambiar la IP y la máscara de subred son:

- Hacemos click derecho en el icono marcado en la **Figura 2.2.2.g** que se encuentra en la esquina inferior derecha del escritorio.

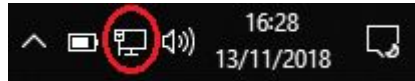


Figura 2.2.2.g Icono Red

2.2.2

- Seleccionamos la opción “Abrir Configuración de red e Internet” (**Figura 2.2.2.h**)

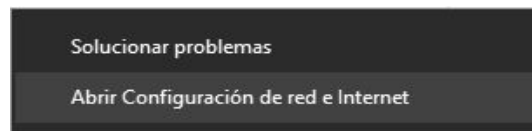


Figura 2.2.2.h Abrir Configuración de red e Internet

- Nos mostrará una ventana y seleccionamos “Cambiar opciones de adaptador” (**Figura 2.2.2.i**)

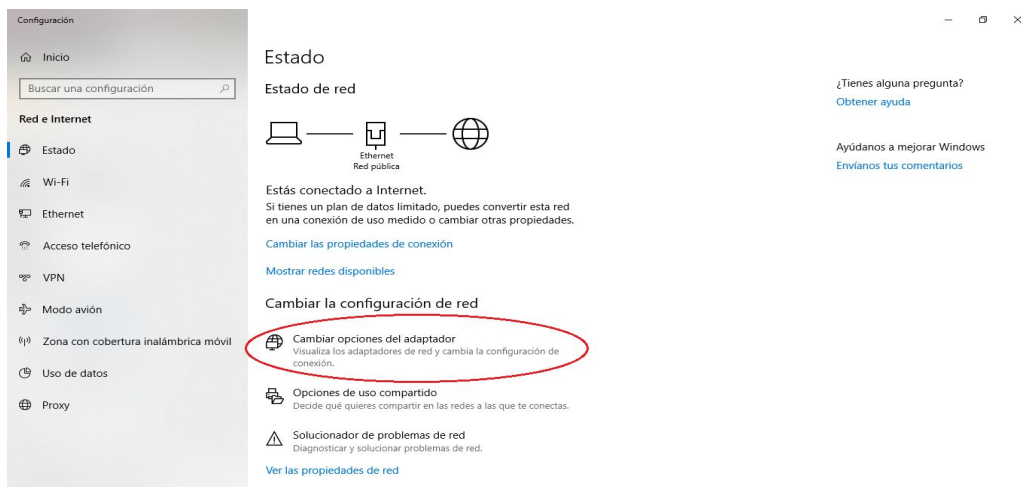


Figura 2.2.2.i Cambiar opciones de adaptador

- En el siguiente paso seleccionamos nuestro adaptador y hacemos click derecho y pinchamos en “Propiedades” (**Figura 2.2.2.j**)



Figura 2.2.2.j Propiedades del adaptador

- En la ventana emergente elegimos el apartado “Protocolo de Internet versión 4 (TCP/IPv4)” y clicamos en “Propiedades”. Véase **Figura 2.2.2.k**

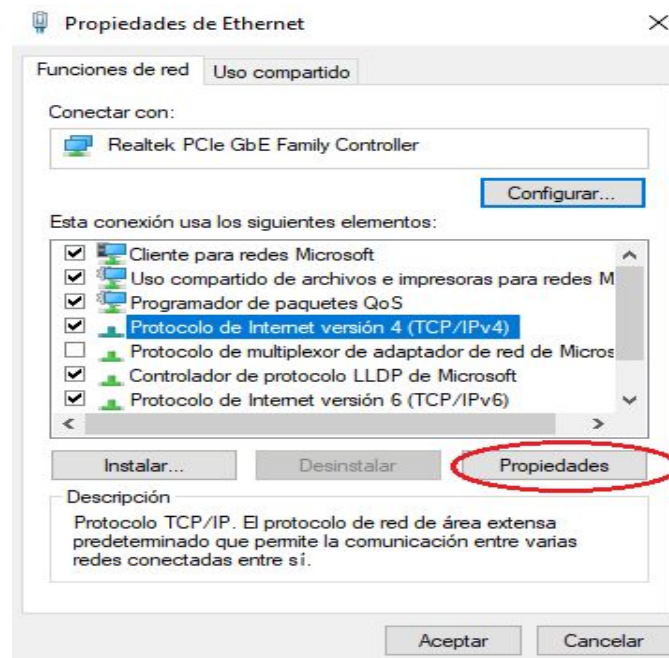


Figura 2.2.2.k Protocolo IPv4

- Entramos en las propiedades y seleccionamos “Usar la siguiente dirección IP” para poder darle de forma manual la IP y la máscara de subred correspondiente. Los demás campos no son necesarios para esta práctica. Véase **Figura 2.2.2.l**

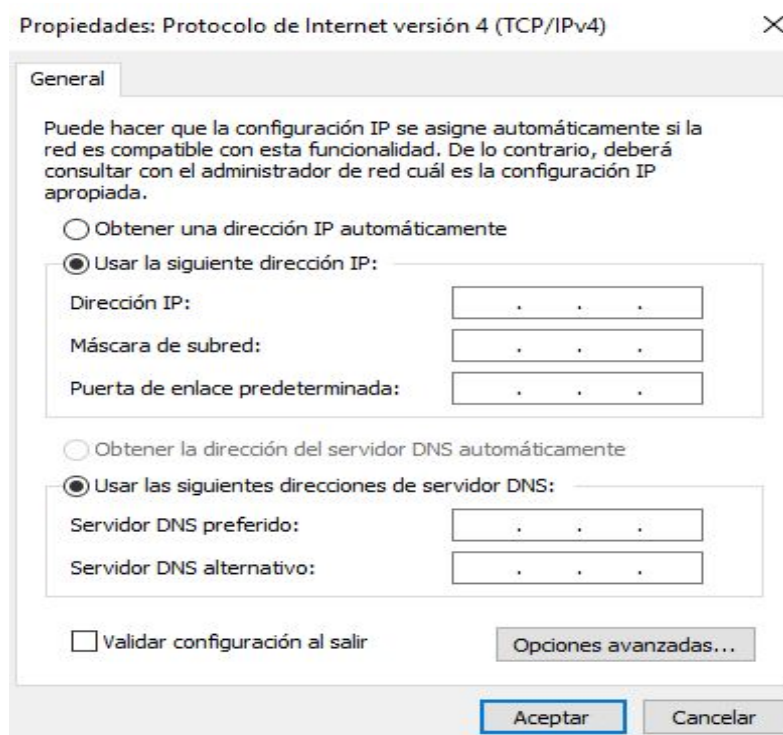


Figura 2.2.2.l Asignar IP y Máscara de Subred

Ya sabemos cómo asignar las IP y las máscaras de subred. Por tanto ya podemos dar IP a los PC de los distintos sectores.

Para realizar las pruebas utilizaremos dos PC de cada sector. Las IP que se les van a poner deben estar dentro del rango calculado en el apartado 2.2.1.

- **Sector de Desarrollo** tenemos estos 2 PC y sus IP:(**Figura 2.2.2.m**) y (**Figura 2.2.2.n**)

Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP: 192 . 168 . 1 . 1

Máscara de subred: 255 . 255 . 255 . 128

Puerta de enlace predeterminada: . . .

Obtener la dirección del servidor DNS automáticamente

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido: 8 . 8 . 8 . 8

Servidor DNS alternativo: 8 . 8 . 4 . 4

Validar configuración al salir

Opciones avanzadas...

Aceptar Cancelar

Figura 2.2.2.m IP y MS Desarrollo PC1

Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP: 192 . 168 . 1 . 126

Máscara de subred: 255 . 255 . 255 . 128

Puerta de enlace predeterminada: . . .

Obtener la dirección del servidor DNS automáticamente

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido: . . .

Servidor DNS alternativo: . . .

Validar configuración al salir

Opciones avanzadas...

Aceptar Cancelar

Figura 2.2.2.n IP y MS Desarrollo PC2

- **Sector de Producción** tenemos estos 2 PC y sus IP:(**Figura 2.2.2.ñ**) y (**Figura 2.2.2.o**)

Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP: 192 . 168 . 1 . 129

Máscara de subred: 255 . 255 . 255 . 192

Puerta de enlace predeterminada: . . .

Obtener la dirección del servidor DNS automáticamente

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido: . . .

Servidor DNS alternativo: . . .

Validar configuración al salir

Opciones avanzadas...

Aceptar Cancelar

Figura 2.2.2.ñ IP y MS Producción PC1

Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP: 192 . 168 . 1 . 130

Máscara de subred: 255 . 255 . 255 . 192

Puerta de enlace predeterminada: 192 . 168 . 1 . 128

Obtener la dirección del servidor DNS automáticamente

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido: . . .

Servidor DNS alternativo: . . .

Validar configuración al salir

Opciones avanzadas...

Aceptar Cancelar

Figura 2.2.2.o IP y MS Producción PC2

2.2.2

- **Sector de Administración** tenemos estos 2 PC y sus IP: (**Figura 2.2.2.p**) y (**Figura 2.2.2.q**)

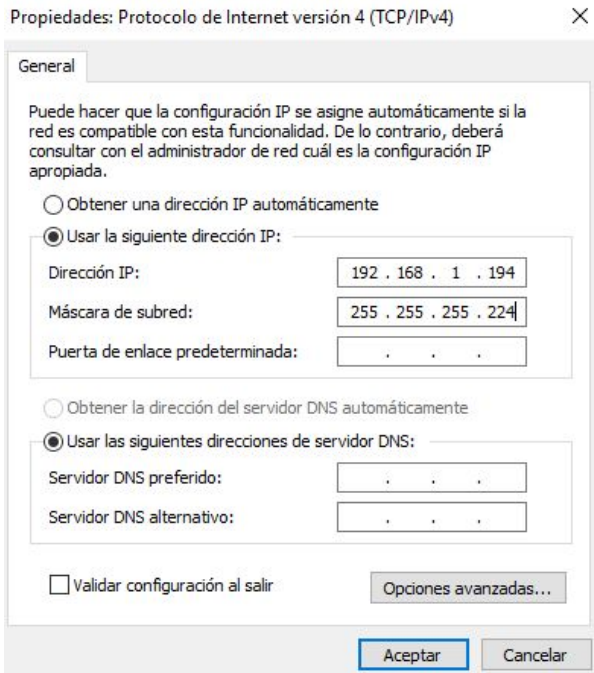


Figura 2.2.2.p IP y MS Administración PC1

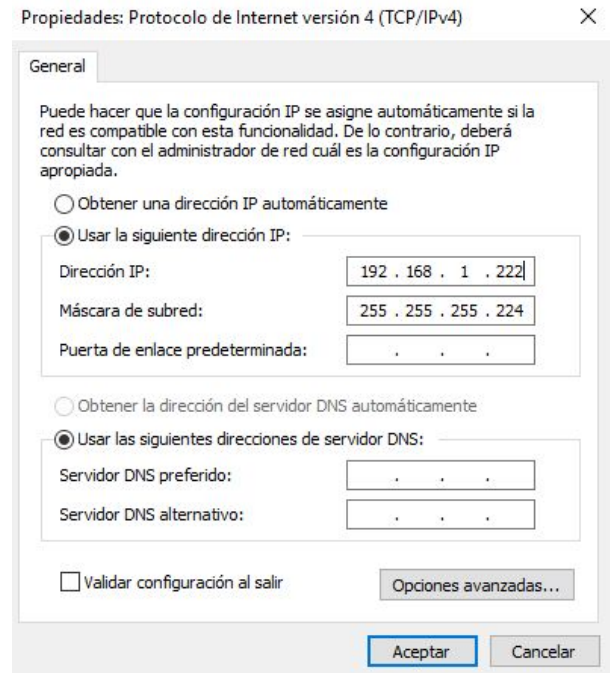


Figura 2.2.2.q IP y MS Administración PC2

2.2.2

Hemos asignado las IP y sus máscaras a los PC, es momento de realizar las comprobaciones pertinentes para confirmar el correcto funcionamiento de la VLSM.

Para esto en cada PC debemos entrar a su consola escribiendo CMD en el explorador y seleccionando "Símbolo del sistema" y entramos a la consola.

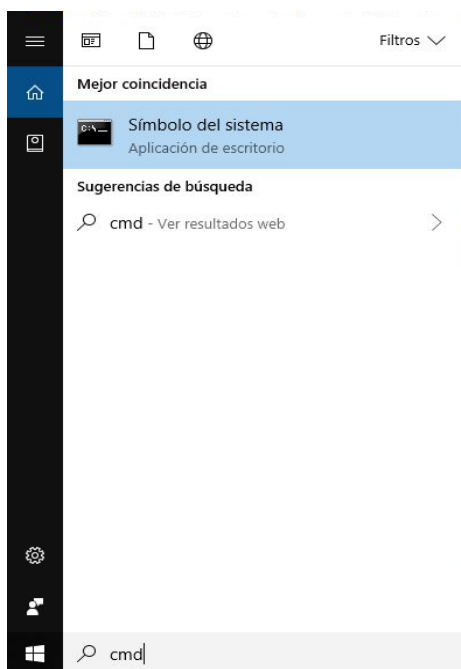


Figura 2.2.2.r Símbolo del sistema

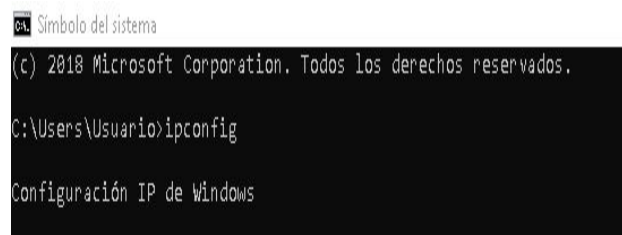


Figura 2.2.2.s Símbolo del sistema

Realizaremos las comprobaciones por sectores. Comprobamos que la ip que pusimos en el paso anterior esta bien asignada al igual que su máscara de subred utilizando el comando "ipconfig". Lo siguiente será comprobar la conexión entre los PC del mismo sector y los que estén fuera de este. Para ello utilizamos el comando "ping" seguido de la IP del PC al que queremos contactar.

Desarrollo

- PC1 (192.168.1.1)

Comprobamos IP, máscara de subred y hacemos "ping" a PC2 de Desarrollo. Como se observa se envían 4 paquetes y recibe 4 por lo que la conexión es correcta (**Figura 2.2.2.t**).

2.2.2

```
ca. Símbolo del sistema
(c) 2018 Microsoft Corporation. Todos los derechos reservados.
C:\Users\Usuario>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::fd8c:ae73:4fca:2a63%5
    Dirección IPv4. . . . . : 192.168.1.1
    Máscara de subred. . . . . : 255.255.255.128
    Puerta de enlace predeterminada. . . . . :

C:\Users\Usuario>ping 192.168.1.126

Haciendo ping a 192.168.1.126 con 32 bytes de datos:
Respuesta desde 192.168.1.126: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.126: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.126: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.126: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.126:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Usuario>
```

Figura 2.2.2.t Comprobar IP y ping a PC2 Desarrollo

A continuación realizamos "ping" a un PC de otro sector en este caso PC1 de Producción.(**Figura 2.2.2.u**). Se observa que se envían 4 paquetes y se reciben 0 por lo que no existe comunicación por lo que la VLSM funciona como debería, ya que no queremos que se puedan comunicar entre los distintos sectores por ahora.

```
C:\Users\Usuario>ping 192.168.1.129

Haciendo ping a 192.168.1.129 con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.

Estadísticas de ping para 192.168.1.129:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Users\Usuario>
```

Figura 2.2.2.u Ping a PC1 Producción

Para corroborar que no existe comunicación entre Desarrollo y Administración haremos “ping” a PC1 de Administración. (Figura 2.2.2.v). Todo funciona como debería.

```
C:\Users\Usuario>ping 192.168.1.194

Haciendo ping a 192.168.1.194 con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.

Estadísticas de ping para 192.168.1.194:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
      (100% perdidos),

C:\Users\Usuario>
```

2.2.2

Figura 2.2.2.v Ping a PC1 Administración

Realizamos este proceso con todos los PC para comprobar que está todo en orden.

- PC2 (192.168.1.126)

```
Símbolo del sistema

C:\Users\Usuario>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::c5a0:11bb:1259:3bdf%3
    Dirección IPv4. . . . . : 192.168.1.126
    Máscara de subred. . . . . : 255.255.255.128
    Puerta de enlace predeterminada. . . . . :

C:\Users\Usuario>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
      (0% perdidos),
    tiempos aproximados de ida y vuelta en milisegundos:
      Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Usuario>ping 192.168.1.129

Haciendo ping a 192.168.1.129 con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.

Estadísticas de ping para 192.168.1.129:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
      (100% perdidos),

C:\Users\Usuario>
```

Figura 2.2.2.w Ipconfig, Ping PC1 Desarrollo y ping PC1 Producción

Producción

- PC1 (192.168.1.129)

```
C:\Users\Usuario>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::7cf3:20d0:6d73:34de%4
    Dirección IPv4. . . . . : 192.168.1.129
    Máscara de subred . . . . . : 255.255.255.192
    Puerta de enlace predeterminada . . . . . :

C:\Users\Usuario>ping 192.168.1.130

Haciendo ping a 192.168.1.130 con 32 bytes de datos:
Respuesta desde 192.168.1.130: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.130: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.130: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.130: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.130:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Usuario>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

2.2.2

Figura 2.2.2.x Ipconfig, Ping PC2 Producción y ping PC1 Desarrollo

- PC2 (192.168.1.130)

```
Símbolo del sistema
Microsoft Windows [Versión 10.0.17134.345]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::fd1a:e865:f8f7:f20c%3
    Dirección IPv4. . . . . : 192.168.1.130
    Máscara de subred . . . . . : 255.255.255.192
    Puerta de enlace predeterminada . . . . . : 192.168.1.128

C:\Users\Usuario>ping 192.168.1.129

Haciendo ping a 192.168.1.129 con 32 bytes de datos:
Respuesta desde 192.168.1.129: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.129: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.129: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.129: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.129:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Usuario>ping 192.168.1.194

Haciendo ping a 192.168.1.194 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.1.130: Host de destino inaccesible.
Respuesta desde 192.168.1.130: Host de destino inaccesible.

Estadísticas de ping para 192.168.1.194:
    Paquetes: enviados = 4, recibidos = 2, perdidos = 2
    (50% perdidos),

C:\Users\Usuario>
```

2.2.2

Figura 2.2.2.y Ipconfig, Ping PC1 Producción y ping PC1 Administración

Administración

- PC1 (192.168.1.194)

```
C:\Users\Usuario>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::3d38:6013:ec8d:b3bb%3
    Dirección IPv4. . . . . : 192.168.1.194
    Máscara de subred . . . . . : 255.255.255.224
    Puerta de enlace predeterminada . . . . . : 192.168.1.193

C:\Users\Usuario>ping 192.168.1.222

Haciendo ping a 192.168.1.222 con 32 bytes de datos:
Respuesta desde 192.168.1.222: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.222: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.222: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.222: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.222:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Usuario>ping 192.168.1.129

Haciendo ping a 192.168.1.129 con 32 bytes de datos:
Respuesta desde 192.168.1.194: Host de destino inaccesible.
Respuesta desde 192.168.1.194: Host de destino inaccesible.
Respuesta desde 192.168.1.194: Host de destino inaccesible.
Respuesta desde 192.168.1.194: Host de destino inaccesible.

Estadísticas de ping para 192.168.1.129:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
```

2.2.2

Figura 2.2.2.z Ipconfig, Ping PC2 Administración y ping PC1 Producción

- PC2 (192.168.1.222)

```
C:\Users\Usuario>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::3423:238b:cce8:8635%5
    Dirección IPv4. . . . . : 192.168.1.222
    Máscara de subred . . . . . : 255.255.255.224
    Puerta de enlace predeterminada . . . . . : 192.168.1.193

C:\Users\Usuario>ping 192.168.1.194

Haciendo ping a 192.168.1.194 con 32 bytes de datos:
Respuesta desde 192.168.1.194: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.194: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.194: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.194: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.194:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Usuario>ping 192.168.1.130

Haciendo ping a 192.168.1.130 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.1.222: Host de destino inaccesible.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.1.222: Host de destino inaccesible.

Estadísticas de ping para 192.168.1.130:
    Paquetes: enviados = 4, recibidos = 2, perdidos = 2
    (50% perdidos).
```

2.2.2

Figura 2.2.2.AA Ipconfig, Ping PC1 Administración y ping PC2 Producción

Ya hemos podido comprobar que toda la red VLSM funciona correctamente.

Fase 2. Uso de routers

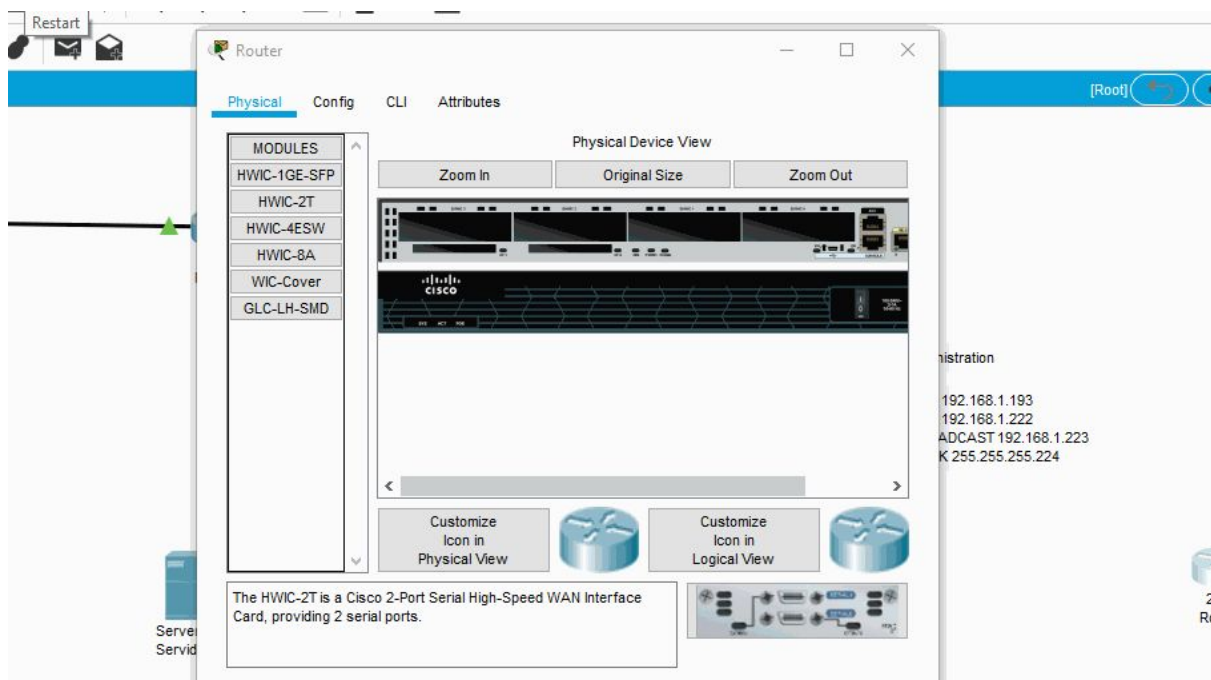
- Usa routers 2901
- Añade a cada router una tarjeta HWIC-2T
- Activa RIPv2 en todos los routers
- Indica en RIPv2 la dirección de red a la que están conectados.
- Configura la dirección IP y la máscara de subred de cada una de las bocas que tiene cada router
- Configura la dirección IP y la máscara de subred de cada uno de los enlaces WAN
- Asigna a cada uno de los PCs la dirección de su Gateway, que será la dirección IP del router que está conectado a la delegación
- Prueba que hay conectividad entre cualquier par de PCs de cualquier sede
- La dirección IP del puerto que gestiona la delegación debe ser la primera válida dentro de esa subred.
- Reasigna IPs a los PCs respetando que la 1ra IP es para el router.

2.2.3

Para explicar el uso de routers usaremos routers 2901



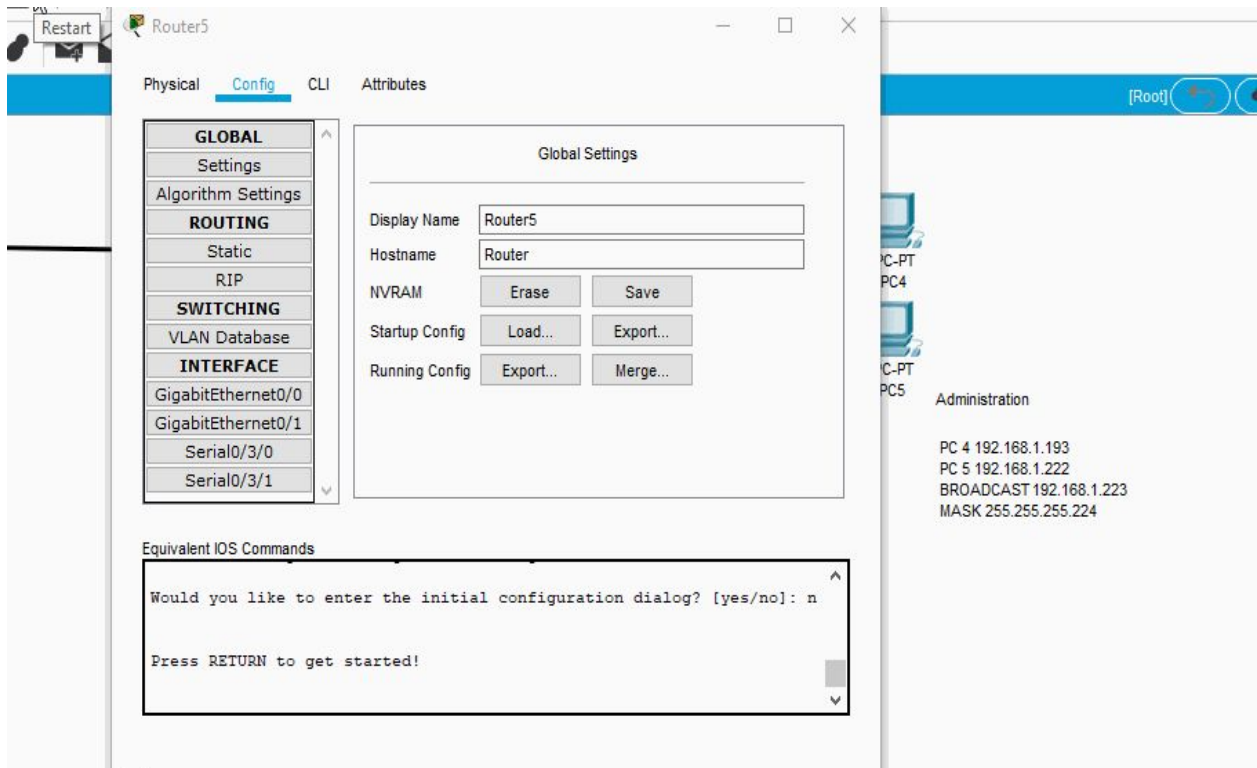
El primer paso para que el router funcione es ponerle una tarjeta HWIC-2T mientras este apagado como se muestra en el siguiente Gif



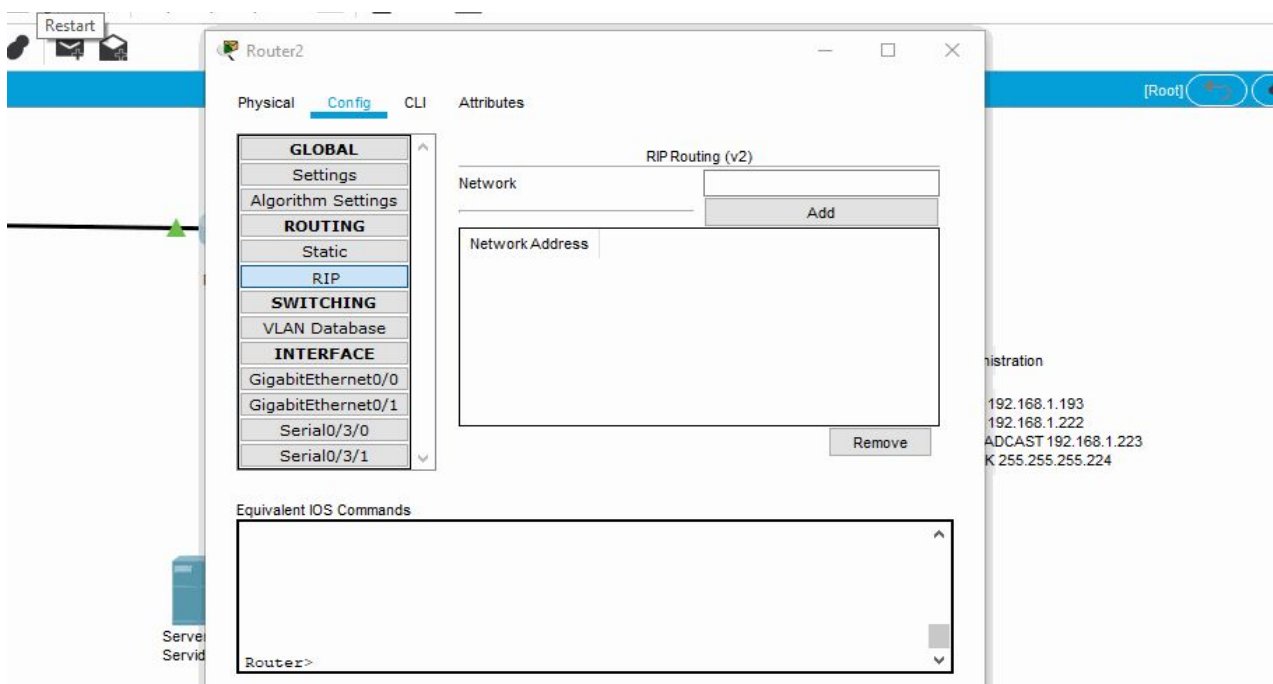
Ahora mostraremos cómo activar el RIPv2 en un router:

-Encendemos el router entramos en config en el menú pinchamos en RIP notamos que solo dice RIP routing.

-Para cambiarlo simplemente vamos al CLI y ponemos **versión 2** y comprobamos que pone (ver 2) al lado de RIP routing.

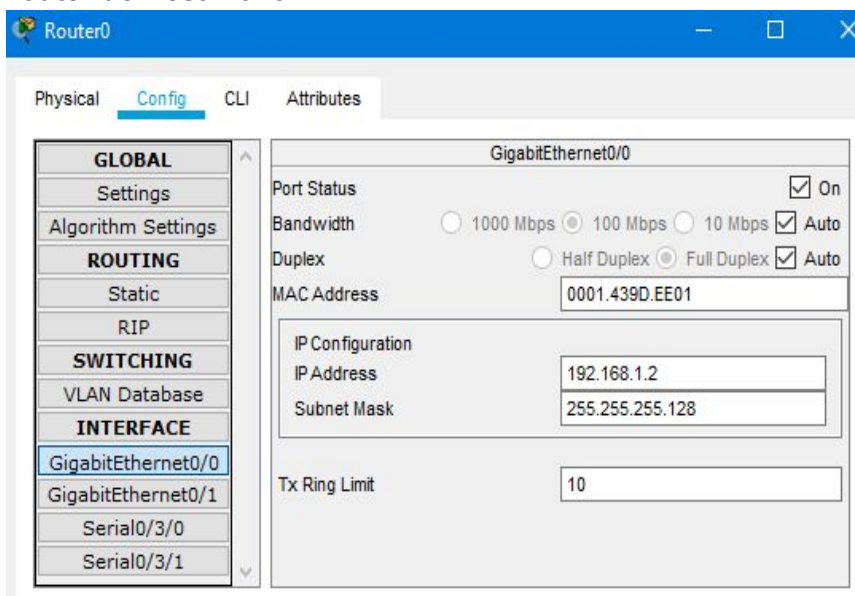


-Hecho esto vamos a poner en RIPv2 la dirección de red a la que nos vamos a conectar (ponemos esta misma dirección en los 3 routers)



-Ahora asignaremos las IP correspondientes y sus máscaras a cada router en cada una de sus bocas así como en sus enlaces WAN(la boca serial se usarán para las ip y máscaras WAN mientras que la boca Gigabit será la ip del router que posteriormente será la Gateway de los pc según su departamento .

Router de Desarrollo:



2.2.3

Figura 2.2.3.a IP y máscara del router de desarrollo (boca Gigabit 0/0)

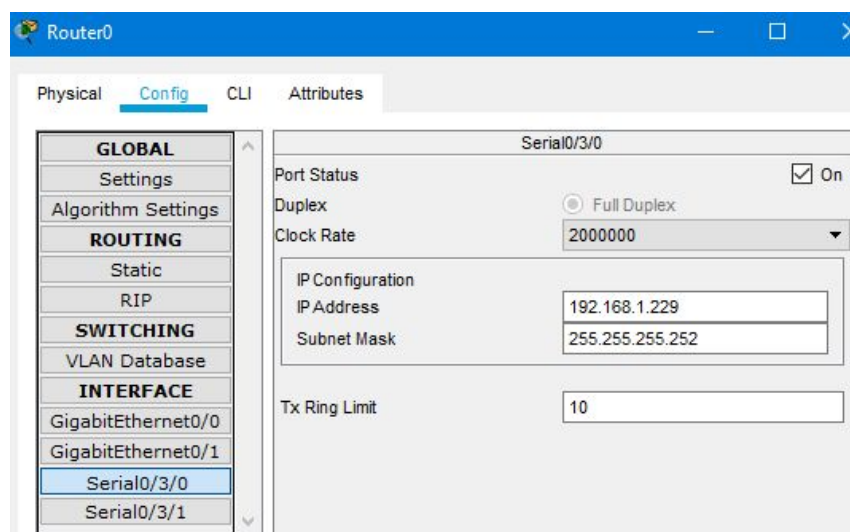


Figura 2.2.3.b IP y máscara del router de desarrollo (boca serial 0/3/0)

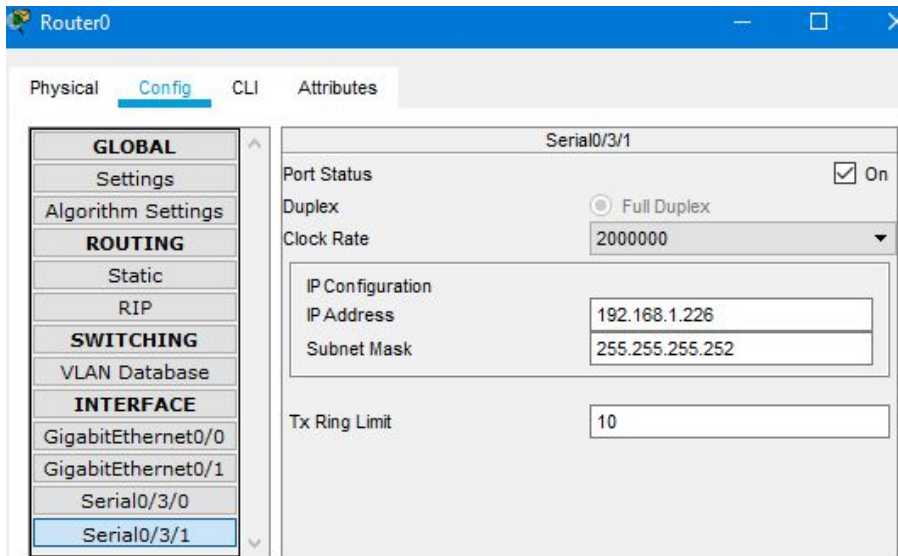


Figura 2.2.3.c IP y máscara del router de desarrollo (boca serial 0/3/1)

Router de Producción:

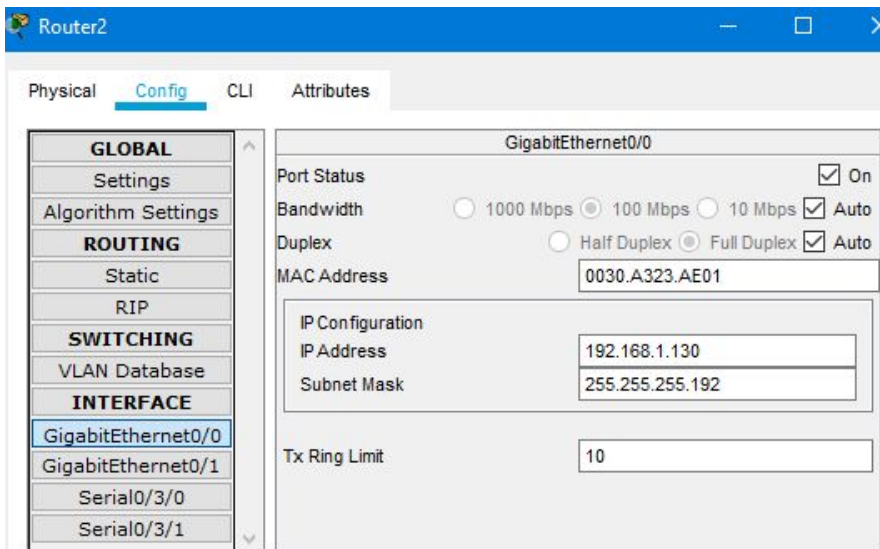


Figura 2.2.3.d IP y máscara del router de produccion (boca gigabit 0/0)

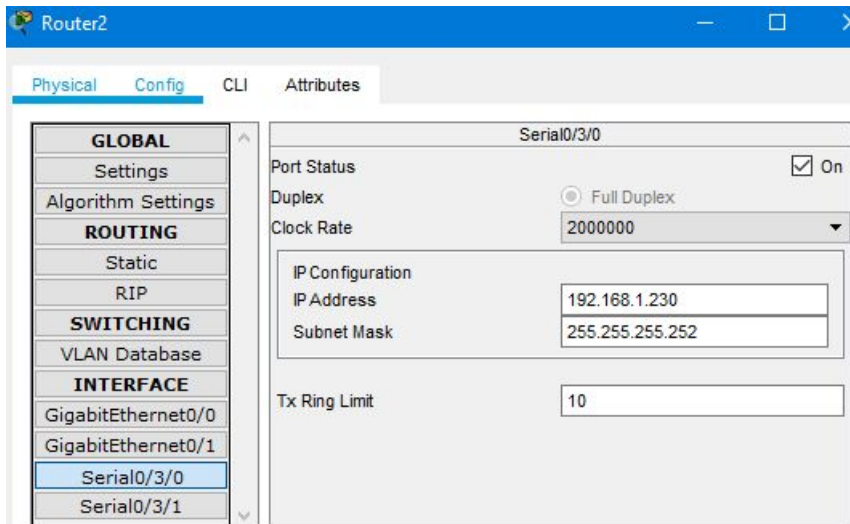


Figura 2.2.3.e IP y máscara del router de produccion (boca serial 0/3/0)

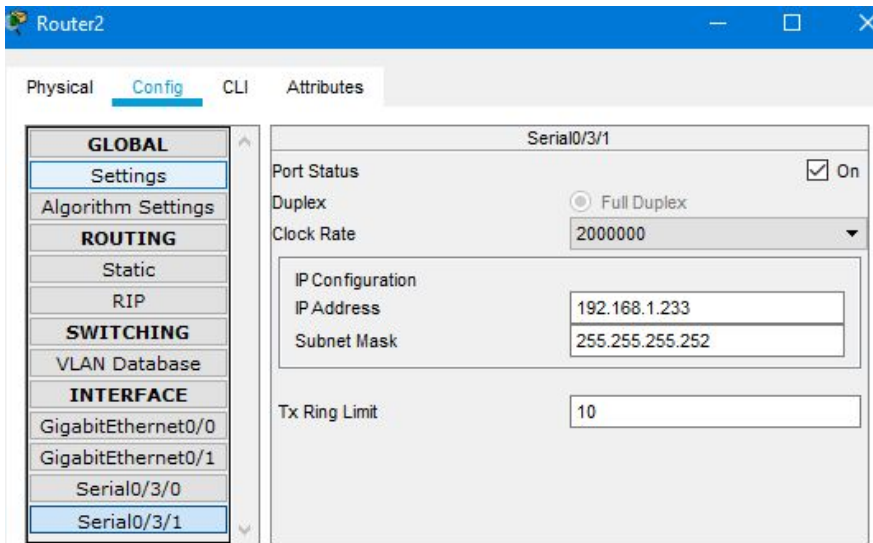


Figura 2.2.3.f IP y máscara del router de producción (boca serial 0/3/1)

Router de Administración:

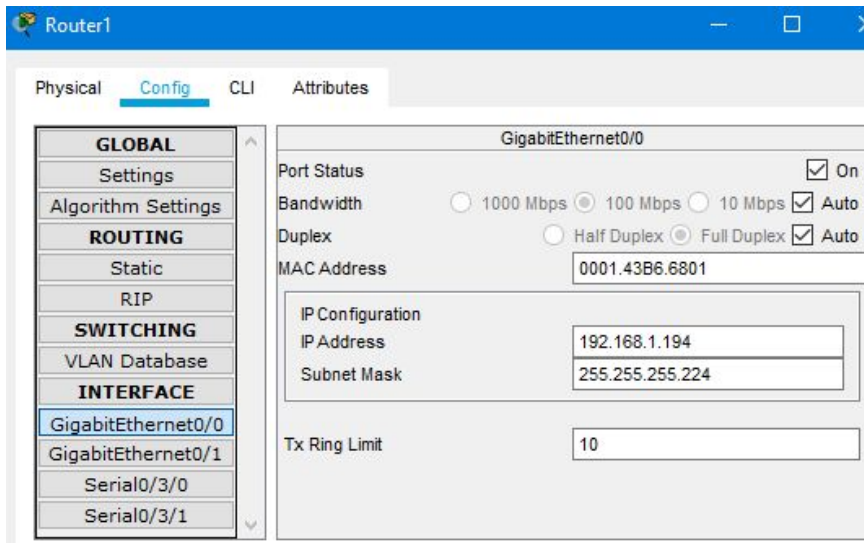


Figura 2.2.3.g IP y máscara del router de administracion (boca gigabit 0/0)

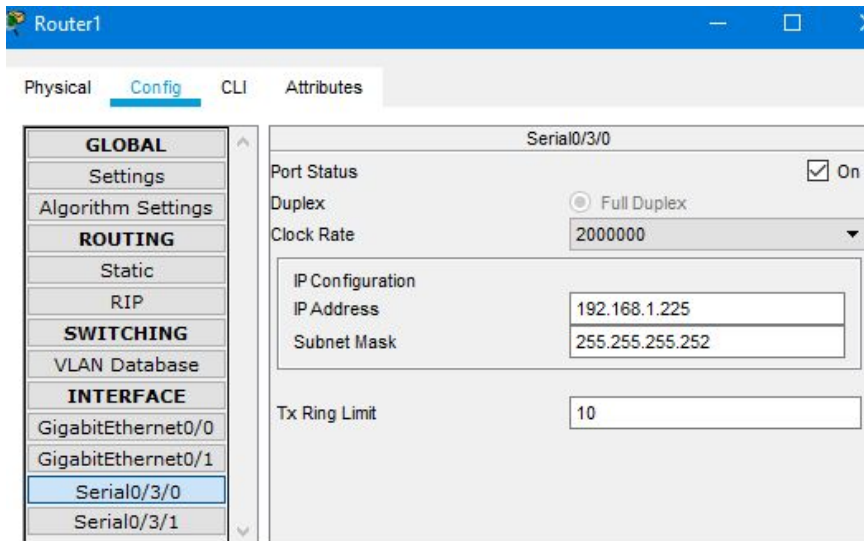


Figura 2.2.3.h IP y máscara del router de administracion (boca serial 0/3/0)

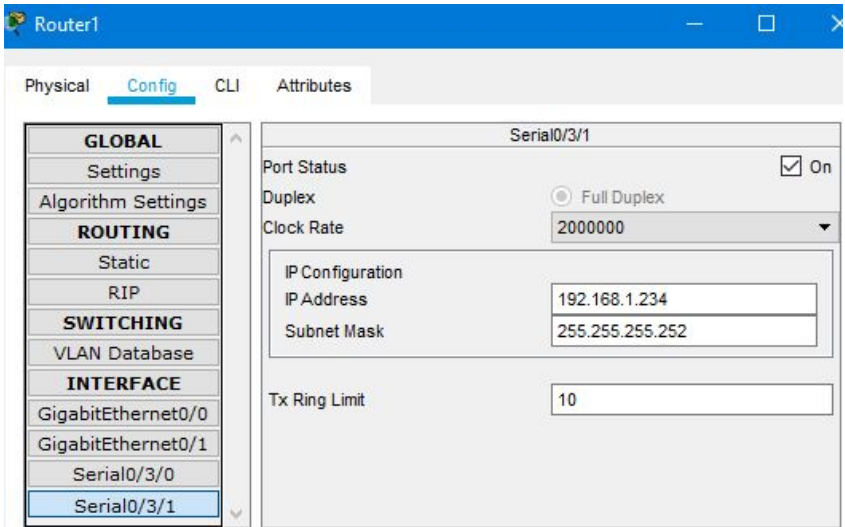


Figura 2.2.3.i IP y máscara del router de administración (boca serial 0/3/1)

-Una vez asignadas las IP y las máscaras en los routers asignaremos la Gateway a cada pc de cada departamento que será la ip del router de la boca Gigabit que está conectada al Switch.

Gateway Desarrollo:

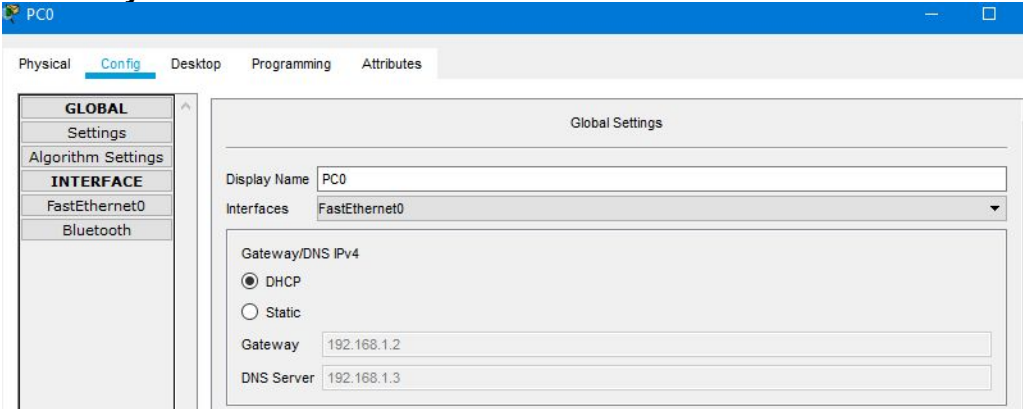


Figura 2.2.3.j Gateway de desarrollo

Gateway Producción:

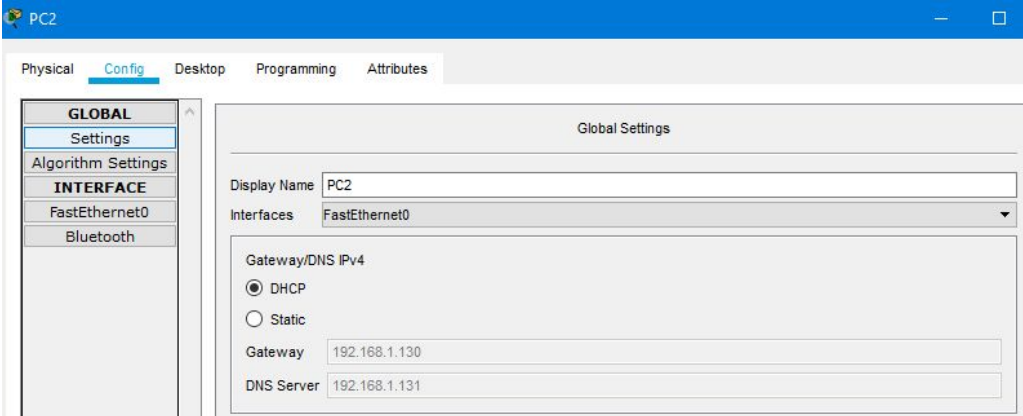
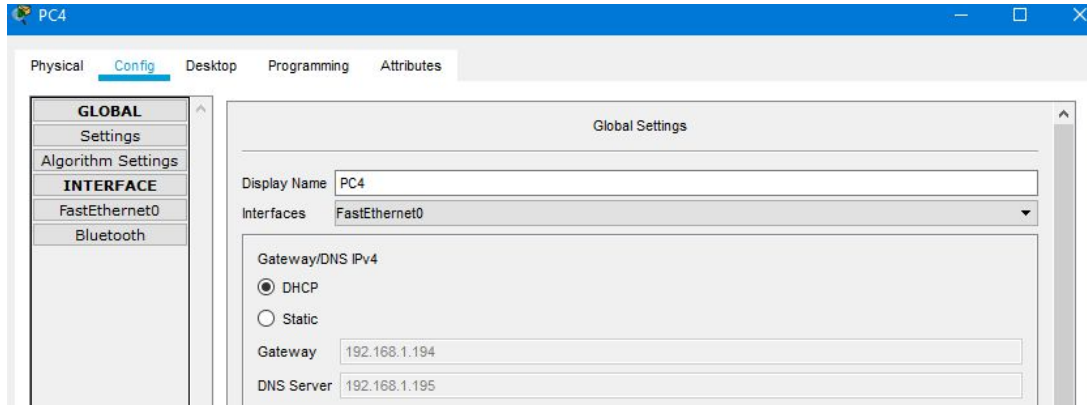


Figura 2.2.3.k Gateway de producción

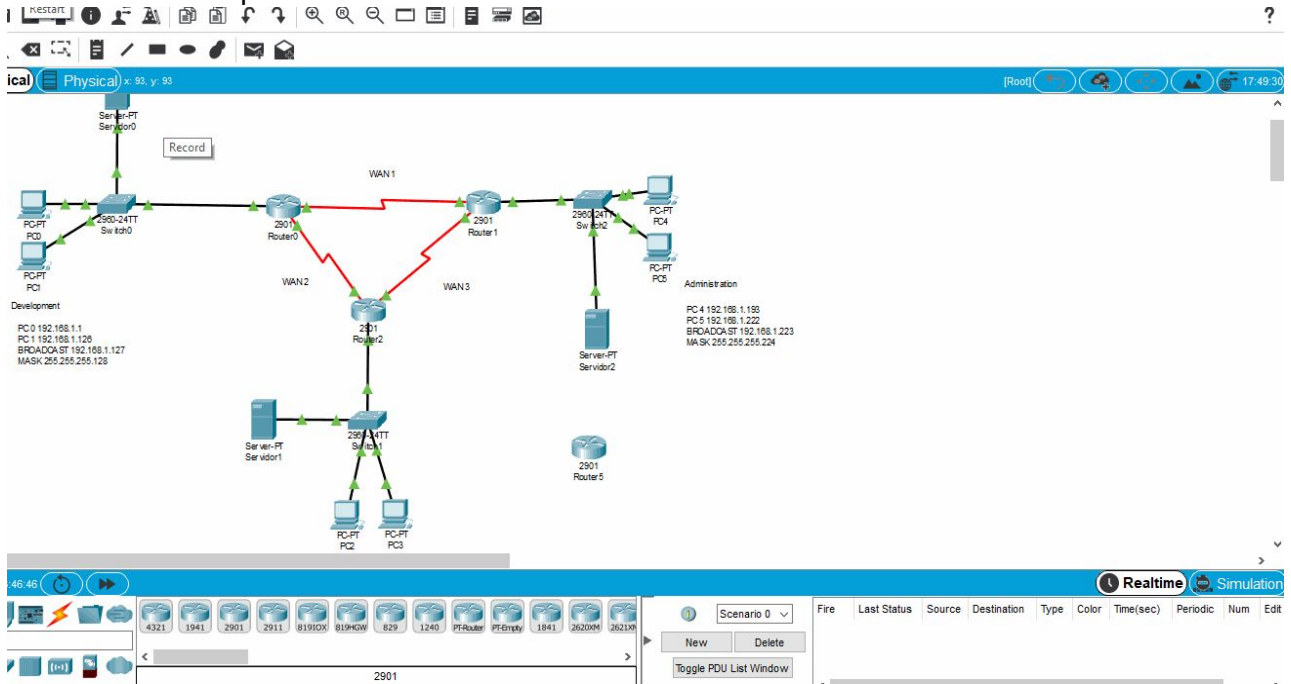
Gateway Administración:



2.2.3

Figura 2.2.3.1 Gateway de administración

-Por último vamos a comprobar la conectividad mandando un ping desde dos sedes distintas en este caso de producción a administración.



Fase 3. Servidor de DHCP

1. Instala ahora en cada delegación un servidor
2. Asígnale unos parámetros de red (IP, máscara,...) válidos dentro de la delegación
3. Su IP debería ser la 2da válida dentro de la delegación
4. Activa el servicio de DHCP de tal manera que entregue de forma automático unos parámetros de red válidos dentro de la delegación
5. Asegúrate de que la 1ra IP que entregue no solape con el router ni con el propio servidor
6. Asegúrate que el nº de IPs que asigna no sea superior al máximo que soporta la subred (según los cálculos que hemos hecho)
7. RE-Asigna las IPs de los hosts de forma automática
8. Comprueba el correcto funcionamiento de todo el montaje

2.2.4

El protocolo DHCP y su funcionamiento

Con el rápido crecimiento de TCP/IP (Trasmision Control Protocol/Internet Protocol), que es un método de transmisión para comunicarse en Internet, se necesitan algunas herramientas para administrar automáticamente algunas funciones gestionando redes TCP/IP. DHCP (Dynamic Host Configuration Protocol) es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red. Una dirección IP es un número que identifica de forma única a un ordenador en la red, ya sea en una red corporativa o en Internet. Una dirección IP es análoga a un número de teléfono. La dirección IP puede ser asignada estáticamente (manualmente) por el administrador o asignada dinámicamente por un servidor central.

2.2.4

Funcionamiento de DHCP

DHCP funciona sobre un servidor central (servidor, estación de trabajo o incluso un PC) el cual asigna direcciones IP a otras máquinas de la red. Este protocolo puede entregar información IP en una LAN o entre varias VLAN. Esta tecnología reduce el trabajo de un administrador, que de otra manera tendría que visitar todos los ordenadores o estaciones de trabajo uno por uno. Para introducir la configuración IP consistente en IP, máscara, gateway, DNS, etc. Un servidor DHSP (DHCP Server) es un equipo en unared que está corriendo un servicio DHCP. Dicho servicio se mantiene a la escucha de peticiones broadcast DHCP. Cuando una de estas peticiones es oída, el servidor responde con una dirección IP y opcionalmente con información adicional.

Un poco de historia

DHCP se deriva de del protocolo Bootstrap (BootP). BootP fue de los primeros métodos para asignar de forma dinámica, direcciones IP a otros equipos (ordenadores, impresoras, etc.). Al ser las redes cada vez más grandes, BootP ya no era tan adecuado y DHCP fue creado para cubrir las nuevas demandas. Como se ha comentado, se puede incluir información adicional en el protocolo DHCP. La configuración básica que puede ser enviada junto con la dirección IP es:

- Dirección IP y la máscara.
- Pasarela o gateway para la máquina que quiere acceder a la red.
- Servidor DNS para que la estación de trabajo pueda resolver nombres a direcciones IP.



Existen otros parámetros como servidores de registro o de sincronización.

Conclusión:

DHCP es un protocolo diseñado principalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP está activo en un servidor donde se centraliza la gestión de la direcciones IP de la red. Hoy en día, muchos sistemas operativos incluyen este servicio dada su importancia.

1. Instala ahora en cada delegación un servidor

Para instalar un servidor DHCP en cada uno de los tres departamentos se realizan los siguientes pasos:

1. En el apartado de la esquina inferior izquierda seleccionaremos el segundo icono de la fila superior () cuyo nombre es 'End Devices' y seleccionaremos el tercer icono () de la fila de dichos dispositivos 'End Devices'.

2.2.4

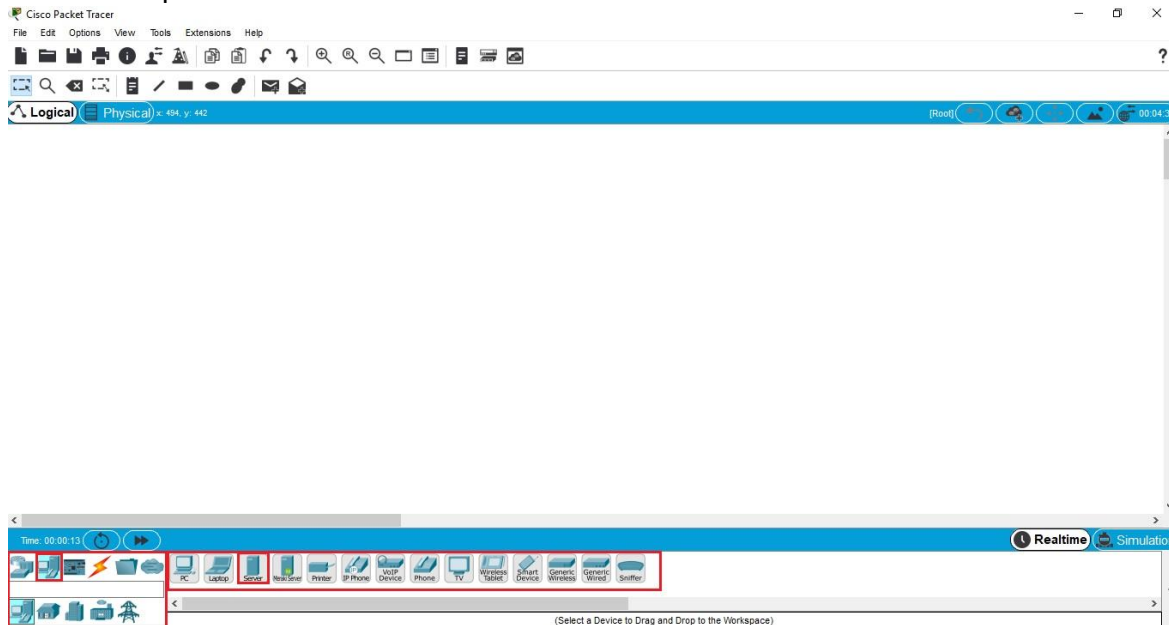



Figura 2.2.3.A. Localización Servidor DHCP

2. Dicho dispositivo lo seleccionamos haciendo click sobre él y lo colocaremos en cada uno de los tres departamentos conectandolos mediante el cable () a cada uno de los switches de los diferentes departamentos. Para ello primero seleccionaremos dicho cable y se conectará primero a la boca 'FastEthernet' del Servidor DHCP, y después al switch de ese departamento a su primera boca 'FastEthernet' libre.

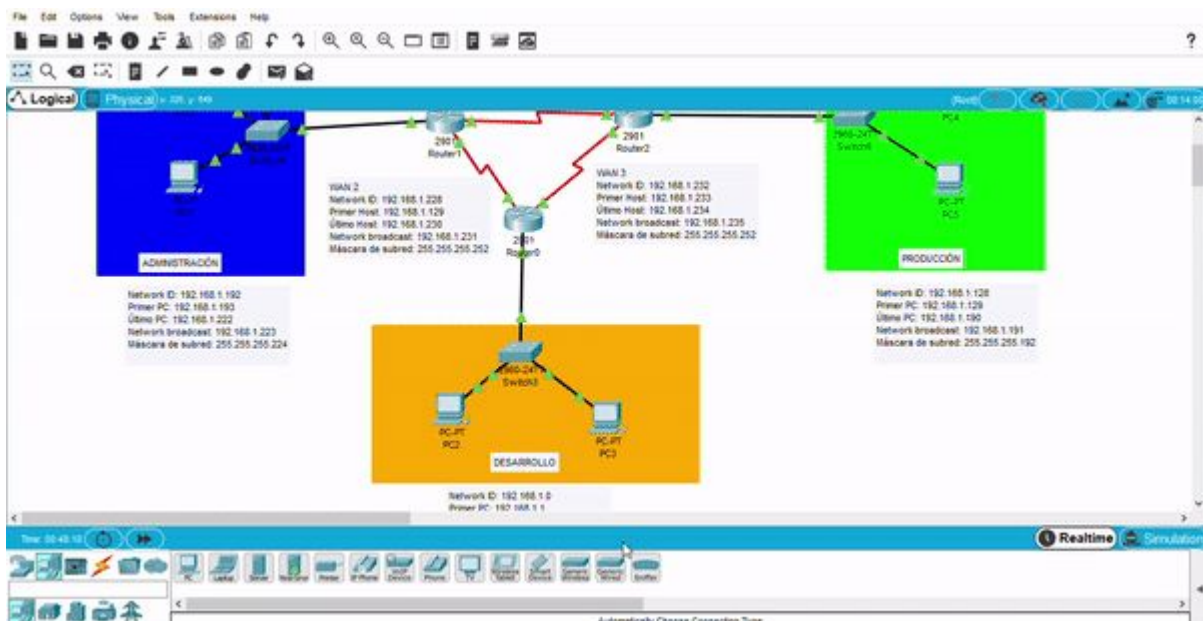


Figura 2.2.3.B. Conexión Servidor DHCP con el switch

2. Asigne unos parámetros de red (IP, máscara,...) válidos dentro de la delegación

Cada servidor DHCP nos exige ponerle una IP, una máscara y la puerta de enlace de su router correspondiente a su boca FastEthernet para que este tenga conectividad con el Switch y por tanto con cada uno de los PCs conectados a dicho Switch. A cada servidor DHCP de cada uno de los departamentos se le debe asignar una red y una máscara los cuales sean válidos dentro de cada departamento, es decir que se encuentre dentro de la misma departamento.

Gracias a los cálculos realizados y explicados anteriormente dicha tarea se hace haciendo click sobre cada uno de los servidores DHCP de cada uno de los departamentos, y en la pestaña de 'Config' podremos configurar primero el 'Gateway' en el subapartado de 'Settings' y segundo la IP y la máscara en el apartado de 'FastEthernet'.

2.2.4

1. Departamento de ADMINISTRACIÓN

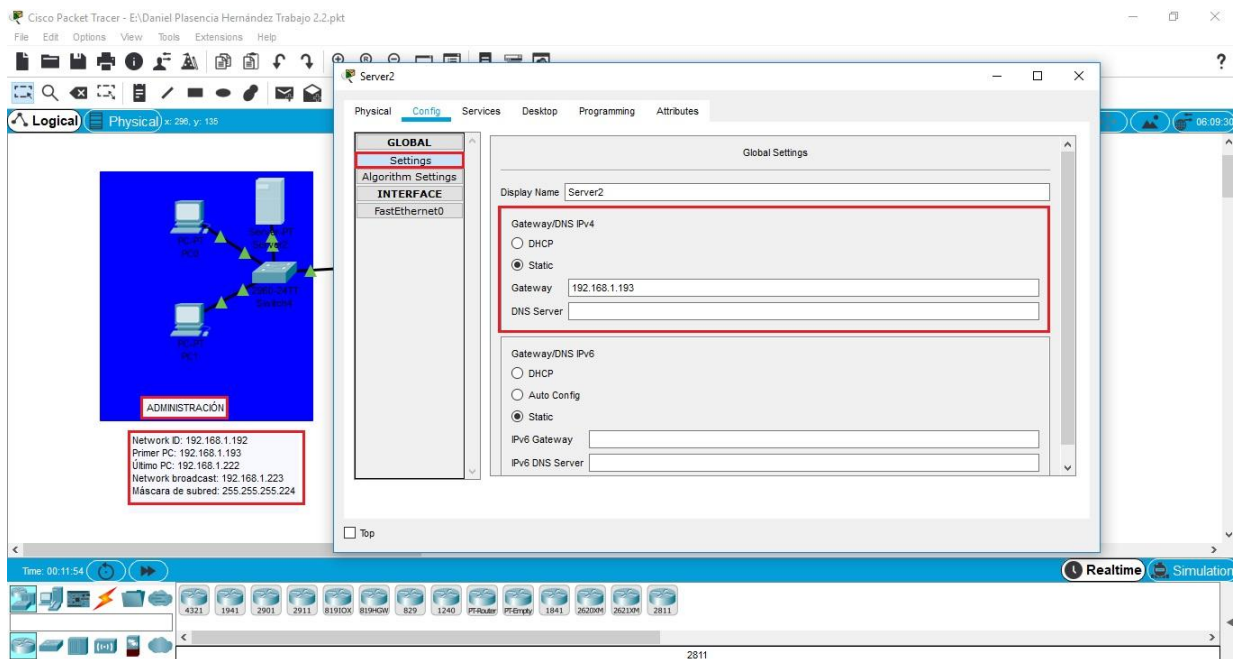


Figura 2.2.3.C. Gateway Servidor Administración

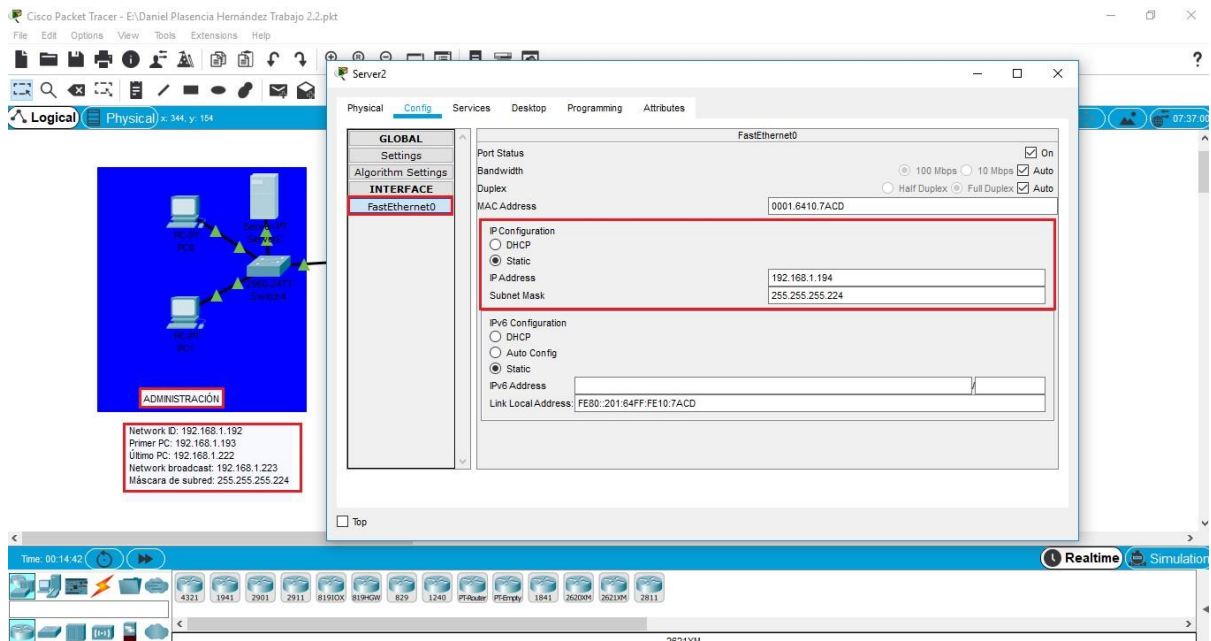
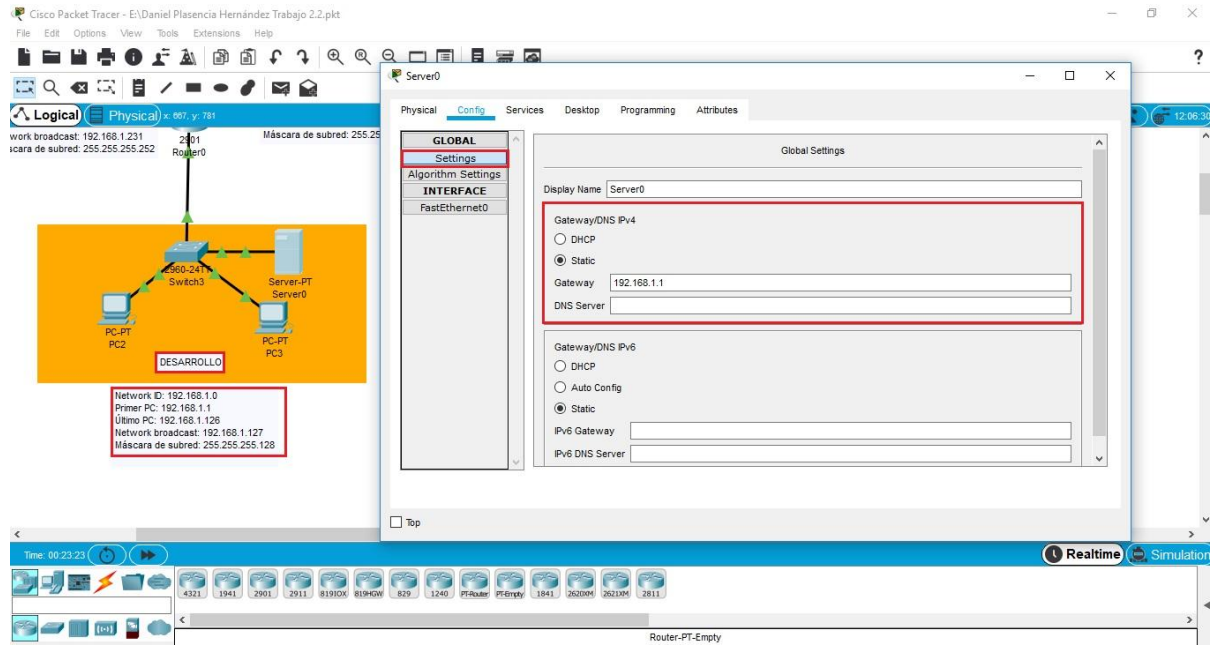


Figura 2.2.3.D. IP Configuration Servidor Administración

2. Departamento de DESARROLLO



2.2.4

Figura 2.2.3.E. Gateway Servidor Desarrollo

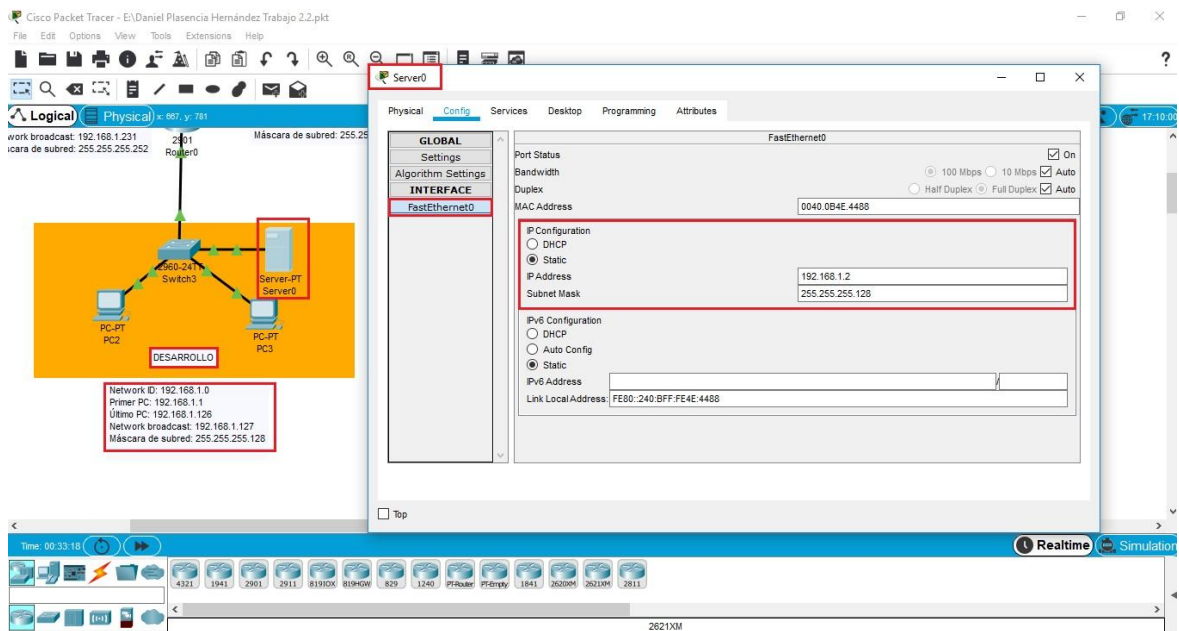
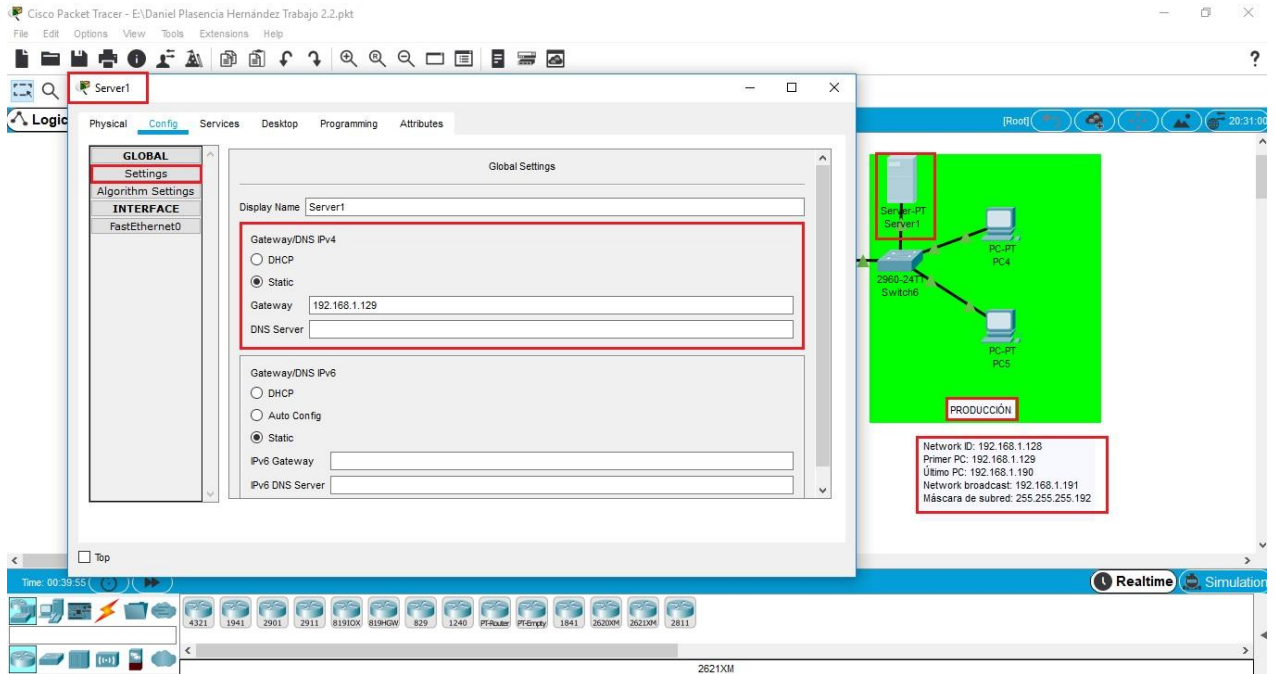


Figura 2.2.3.F. IP Configuration Servidor Desarrollo

<DPLAHER>

3. Departamento de PRODUCCIÓN



2.2.4

Figura 2.2.3.G. Gateway Servidor Producción

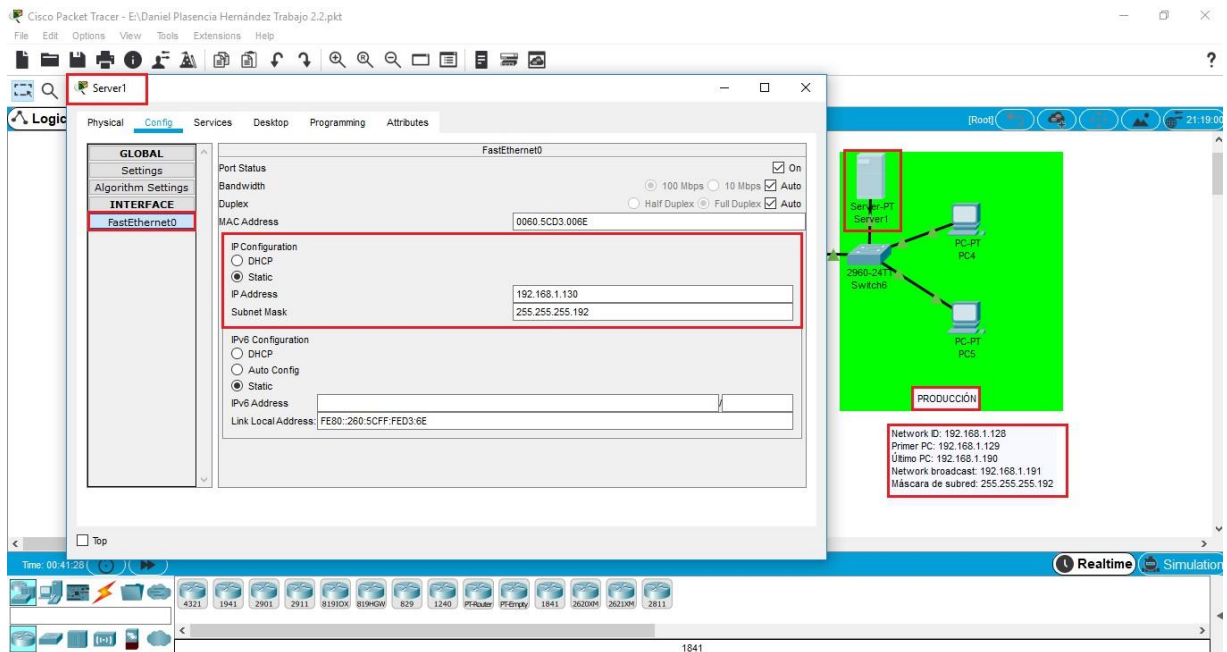


Figura 2.2.3.H. IP Configuration Servidor Producción

3. Su IP debería ser la 2da válida dentro de la delegación

Como se puede observar en las imágenes anteriores la IP de la boca 'FastEthernet' de cada servidor DHCP de los tres departamentos es la 2da válida de la subred correspondiente. Esto es debido porque los routers que se conectan a cada uno de los switches de cada departamento poseen en su boca 'GigabitEthernet0/0' la primera IP válida de dicha subred como se muestra a continuación.

2.2.4

1. Departamento de ADMINISTRACIÓN

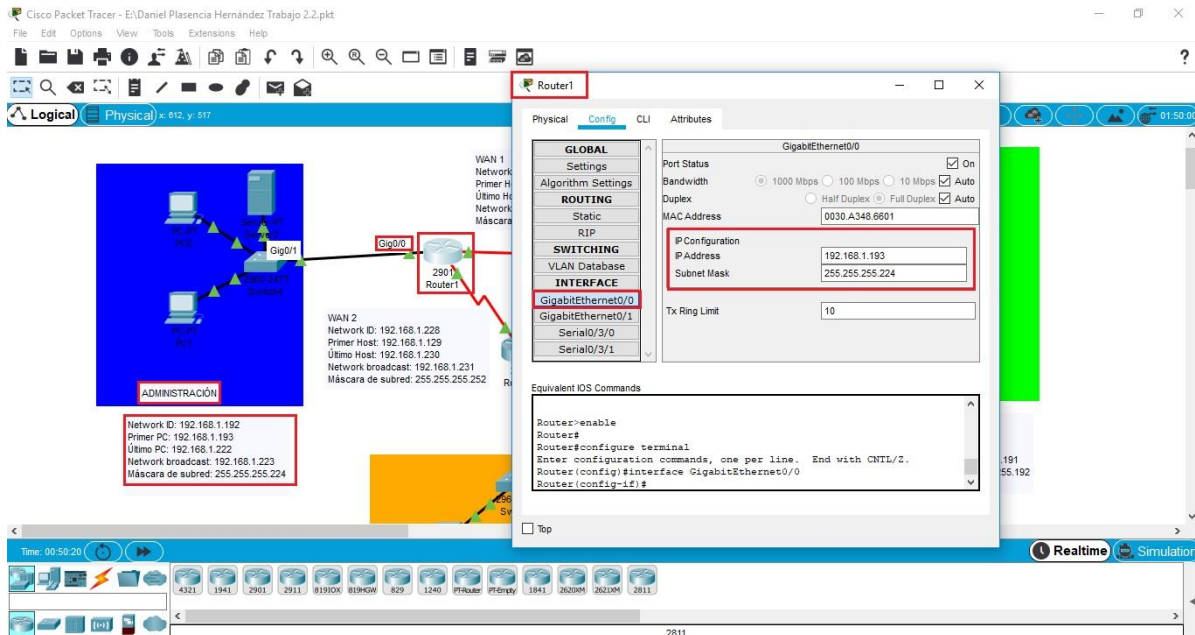


Figura 2.2.3.H. Boca GigabitEthernet0/0 Router Administración

2. Departamento de DESARROLLO

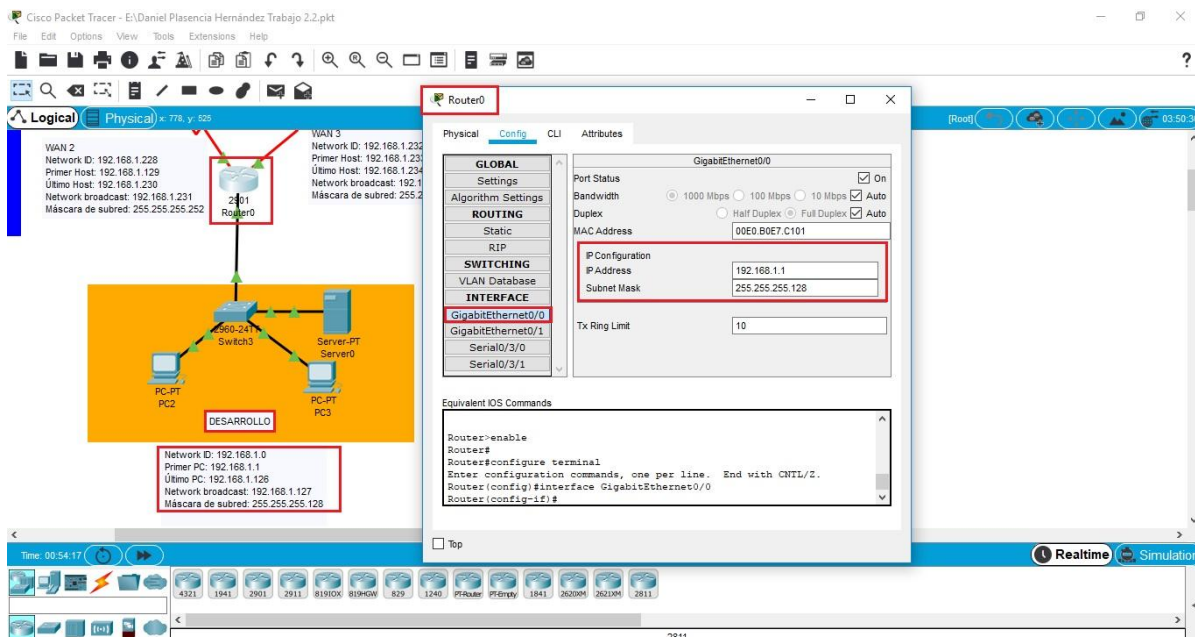
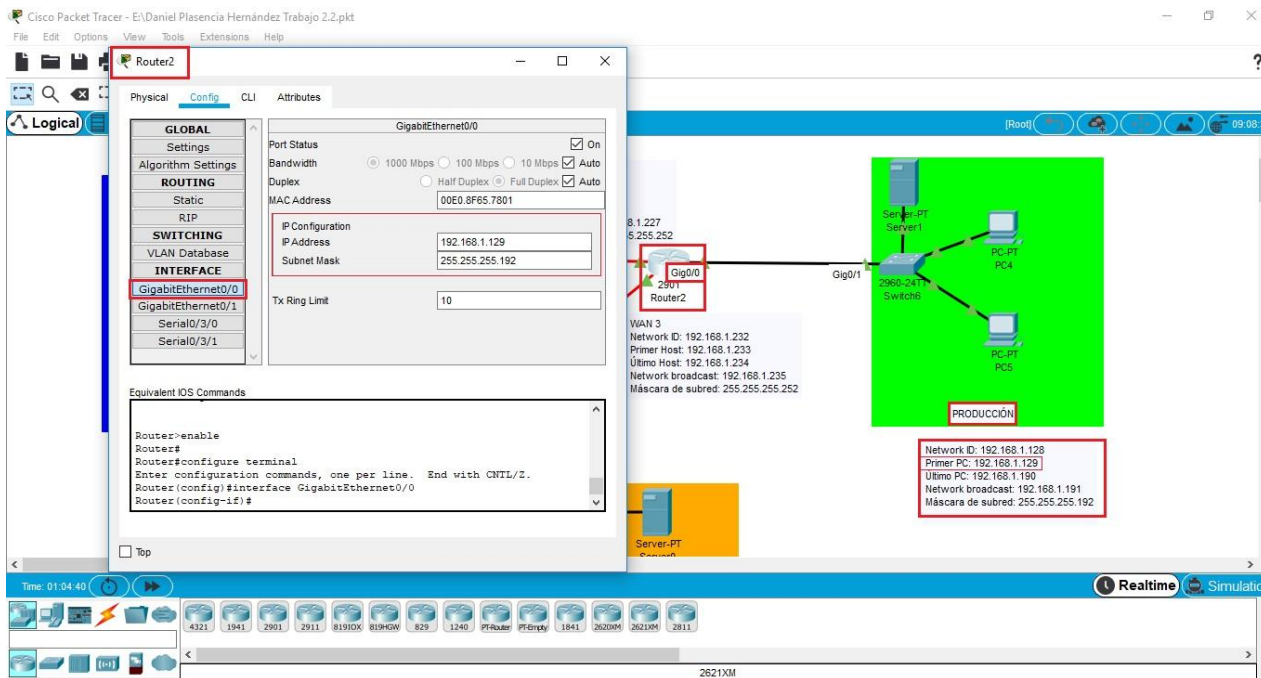


Figura 2.2.3.I. Boca GigabitEthernet0/0 Router Desarrollo

3. Departamento de PRODUCCIÓN



2.2.4

Figura 2.2.3.J. Boca GigabitEthernet0/0 Router Administración

- Activa el servicio de DHCP de tal manera que entregue de forma automática unos parámetros de red válidos dentro de la delegación
- Asegúrate que el nº de IPs que asigna no sea superior al máximo que soporta la subred (según los cálculos que hemos hecho)

Cada uno de los diferentes servidores deberán ser configurados que tal manera que entregue de forma automática a cada PCs unos parámetros de red válidos dentro de su departamento. Para realizar la configuración del servidor DHCP se debe hacer click sobre servidor, acceder a la pestaña llamada 'Services' y por último entrar en el subapartado llamado 'DHCP'. Una vez aquí dentro activaremos el Servidor seleccionando 'ON' para encenderlo. Y desde allí realizar la siguiente configuración en cada departamento:

1. Departamento de ADMINISTRACIÓN

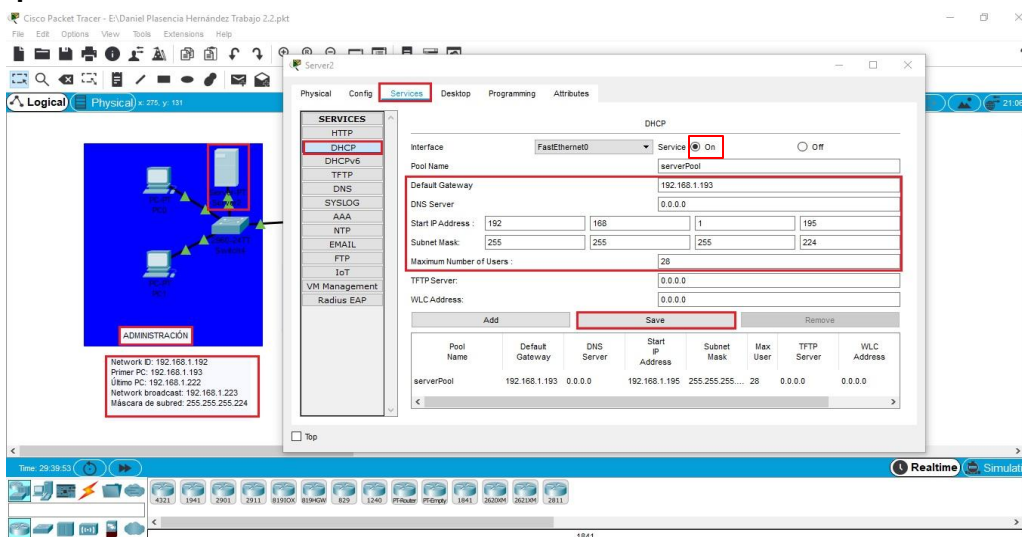


Figura 2.2.3.K. Configuración DHCP Departamento Administración

<DPLAHER>

En el departamento de administración ha sido configurado su servidor DHCP de la siguiente manera:

1. Default Gateway: El dato a introducir en dicho apartado es la puerta enlace del Router la cual como ha sido mostrada anteriormente esta es el primer Host de la subred de cada departamento, por eso en este caso es la 192.168.1.193

2. Start IP Address: El dato a introducir en dicho apartado es la primera IP que el servidor debe dar a cada uno de los Pcs los cuales se encuentren conectados al switch. En este caso la primera IP que queremos que éste dé a cada uno de los PCs conectados al switch es la 192.168.1.195, debido a que la 192.168.1.193 esta siendo usada por el Router y la 192.168.1.194 esta siendo usada por el propio servidor DHCP, como se muestra anteriormente.

2.2.4

3. Subnet Mask: El dato a introducir en dicho apartado en este caso la máscara de subred (255.255.255.224) en este caso como se muestra y enseña anteriormente en los cálculos.

4. Maximum Number of Users: El dato a introducir en dicho apartado es el número máximo de usuarios que van a usar dicha subred. En este caso el número máximo de usuarios que queremos que de el servidor DHCP es de 28 usuarios, qué es exactamente el número de host que pide dicho problema. Esto es debido a que para el departamento de administración se ha creado un subneteo usando 3 bits de subred creando de esta manera una subred con 32 host, pero no pudiendo usar la 'ID Network', ni la dirección de broadcast, ni el primer host el cual está siendo usado por el router ni el segundo que está siendo usado por el propio servidor se queda en 28 número de usuarios posibles.

Por último tras introducir todos los datos es importante darle al botón Save para que el Servidor DHCP guarde los cambios que hayas realizado correctamente.

2. Departamento de DESARROLLO

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.1.1	0.0.0.0	192.168.1.3	255.255.255...	124	0.0.0.0	0.0.0.0

Figura 2.2.3.L. Configuración DHCP Departamento Desarrollo

En el departamento de desarrollo ha sido configurado su servidor DHCP de la siguiente manera:

1. Default Gateway: El dato a introducir en dicho apartado es la puerta enlace del Router la cual como ha sido mostrada anteriormente esta es el primer Host de la subred de cada departamento, por eso en este caso es la 192.168.1.1

2. Start IP Address: El dato a introducir en dicho apartado es la primera IP que el servidor debe dar a cada uno de los Pcs los cuales se encuentren conectados al switch. En este caso la primera IP que queremos que esté de a cada uno de los PCs conectados al switch es la 192.168.1.3, debido a que la 192.168.1.1 esta siendo usada por el Router y la 192.168.1.2 esta siendo usada por el propio servidor DHCP, como se muestra anteriormente.

3. Subnet Mask: El dato a introducir en dicho apartado en este caso la máscara de subred (255.255.255.128) en este caso como se muestra y enseña anteriormente en los cálculos.

4. Maximum Number of Users: El dato a introducir en dicho apartado es el número máximo de usuarios que van a usar dicha subred. En este caso el número máximo de usuarios que queremos que de el servidor DHCP es de 124 usuarios, debido a que el problema para dicho departamento exige 74 hosts. Esto es debido a que para el departamento de desarrollo se ha creado un subneteo usando 1 bit de subred creando de esta manera una subred con 128 host, pero no pudiendo usar la 'ID Network', ni la dirección de broadcast, ni el primer host el cual está siendo usado por el router ni el segundo que está siendo usado por el propio servidor se queda en 124 número de usuarios posibles.

Por último tras introducir todos los datos es importante darle al botón Save para que el Servidor DHCP guarde los cambios que hayas realizado correctamente.

3. Departamento de PRODUCCIÓN

The screenshot displays the DHCP configuration interface in Cisco Packet Tracer. The configuration is for a server named 'Server1' on the 'FastEthernet0' interface. The DHCP service is enabled. The configuration details are as follows:

- Interface: FastEthernet0
- Service: On
- Pool Name: serverPool
- Default Gateway: 192.168.1.129
- DNS Server: 0.0.0.0
- Start IP Address: 192.168.1.131
- Subnet Mask: 255.255.255.192
- Maximum Number of Users: 60
- TFTP Server: 0.0.0.0
- WLC Address: 0.0.0.0

The 'Save' button is highlighted in red. Below the configuration fields, a table shows the configuration for the 'serverPool':

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.1.129	0.0.0.0	192.168.1.131	255.255.255.192	60	0.0.0.0	0.0.0.0

The network diagram on the right shows the 'PRODUCCIÓN' department with a switch (2960-24T1) connected to three PCs (PC4, PC5, PC6). A summary box for the 'PRODUCCIÓN' network shows the following details:

- Network ID: 192.168.1.128
- Primer PC: 192.168.1.129
- Último PC: 192.168.1.190
- Network broadcast: 192.168.1.191
- Máscara de subred: 255.255.255.192

Figura 2.2.3.M. Configuración DHCP Departamento Producción

En el departamento de producción ha sido configurado su servidor DHCP de la siguiente manera:

1. Default Gateway: El dato a introducir en dicho apartado es la puerta enlace del Router la cual como ha sido mostrada anteriormente esta es el primer Host de la subred de cada departamento, por eso en este caso es la 192.168.1.129

2. Start IP Address: El dato a introducir en dicho apartado es la primera IP que el servidor debe dar a cada uno de los Pcs los cuales se encuentren conectados al switch. En este caso la primera IP que queremos que esté de a cada uno de los PCs conectados al switch es la 192.168.1.131, debido a que la 192.168.1.129 esta siendo usada por el Router y la 192.168.1.30 esta siendo usada por el propio servidor DHCP, como se muestra anteriormente.

3. Subnet Mask: El dato a introducir en dicho apartado en este caso la máscara de subred (255.255.255.192) en este caso como se muestra y enseña anteriormente en los cálculos.

4. Maximum Number of Users: El dato a introducir en dicho apartado es el número máximo de usuarios que van a usar dicha subred. En este caso el número máximo de usuarios que queremos que de el servidor DHCP es de 60 usuarios, debido a que el problema para dicho departamento exige 52 hosts. Esto es debido a que para el departamento de desarrollo se ha creado un subneteo usando 2 bits de subred creando de esta manera una subred con 64 host, pero no pudiendo usar la 'ID Network', ni la dirección de broadcast, ni el primer host el cual está siendo usado por el router ni el segundo que está siendo usado por el propio servidor se queda en 60 número de usuarios posibles.

Por último tras introducir todos los datos es importante darle al botón Save para que el Servidor DHCP guarde los cambios que hayas realizado correctamente.

5. Asegúrate de que la 1ra IP que entregue no solape con el router ni con el propio servidor

7. RE-Asigna las IPs de los hosts de forma automática

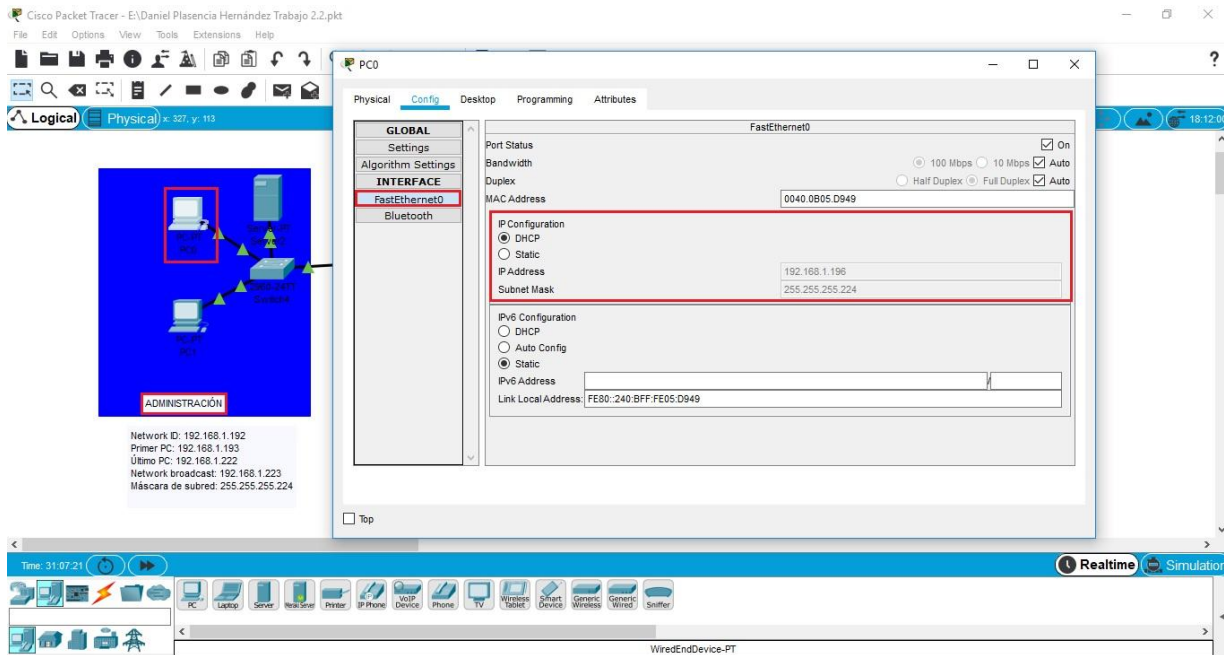
Como se puede observar en las siguientes imágenes ambos PCs de cada departamento se encuentran tanto con el Gateway como la IP Configuration en automática. También se puede observar que la 1ra IP que entrega el servidor DHCP no se solapa ni con el router ni con el propio servidor.

1. PCs de ADMINISTRACIÓN

Primer PC:

The screenshot shows the Cisco Packet Tracer interface. The main window displays the configuration for PC0. The 'Config' tab is active, showing the 'Global Settings' section. The 'Gateway/DNS IPv4' section is highlighted with a red box, indicating the DHCP configuration. The 'Gateway' is set to 192.168.1.193 and the 'DNS Server' is set to 0.0.0.0. The 'Physical' window shows a network diagram with PC0 connected to a switch. The status bar at the bottom indicates 'Realtime' simulation mode.

Figura 2.2.3.N. Gateway PC0 Administración



2.2.4

Figura 2.2.3.O. IP Configuration PC0 Administración

Segundo PC:

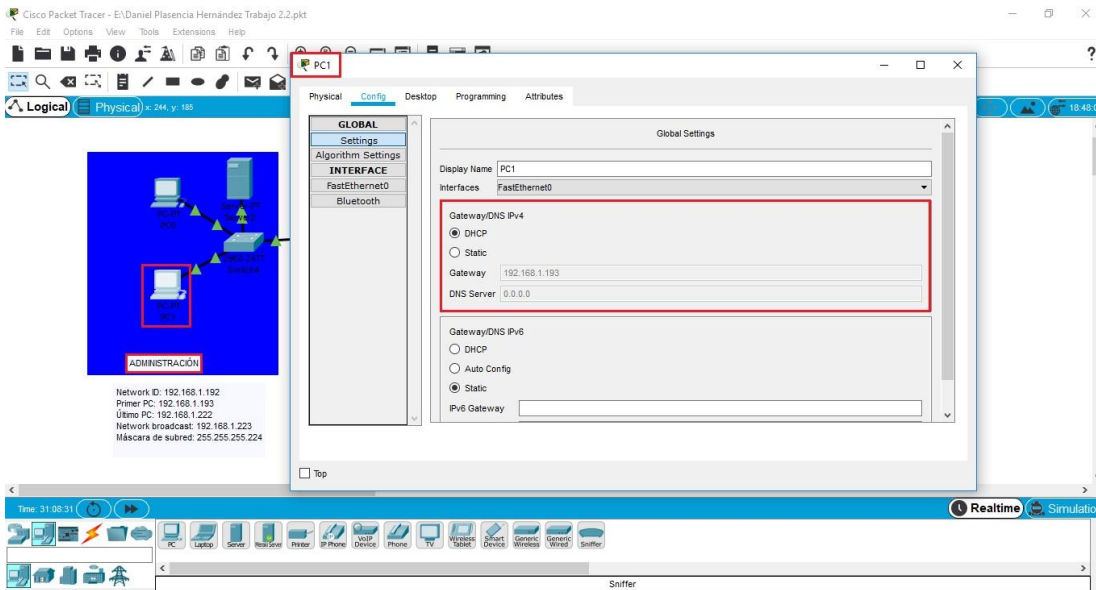
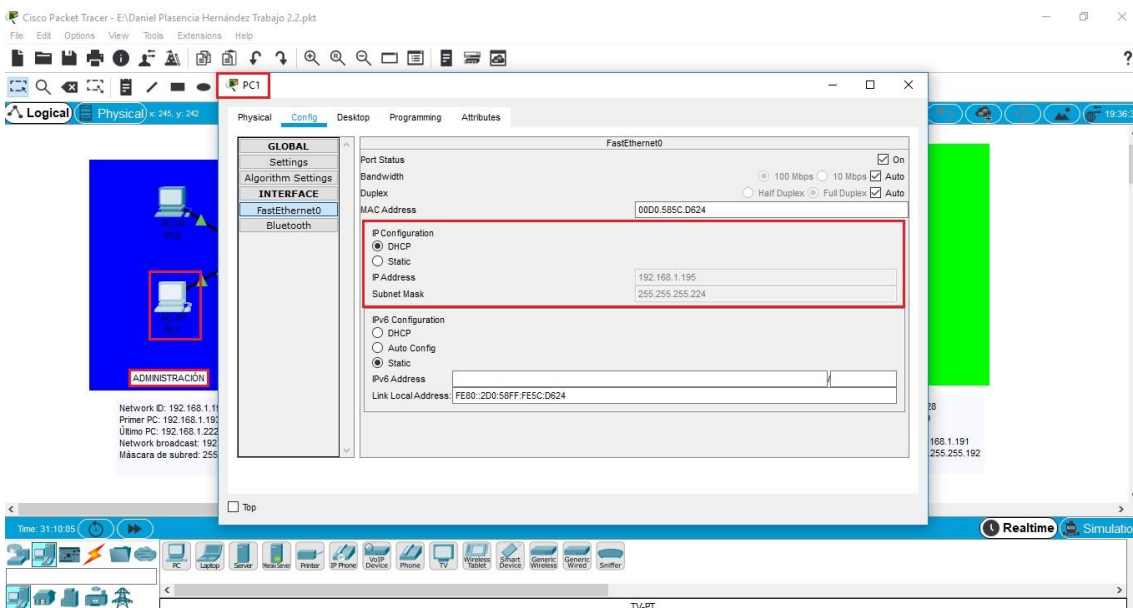


Figura 2.2.3.P. Gateway PC1 Administración



<DPLAHER>

Figura 2.2.3.Q. IP Configuration PC1 Administración

2. PCs de DESARROLLO

Primer PC:

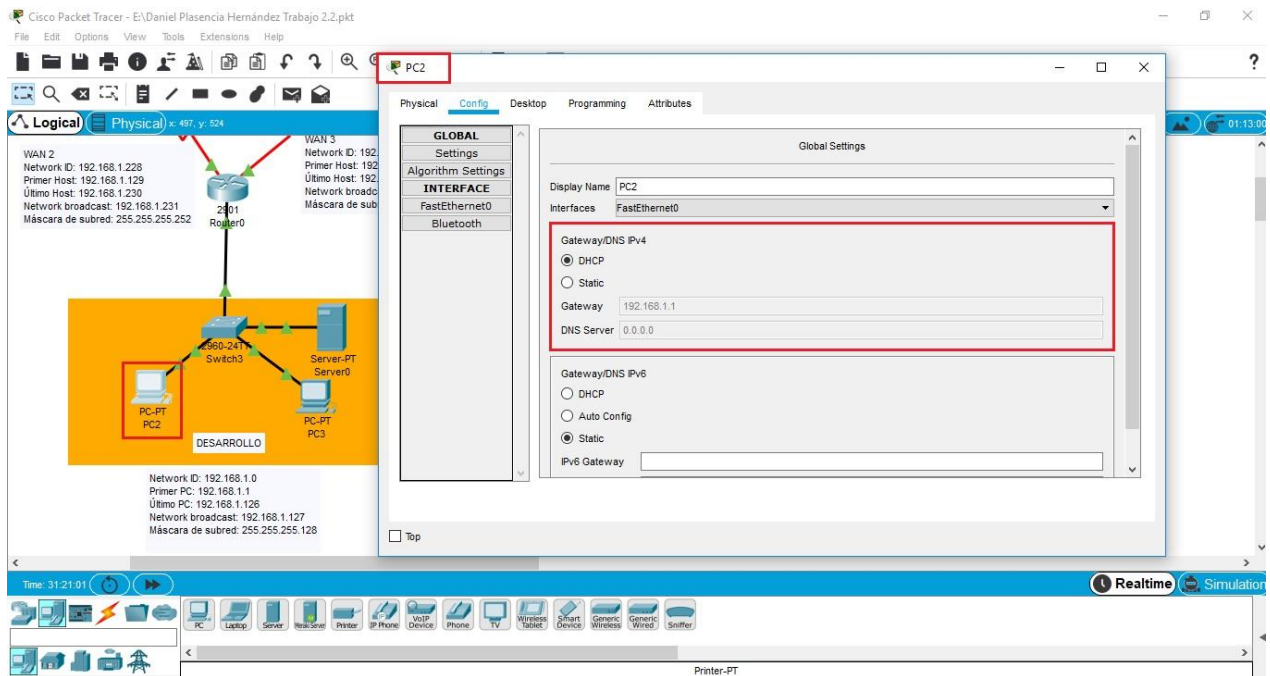
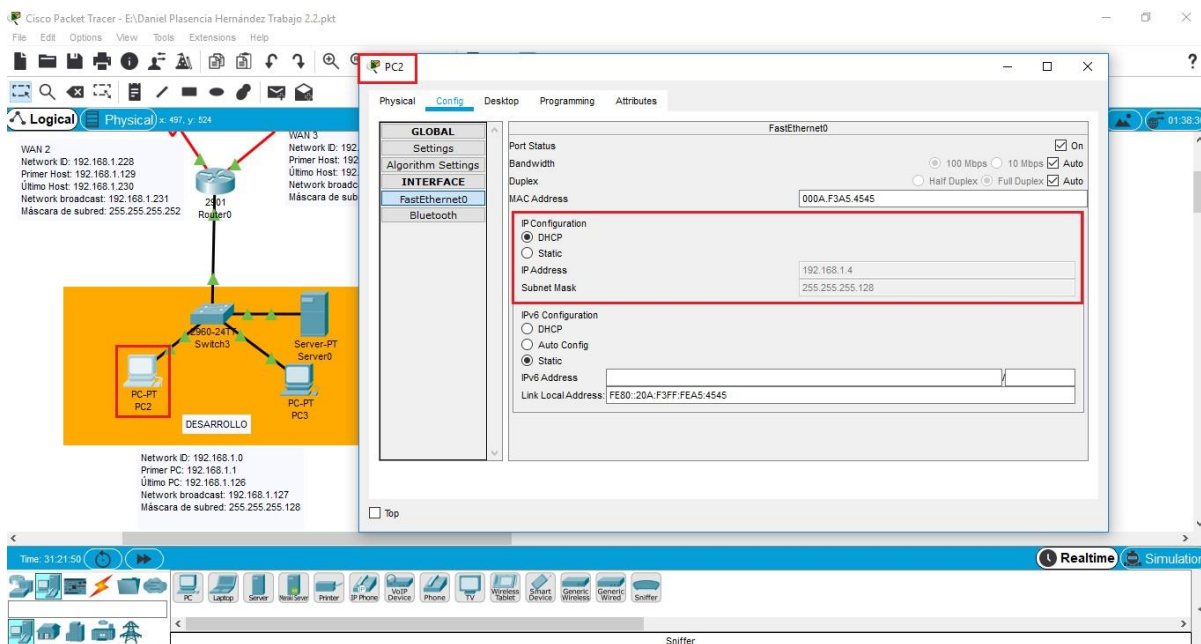
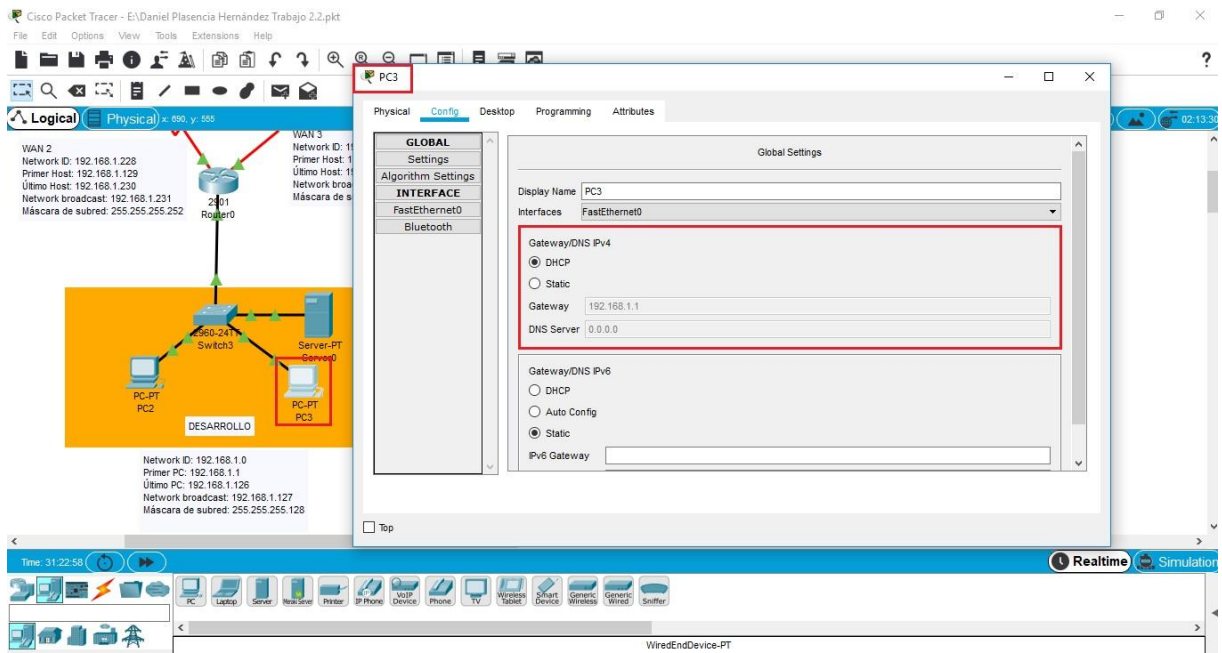


Figura 2.2.3.R. Gateway PC2 Desarrollo



Segundo PC:



2.2.4

Figura 2.2.3.T. Gateway PC3 Desarrollo

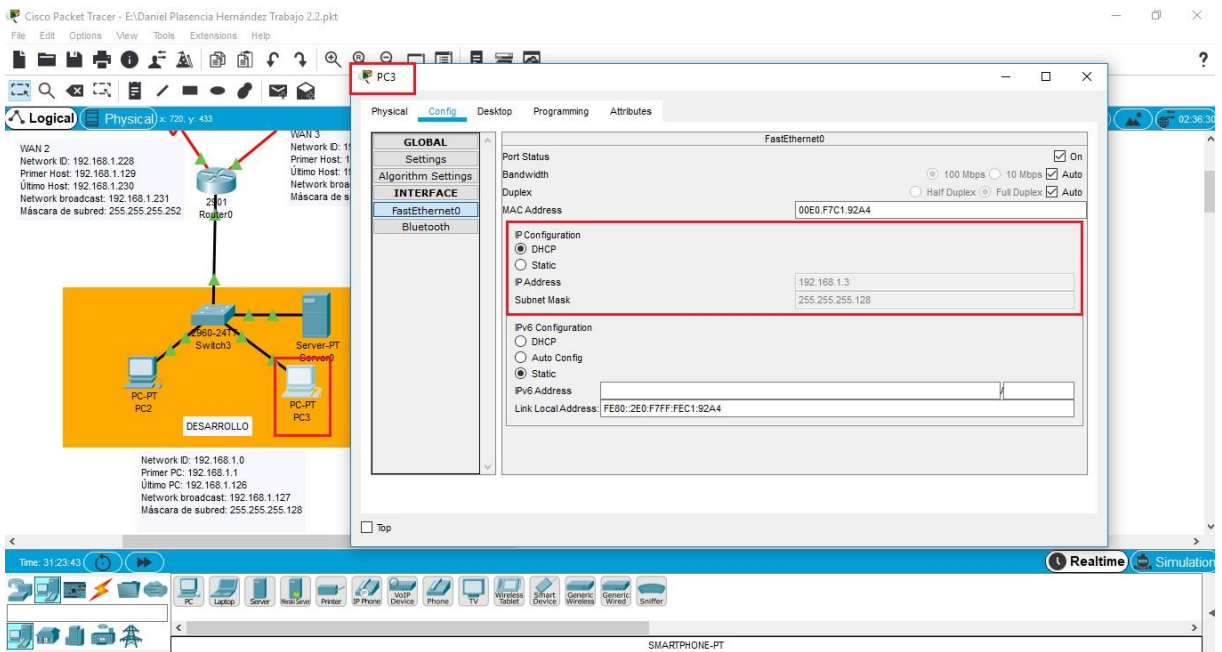
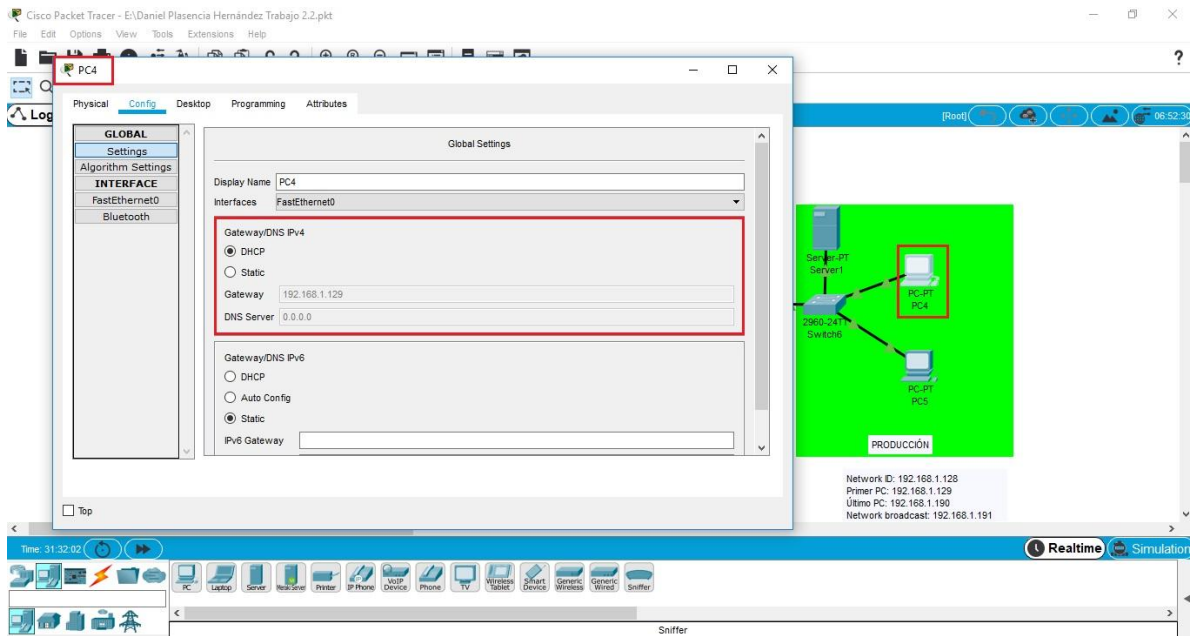


Figura 2.2.3.U. IP Configuration PC3 Desarrollo

3. PCs de PRODUCCIÓN

Primer PC:



2.2.4

Figura 2.2.3.V. Gateway PC4 Producción

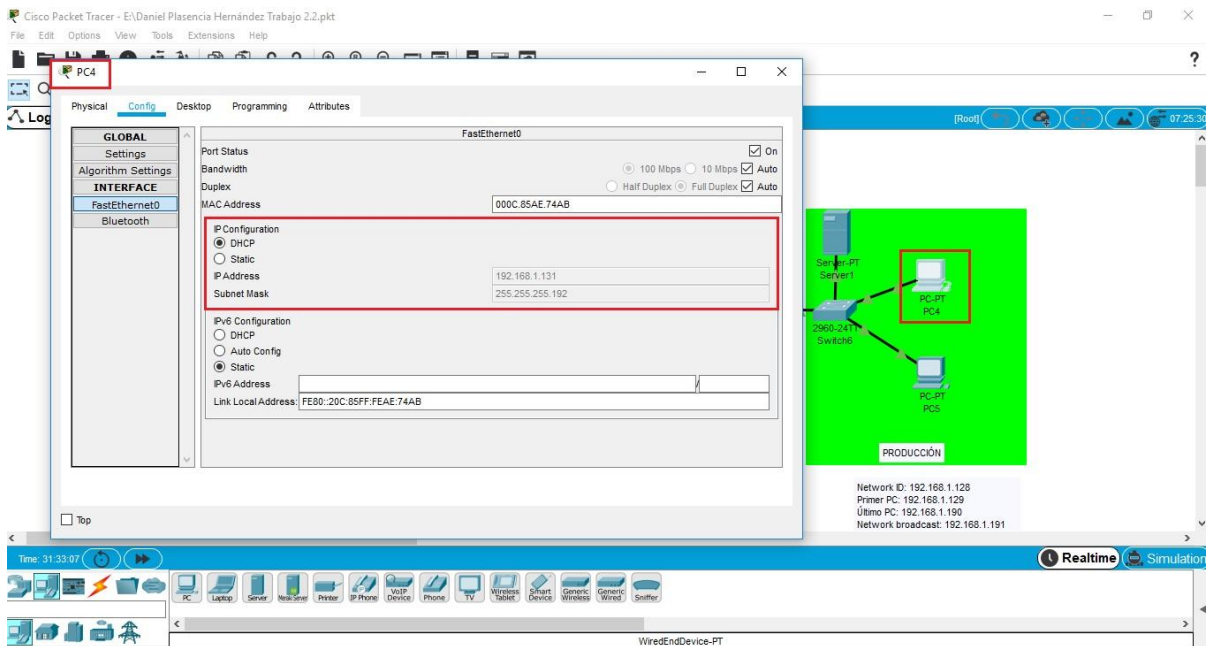
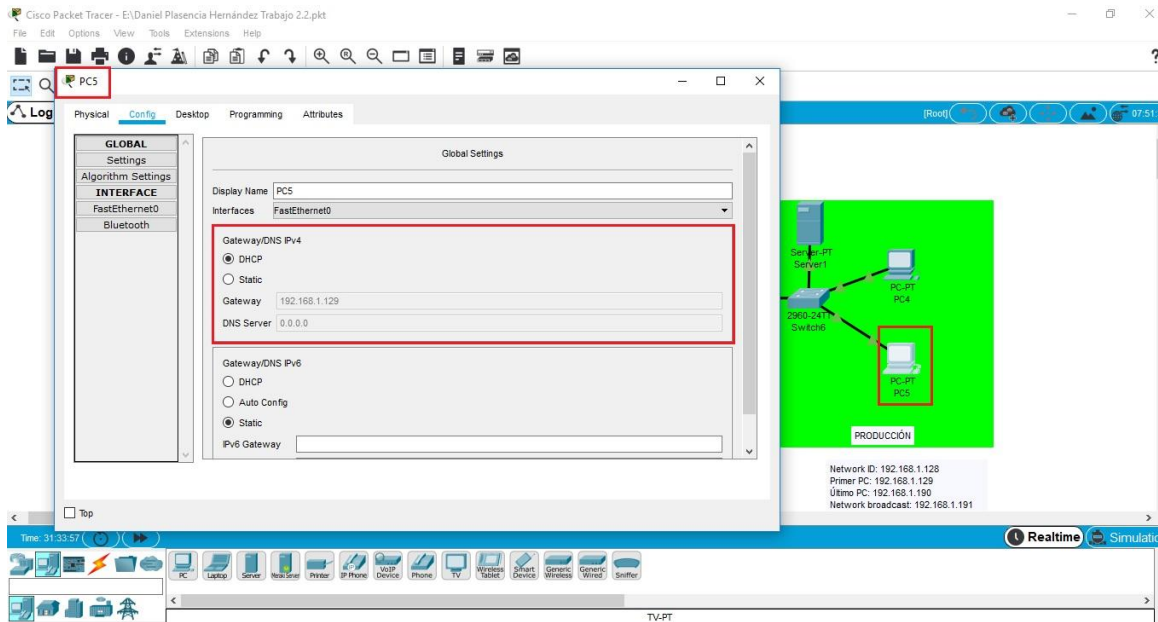


Figura 2.2.3.W. IP Configuration PC4 Producción

Segundo PC:



2.2.4

Figura 2.2.3.X. Gateway PC5 Producción

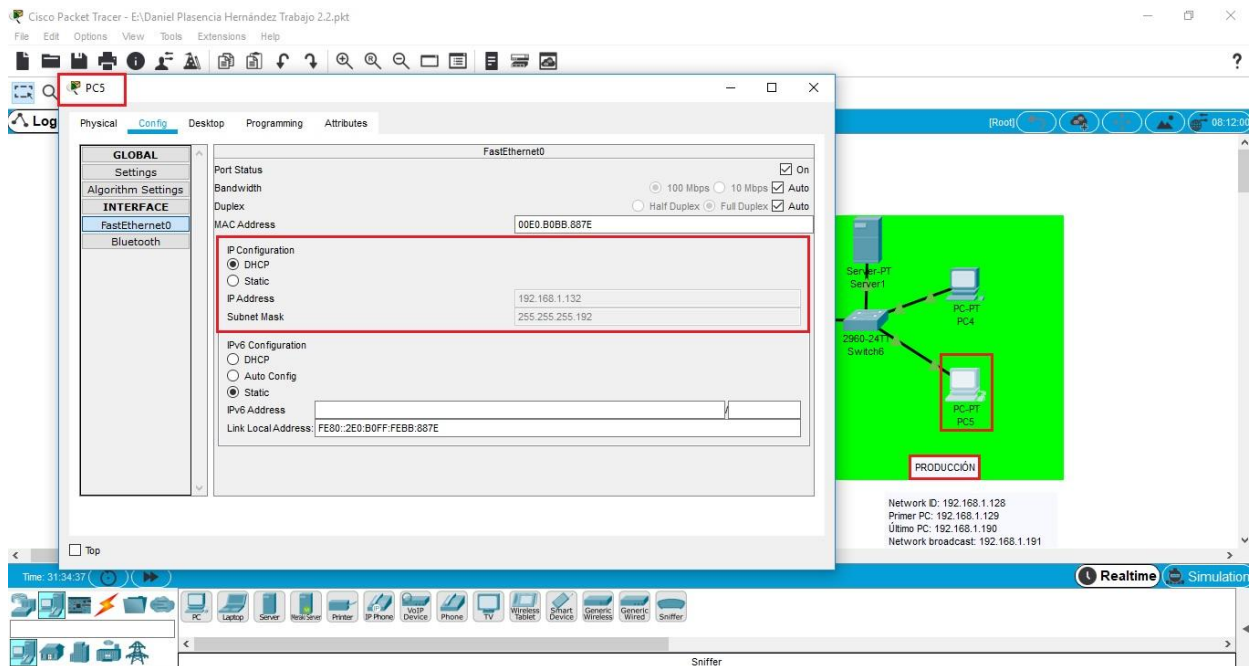


Figura 2.2.3.Y. IP Configuration PC4 Producción

8. Comprueba el correcto funcionamiento de todo el montaje

Para comprobar el correcto funcionamiento de todo el montaje puede hacerlo a través del siguiente link:

<https://www.youtube.com/watch?v=bAlmZz7wAYk&feature=youtu.be>

2.2.4

También puede acceder a él mediante el siguiente QR:



Fase 4. BOOTP

- ¿Qué es BOOTP?
- ¿Para qué sirve?
- ¿Es anterior o posterior a DHCP?
- ¿Qué diferencias existen entre uno y otro?
- ¿Qué ventajas/desventajas incluye el uno frente al otro?
- ¿Cuál de los dos protocolos se usa en la actualidad?
- ...

2.2.5

-¿Qué es BOOTP?

El **protocolo de arranque**, conocido por las siglas **BOOTP** de *Bootstrap Protocol*, es un protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente, su nombre original está definido como RFC 951, el proceso de BOOTP se realiza normalmente al arrancar el PC o al inicio del sistema operativo.

-¿Para qué sirve?

Sirve para permitir la configuración de inicio de estaciones de trabajo sin disco en sistemas antiguos. Este protocolo era necesario, ya que los clientes de este tipo tienen una capacidad limitada para almacenar la información configurable, necesaria durante los respectivos procesos de inicio que se utilizan para iniciar y participar en una red.

El protocolo BOOTP se utiliza para efectuar arranques remotos en redes IP. Permite que una pila de IP mínima sin información de configuración, típicamente almacenada en la ROM, obtenga información suficiente para comenzar el proceso de descargar el código de arranque necesario

-¿Es anterior o posterior a DHCP?

El protocolo BOOTP fue definido en septiembre de 1985 mientras que el protocolo DHCP fue definido en octubre de 1993 como una extensión del protocolo BOOTP, por tanto el protocolo BOOTP es el predecesor del protocolo DHCP.

-¿Qué diferencias existen entre uno y otro?

BOOTP Y DHCP Tienen Más Similitudes Que Diferencias. DHCP Se Basa En BOOTP y toma sus procedimientos y estructura del mensaje. DHCP fue escrito para ser compatible con BOOTP, pero recorta parte de las responsabilidades de BOOTP. BOOTP no solo entrega Direcciones IP, sino que también es capaz de hacer un programa de arranque de red disponible para los equipos de la Red. este programa contiene las instrucciones de inicio para el equipo. DHCP no requiere un archivo que se transfiere al cliente , ya que su definición de mensaje contiene más campos que se comunican los ajustes en el cuerpo del mensaje, en lugar de un en un archivo separado.

2.2.5

BOOTP	DHCP
Diseñado antes que DHCP.	Diseñado después que BOOTP.
Pensado para configurar estaciones de trabajo sin disco con capacidades de arranque limitadas.	Pensado para configurar equipos conectados en red que cambian de ubicación con frecuencia (como portátiles) que disponen de discos duros locales y capacidades completas de arranque.
BOOTP dinámico tiene una expiración predeterminada de 30 días para las concesiones de direcciones IP.	DHCP tiene una expiración predeterminada de ocho días para las concesiones de direcciones IP.
Admite un número limitado de parámetros de configuración de clientes denominados <i>extensiones del proveedor</i> .	Admite un conjunto mayor y extensible de parámetros de configuración de clientes denominados <i>opciones</i> .

Figura 2.2.5.a Diferencias entre DHCP Y BOOTP

BOOTP	DHCP
Describe un proceso de configuración de arranque en dos fases, de la manera siguiente: Los clientes se ponen en contacto con los servidores BOOTP para realizar la determinación de las direcciones y la selección del nombre del archivo de arranque.	Describe un proceso de configuración de arranque de una sola fase donde un cliente DHCP negocia con un servidor DHCP para determinar su dirección IP y obtener cualquier otro detalle de configuración inicial que se necesite para el funcionamiento de la red.
Los clientes se ponen en contacto con los servidores del Protocolo trivial de transferencia de archivos (TFTP) para realizar la transferencia de archivos de su imagen de arranque.	

Figura 2.2.5.b Diferencias entre DHCP Y BOOTP

BOOTP	DHCP
Los clientes BOOTP no reenlazan ni renuevan la configuración con el servidor BOOTP salvo cuando se reinicia el sistema.	Los clientes DHCP no necesitan un reinicio del sistema para reenlazar o renovar la configuración con el servidor DHCP. En su lugar, los clientes entran automáticamente en un estado de reenlace a intervalos establecidos para renovar la asignación de sus direcciones concedidas con el servidor DHCP. Este proceso tiene lugar en segundo plano y es transparente para el usuario.

Figura 2.2.5.c Diferencias entre DHCP Y BOOTP

-¿Qué ventajas/desventajas incluye el uno frente al otro?

BOOTP da las direcciones IP estáticas mientras que el protocolo DHCP puede darlas tanto dinámicas como estáticas

- DHCP es la mejor opción cuando los dispositivos y las direcciones varían.

-BOOTP es un protocolo más simple que DHCP por lo que BOOTP es más eficiente a la hora de entregar las direcciones IP.

-El protocolo DHCP contiene más información que el protocolo BOOTP.

-Con el protocolo DHCP no es necesario pre configurar los servidores con las direcciones MAC de cada cliente.

2.2.5

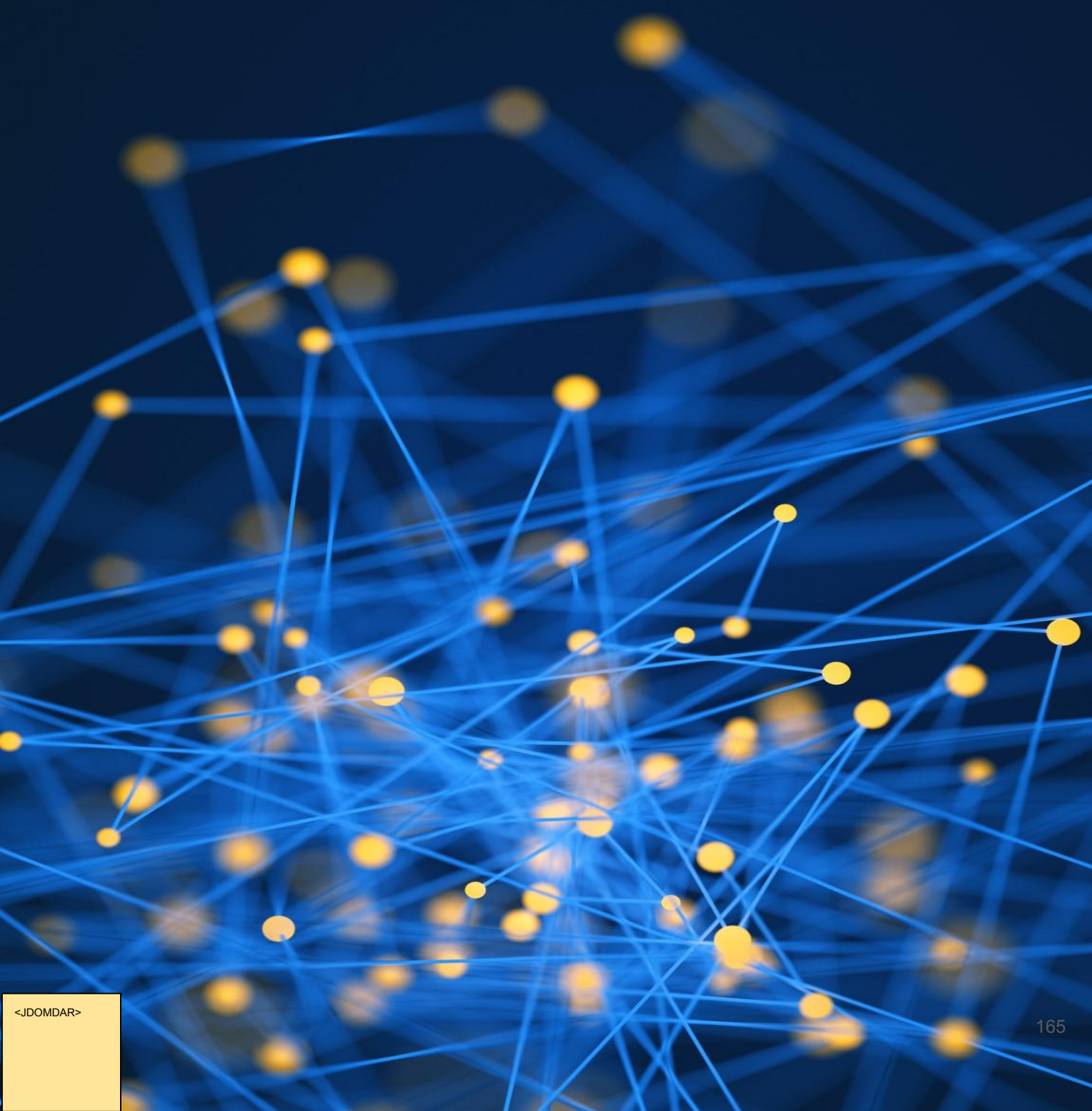
-¿Cuál de los dos protocolos se usa en la actualidad?

El protocolo que prevalece hoy día es el de DHCP

Trabajo 2.3

Subnetting

Cálculo



Trabajo 2.3. Subnetting: Cálculo

Dada la siguiente dirección IP **124.148.14.137/12** calcular:

1. Número de bits de red
2. Número de bits de subred
3. Número de bits de host
4. Indica de forma razonada cuántas subredes hay
5. Indica de forma razonada cuántos PCs por subred hay
6. ID de red de cada subred
7. Máscara de subred
8. Dirección IP de broadcast de cada subred
9. Dirección IP de 2 Pcs por subred

Apartados 1, 2, 3, 4 y 5

Dada la siguiente dirección IP **124.148.14.137/12** calcular:

1. Número de bits de red

Antes de nada, tenemos que averiguar a qué clase de red pertenece esa IP.

Clase de dirección	Bits de mayor peso	Intervalo de dirección del primer octeto	Número de bits en la dirección de red	Número de redes	Número de hosts por red
Clase A	0	0-127	8	126	16,777,216
Clase B	10	128-191	16	16,384	65,536
Clase C	110	192-223	24	2,097,152	254
Clase D	1110	224-239	28	No es aplicable	No es aplicable

Figura 2.3. Tabla con las diferentes clases de red.

Como vemos, el primer octeto de nuestra dirección IP (124) se encuentra dentro del intervalo 0-127, lo que hace que pertenezca a una red de clase A.

Para esta clase de red, el número de bits de red (representado por la letra N) es equivalente a 8, por lo que tenemos que **N = 8**.

2. Número de bits de subred

Para obtener el número de bits de subred (S), tendremos que restarle a la longitud de la máscara de subred (12) los bits de red (N); por tanto:

$$\text{Número de bits de subred (S)} = 12 - 8 = 4$$

3. Número de bits de host

Una dirección IP consta de 32 bits. Sabiendo esto, para obtener el número de bits de host (H), habrá que restarle a los 32 bits el número de bits de la longitud de la máscara de subred.

$$\text{Número de bits de host (H)} = 32 - 12 = 20$$

4. Indica de forma razonada cuántas subredes hay

El número de subredes que hay vendrá dado por el cálculo de la siguiente ecuación:

$$\text{Nº subredes} = 2^S = 2^4 = 16$$

5. Indica de forma razonada cuántos PCs por subred hay

El número de PCs (hosts) que hay por subred, vendrá dado por el cálculo de la siguiente ecuación:

$$\text{Nº de hosts} = 2^H - 2 = 2^{20} - 2 = 1.048.576 - 2 = 1.048.574$$

¿Por qué se resta -2? Esto se debe a que en cada red/subred se reservan dos direcciones IP, una para la ID de red, y otra para la dirección de broadcast.

Apartados 6 y 7

6. ID de red de cada subred

Al tratarse de una red de clase B, se trabajará sobre el 2º octeto. Este octeto de 8 bits tendrá un valor máximo de $2^8 = 256$. Dividiremos este valor por el número de subredes (S), obteniendo el valor de ID: $256/16 = 16$

Multiplicando este valor por el número de subred (que empezará en 0), obtendremos el valor del 2º octeto que definirá la ID de dicha subred:

- Subred **0**: $16 \cdot 0 = 0$ → 124.**0**.0.0
- Subred **1**: $16 \cdot 1 = 16$ → 124.**16**.0.0
- Subred **2**: $16 \cdot 2 = 32$ → 124.**32**.0.0
- Subred **3**: $16 \cdot 3 = 48$ → 124.**48**.0.0
- Subred **4**: $16 \cdot 4 = 64$ → 124.**64**.0.0
- Subred **5**: $16 \cdot 5 = 80$ → 124.**80**.0.0
- Subred **6**: $16 \cdot 6 = 96$ → 124.**96**.0.0
- Subred **7**: $16 \cdot 7 = 112$ → 124.**112**.0.0
- Subred **8**: $16 \cdot 8 = 128$ → 124.**128**.0.0
- Subred **9**: $16 \cdot 9 = 144$ → 124.**144**.0.0
- Subred **10**: $16 \cdot 10 = 160$ → 124.**160**.0.0
- Subred **11**: $16 \cdot 11 = 176$ → 124.**176**.0.0
- Subred **12**: $16 \cdot 12 = 192$ → 124.**192**.0.0
- Subred **13**: $16 \cdot 13 = 208$ → 124.**208**.0.0
- Subred **14**: $16 \cdot 14 = 224$ → 124.**224**.0.0
- Subred **15**: $16 \cdot 15 = 240$ → 124.**240**.0.0

7. Máscara de subred

La máscara de red por defecto de una red de clase A será 255.0.0.0 en valor decimal por puntos (/8 en valor por prefijo):

1111 1111 . 0000 0000 . 0000 0000 . 0000 0000 (valor binario)

La máscara de subred variará en el 2º octeto, tomando valor 1 los bits de subred (S = 4 en este caso) desde el más significativo (empezando desde la izquierda):

1111 1111 . **1111** 0000 . 0000 0000 . 0000 0000

Pasando a decimal el 2º octeto (**1111** 0000) tenemos que su valor es 240 ($2^7+2^6+2^5+2^4$), quedando la máscara de subred de la siguiente manera en valor decimal:

255.**240**.0.0

Apartado 8

8. Dirección IP de broadcast de cada subred

Para obtener la dirección IP de broadcast de la primera subred (subred 0), deberemos restarle 1 al valor de ID (16) y colocar el valor obtenido en el 2º octeto, Los octetos 3º y 4º, tomarán valor 255.

Para las subredes siguientes, el 2º octeto resultará de ir sumando el valor de ID al valor del 2º octeto de la anterior subred.

2.3

- Subred 0: $16 - 1 = 15$ → 124.**15**.255.255
- Subred 1: $15 + 16 = 31$ → 124.**31**.255.255
- Subred 2: $31 + 16 = 47$ → 124.**47**.255.255
- Subred 3: $47 + 16 = 63$ → 124.**63**.255.255
- Subred 4: $63 + 16 = 79$ → 124.**79**.255.255
- Subred 5: $79 + 16 = 95$ → 124.**95**.255.255
- Subred 6: $95 + 16 = 111$ → 124.**111**.255.255
- Subred 7: $111 + 16 = 127$ → 124.**127**.255.255
- Subred 8: $127 + 16 = 143$ → 124.**143**.255.255
- Subred 9: $143 + 16 = 159$ → 124.**159**.255.255
- Subred 10: $159 + 16 = 175$ → 124.**175**.255.255
- Subred 11: $175 + 16 = 191$ → 124.**191**.255.255
- Subred 12: $191 + 16 = 207$ → 124.**207**.255.255
- Subred 13: $207 + 16 = 223$ → 124.**223**.255.255
- Subred 14: $223 + 16 = 239$ → 124.**239**.255.255
- Subred 15: $239 + 16 = 255$ → 124.**255**.255.255

Si nos fijamos, la dirección de broadcast de cada subred es la resta de 1 de la ID de red de la siguiente subred:

$$[124.**15**.255.255 = IP_{\text{BCAST}} \text{ subred 0 ; } 124.**16**.0.0 = ID_{\text{RED}} \text{ subred 1}]$$

Siguiendo la lógica sugerida, nos quedaría por saber la IP de broadcast de la última subred, la cual siempre acabará en 255 en los octetos que no son de red (en clase A, octetos 2, 3 y 4).

124.255.255.255

Apartado 9

9. Dirección IP de 2 Pcs por subred

Para obtener el primer host disponible por subred, deberemos sumar 1 en el último (4º) octeto del ID de red de dicha subred.

Para obtener el último host disponible por subred, deberemos restar 1 en el último octeto de la IP de broadcast de dicha subred.

En este caso nos quedaría de la siguiente manera:

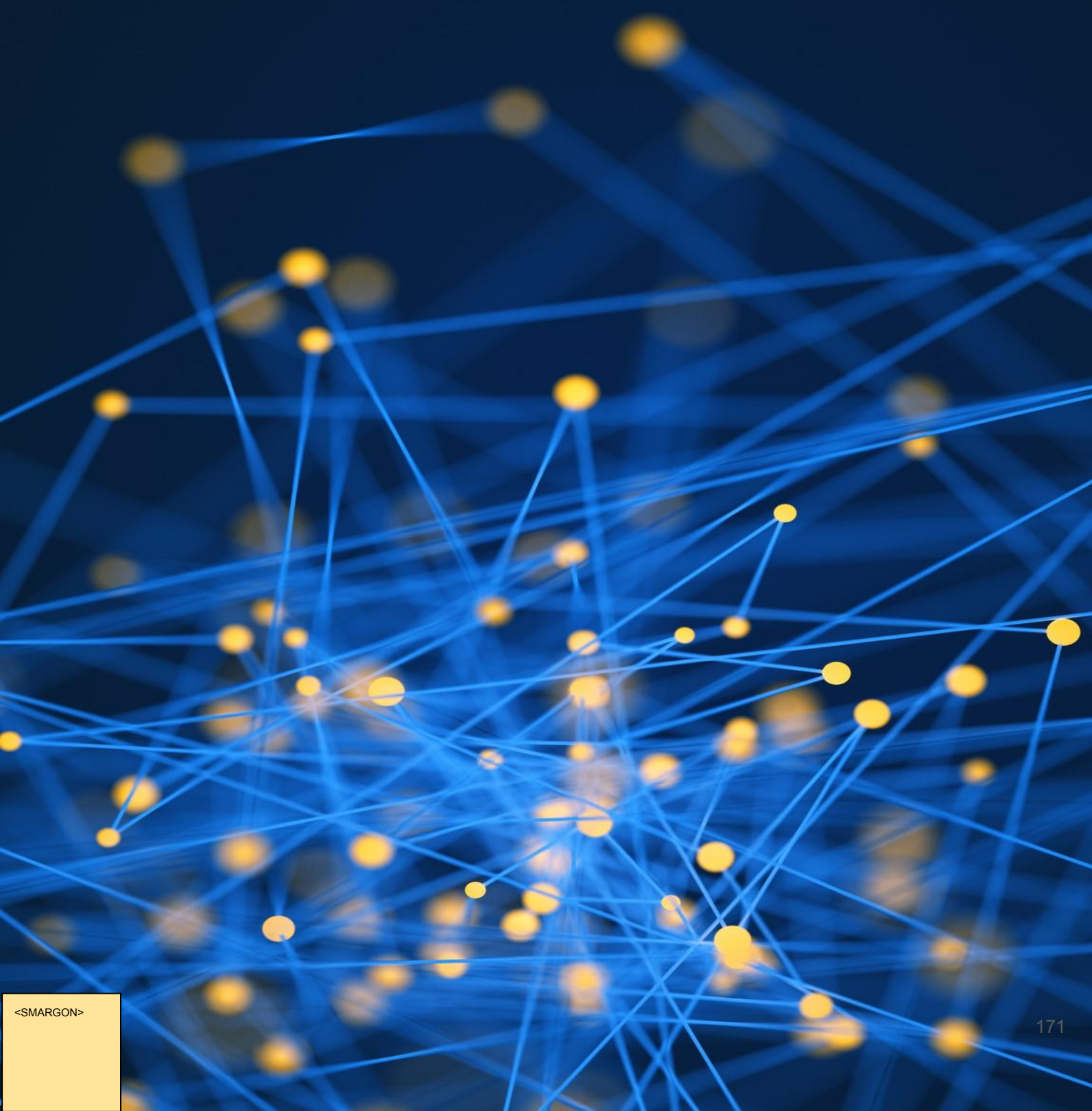
2.3

Nº SUBRED	ID SUBRED	PRIMER HOST	ÚLTIMO HOST	IP BROADCAST
0	124.0.0.0	124.0.0.1	124.15.255.254	124.15.255.255
1	124.16.0.0	124.16.0.1	124.31.255.254	124.31.255.255
2	124.32.0.0	124.32.0.1	124.47.255.254	124.47.255.255
3	124.48.0.0	124.48.0.1	124.63.255.254	124.63.255.255
4	124.64.0.0	124.64.0.1	124.79.255.254	124.79.255.255
5	124.80.0.0	124.80.0.1	124.95.255.254	124.95.255.255
6	124.96.0.0	124.96.0.1	124.111.255.254	124.111.255.255
7	124.112.0.0	124.112.0.1	124.127.255.254	124.127.255.255
8	124.128.0.0	124.128.0.1	124.143.255.254	124.143.255.255
9	124.144.0.0	124.144.0.1	124.159.255.254	124.159.255.255
10	124.160.0.0	124.160.0.1	124.175.255.254	124.175.255.255
11	124.176.0.0	124.176.0.1	124.191.255.254	124.191.255.255
12	124.192.0.0	124.192.0.1	124.207.255.254	124.207.255.255
13	124.208.0.0	124.208.0.1	124.223.255.254	124.223.255.255
14	124.224.0.0	124.224.0.1	124.239.255.254	124.239.255.255
15	124.240.0.0	124.240.0.1	124.255.255.254	124.255.255.255

Trabajo 2.4

Cisco Lab 2

Configurando Interfaces

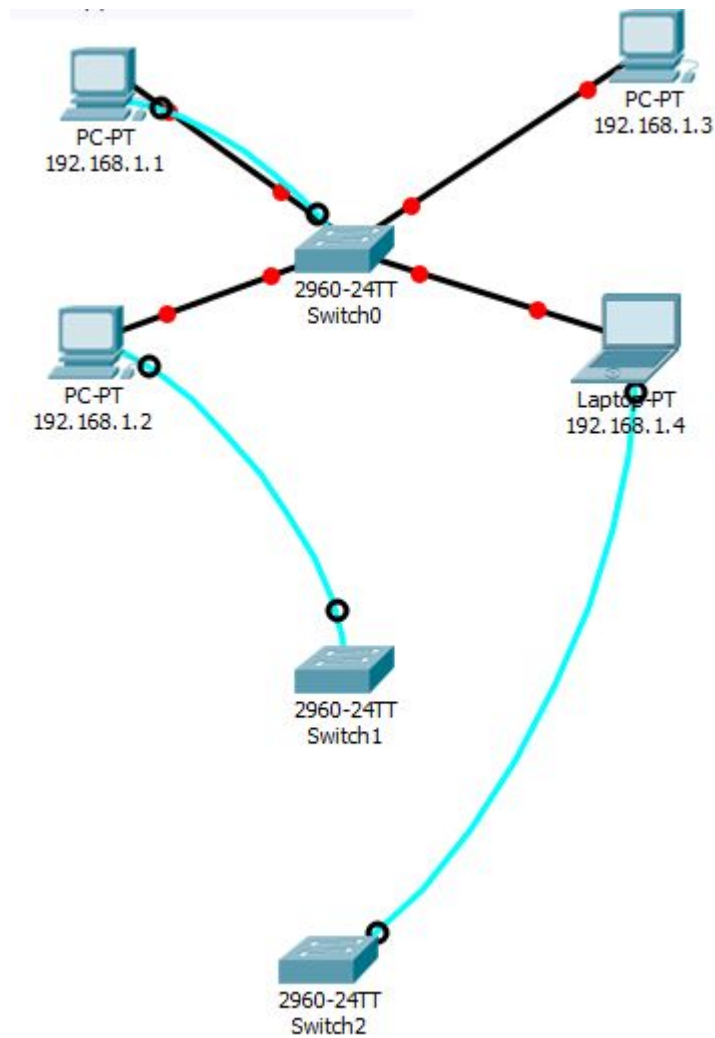


Cisco Lab 2: Configurando Interfaces

Cisco incluye en su academia de estudio numerosos ficheros de práctica para mejorar nuestra habilidad en el diseño, la configuración, la administración y la monitorización de redes de datos.

En este ejercicio se quiere que la red funcione correctamente.

La Red:



2.4

Figura 2.4.1. Red estropeada, 4 Pc 3 Switch

1º Entrar en la interfaz del Switch0 usando la consola y configurar cada puerto fastethernet
Port type: Access port
Speed : 100 Mbit/s
Duplex: Full Duplex
Autonegotiation deshabilitada

Primero, elegimos el pc 192.168.1.1 que está conectado por cable al Switch0 luego entramos en la terminal y nos disponemos a activar la configuración de los puertos Fastethernet.

2.4

Modo administrador:	Enable
Configurar terminal:	Configure terminal
Configurar Fastethernet 1-4:	interface range fastethernet 0/1 - 4
velocidad:	speed
duplex:	duplex full
	no shutdown

¿Por qué no podemos hacer ping con el PC4? - Porque se encuentra en otra vlan.

Para ver las vlan y las bocas fastethernet a las que pertenecen usamos este comando:

`"show vlan brief"`

2º.- Necesitamos que el PC4 "192.168.1.4" pueda comunicarse con los demás.

Una vez sabemos que está en otra vlan , nos dirigimos al Switch y configuramos la boca fastethernet en la que se encuentre conectado el PC4.

La boca en la que está es la Fastethernet 4

Modo administrador:	Enable
Configurar terminal:	Configure terminal
Configurar Fastethernet 4:	interface range fastethernet 0/ 4
Configurar el acceso a la vlan 1	switchport access vlan 1

3. Elegir el cable correcto :

- Switch0 gigabitethernet 0/1 to Switch1 gigabitethernet 0/1
- Switch1 gigabitethernet 0/2 to Switch2 gigabitethernet 0/2

El cable necesario para unir dos Switch es el cable cruzado



Así queda la red una vez unidos:

2.4

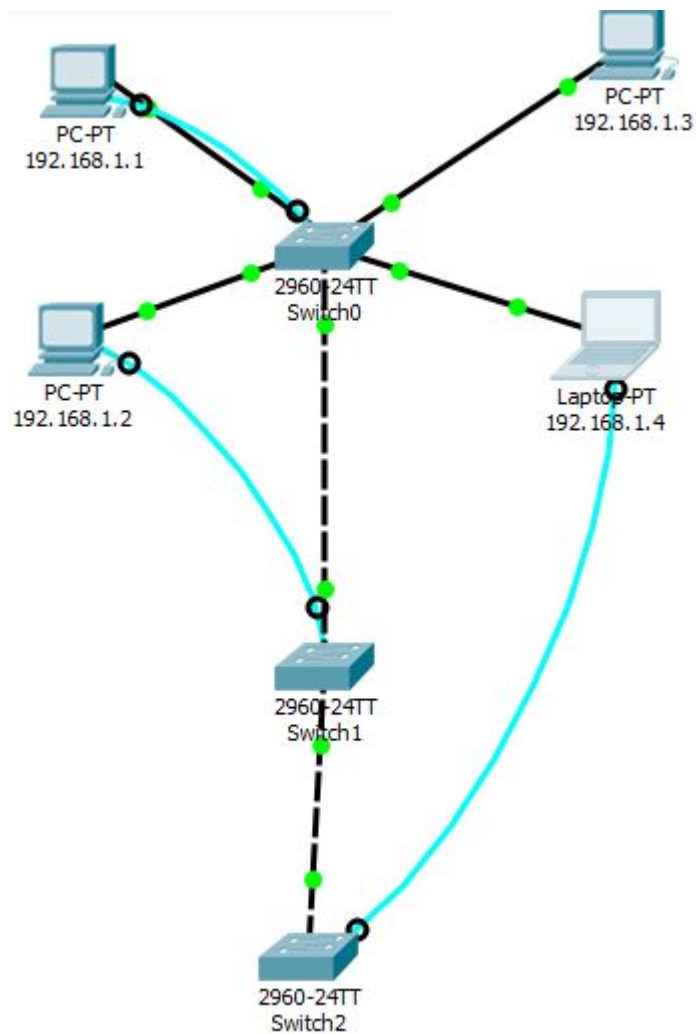


Figura 2.4.3. Red Switch conectados

4. Configurar las dos líneas como modo trunk.

Entramos en la terminal del Switch0 y configuramos el puerto **Gigabitethernet 0/1** que está conectado al Switch 1.

	"Enable"
	"Configure terminal"
Configurar Gigabitethernet 0/1	"interface gigabitethernet 0/1"
Configurar puerto modo trunk:	"switchport mode trunk"
	"no shutdown"

2.4

En el switch1 realizamos los mismos pasos para la boca gigabitethernet 0/1 y 0/2 ya que este switch está conectado con el Switch0 y el Switch2.

Por último, configuramos el Switch2 su boca gigabitethernet 0/2 , la cual está conectada con el Switch1 .

Prueba de conexión del PC4 con otro pc de la red.

```
C:\>ping 192.168.1.1

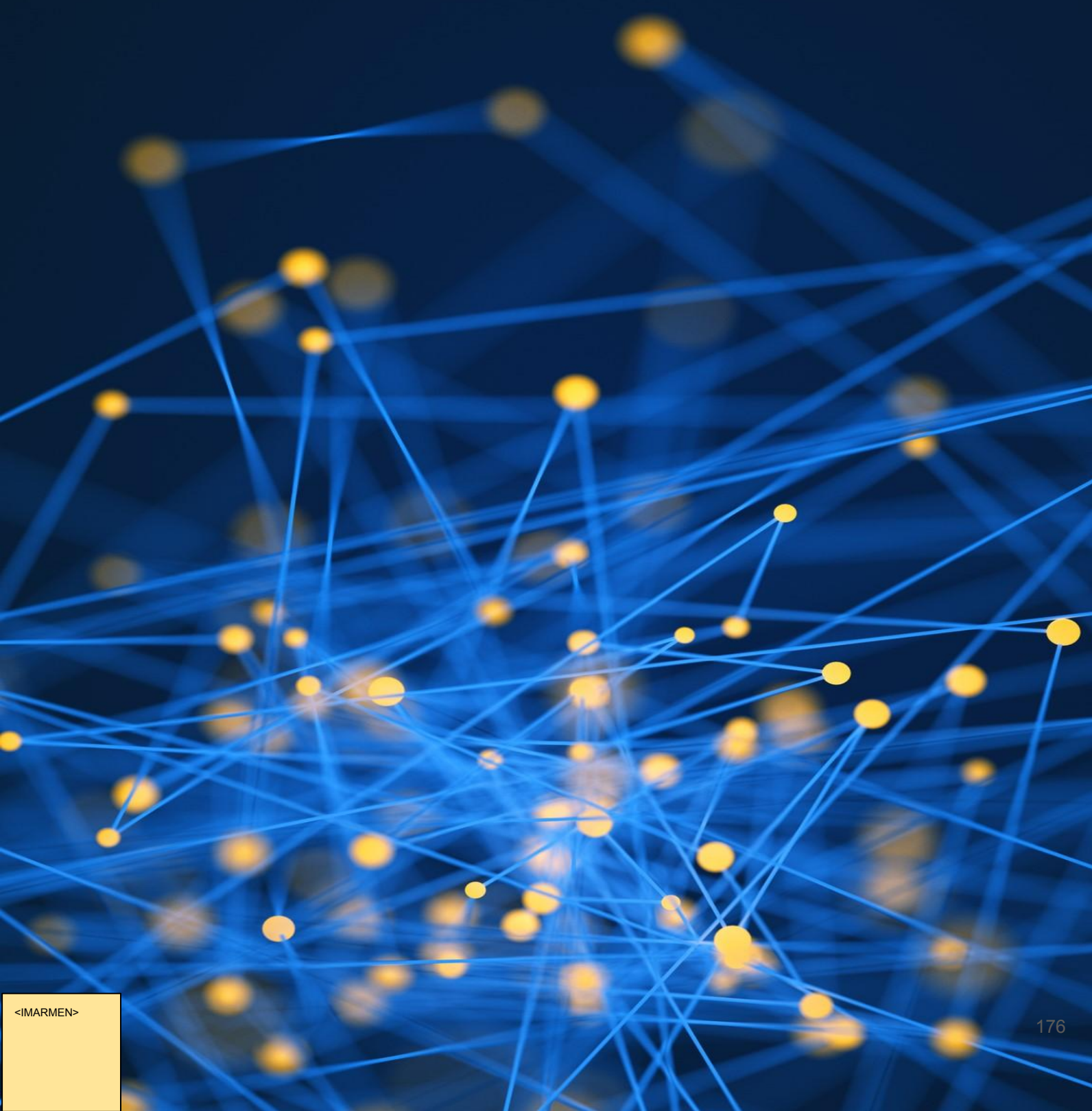
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=5ms TTL=128
Reply from 192.168.1.1: bytes=32 time=3ms TTL=128
```

Figura 2.4.2. Ping desde PC0 a PC4

Trabajo 3.1

Enrutamiento estático en routers corporativos.



Trabajo 3.1 Enrutamiento estático en routers corporativos

3.1.1 Diseño de la red.

- Diseña la red tal y como se muestra en la imagen:
 - Añade los componentes (routers, switches y PCs)
 - Une los routers mediante líneas seriales (es posible que tengas que añadir a los routers módulo serial)
 - Añade las etiquetas de texto de las redes y de las líneas seriales
 - Añade los cuadros de colores para cada subred

3.1.2 Configura las bocas de los routers

- Teniendo el diseño en mente en todo momento
- Asigna la dirección IP y la máscara
- Activa la boca

3.1.3 Muestra el estado de las bocas del router

- Comprueba el estado a nivel físico y el estado a nivel de enlace está activo
- Desactiva una de las bocas y comprueba qué ocurre con el estado a nivel físico
- Vuelve a activarla
- Elimina el cable de conexión y comprueba qué ocurre con el estado

3.1.4 Otra visualización del estado del router show protocols

- Con las bocas ya configuradas y las conexiones establecidas, muestra el estado del router utilizando el comando show protocols
- Comenta la información aportada

3.1.5 Más información sobre el router show version

- Mediante el comando show version recupera la siguiente información:
 - Tiempo que lleva el router encendido de forma no interrumpida
 - Número de puertos Gigabit Ethernet
 - Número de puertos serie
 - Versión de la ROM instalada

3.1.6 Configuración de rutas estáticas.

a) Gráficamente.

- Llegados a este punto ya tenemos el diseño de la red realizado
- Todavía NO hay conectividad entre los PCs
- Vamos ahora a configurar de forma estática las rutas
- Debes tener en mente tu esquema de la red
- Dentro de cada router establecemos:
 - Dirección de red
 - Máscara
 - Siguiendo salto

b) Desde línea de comandos.

3.1.7 Configuración de los PCs

- Respetar la dirección de subred de cada uno
- Establece correctamente la máscara de subred
- Configura la dirección del gateway (router) de cada uno de ellos

3.1.8 Comprobamos la conectividad

- Razona sobre la siguiente cuestión:
- ¿Puede haber conectividad del PC0 al PC1 y NO al contrario? ¿Es eso posible?

Trabajo 3.1 Enrutamiento estático en routers corporativos

3.1.9 Diseño de la red.

- ver
- Vemos las rutas estáticas definidas

3.1.10 Mostrar tabla de routeo

- Show ip route
 - L rutas locales a una IP específica, a un host específico
- Los routers usan rutas locales para aumentar rendimiento
 - C redes directamente conectadas
 - Nos muestra también por qué boca están conectadas

3.1.11 Probamos el routing con traceroute

- Prueba una consola de comandos de un PC el funcionamiento del comando tracert y explica razonadamente la salida que muestra por pantalla

3.1.12 Uso del comando arp

- Prueba desde una consola de comandos de un PC el funcionamiento del comando arp
- Muestra cómo inicialmente la tabla arp de un equipo está vacía y poco a poco va completando
- Demuestra además que en esta tabla únicamente se completan direcciones asociadas a equipos de la misma subred

Añadido 1. Delegación en Bilbao (172.16.7.0)

- Ahora añade una nueva delegación en Bilbao
- que tenga como identificador de red 172.16.6.0/24
- Esta nueva delegación está conectada a Barcelona.
- Prueba ahora que hay conectividad entre toda la red.

Añadido 2. Enlace Barcelona-Sevilla. Envío Sevilla-Bilbao vía Barcelona, NO vía Madrid

- Añade ahora un enlace WAN que una Barcelona con Sevilla
- A partir de este momento, los paquetes de Sevilla con destino Bilbao irán directamente a Barcelona, sin pasar por Madrid.
- El resto de envíos desde Sevilla a cualquier otra delegación deberán ir vía Madrid

3.1.1 Diseño de la red.

- Diseña la red tal y como se muestra en la imagen:
 - Añade los componentes (routers, switches y PCs)
 - Une los routers mediante líneas seriales (es posible que tengas que añadir a los routers módulo serial)
 - Añade las etiquetas de texto de las redes y de las líneas seriales
 - Añade los cuadros de colores para cada subred

-Usaremos 3 routers 2901 para esta práctica conectados entre sí con el cable wan.

-Tendremos 3 sedes Madrid, Barcelona y Sevilla con 2 PC en cada sede y su respectivo switch.

-El esquema final quedaría así:

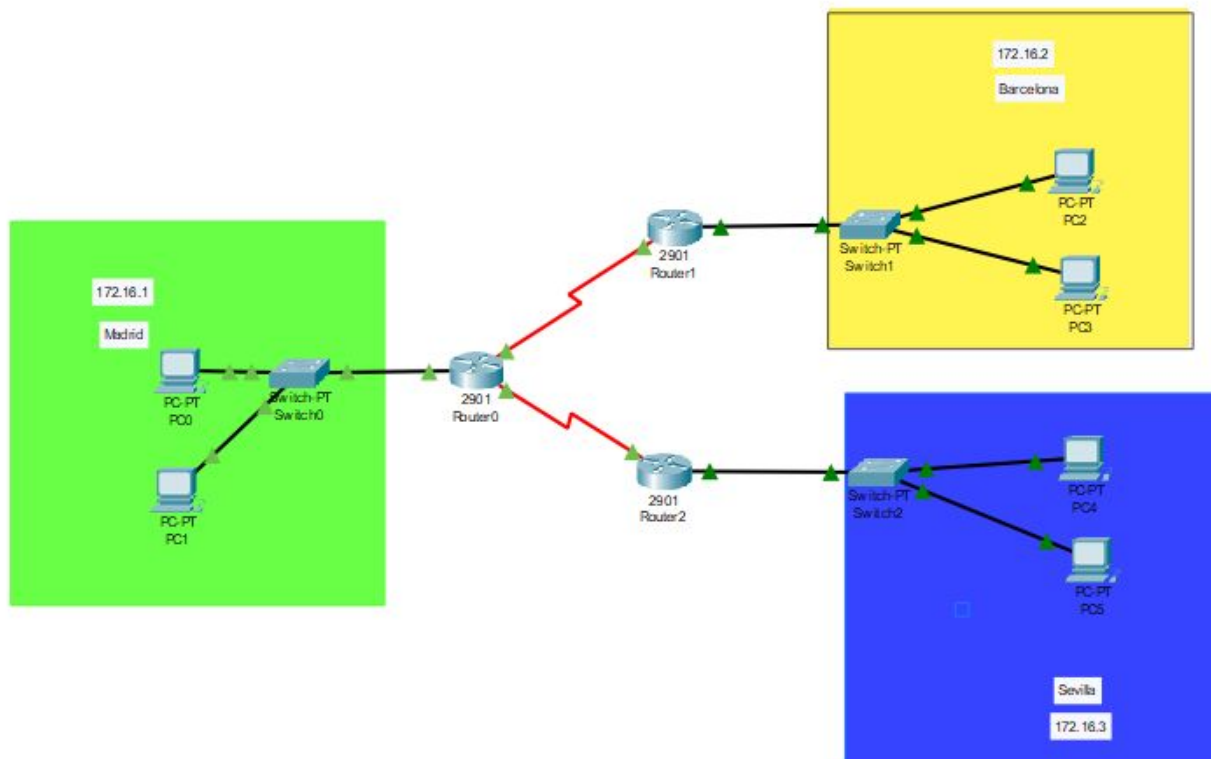


Figura 3.1.1.a Resultado de la red

Apartado 2 (I)

3.1.2 Configura las bocas de los routers

- Teniendo el diseño en mente en todo momento
- Asigna la dirección IP y la máscara
- Activa la boca

Router0:

Boca gigabitEthernet 0/0:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 172.16.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

3.1.2

Boca Serial 0/3/0:

```
Router(config)#interface Serial0/3/0
Router(config-if)#ip address 172.16.4.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Boca Serial 0/3/1:

```
Router(config)#interface Serial0/3/1
Router(config-if)#ip address 172.16.5.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

CopyRouter0:

Boca gigabitEthernet 0/0:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 172.16.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Boca Serial 0/3/0:

```
Router(config)#interface Serial0/3/0
Router(config-if)#ip address 172.16.4.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Apartado 2 (II)

3.1.2 Configura las bocas de los routers

- Teniendo el diseño en mente en todo momento
- Asigna la dirección IP y la máscara
- Activa la boca

Router4:

Boca gigabitEthernet 0/0:

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 172.16.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

3.1.2

Boca Serial 0/3/1:

```
Router(config)#interface Serial0/3/1
Router(config-if)#ip address 172.16.5.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Una vez hecho todo esto, quedaría la red tal que así:

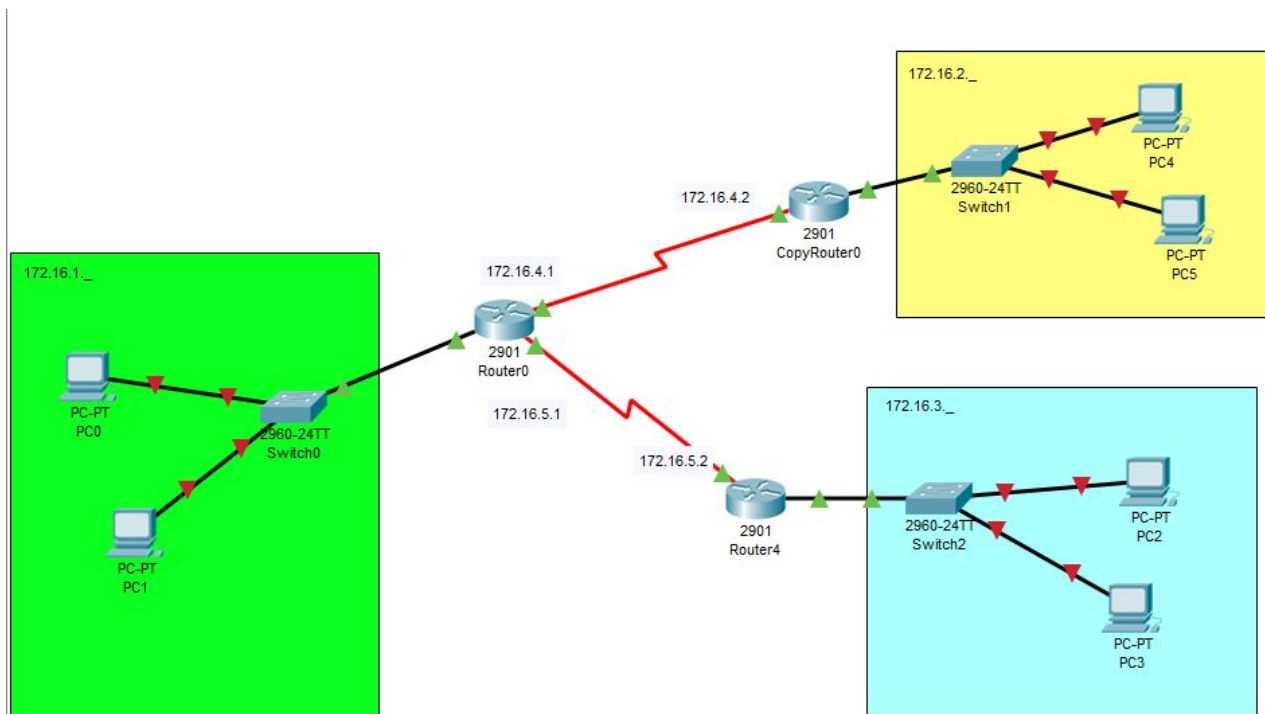


Figura 3.1.2.a Resultado de la red

3.1.3 Muestra el estado de las bocas del router

- Comprueba que el estado a nivel físico y el estado a nivel de enlace está activo
- Desactiva una de las bocas y comprueba qué ocurre con el estado a nivel físico
- Vuelve a activarla
- Elimina el cable de conexión y comprueba qué ocurre con el estado

Se puede observar en la **Figura 3.1.3.a** el estado de los enlaces de manera física identificándose con los triángulos en verde en todos los puntos de enlace.

3.1.3

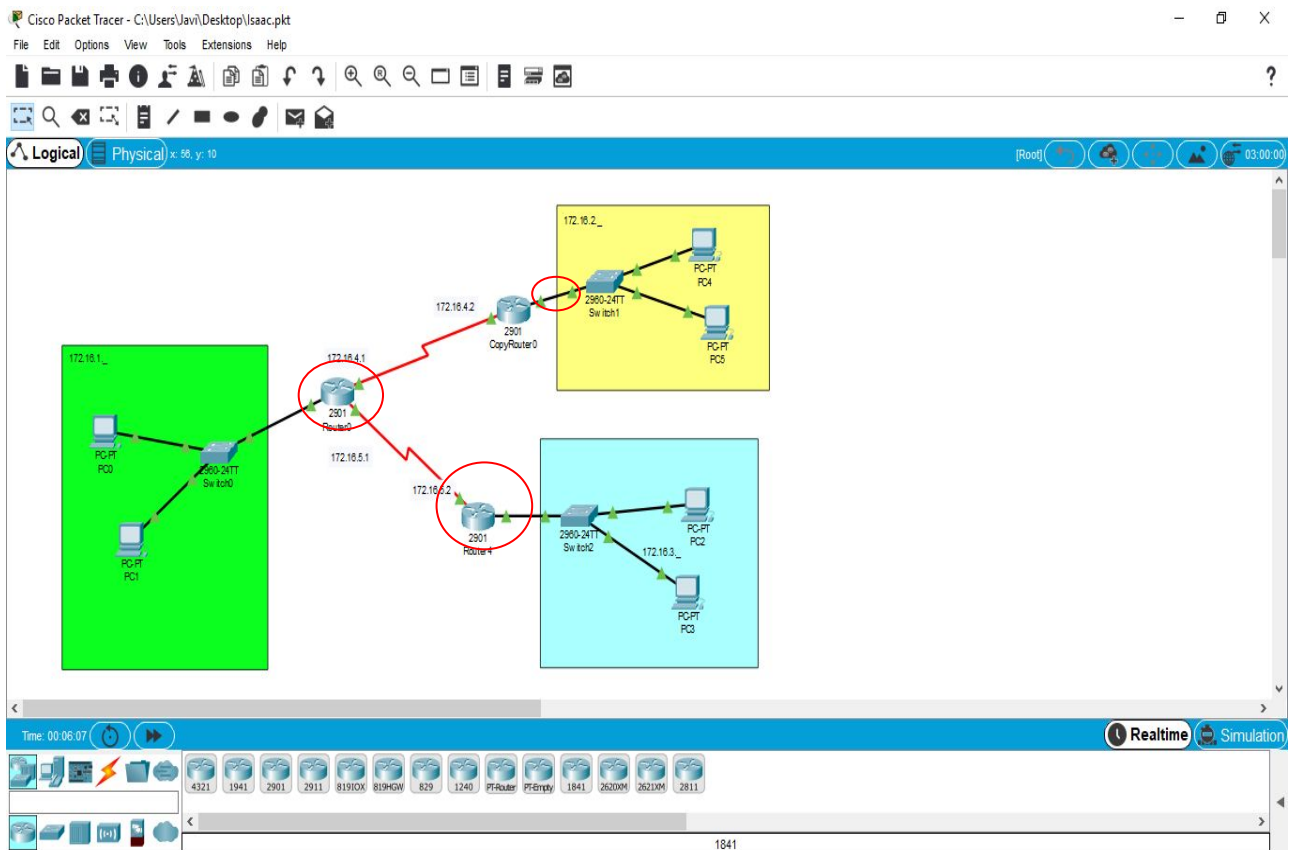


Figura 3.1.3.a Mostrar estado del router a nivel físico

- Estado de la red a nivel de enlace

Para ver el estado del router a nivel de enlace entramos en la CLI y escribiremos el comando "show ip interface brief". Véase Figura 3.1.3.b y obsérvese que los dos códigos de estado marcan UP.

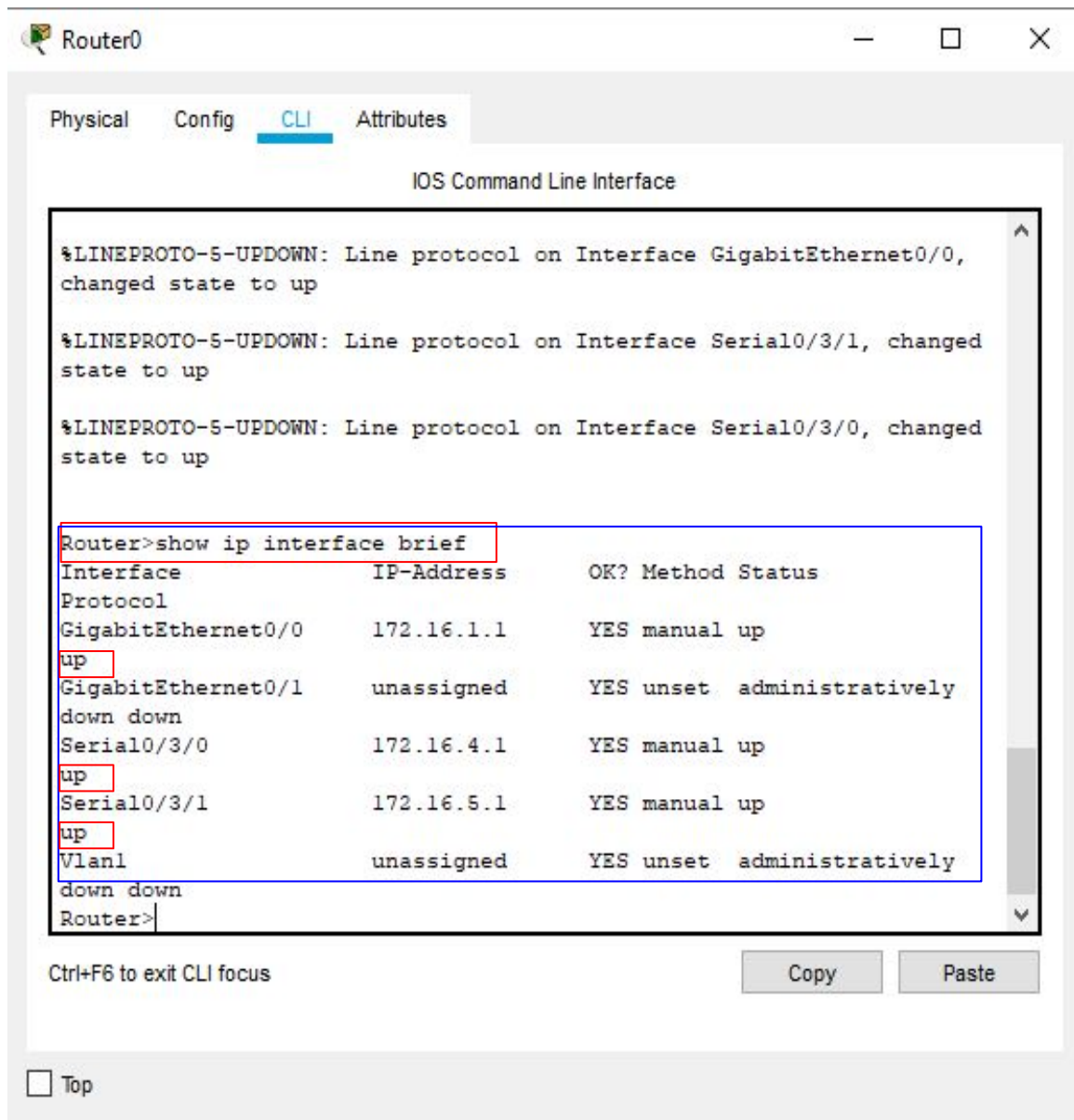
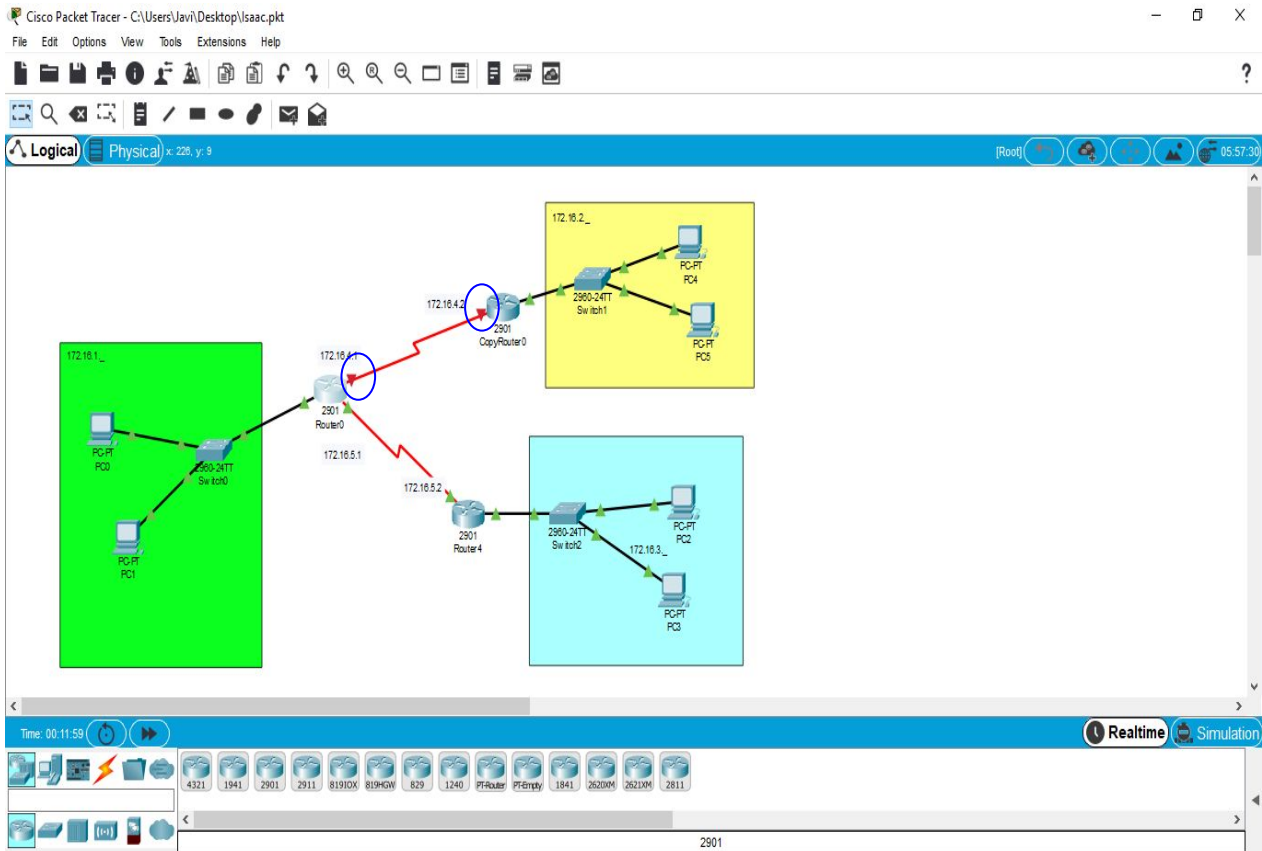


Figura 3.1.3.b Mostrar estado del router a nivel enlace

- Estado de la red a nivel físico y enlace con boca mal. Apagamos la boca serial 0/3/0 y en la imagen se muestra como el enlace está en rojo es decir no hay conexión y a nivel de enlace se puede apreciar como está apagada dicha boca.



3.1.3

Figura 3.1.3.c Mostrar estado del router a nivel fisico boca mal

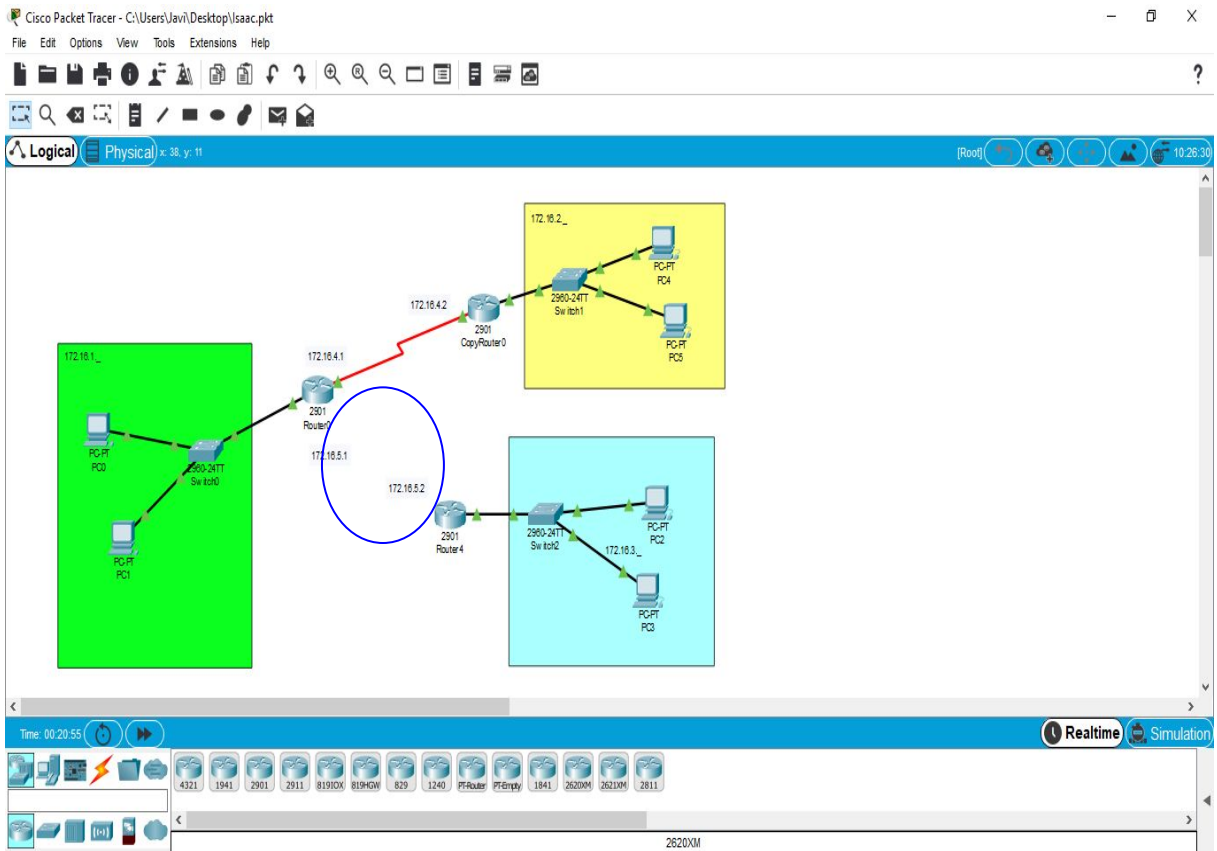
```

Router0
Physical Config CLI Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed
state to down
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0 172.16.1.1     YES manual up
up
GigabitEthernet0/1 unassigned     YES unset  administratively
down down
Serial0/3/0        172.16.4.1     YES manual administratively
down down
Serial0/3/1        172.16.5.1     YES manual up
up
Vlan1              unassigned     YES unset  administratively
down down
Router#
  
```

Figura 3.1.3.d Mostrar estado del router a nivel enlace boca mal

<JACOGON>

- Estado de la red a nivel enlace quitando cable. Volvemos activar la boca y para realizar una comprobación más directa desconectas un cable. Para evitar conflictos quitamos el cable del otro serial 0/3/1.



3.1.3

Figura 3.1.3.e Mostrar estado del router a nivel fisico sin cable

```

Router0
Physical Config CLI Attributes
IOS Command Line Interface
*SYS-5-CONFIG_I: Configured from console by console
Router#
*LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed
state to up
*LINK-3-UPDOWN: Interface Serial0/3/1, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed
state to down
Router#show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0 172.16.1.1      YES manual up
up
GigabitEthernet0/1 unassigned      YES unset  administratively
down down
Serial0/3/0        172.16.4.1      YES manual up
up
Serial0/3/1        172.16.5.1      YES manual down
down
Vlan1              unassigned      YES unset  administratively
down down
Router#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
  
```

Figura 3.1.3.f Mostrar estado del router a nivel enlace sin cable

Apartado 4

3.1.4 Otra visualización del estado del router show protocols

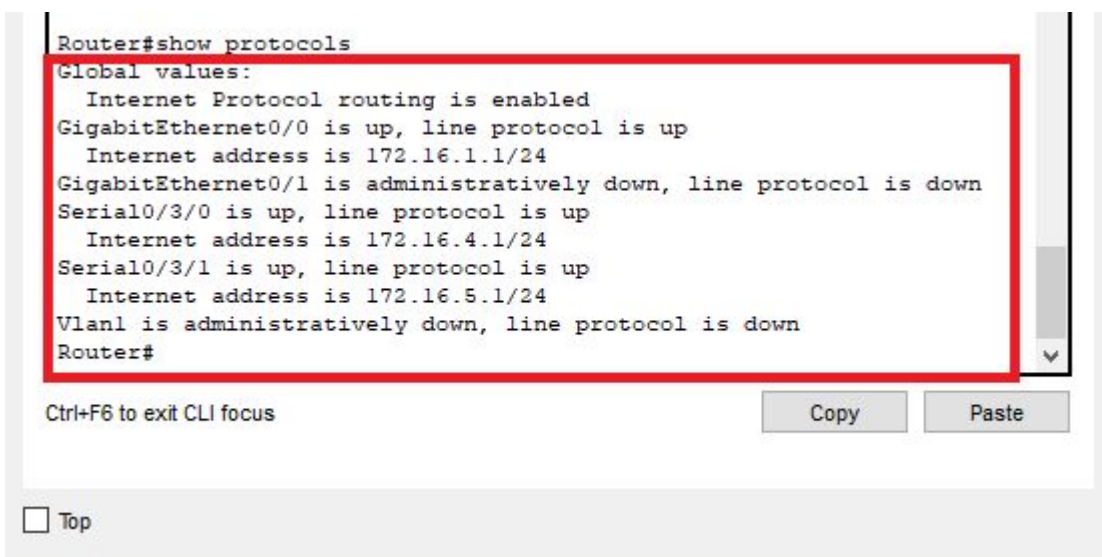
- Con las bocas ya configuradas y las conexiones establecidas, muestra el estado del router utilizando el comando show protocols
- Comenta la información aportada

Con las bocas seriales y las bocas Gigabit Ethernet encendidas y con sus correspondientes ips, entraremos en la consola del router y entramos al modo administrador a continuación introducimos el comando `show protocols` y veremos como nos aparece una serie de información acerca del estado de las bocas presionando podremos desplegar toda la información. la cadena de comandos sería la siguiente:

```
Router>enable
Router#show protocols
```

3.1.4

Esta sería toda la información de las bocas del router 1:

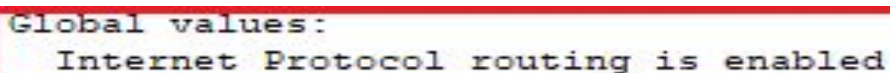


```
Router#show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.16.1.1/24
GigabitEthernet0/1 is administratively down, line protocol is down
Serial0/3/0 is up, line protocol is up
  Internet address is 172.16.4.1/24
Serial0/3/1 is up, line protocol is up
  Internet address is 172.16.5.1/24
Vlan1 is administratively down, line protocol is down
Router#
```

Figura 3.1.4 a. Ejecución del comando `show protocols`

A continuación pasaré a explicar qué significa cada una de esas líneas que nos dan información acerca del estado de las bocas del router:

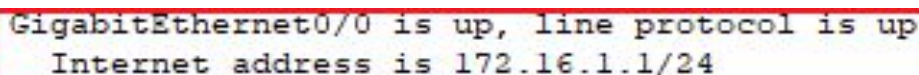
En la primera línea nos indica que el protocolo de routing está habilitado de manera global.



```
Global values:
  Internet Protocol routing is enabled
```

Figura 3.1.4 b. Protocolo de internet habilitado

En la segunda línea nos indica que la boca Gigabit Ethernet 0/0 está activada, "Gigabit Ethernet is up". También nos indica que hay un cable conectado en esta boca "line protocol is up" y por último nos dice la dirección ip de la boca "internet address is 172.16.1.1/24"



```
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.16.1.1/24
```

Figura 3.1.4 c. Estado de la boca Gigabit ethernet 0/0

Apartado 4

3.1.4 Otra visualización del estado del router show protocols

- Con las bocas ya configuradas y las conexiones establecidas, muestra el estado del router utilizando el comando show protocols
- Comenta la información aportada

En la tercera línea nos indica que la boca Gigabit Ethernet 0/1 está desactivada, "Gigabit Ethernet 0/1 is administratively down". También nos indica que no hay un cable conectado en esta boca "line protocol is down".

```
GigabitEthernet0/1 is administratively down, line protocol is down
```

Figura 3.1.4 d. Estado de la boca Gigabit Ethernet 0/1

3.1.4

En la cuarta y quinta línea nos encontramos con las bocas seriales 0/3/0 y 0/3/1 ambas están activadas "serial *x/x/x* is up" y ambas tienen un cable conectado "line protocol is up", por último se nos indica la ip de cada una de las bocas "internet address is *x.x.x/x*"

```
Serial0/3/0 is up, line protocol is up
  Internet address is 172.16.4.1/24
Serial0/3/1 is up, line protocol is up
  Internet address is 172.16.5.1/24
```

Figura 3.1.4 e. Estado de las bocas seriales 0/3/0 y 0/3/1

Por último nos encontramos con la información acerca de las VLANs como podemos observar la vlan 1 está desactivada, "Vlan1 is administratively down" y tampoco tiene ningún cable conectado a una boca que pertenezca a esta Vlan, "line protocol is down"

```
Vlan1 is administratively down, line protocol is down
```

Figura 3.1.4 f. Estado de la Vlan1

3.1.5 Más información sobre el router show version

- Mediante el comando show version recupera la siguiente información:
- Tiempo que lleva el router encendido de forma no interrumpida
- Número de puertos Gigabit Ethernet
- Número de puertos serie
- Versión de la ROM instalada

Mediante el comando **show version** recupera la siguiente información:

- Tiempo que lleva el router encendido de forma no interrumpida
- Número de puertos Gigabit Ethernet
- Número de puertos serie – Versión de la ROM instalada
- **Información de reinicio del sistema:** método de reinicio (por ejemplo, apagado y encendido, colapso).
- **Nombre de la imagen del software:** nombre del archivo de IOS almacenado en la memoria flash.
- **Tipo de router y tipo de procesador:** número de modelo y tipo de procesador.
- **Tipo y asignación de memoria (compartida/principal):** memoria RAM del procesador principal y almacenamiento en búfer de E/S de paquetes compartidos.
- **Características del software:** protocolos y conjuntos de características admitidos.
- **Interfaces de hardware:** interfaces disponibles en el dispositivo.
- **Registro de configuración:** establece especificaciones de arranque, la configuración de velocidad de la consola y parámetros relacionados.

3.1.5

```
Router#show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, REL
EASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco2901 uptime is 1 hours, 15 minutes, 33 seconds
System returned to ROM by power-on
System image file is "flash0:c2900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wvl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO2901/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:
-----
Device# PID SN
-----
*0 CISCO2901/K9 FTX15240000

Technology Package License Information for Module:'c2900'
-----
Technology Technology-package Technology-package
```

Figura 3.1.5. Ejecución del comando show version

Apartado 6

3.1.6 Configuración de rutas estáticas

a) Gráficamente.

- Llegados a este punto ya tenemos el diseño de la red realizado
- Todavía NO hay conectividad entre los PCs
- Vamos ahora a configurar de forma estática las rutas
- Debes tener en mente tu esquema de la red
- Dentro de cada router establecemos:
 - Dirección de red
 - Máscara
 - Siguiente salto

Para realizar este ejercicio, lo primero que debemos tener claro es qué es el enrutamiento, y entrando más en detalle, qué es una ruta estática.

3.1.6

De manera simple podemos decir que el enrutamiento es el proceso que el router utiliza para decidir dónde enviar un paquete. Podemos imaginar el router como un centro de tratamiento de cartas de correo, encargándose de recibir todas las cartas, separar de acuerdo a su destino y enviarlas por el mejor camino.

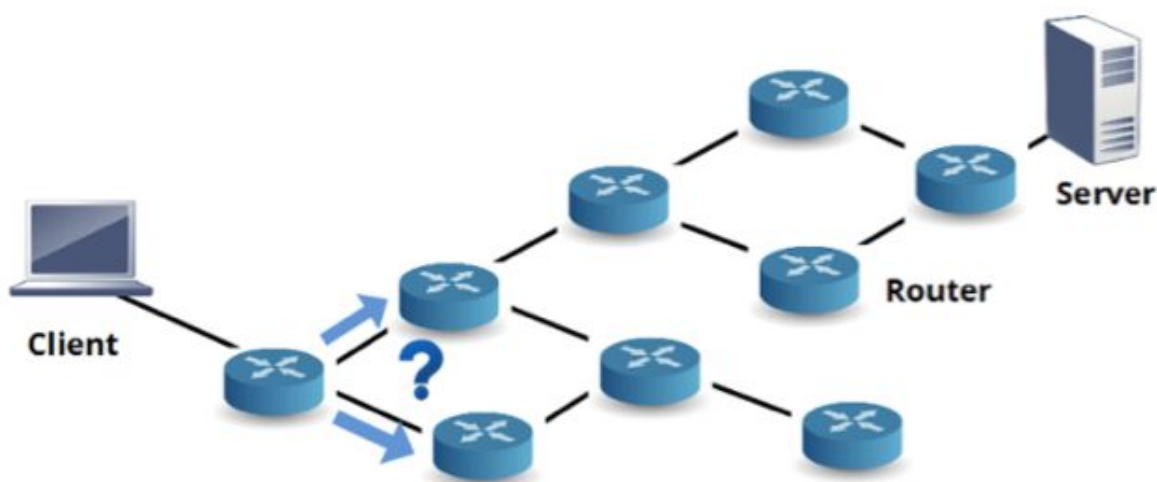


Figura 3.1.6.A. Mapa de posibles rutas Cliente-Servidor de un paquete.

Para ello, el router consulta la tabla de ruteo que le dice cuál es el mejor camino por donde enviar este paquete. Esta tabla puede rellenarse de manera dinámica, utilizando un algoritmo, o de manera estática.

Para crear las rutas estáticas hay que tener un pleno conocimiento de la red, pues las rutas tienen que ser agregadas de manera manual por todo el camino, es decir, estableciendo paso a paso el camino que deberán seguir los paquetes hacia un destino, haciendo que esta solución no sea muy escalable.

Apartado 6

Teniendo en mente el esquema de nuestra red, nos dispondremos a realizar la configuración de una ruta estática de manera gráfica. Para ello, deberemos pulsar en el router a configurar, como puede ser el Router0:



Ahora, pulsaremos en la pestaña 'config', y nos iremos al apartado 'Routing/Static', como se puede ver en la **Figura 3.1.6.B**.

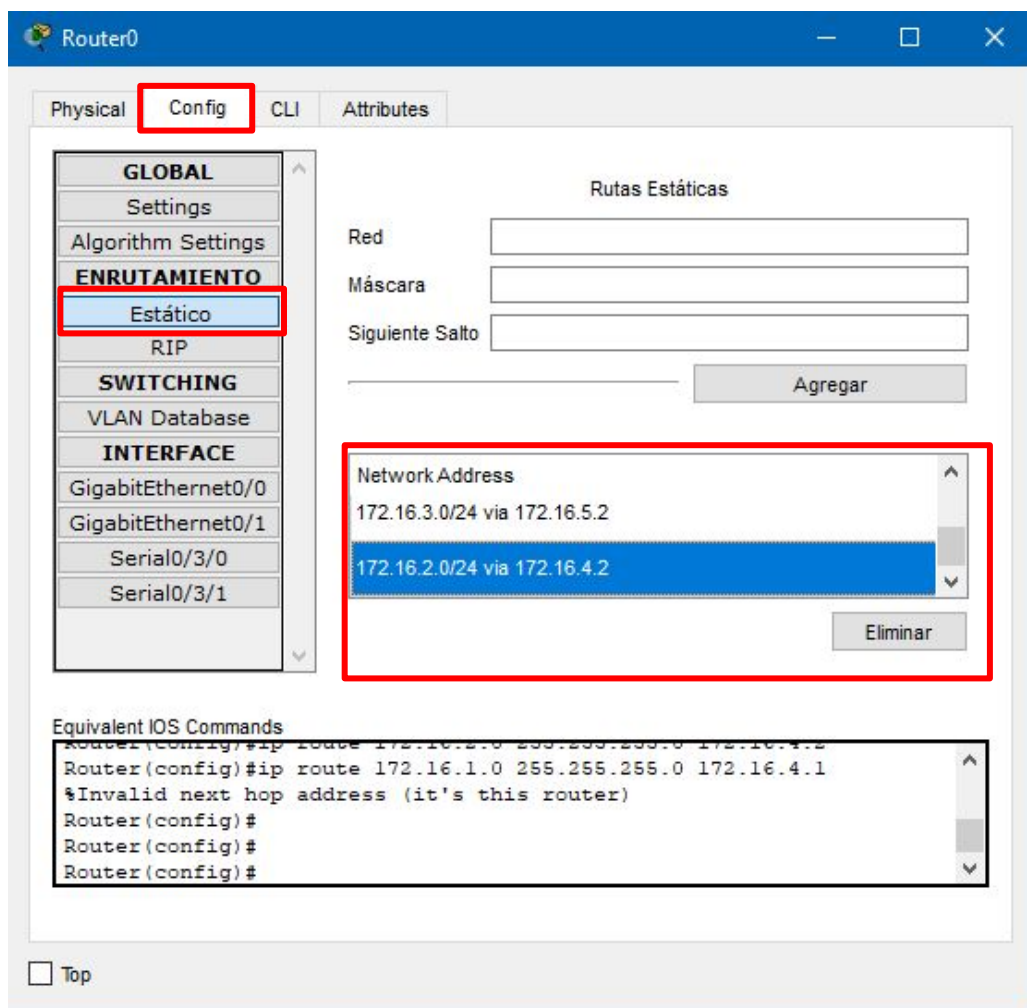
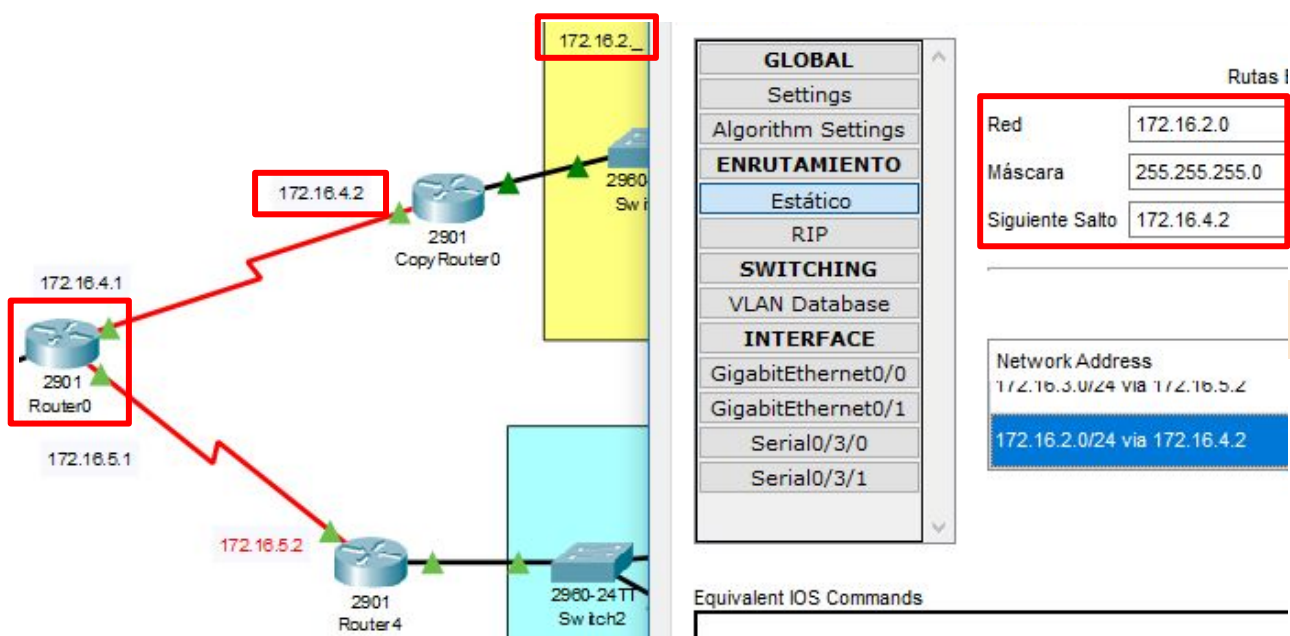


Figura 3.1.6.B. Pestaña de configuración gráfica del router.

Como vemos en dicha **Figura 3.1.6.B**, en el cuadro remarcado en rojo '**Network Address**', tenemos configuradas dos rutas. Esto se ha conseguido rellenando las casillas de *Network*, *Mask* y *Next Hop*.

Apartado 6

En *Network* y *Mask* pondremos la dirección de red, y la máscara asociada, a la que queremos “llegar”, y en *Next Hop*, deberemos poner la IP de la boca del enlace WAN del router más cercano a dicha red.



3.1.6

Figura 3.1.6.C. Configuración de rutas estáticas.

Como vemos en la **Figura 3.1.6.C**, desde el Router0, para llegar a la red 172.16.2.0, deberemos ir hasta el CopyRouter0 a través de la boca de este router con IP 172.16.4.2.

Por tanto, deberemos usar estos datos para rellenar los apartados *Network* (172.16.2.0), *Mask* (255.255.255.0) y *Next Hop* (172.16.4.2), como así aparece resaltado en color rojo.

Si te da algún problema, prueba a:

Esto deberá ser realizado después de haber entrado en el modo #enable de la consola.

3.1.6 Configuración de rutas estáticas

b) Desde línea de comandos.

Por otra parte, esto podrá ser configurado también a través de la consola mediante comandos. Para ello, procederemos a realizar la siguiente secuencia de comandos a través de la CLI del router:

```
enable
configure terminal
ip route 172.16.2.0 255.255.255.0 172.16.4.2
```

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#ip route 172.16.2.0 255.255.255.0 172.16.4.2
```

Figura 3.1.6.D. CLI del Router0 mostrando la secuencia de comandos utilizada.

12.8 Comprobamos la conectividad


1. Razona sobre la siguiente cuestión:

- ¿Puede haber conectividad del PC0 al PC1 y NO al contrario? ¿Es eso posible?

3.1.8

Para comprobar si existe conectividad entre los diferentes equipos de cada uno de los tres departamentos (Madrid, Sevilla y Barcelona) se puede realizar de dos diferentes maneras, usando el modo gráfico del Cisco Packet Tracer o ingresando en la consola de uno de los PCs de estos departamentos y utilizar el comando ping:

1. Usando el modo gráfico del Cisco Packet Tracer.

Para comprobar si existe conectividad entre dos ordenadores usando el modo gráfico del Cisco Packet Tracer debemos como en la parte superior de la pantalla principal del programa existe este icono (), el cual si hacemos click sobre él y seguidamente hacemos click sobre los dos PCs los cuales queremos comprobar si hay conectividad, éste enviará paquete ICMP entre dichos PCs. Para comprobar si este envío ha sido favorable en la parte inferior derecha existe la siguiente barra la cual muestra los últimos paquetes ICMP enviados, y en el caso de existe conectividad aparecerá el mensaje 'Successful' o en el caso de que no exista conectividad aparecerá el mensaje 'Failed'.

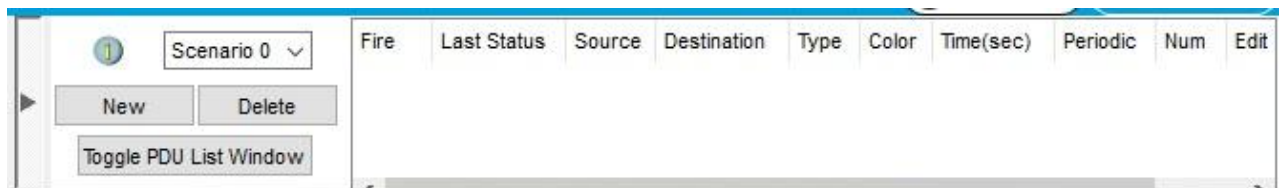


Figura 4.1.8.A. Barra Comprobación Paquetes

Ahora vamos a comprobar de esta manera si existe conectividad entre los diferentes departamentos:

Barcelona con Madrid y Sevilla.

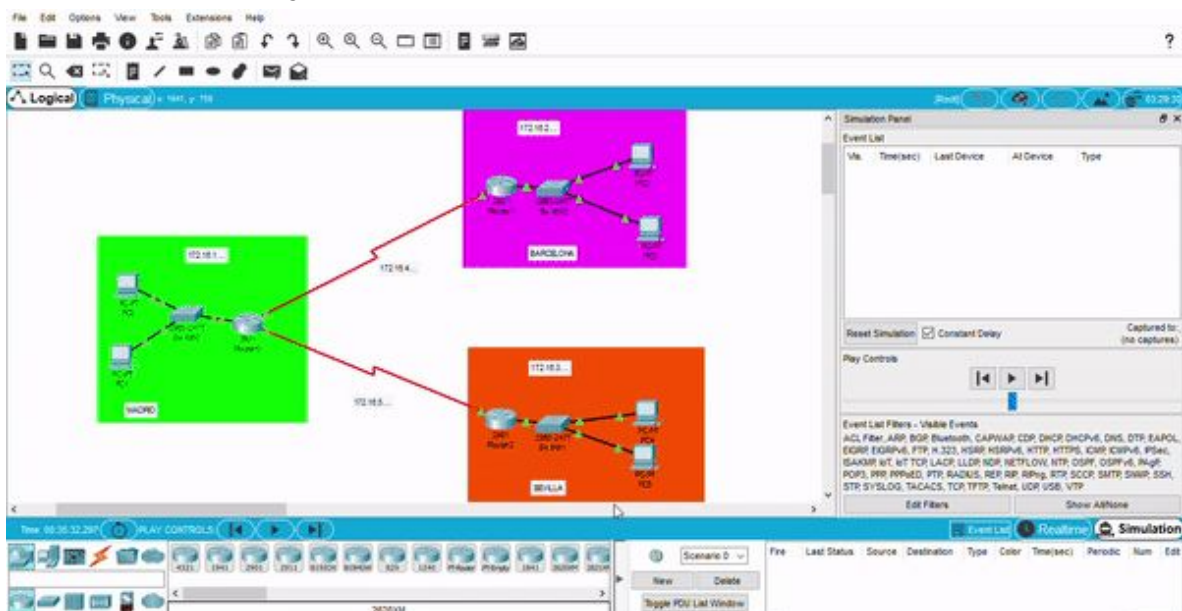
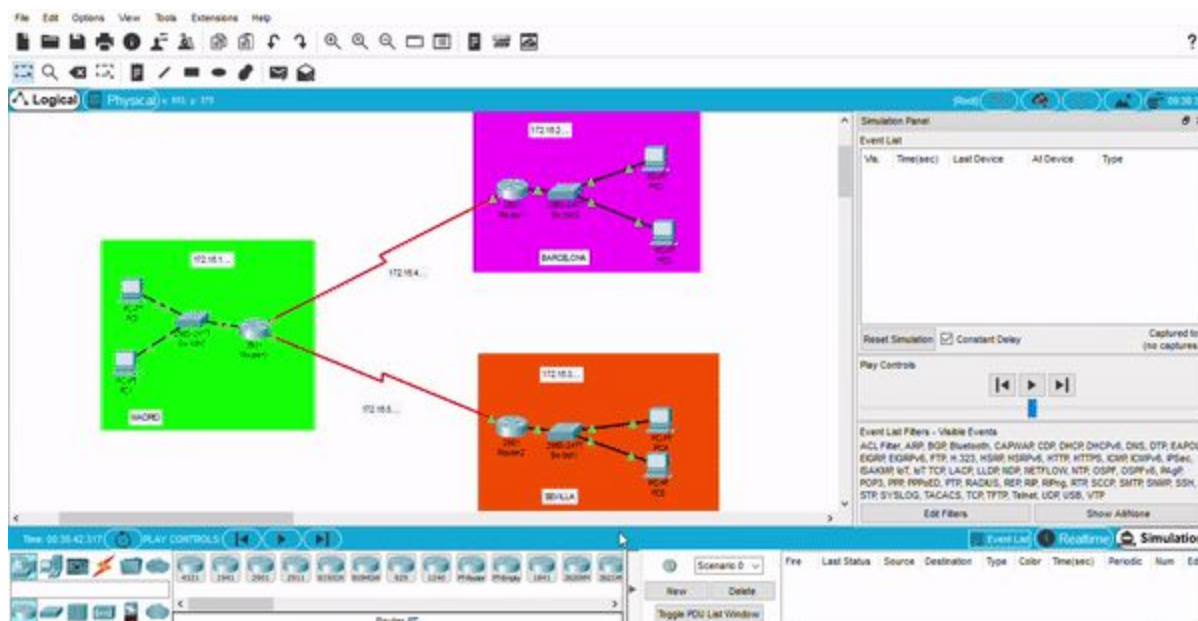


Figura 4.1.8.B. Conectividad Barcelona con Madrid y Sevilla

Madrid con Barcelona y Sevilla:



3.1.8

Figura 4.1.8.C. Conectividad Madrid con Barcelona y Sevilla

Sevilla con Madrid y Barcelona:

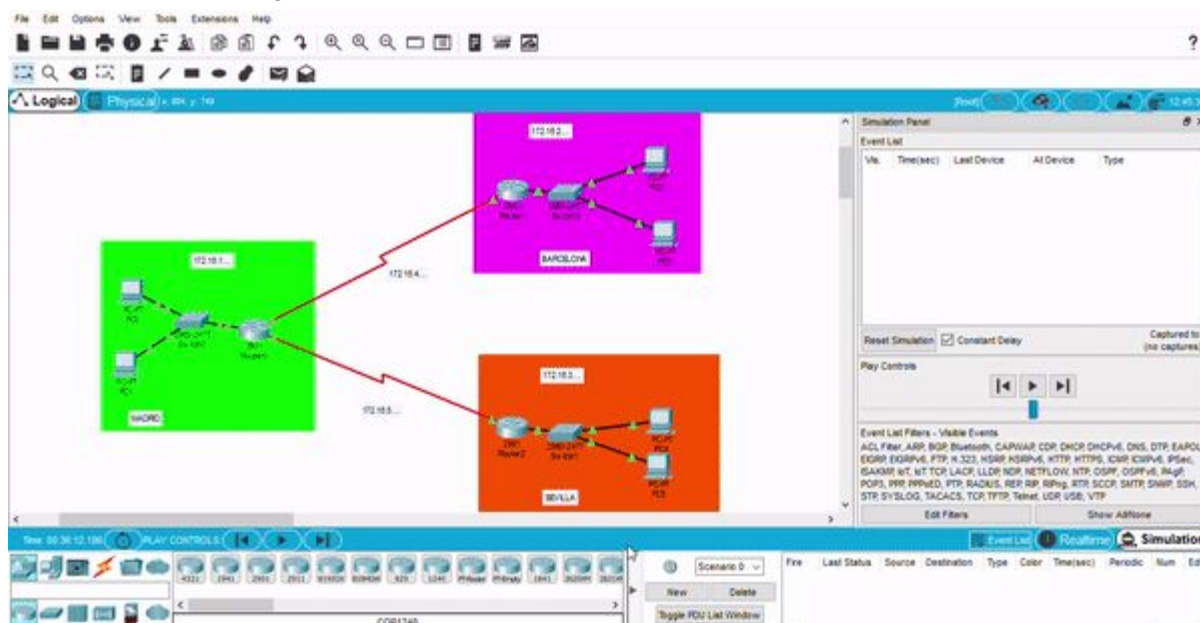


Figura 4.1.8.D. Conectividad Sevilla con Barcelona y Madrid

2. Usando la consola de los PCs y el comando Ping.

Para comprobar si existe conectividad entre dos PCs de dos diferentes departamentos se puede usar el comando 'ping' dentro de la consola de un PC de un departamento. Para acceder a dicha consola se realiza desde el 'Command Prompt' de cada PC al cual se accede desde la pestaña 'Desktop'.

Barcelona con Madrid y Sevilla.

The screenshot shows a Cisco Packet Tracer network configuration. The network is divided into three regions: Madrid (green), Barcelona (pink), and Sevilla (orange). Each region contains a 2901 Router and a 2950-24TT Switch. The Madrid region is connected to the Barcelona region via a 172.16.4... link, and to the Sevilla region via a 172.16.5... link. A Command Prompt window on PC2 shows the following output:

```

Packet Tracer PC Command Line 1.0
C:\>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.1.2: bytes=32 time=51ms TTL=126
Reply from 172.16.1.2: bytes=32 time=1ms TTL=126
Reply from 172.16.1.2: bytes=32 time=33ms TTL=126
Reply from 172.16.1.2: bytes=32 time=13ms TTL=126

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 61ms, Average = 24ms

C:\>ping 172.16.3.2

Pinging 172.16.3.2 with 32 bytes of data:

Reply from 172.16.3.2: bytes=32 time=3ms TTL=125
Reply from 172.16.3.2: bytes=32 time=1ms TTL=125
Reply from 172.16.3.2: bytes=32 time=27ms TTL=125
Reply from 172.16.3.2: bytes=32 time=14ms TTL=125

Ping statistics for 172.16.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 27ms, Average = 13ms

C:\>
    
```

3.1.8

Figura 4.1.8.E. Conectividad PING Barcelona con Madrid y Sevilla

Madrid con Barcelona y Sevilla.

The screenshot shows the same Cisco Packet Tracer network configuration as Figure 4.1.8.E. A Command Prompt window on PC0 shows the following output:

```

Packet Tracer PC Command Line 1.0
C:\>ping 172.16.2.2

Pinging 172.16.2.2 with 32 bytes of data:

Reply from 172.16.2.2: bytes=32 time=32ms TTL=126
Reply from 172.16.2.2: bytes=32 time=16ms TTL=126
Reply from 172.16.2.2: bytes=32 time=10ms TTL=126
Reply from 172.16.2.2: bytes=32 time=11ms TTL=126

Ping statistics for 172.16.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 25ms, Average = 15ms

C:\>ping 172.16.3.2

Pinging 172.16.3.2 with 32 bytes of data:

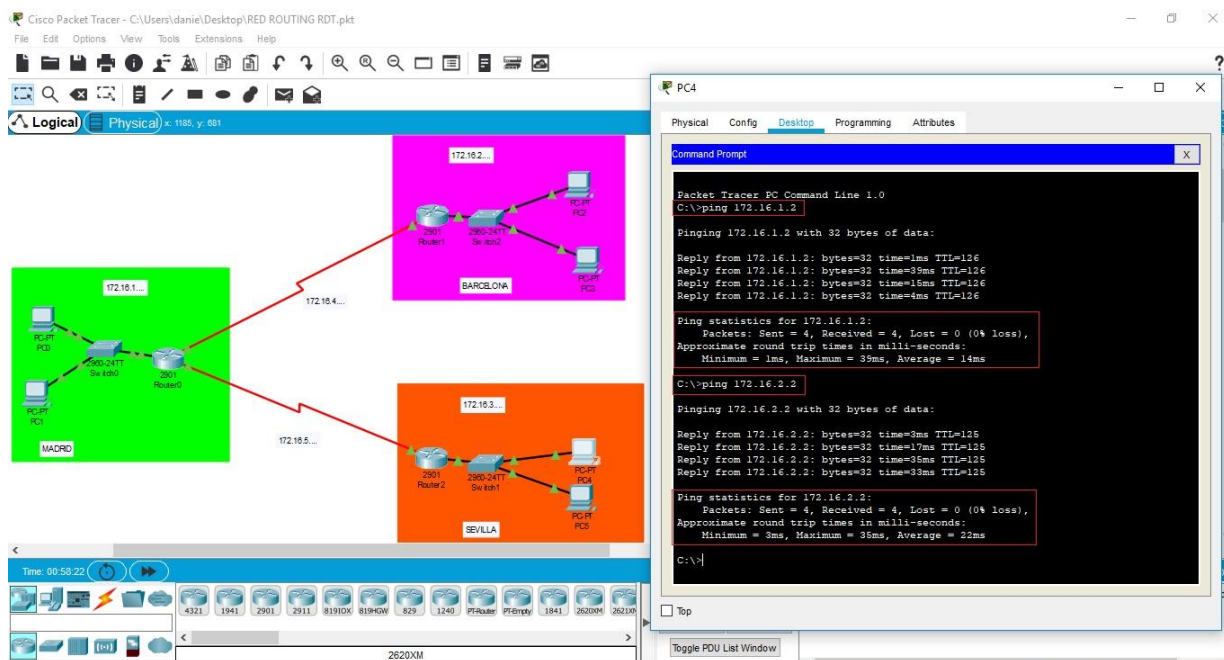
Reply from 172.16.3.2: bytes=32 time=1ms TTL=126
Reply from 172.16.3.2: bytes=32 time=13ms TTL=126
Reply from 172.16.3.2: bytes=32 time=33ms TTL=126
Reply from 172.16.3.2: bytes=32 time=11ms TTL=126

Ping statistics for 172.16.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 33ms, Average = 14ms

C:\>
    
```

Figura 4.1.8.F. Conectividad PING Madrid con Barcelona y Sevilla

Sevilla con Madrid y Barcelona:



3.1.8

Figura 4.1.8.G. Conectividad PING Sevilla con Barcelona y Madrid

En cuanto a la respuesta a la pregunta:

¿Puede haber conectividad del PC0 al PC1 y NO al contrario? ¿Es eso posible?

No, esto no es posible debido a que para que haya conectividad entre dos equipos, en este caso dos PCs, deben estar configurados de manera correcta ambos. Si yo tengo bien configurado a nivel de red el PC0 pero el PC1 no lo está al yo mandar un 'PING', por ejemplo, del PC0 al PC1 va a dar error debido a que el PC1 se encuentra mal configurado y por tanto este no va a responder al PC0 dando error.

3.1.9 Mostrar la configuración del router

Para ver la configuración del router usaremos el mismo comando que usamos con el switch

```
show running config
```

3.1.9

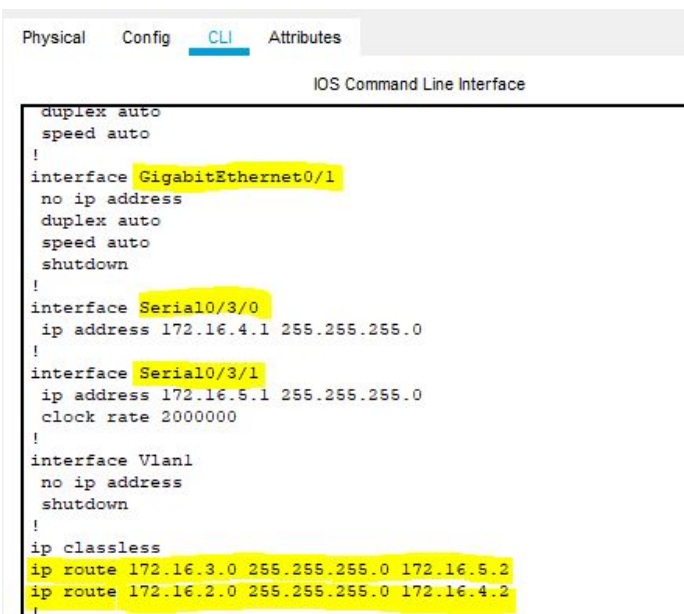
-Entramos en el CLI de cualquier router y ponemos el comando:

```
Router>ena
Router#show ru
Router#show running-config
Building configuration...

Current configuration : 859 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
```

Figura 3.1.9.a comando show running config

De esta forma veremos cada una de las bocas del router y las rutas estáticas definidas



```
Physical  Config  CLI  Attributes
IOS Command Line Interface

duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
ip address 172.16.4.1 255.255.255.0
!
interface Serial0/3/1
ip address 172.16.5.1 255.255.255.0
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 172.16.3.0 255.255.255.0 172.16.5.2
ip route 172.16.2.0 255.255.255.0 172.16.4.2
!
```

Figura 3.1.9.b bocas del Router y sus rutas

Apartado 10 (I)

3.1.10 Mostrar tabla de routeo

- Show ip route
 - L rutas locales a una IP específica, a un host específico
- Los routers usan rutas locales para aumentar rendimiento
 - C redes directamente conectadas
 - Nos muestra también por qué boca están conectadas

Router0:

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C 172.16.1.0/24 is directly connected, GigabitEthernet0/0
L 172.16.1.1/32 is directly connected, GigabitEthernet0/0
S 172.16.2.0/24 [1/0] via 172.16.4.2
S 172.16.3.0/24 [1/0] via 172.16.5.2
C 172.16.4.0/24 is directly connected, Serial10/3/0
L 172.16.4.1/32 is directly connected, Serial10/3/0
C 172.16.5.0/24 is directly connected, Serial10/3/1
L 172.16.5.1/32 is directly connected, Serial10/3/1
```

3.1.10

Comprobamos que es verdad lo que dice la tabla:

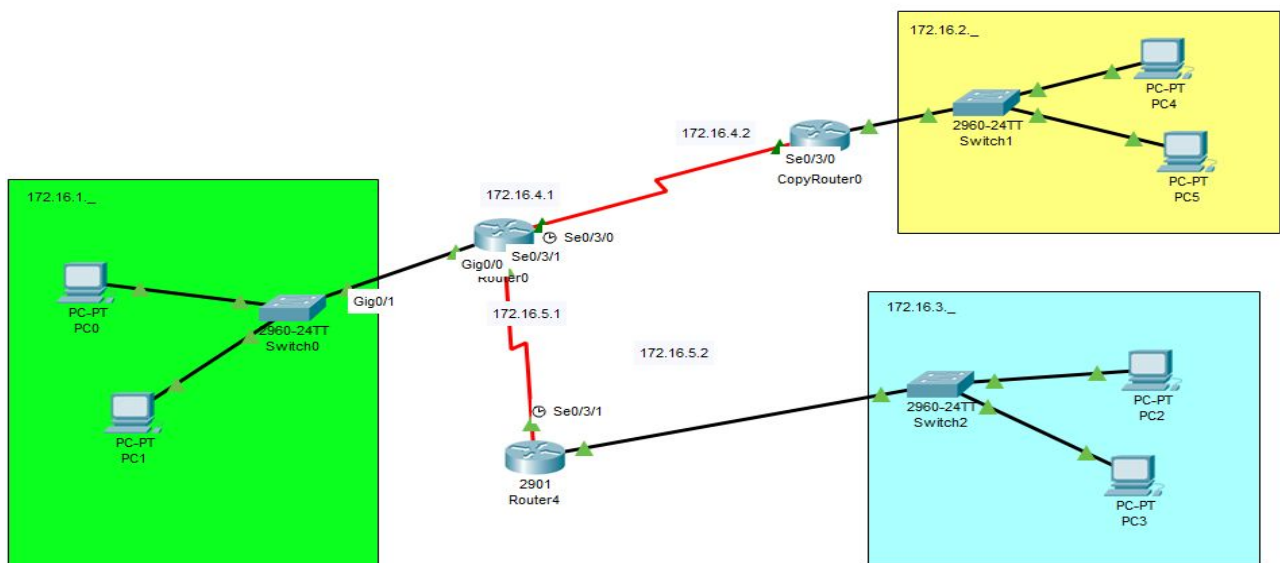


Figura 3.1.10.a Comprobación de la tabla del Router 0

Apartado 10 (II)

3.1.10 Mostrar tabla de routeo

- Show ip route
 - L rutas locales a una IP específica, a un host específico
- Los routers usan rutas locales para aumentar rendimiento
 - C redes directamente conectadas
 - Nos muestra también por qué boca están conectadas

CopyRouter0:

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
S 172.16.1.0/24 [1/0] via 172.16.4.1
C 172.16.2.0/24 is directly connected, GigabitEthernet0/0
L 172.16.2.1/32 is directly connected, GigabitEthernet0/0
S 172.16.3.0/24 [1/0] via 172.16.4.1
C 172.16.4.0/24 is directly connected, Serial0/3/0
L 172.16.4.2/32 is directly connected, Serial0/3/0
```

3.1.10

Comprobamos que es verdad lo que dice la tabla:

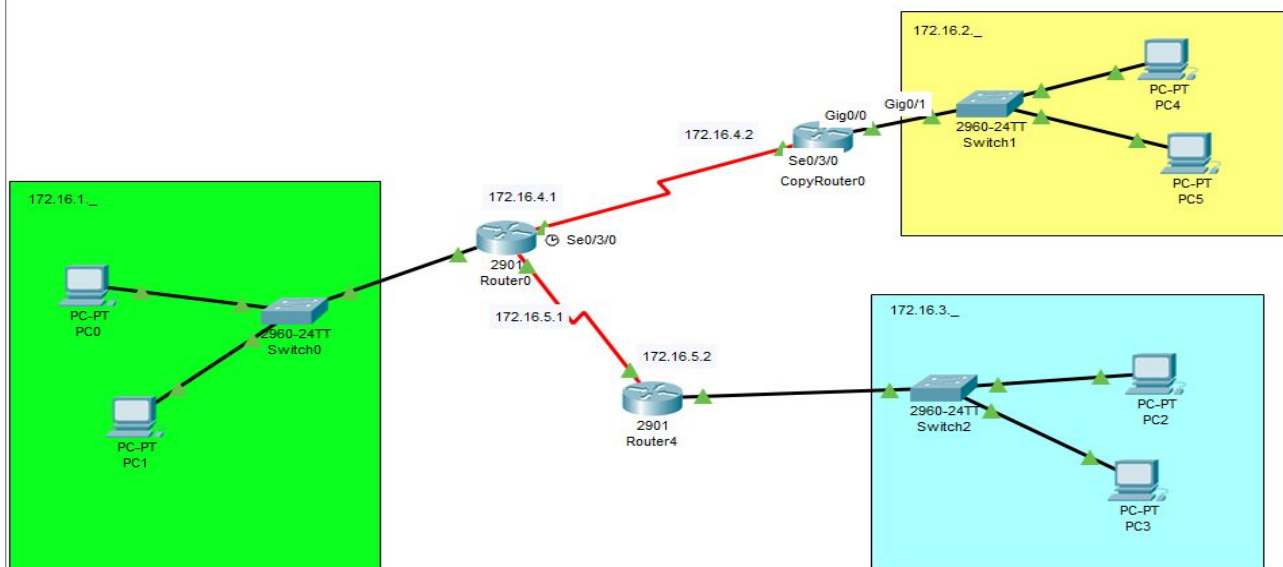


Figura 3.1.10.b Comprobación de la tabla del CopyRouter 0

Apartado 10 (III)

3.1.10 Mostrar tabla de routeo

- Show ip route
 - L rutas locales a una IP específica, a un host específico
- Los routers usan rutas locales para aumentar rendimiento
 - C redes directamente conectadas
 - Nos muestra también por qué boca están conectadas

Router4:

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
S 172.16.1.0/24 [1/0] via 172.16.5.1
S 172.16.2.0/24 [1/0] via 172.16.5.1
C 172.16.3.0/24 is directly connected, GigabitEthernet0/0
L 172.16.3.1/32 is directly connected, GigabitEthernet0/0
C 172.16.5.0/24 is directly connected, Serial0/3/1
L 172.16.5.2/32 is directly connected, Serial0/3/1
```

3.1.10

Comprobamos que es verdad lo que dice la tabla:

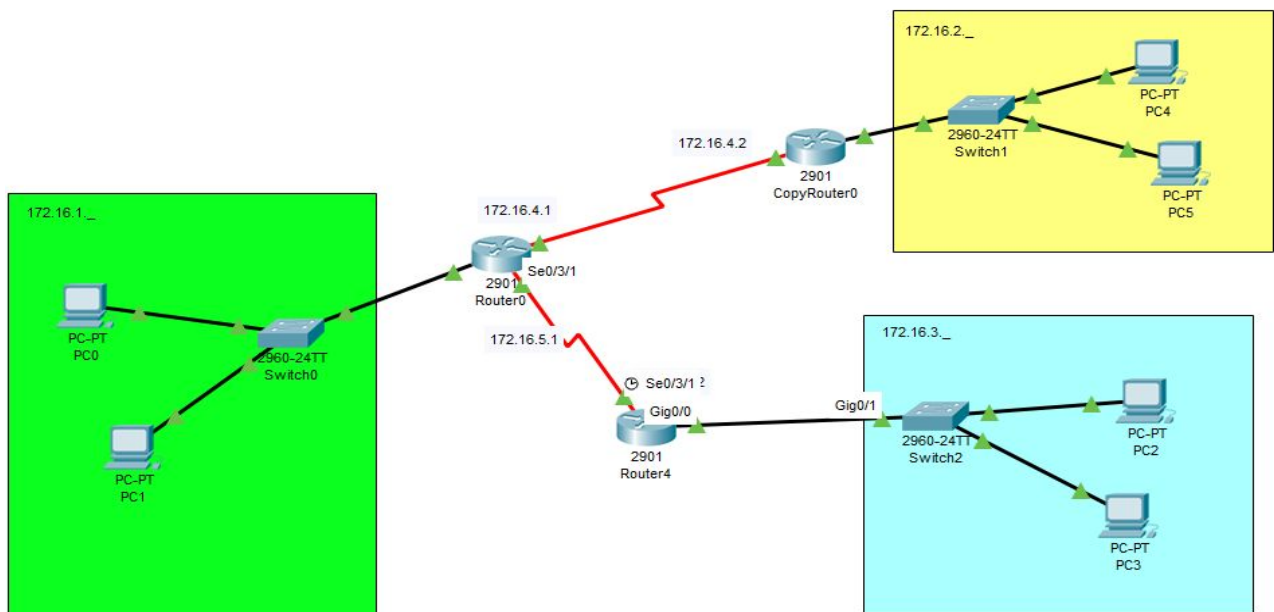


Figura 3.1.10.c Comprobación de la tabla del Router 4

3.1.11 Probamos el routing con traceroute

- Prueba desde una consola de comandos de un PC el funcionamiento del comando tracert y explica razonadamente la salida que muestra por pantalla

¿Qué es traceroute?: Traceroute es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host. Se obtiene además una estadística del RTT o latencia de red de esos paquetes, lo que viene a ser una estimación de la distancia a la que están los extremos de la comunicación.

Comprobamos el enlace entre los dos PC antes de comprobar la ruta del paquete:

3.1.11

Hacemos ping de PC1 a PC2 . Después usamos el comando “tracert” y ponemos la ip de PC2 y nos mostrará la ruta que sigue el paquete hasta llegar al destino. Figura 3.1.11

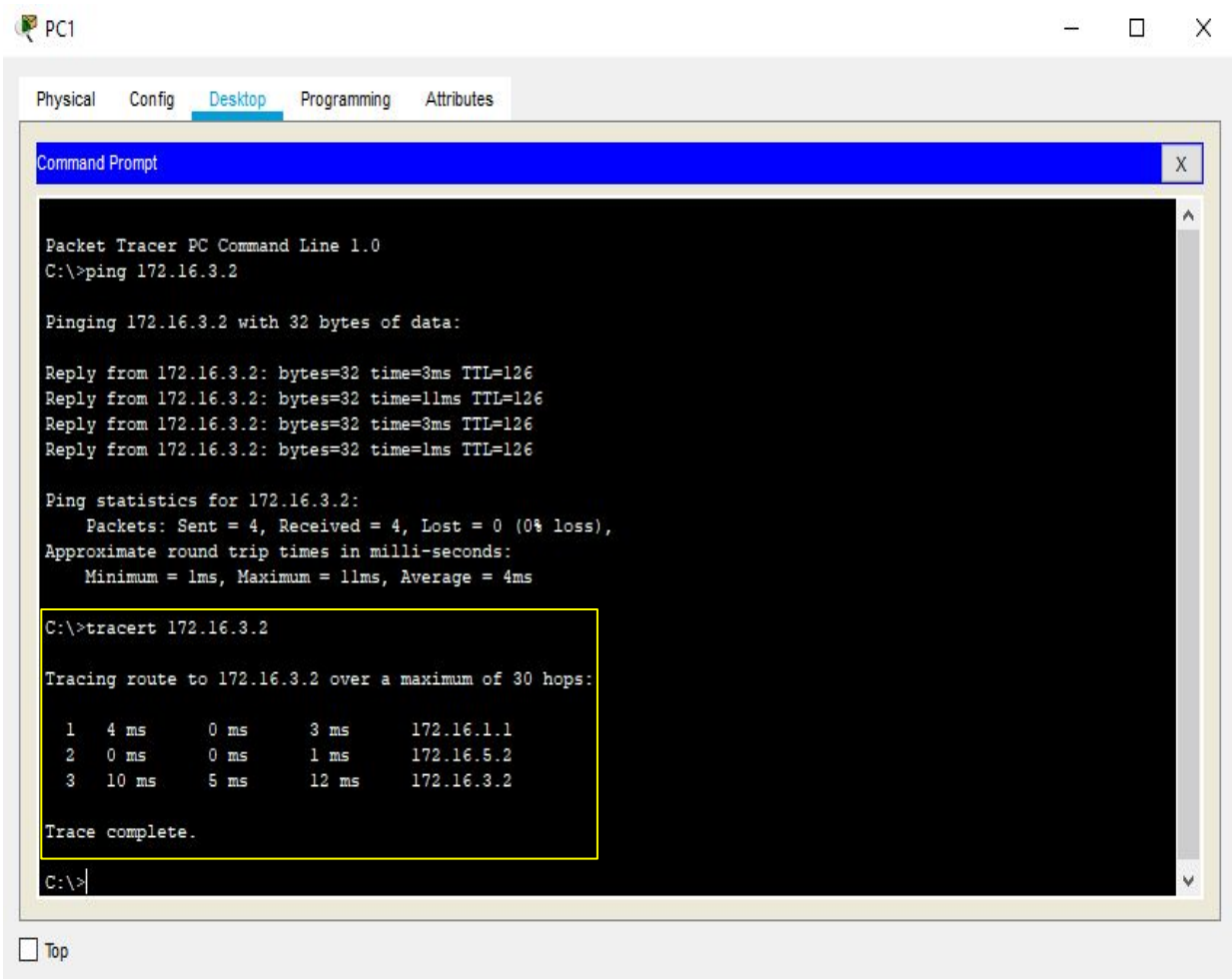


Figura 3.1.11. Ruta de viaje del paquete

Como se vé en la figura 3.1.11 se muestra las ip de los dispositivos que debe pasar para que el paquete llegue a su destino y el tiempo que tarda. En este caso pasa a su router que es su puerta de enlace, a continuación viaja hasta la boca serial del router de destino y de allí al PC2.

Apartado 12

3.1.12 Uso del comando arp

- Prueba desde una consola de comandos de un PC el funcionamiento del comando arp
- Muestra cómo inicialmente la tabla arp de un equipo está vacía y poco a poco va completando
- Demuestra además que en esta tabla únicamente se completan direcciones asociadas a equipos de la misma subred

Primero iremos a la consola de comandos del PC0 luego introduciremos el comando `arp` a continuación se nos mostrarán dos comandos `arp -a` y `arp -d`.



```
C:\>arp
Packet Tracer PC ARP
Display ARP entries: arp -a
Clear ARP table: arp -d
C:\>
```

3.1.12

Figura 3.1.12 a. Ejecución comando `arp`

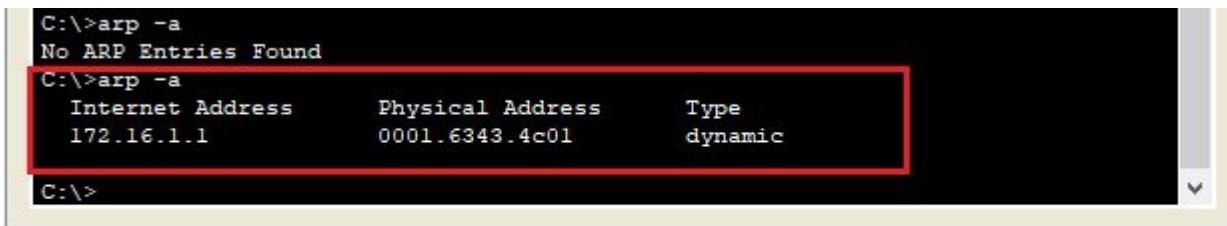
A continuación vamos a usar el comando `arp -a` sin haber hecho ningún ping, como podemos observar la tabla de ARP no tiene ninguna entrada



```
C:\>arp -a
No ARP Entries Found
C:\>
```

Figura 3.1.12 b. Ejecución comando `arp -a` sin haber hecho pings

Ahora haremos ping a ambos equipos de la sede de Barcelona, desde el pc0 y luego volveremos a introducir el comando `arp -a`, como podemos observar en la imagen, en la tabla de ARP ahora figura la dirección IP y MAC del Router y el tipo de conexión.



```
C:\>arp -a
No ARP Entries Found
C:\>arp -a
Internet Address      Physical Address      Type
172.16.1.1            0001.6343.4c01       dynamic
C:\>
```

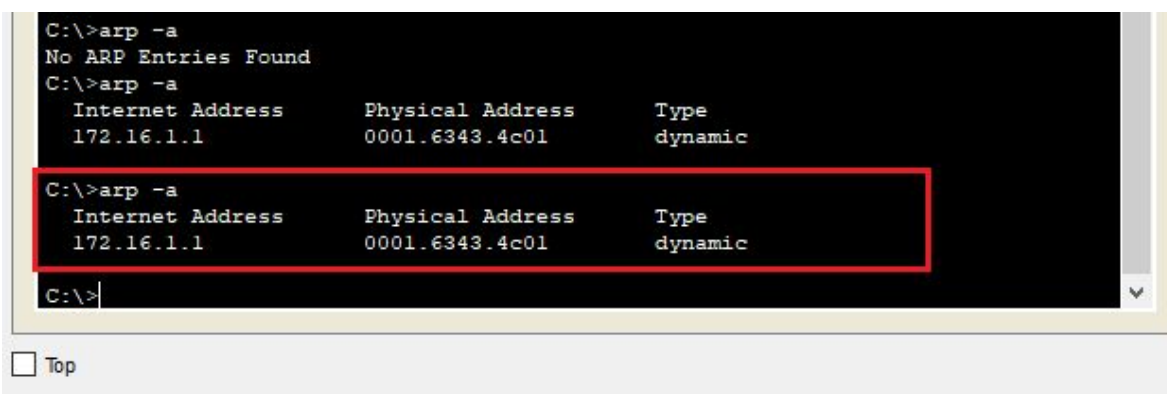
Figura 3.1.12 c. Ejecución comando `arp -a` habiendo hecho ping a equipos de Barcelona

Apartado 12

3.1.12 Uso del comando arp

- Prueba desde una consola de comandos de un PC el funcionamiento del comando arp
- Muestra cómo inicialmente la tabla arp de un equipo está vacía y poco a poco va completando
- Demuestra además que en esta tabla únicamente se completan direcciones asociadas a equipos de la misma subred

Ahora haremos ping a ambos equipos de la sede de Sevilla, desde el pc0 y luego volveremos a introducir el comando `arp -a`, como podemos observar nuevamente en la imagen, en la tabla de ARP sigue figurando solo la dirección IP y MAC del Router y el tipo de conexión.

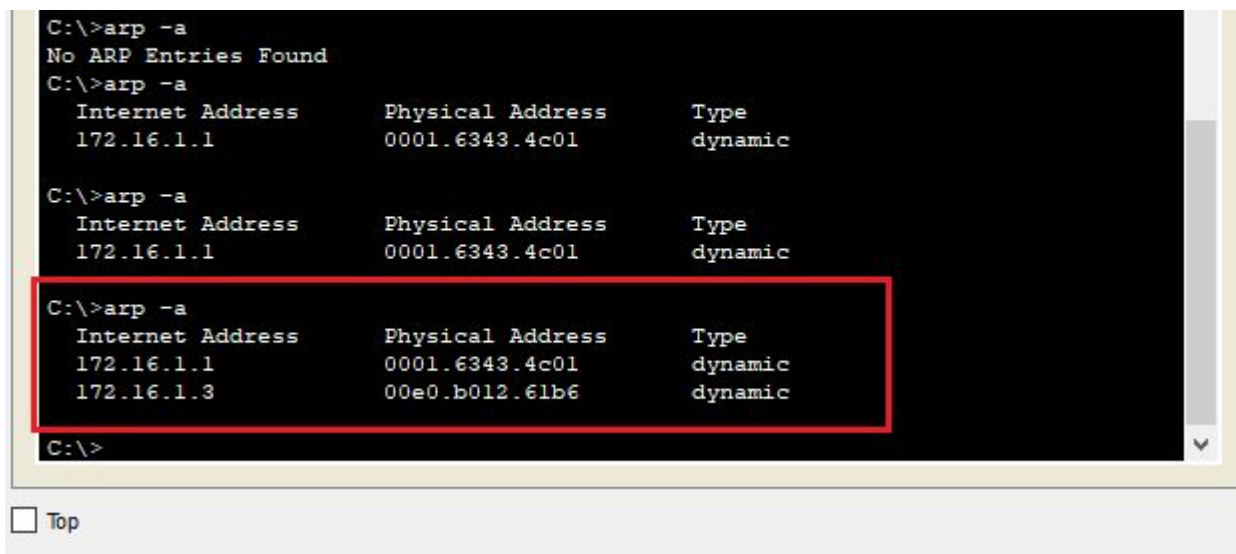


```
C:\>arp -a
No ARP Entries Found
C:\>arp -a
Internet Address      Physical Address      Type
172.16.1.1           0001.6343.4c01      dynamic
C:\>arp -a
Internet Address      Physical Address      Type
172.16.1.1           0001.6343.4c01      dynamic
C:\>
```

3.1.12

Figura 3.1.12 d. Ejecución comando `arp -a` habiendo hecho ping a equipos de Sevilla

Por último le haremos al ping al PC1 de Madrid que está en nuestra misma subred, y volvemos a ejecutar el comando `arp -a`, como podemos observar en la imagen ahora tenemos en la tabla de ARP las direcciones IPs y MACs y el tipo de conexión que tenemos con el Router y el PC1.



```
C:\>arp -a
No ARP Entries Found
C:\>arp -a
Internet Address      Physical Address      Type
172.16.1.1           0001.6343.4c01      dynamic
C:\>arp -a
Internet Address      Physical Address      Type
172.16.1.1           0001.6343.4c01      dynamic
C:\>arp -a
Internet Address      Physical Address      Type
172.16.1.1           0001.6343.4c01      dynamic
172.16.1.3           00e0.b012.61b6      dynamic
C:\>
```

Figura 3.1.12 e. Ejecución comando `arp -a` habiendo hecho ping a equipos de Madrid

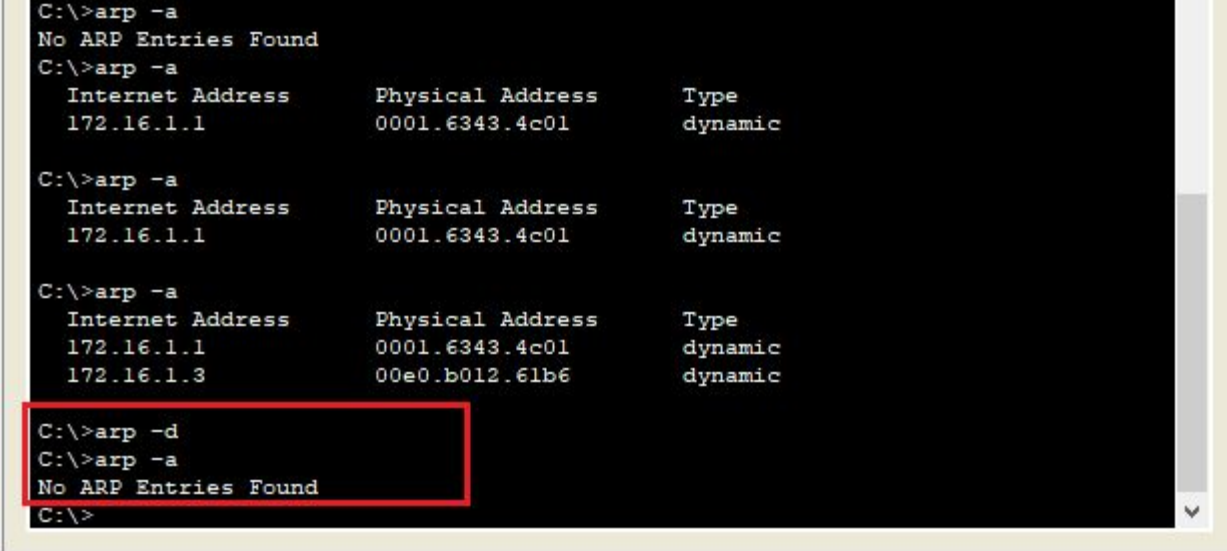
Como podemos observar aún habiendo hecho ping a todos los PCs de la red, en la tabla de ARP sólo aparecen los equipos que están en su misma subred que en este caso son el PC1 y el Router.

Apartado 12

3.1.12 Uso del comando arp

- Prueba desde una consola de comandos de un PC el funcionamiento del comando arp
- Muestra cómo inicialmente la tabla arp de un equipo está vacía y poco a poco va completando
- Demuestra además que en esta tabla únicamente se completan direcciones asociadas a equipos de la misma subred

Por último veremos cómo podemos borrar dicha tabla de ARP en caso de que queramos hacer más pruebas, tan solo tendremos que introducir el comando `arp -d` en el PC0 y la tabla de ARP que estaba registrada en el pc será eliminada. Para comprobar que la operación ha sido realizada correctamente volveremos a introducir el comando `arp -a`



```
C:\>arp -a
No ARP Entries Found
C:\>arp -a
  Internet Address      Physical Address      Type
  172.16.1.1            0001.6343.4c01       dynamic

C:\>arp -a
  Internet Address      Physical Address      Type
  172.16.1.1            0001.6343.4c01       dynamic

C:\>arp -a
  Internet Address      Physical Address      Type
  172.16.1.1            0001.6343.4c01       dynamic
  172.16.1.3            00e0.b012.61b6       dynamic

C:\>arp -d
C:\>arp -a
No ARP Entries Found
C:\>
```

Top

3.1.12

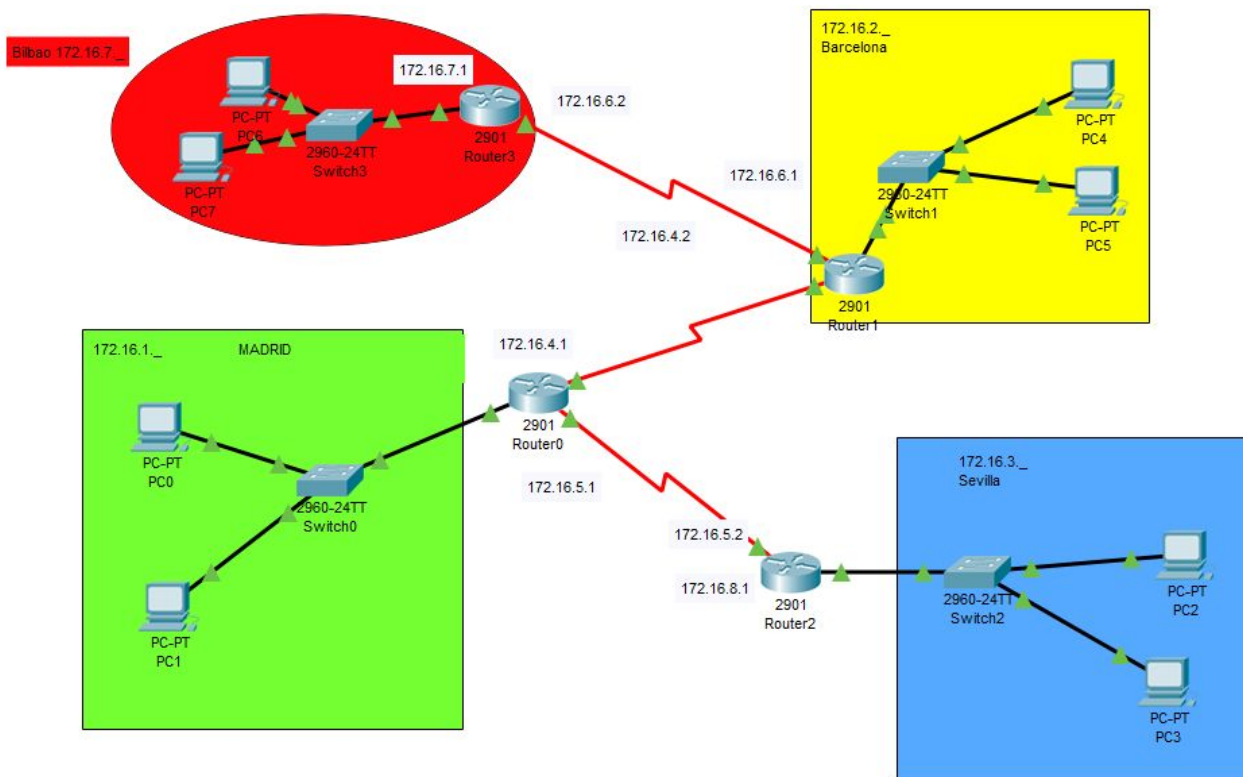
Figura 3.1.12 f. Ejecución del comando `arp -d` y comprobación de su funcionamiento

Añadido 1

Añadido 1. Delegación en Bilbao (172.16.7.0)

- Ahora añade una nueva delegación en Bilbao
- que tenga como identificador de red 172.16.6.0/24
- Esta nueva delegación está conectada a Barcelona.
- Prueba ahora que hay conectividad entre toda la red.

Añadiremos una nueva delegación con el nombre Bilbao(172.16.7.0) y con un **identificador de red** 172.16.6.0/24



3.1.A1

Figura 3.1.A1.A. Nueva delegación añadida "Bilbao".

Después de añadir esta nueva delegación a la tabla de routeo de las otras delegaciones.



Figura 3.1.A1.B. Ejemplo añadir Bilbao a tabla de routeo.

Añadido 1

Ahora vamos a ver si hay conectividad en toda la red.

Bilbao(172.16.7.0) - Barcelona(172.16.2.0)

Desde Pc 7



Fire	Last Status	Source	Destination	Type	Color
	Successful	PC7	PC4	ICMP	

Hasta pc 4



Bilbao(172.16.7.0) - Madrid(172.16.1.0)

Desde Pc 6



Fire	Last Status	Source	Destination	Type	Color
	Successful	PC6	PC0	ICMP	

Hasta pc 0



Bilbao(172.16.7.0) - Sevilla(172.16.3.0)

Desde Pc 6



Fire	Last Status	Source	Destination	Type	Color
	Successful	PC6	PC2	ICMP	

Hasta pc 2



Como podemos observar existe conectividad entre toda la red.

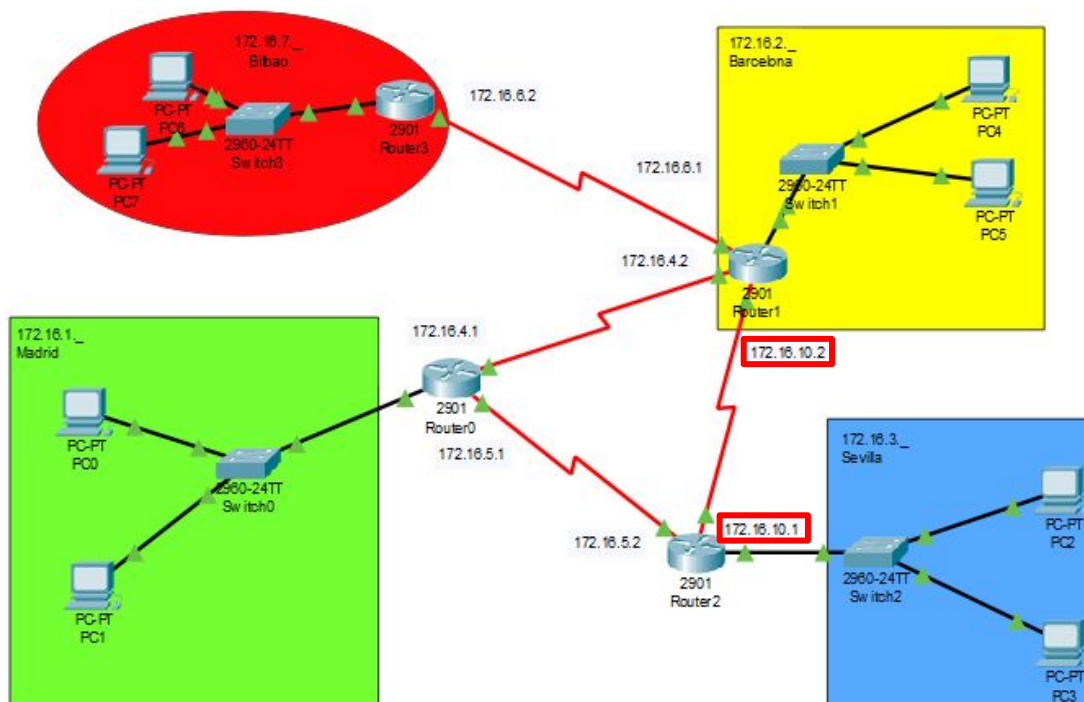
3.1.A1

Añadido 2

Añadido 2. Enlace Barcelona-Sevilla. Envío Sevilla-Bilbao vía Barcelona, NO vía Madrid

- Añade ahora un enlace WAN que una Barcelona con Sevilla
- A partir de este momento, los paquetes de Sevilla con destino Bilbao irán directamente a Barcelona, sin pasar por Madrid.
- El resto de envíos desde Sevilla a cualquier otra delegación deberán ir vía Madrid

Con el enlace WAN entre Barcelona y Sevilla creado y configurado con sus respectivas IPs (172.16.10.1 + 172.16.10.2, ver **Figura 3.1.A2.A**), procederemos a configurar la ruta estática para los envíos desde Sevilla a Bilbao (**Figura 3.1.A2.B**).



3.1.A2

Figura 3.1.A2.A. Actualización de la red con el enlace WAN SEV-BCN.

Rutas Estáticas

Red	172.16.7.0
Máscara	255.255.255.0
Siguiente Salto	172.16.10.2
<input type="button" value="Agregar"/>	

Figura 3.1.A2.B. Pestaña de configuración gráfica del router2 (Sevilla) para envíos Sevilla - Bilbao.

Como vemos en la **Figura 3.1.A2.B**, cualquier envío desde Sevilla hacia Bilbao (**Red 172.16.7.0**) deberá dirigirse a través del enlace WAN recientemente creado hacia el router situado en Barcelona, por lo que el siguiente salto será la IP del enlace WAN asignada a la boca del router de barcelona (**172.16.10.2**).

Añadido 2

Para los envíos desde **Sevilla hacia Madrid (Red 172.16.1.0)** y **Barcelona (Red 172.16.2.0)**, los paquetes **deberán pasar por Madrid**, por tanto, nuestro siguiente salto desde el router de Sevilla será la **IP 172.16.5.1**, asignada a la boca del router de Madrid del enlace WAN Sevilla-Madrid.

Rutas Estáticas		Rutas Estáticas	
Red	172.16.1.0	Red	172.16.2.0
Máscara	255.255.255.0	Máscara	255.255.255.0
Siguiente Salto	172.16.5.1	Siguiente Salto	172.16.5.1
<input type="button" value="Agregar"/>		<input type="button" value="Agregar"/>	

Figura 3.1.A2.C. Configuración de las rutas estáticas Sevilla - Resto.

3.1.A2

Con el comando `show ip route`, comprobaremos las rutas estáticas creadas, como vemos en la siguiente **Figura 3.1.A2.D**:

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B
- BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 9 subnets, 2 masks
S       172.16.1.0/24 [1/0] via 172.16.5.1
S       172.16.2.0/24 [1/0] via 172.16.5.1
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0
C       172.16.5.0/24 is directly connected, Serial0/3/1
L       172.16.5.2/32 is directly connected, Serial0/3/1
S       172.16.7.0/24 [1/0] via 172.16.10.2
C       172.16.10.0/24 is directly connected, Serial0/2/0
L       172.16.10.1/32 is directly connected, Serial0/2/0
```

Figura 3.1.A2.D. Tabla de routeo del router de Sevilla.

Trabajo 3.2

InterVLAN routing: router on a stick



Trabajo 3.2 InterVLAN routing: router on a stick

Router on a stick es una técnica que nos permite el enrutamiento entre las diferentes VLANs que tengamos definidas en nuestra red.

A continuación, mostraremos un guión de lo que hay que hacer para que funcione el enrutamiento entre VLAN.

Router on a stick es un término frecuentemente usado para describir una configuración que consiste de un router y un switch conectados usando un cable Ethernet como un enlace de trunk 802.1q. En esta configuración, el switch está configurado con múltiples VLANs y el router realiza todas las tareas enrutamiento entre las diferentes redes/VLANs.

3.2

En primer lugar, haremos una red de ejemplo como la siguiente:

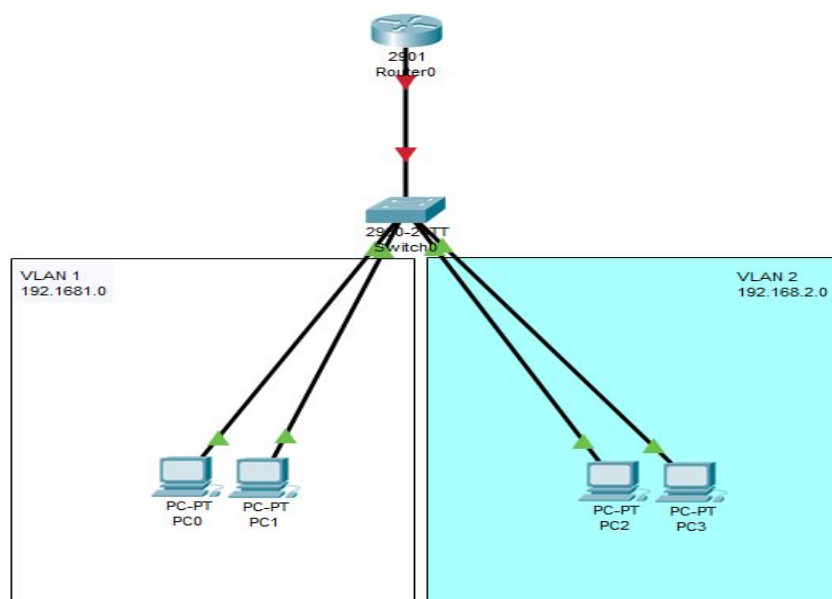


Figura 3.2.A. Red de ejemplo.

Una vez establecida la red, debemos establecer el enlace entre el switch y el router como trunking. Así que entramos en la consola del switch y hacemos lo siguiente:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gigabit
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
```

Ahora crearemos las VLAN como hemos hecho siempre, sin ningún tipo de cambio y seguidamente meteremos las bocas necesarias en cada vlan.

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface vlan 2
Switch(config-if)#ip address 192.168.2.2 255.255.255.0
```

3.2

Una vez hecho esto, pasamos al router donde haremos lo siguiente:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#no ip address
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/1.1
%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1, changed state to
up

Router(config-subif)#encapsulation dot1Q 1 native
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/1.2
%LINK-5-CHANGED: Interface GigabitEthernet0/1.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.2, changed state to
up

Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
```

Para formar un enlace troncal con nuestro switch, es necesario crear una sub-interfaz para cada VLAN configurada en nuestro conmutador. Después de crear la sub-interfaz, le asignamos una dirección IP y configuramos el tipo de encapsulación en 802.1q junto con la VLAN a la que pertenece la subinterfaz. El comando `encapsulation dot1Q 2` define la encapsulación 802.1q y establece la subinterfaz en VLAN 2. El parámetro nativo que usamos para la subinterfaz gigabitEthernet0/1.1 le dice al switch que la VLAN por defecto es la VLAN 1. Este es un parámetro predeterminado en cada conmutador de Cisco y, por lo tanto, también debe coincidir con el switch.

Por último, pondremos las direcciones IP correspondientes a cada PC, en nuestro caso hemos usado para el PC0 y PC1 las direcciones 192.168.1.5/24-192.168.1.10/24 y para el PC2 y PC3 las direcciones 192.168.2.5/24-192.168.2.10/24 respectivamente.

3.2

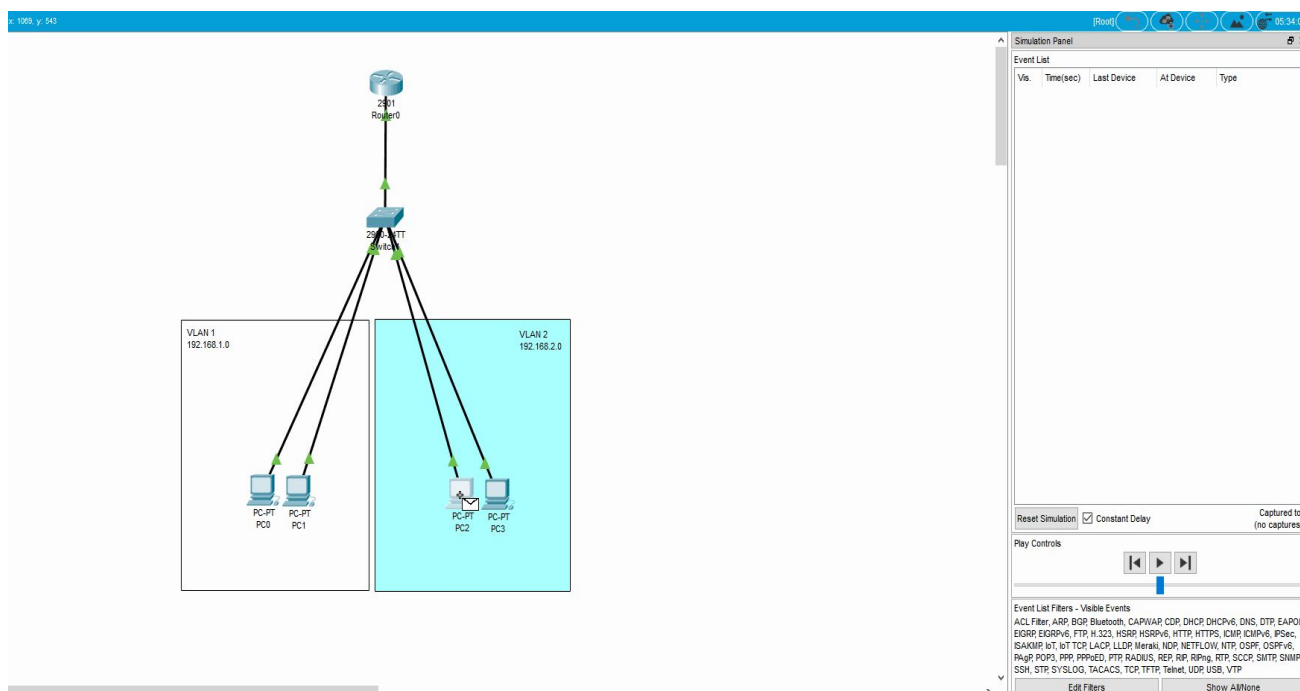


Figura 3.2.B. Comprobación de conexión.

Se adjunta un vídeo explicativo:

<https://youtu.be/ZaUmSiFAMDc>



Preguntas de repaso

3.2. Router on stick

JACOGON

- ¿Que tipo de enlace debe existir entre el switch y el router?
- ¿Que encapsulación debe asignar a las sub-interfaces?
- ¿Para qué sirve el comando native al realizar la encapsulación?

VCARLEO

- ¿En qué consiste router on a stick?
- ¿Como hay que configurar el switch para realizar esta técnica?
- ¿De qué tarea se ocupa el router?

3.2



Trabajo 3.3
VTP: VLAN Trunking Protocol.
Cisco Lab 3

Trabajo 3.3 VTP: VLAN Trunking Protocol. Cisco Lab 3

VTP es un protocolo que nos facilita replicar las VLAN que hayamos definido en toda nuestra red.

En el siguiente enlace de Cisco se explica en detalle cómo llevar a cabo la configuración de VTP:

<https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html>

En este otro enlace, de forma simplificada podrás entender los fundamentos de VTP:

<https://todopacketracer.com/2011/11/05/configurar-vtp/>

Con estos conocimientos, aborda el lab de Cisco que se incluye adjunto en esta actividad.

1. Configure the VTP-SERVER switch as a VTP server
2. Connect to the 3 other switches and configure them as VTP clients. All links between switches must be configured as trunk lines.
3. Configure VTP domain name as "TESTDOMAIN" and VTP password as "cisco"
4. Configure VLAN 10 with name "STUDENTS" and VLAN 50 with name "SERVERS"
5. Check propagation on all switches of the VTP domain.

Añadidos:

1. Comprueba que los cambios en VLAN que se hagan en el maestro se replican de forma automática en todos los clientes
2. Comprueba que NO puedes realizar ningún cambio a nivel de VLAN en los clientes.
3. Añade un switch a tu topología y créale la VLAN 2 (bocas 1 ~ 12) y 3 (bocas 13 ~ 24). Luego añádelo al dominio VTP. ¿Qué ocurre con las VLAN que tenía creadas, las mantiene, las elimina?
4. ¿Pueden convivir varios dominios en una misma red?
 1. Para ello, crea ahora un nuevo dominio llamado IB_DOMAIN, con un VTP Server y un VTP Cliente. Crea la VLAN 10 con exactamente las mismas bocas que la VLAN del TESTDOMAIN del ejercicio y la VLAN 60 con las mismas bocas que la vlan 50 de TESTDOMAIN. Une ahora IB_DOMAIN a la red TESTDOMAIN con un enlace troncal.
5. ¿Hay conectividad entre los dominios?
 1. Para ello, conecta un PC a la VLAN 10 en el TESTDOMAIN y un PC a la VLAN 10 en el IB_DOMAIN
 2. ¿Hay conectividad entre ellos?

Trabajo 3.3. VTP: VLAN Trunking Protocol.

Cisco Lab 3

6. ¿Qué ocurre si le cambiamos la clave VTP al servidor? ¿Se pierden las VLAN de los clientes?
7. ¿Está VTP descatalogado o está vigente en la actualidad? De estar descatalogado, ¿cuál es el protocolo que lo sustituye?
8. ¿Hay alguna forma de que VTP se repliquen no solo las VLAN, su ID y su nombre, sino también las bocas asociadas?

3.3

Apartado 1

1. Configure the VTP-SERVER switch as a VTP server

Para empezar a desarrollar este Cisco Lab el primer paso a cumplir es el de cómo se puede apreciar configurar el Switch llamado **'VTP-SERVER'** de la red como un servidor VTP. El primer paso para realizar esta acción es saber que es **VTP** y qué hace en este caso el **VTP-SERVER** tras activarlo en **VTP Server**.

VTP son las siglas de **VLAN Trunking Protocol**, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo **VTP** nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

3.3.1

Y en este caso cuando pongamos dicho Switch en modo server ocurrirá lo siguiente:

Switch en modo servidor: Desde él se pueden crear, eliminar o modificar VLANs. Su cometido es anunciar su configuración al resto de switches del mismo dominio VTP y sincronizar dicha configuración con la de otros servidores, basándose en los mensajes VTP recibidos a través de sus enlaces trunk. Debe haber al menos un servidor en una red.

Bueno ahora que ya sabemos con ocurrirá con este switch vamos a cumplir con este paso del Cisco Lab. Para empezar debemos acceder a la consola del Switch llamado **VTP-SERVER**. Para ello podemos ver que el modo gráfico de este switch no funciona y para acceder a la consola de este switch se debe hacer desde el **PC0**, el cual ya tiene el cable de consola azul conectado a este Switch nada más abrir el Cisco Lab. Entonces, lo que debemos hacer es hacer click sobre el **PC0** y acceder a la tercera pestaña superior la cual recibe el nombre de **'Desktop'** y dentro de ella acceder a la tercera opción llamada **'Terminal'**.

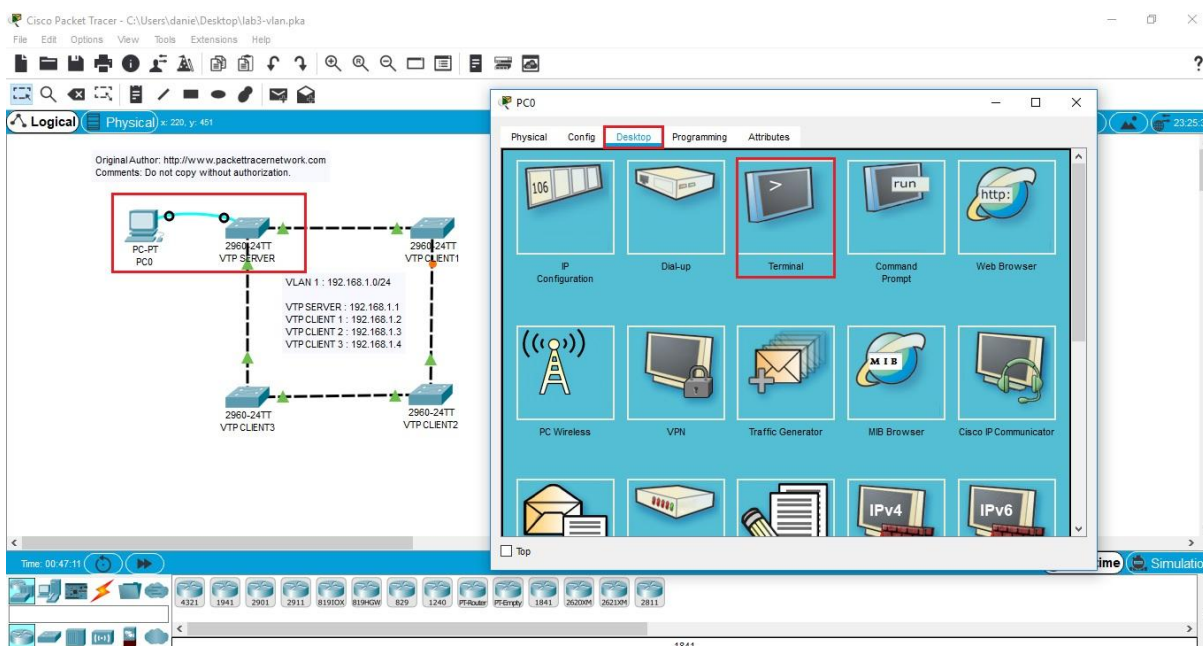
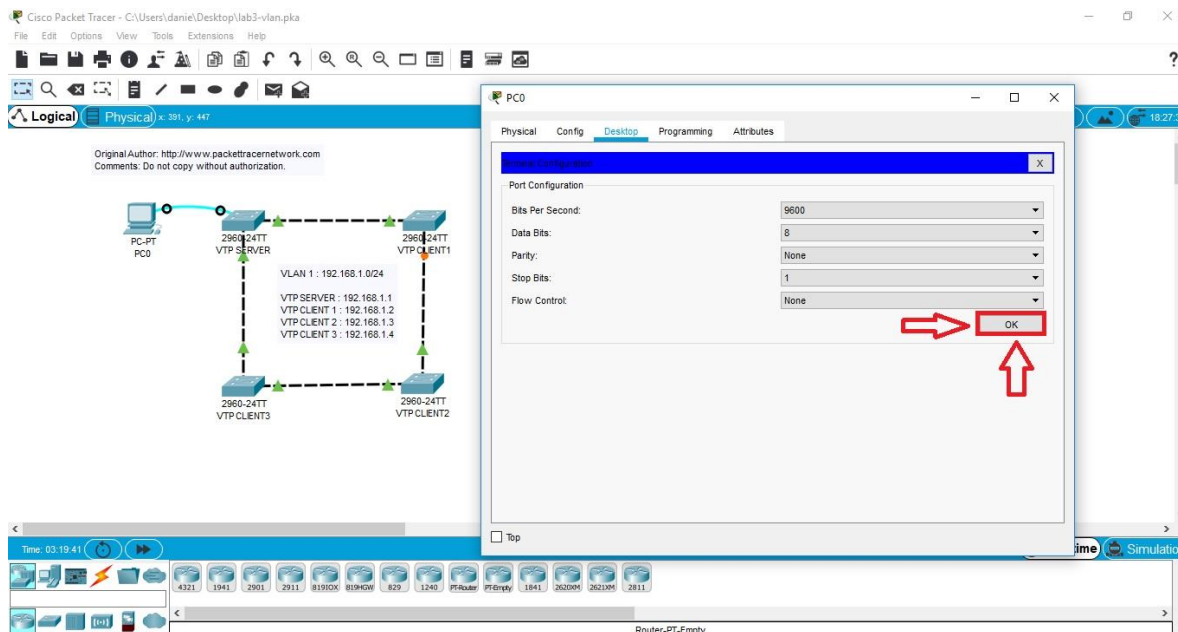


Figura 3.3.1.A. Acceso consola switch VTP-SERVER.

Tras hacer click sobre dicha opción llamada **'Terminal'**, se abrirá otra ventana que nos ofrece cambiar diferentes parámetros, los cuales dejamos como se encuentran y le damos al botón 'OK' situado en la esquina inferior derecha. Tras presionar este botón se abrirá la consola del switch llamado **'SWITCH-SERVER'**.



3.3.1

Figura 3.3.1.B. Acceso consola switch VTP-SERVER.

Ya dentro de la consola del switch para configurar éste como servidor VTP debemos realizar en este los siguientes comandos:

```
enable
configure terminal
vtp mode server
```

En la siguiente imagen se puede observar cómo se realizan estos comandos:

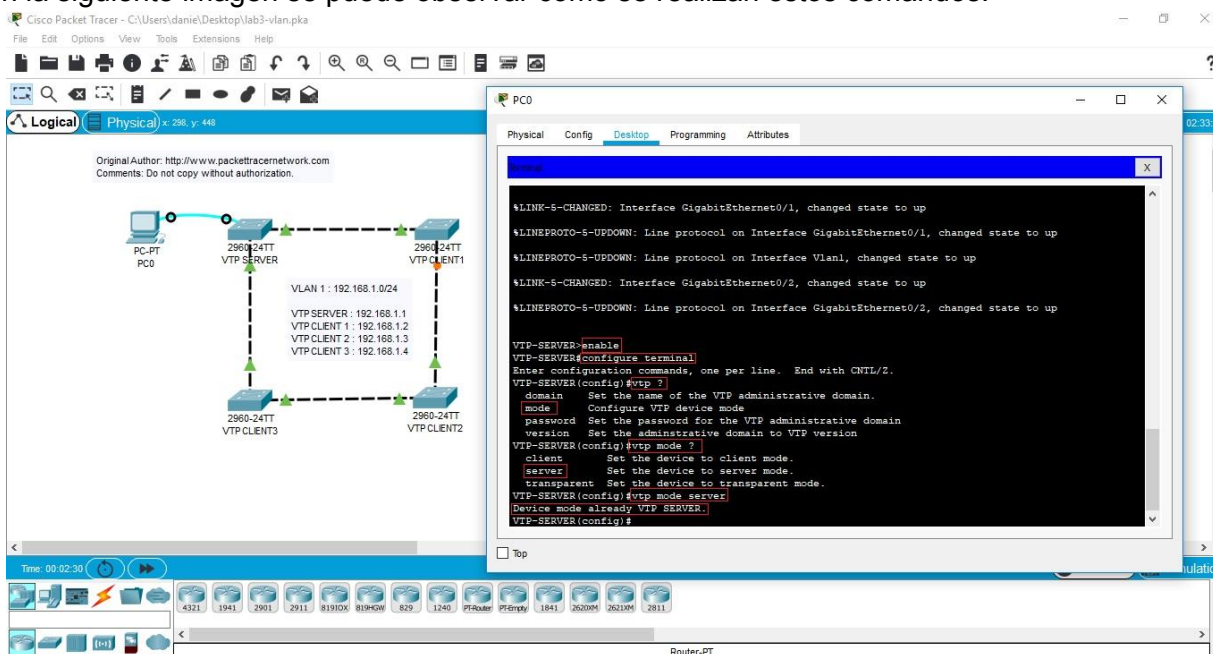

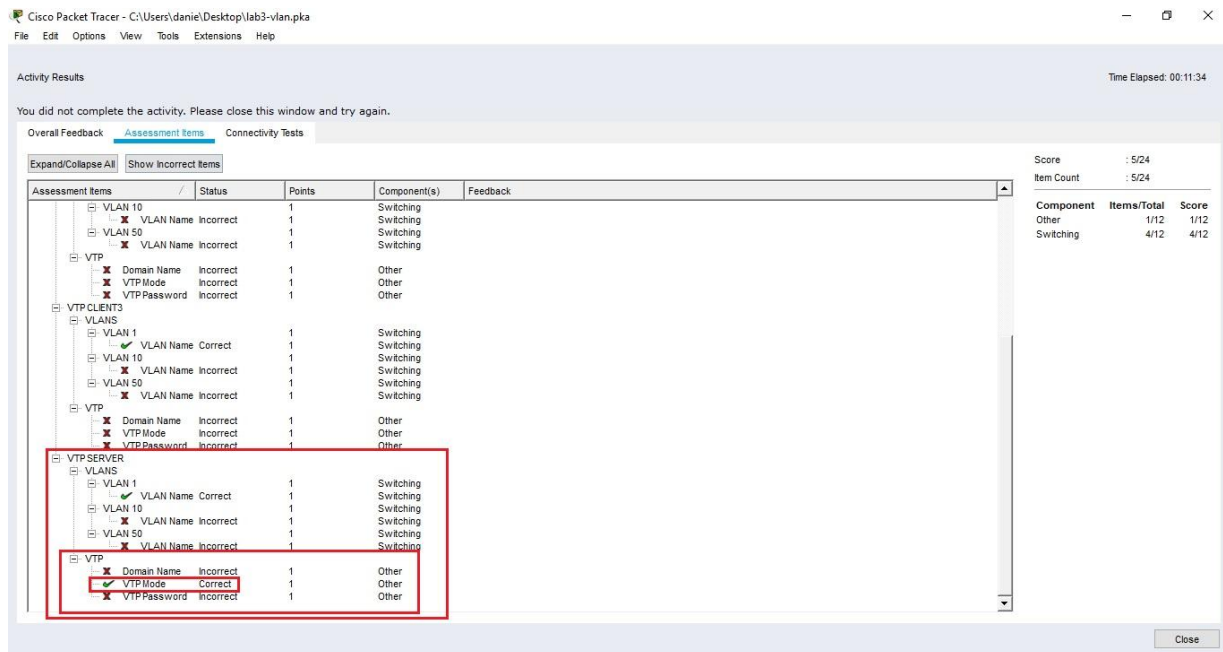


Figura 3.3.1.C. Configuración switch VTP-SERVER en modo Server.

<DPLAHER>

Tras realizar estos pasos podemos observar cómo saldrá un  en los resultados de este Cisco Lab como se puede comprobar a continuación. Dentro de los resultados del Switch llamado **VTP-SERVER** en el apartado llamado **VTP** sale el apartado **VTP Mode** el cual está en el estado correcto.



The screenshot shows the 'Activity Results' window in Cisco Packet Tracer. The 'Assessment Items' tab is active, displaying a table of test results. A red box highlights the 'VTP-SERVER' section, specifically the 'VTP Mode' row which is marked as 'Correct'.

Assessment Items	Status	Points	Component(s)	Feedback
VLAN 10		1	Switching	
VLAN Name	Incorrect	1	Switching	
VLAN 50		1	Switching	
VLAN Name	Incorrect	1	Switching	
VTP				
Domain Name	Incorrect	1	Other	
VTP Mode	Incorrect	1	Other	
VTP Password	Incorrect	1	Other	
VTP CLIENT3				
VLAN1S				
VLAN 1		1	Switching	
VLAN Name	Correct	1	Switching	
VLAN 10		1	Switching	
VLAN Name	Incorrect	1	Switching	
VLAN 50		1	Switching	
VLAN Name	Incorrect	1	Switching	
VTP				
Domain Name	Incorrect	1	Other	
VTP Mode	Incorrect	1	Other	
VTP Password	Incorrect	1	Other	
VTPSERVER				
VLAN1S				
VLAN 1		1	Switching	
VLAN Name	Correct	1	Switching	
VLAN 10		1	Switching	
VLAN Name	Incorrect	1	Switching	
VLAN 50		1	Switching	
VLAN Name	Incorrect	1	Switching	
VTP				
Domain Name	Incorrect	1	Other	
VTP Mode	Correct	1	Other	
VTP Password	Incorrect	1	Other	

3.3.1

Figura 3.3.1.D. Comprobación estado correcto Switch.

Apartado 2

2. Connect to the 3 other switches and configure them as VTP clients. All links between switches must be configured as trunk lines.

Para configurar un switch en VTP cliente simplemente entramos en el CLI o por el PC con el cable de consola en el terminal y ponemos lo siguiente:

```
Configure terminal
vtp mode client
```

3.3.2

```
VTP-CLIENT3(config)#vtp ?
  domain      Set the name of the VTP administrative domain.
  mode        Configure VTP device mode
  password    Set the password for the VTP administrative domain
  version     Set the administrative domain to VTP version
VTP-CLIENT3(config)#vtp mode ?
  client      Set the device to client mode.
  server      Set the device to server mode.
  transparent Set the device to transparent mode.
VTP-CLIENT3(config)#vtp mode client ←
Setting device to VTP CLIENT mode.
VTP-CLIENT3(config)#
```

Figura 3.3.2 comando vtp client

*Recordar que para que se dupliquen las vlan los switch clientes deben estar en modo trunk.

Apartado 3

3. Configure VTP domain name as "TESTDOMAIN" and VTP password as "cisco".

Para esto, debemos estar conectados al Switch que usaremos como Maestro VTP, en este caso el Switch llamado "VTP Server".

En primer lugar, cambiemos el nombre de dominio de VTP, necesitaremos usar el comando "vtp domain" y escribiendo después el nombre desado ("TESTDOMAIN" en este caso). En la Terminal debería mostrarse algo tal que así:

```
VTP-SERVER(config)#vtp domain TESTDOMAIN
Changing VTP domain name from NULL to TESTDOMAIN
```

3.3.3

Ahora necesitaremos usar el comando "vtp password" y escribir inmediatamente después la contraseña deseada ("cisco" en este caso). En la Terminal debería mostrarse esto:

```
VTP-SERVER(config)#vtp password cisco
Setting device VLAN database password to cisco
```

Si usamos el comando "show vtp status", comprobaremos que efectivamente se ha cambiado el nombre de dominio.

```
VTP-SERVER#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode         : Server
VTP Domain Name            : TESTDOMAIN
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MDS digest                 : 0x35 0x56 0x18 0x00 0xF6 0x7E 0x71 0xAB
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 192.168.1.1 on interface V11 (lowest numbered VLAN interface found)
```

Figura 3.3.3 a. Ejecución comando "show vtp status".

Apartado 4

4. Configure VLAN 10 with name "STUDENTS" and VLAN 50 with name "SERVERS"

Nos conectamos al Switch que usaremos como Maestro VTP, en este caso el Switch llamado "VTP Server".

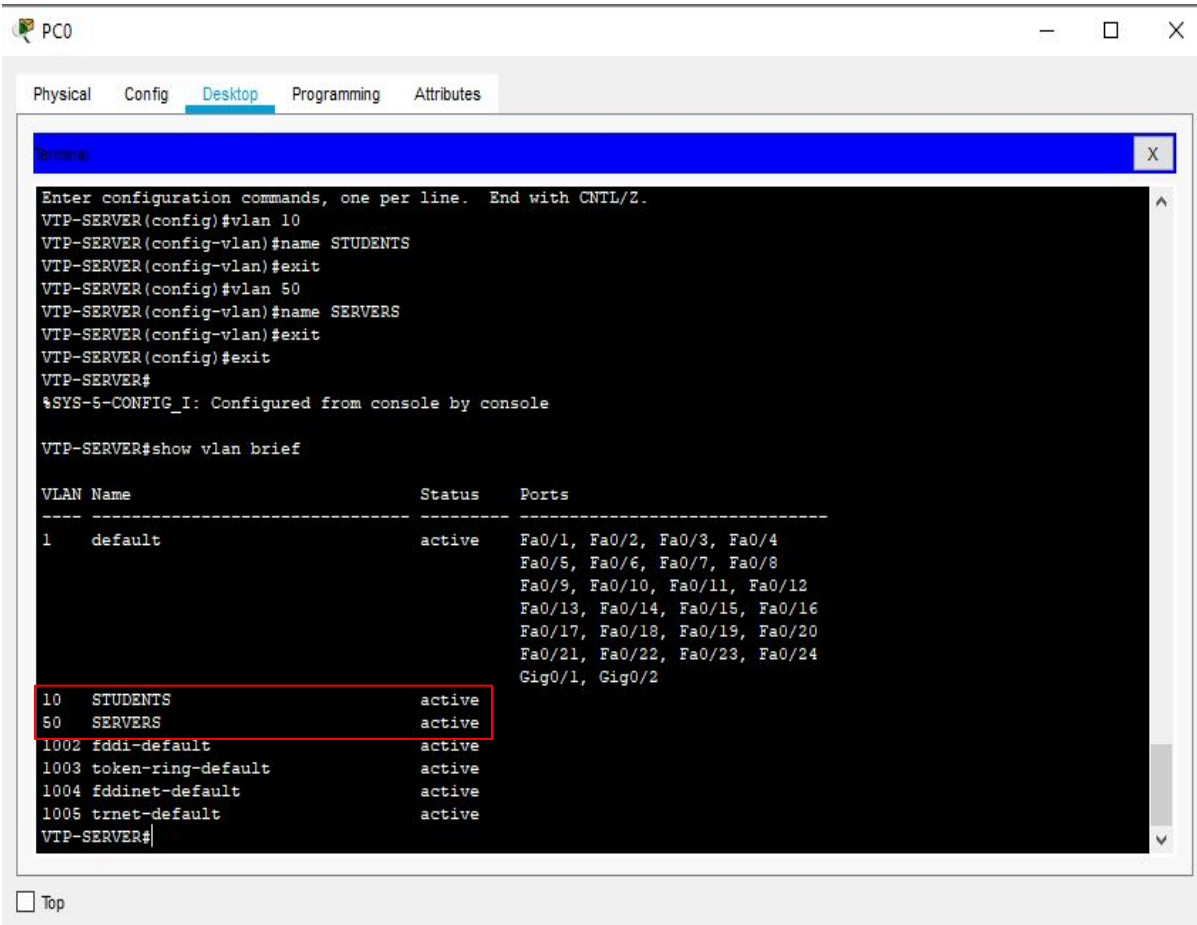
Entramos a la configuración del terminal y escribiremos el comando "vlan" acompañado del número de la vlan. Ya estamos configurando la vlan. Para cambiar su nombre debemos escribir el comando "name" y al lado el nombre deseado.

En nuestro caso para la VLAN 10 la nombraremos "STUDENTS" y VLAN 50 "SERVERS".

```
VTP-SERVER(config)#vlan 10
VTP-SERVER(config-vlan)#name STUDENTS
VTP-SERVER(config-vlan)#exit
```

3.3.4

Repetimos el mismo proceso para la VLAN 50 y para comprobar que se ha aplicado correctamente salimos de la configuración y usamos el comando "show vlan brief"



The screenshot shows a terminal window titled "PC0" with tabs for Physical, Config, Desktop, Programming, and Attributes. The terminal output is as follows:

```
Enter configuration commands, one per line. End with CNTL/Z.
VTP-SERVER(config)#vlan 10
VTP-SERVER(config-vlan)#name STUDENTS
VTP-SERVER(config-vlan)#exit
VTP-SERVER(config)#vlan 50
VTP-SERVER(config-vlan)#name SERVERS
VTP-SERVER(config-vlan)#exit
VTP-SERVER(config)#exit
VTP-SERVER#
%SYS-5-CONFIG_I: Configured from console by console

VTP-SERVER#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
                                           Gig0/1, Gig0/2
10   STUDENTS                active
50   SERVERS                 active
1002 fddi-default           active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default          active
VTP-SERVER#
```

The rows for VLAN 10 (STUDENTS) and VLAN 50 (SERVERS) are highlighted with a red box in the original image.

Figura 3.3.4 a. Demostración cambio de nombres de VLAN

Apartado 5

5. Check propagation on all switches of the VTP domain.

Nos conectamos a un Switch que sea cliente para comprobar que el VTP se ha propagado correctamente.

Para ello haremos uso del comando el comando "show vtp status" el cual nos mostrará toda la información relacionada con el VTP. Podremos ver el modo en el que está puesto el switch si está como cliente o server, el dominio de VTP en el que está, etc.

Una vez dentro nos aseguramos de que los datos que figuran allí son los mismos que nuestro servidor de VTP.

Para comprobar la contraseña de VTP usaremos "show vtp password" y comprobaremos que está se corresponda con la del servidor VTP.

3.3.5

```
VTP-CLIENT#show vtp status
```

```
VTP-CLIENT#show vtp password
```

```
VTP-CLIENT1>enable
Password:
VTP-CLIENT1#show vtp status
VTP Version          : 2
Configuration Revision : 4
Maximum VLANs supported locally : 255
Number of existing VLANs : 7
VTP Operating Mode   : Client
VTP Domain Name      : TESTDOMAIN
VTP Pruning Mode     : Disabled
VTP V2 Mode          : Disabled
VTP Traps Generation : Disabled
MD5 digest           : 0x53 0x6D 0xA1 0x5B 0x9E 0xB7 0x41 0xD8
Configuration last modified by 192.168.1.1 at 3-1-93 00:14:36
VTP-CLIENT1#
```

Figura 3.3.5 a. Ejecución comando `show vtp status`

```
VTP-CLIENT1#show vtp password
VTP Password: cisco
VTP-CLIENT1#
```

Figura 3.3.5 b. Ejecución comando `show vtp password`

Por último haremos un `show VLAN brief` en todos los switches para comprobar que tienen las mismas VLAN que el servidor VTP.

```
VTP-CLIENT1#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
10   STUDENTS                active
50   SERVERS                 active
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
VTP-CLIENT1#
```

Figura 3.3.5 c. Ejecución comando `show vlan brief`

Añadido 1

1. Comprueba que los cambios en VLAN que se hagan en el maestro se replican de forma automática en todos los clientes

Comprobamos las VLAN que tiene el VTPCliente:

```
VTP-CLIENT2#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

10   STUDENTS                active
50   SERVERS                 active
1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
VTP-CLIENT2#
```

3.3A1

Figura 3.3.A1.A. Muestra Vlan del VTPCliente.

Y ahora realizaremos cambios en el Servidor ,por ejemplo creando la Vlan “Prueba” y observaremos como se replica en los clientes.

```
VTP-CLIENT3#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

10   STUDENTS                active
50   SERVERS                 active
69   Prueba                  active
1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
VTP-CLIENT3#
```

Figura 3.3.A1.B. Muestra Vlan del VTPCliente Replicado.

Añadido 2

2. Comprueba que NO puedes realizar ningún cambio a nivel de VLAN en los clientes.

Con el VTP del switch configurado como cliente, comprobaremos cómo no podremos realizar ningún cambio a nivel de VLAN en éstos.

```
VTP-CLIENT1#
%SYS-5-CONFIG_I: Configured from console by console

VTP-CLIENT1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
VTP-CLIENT1(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
VTP-CLIENT1(config)#
```

3.3.A2

Figura 3.3.A2.A. Intento de configuración fallido de la VLAN10 en un cliente.

Como vemos en la **Figura 3.3.A2.A**, tras intentar variar la configuración de la VLAN10 en un switch VTP configurado como cliente, la consola del mismo nos informa que la configuración de VLAN no está permitido para dispositivos configurados como clientes.

Esto se debe a que los clientes reciben la configuración de las VLAN únicamente del dispositivo configurado como servidor, y, por tanto, cualquier cambio deberá ser realizado en éste.

Añadido 4

4. ¿Pueden convivir varios dominios en una misma red?

1. Para ello, crea ahora un nuevo dominio llamado **IB_DOMAIN**, con un VTP Server y un VTP Cliente. Crea la VLAN 10 con exactamente las mismas bocas que la VLAN del TESTDOMAIN del ejercicio y la VLAN 60 con las mismas bocas que la vlan 50 de TESTDOMAIN. Une ahora IB_DOMAIN a la red TESTDOMAIN con un enlace troncal.

Para comprobar esto se va añadir a la red con el nombre 'TESTDOMAIN' dos switches los cuales llamaremos, el que va ser configurado como VTP Server, recibe el nombre de 'SERVER' y el que va a ser configurado como cliente, recibe el nombre de 'CLIENTE'. A esta red la llamaremos **IB_DOMAIN**.

Seguidamente se configurará el switch que recibe el nombre de **SERVER** de la red llamada **IB_DOMAIN** como VTP modo Server, y el switch que recibe el nombre de **CLIENTE** se configurará como VTP modo Cliente.

A continuación, se creará en en el switch llamado **SERVER** la VLAN 10 con exactamente las mismas bocas que la VLAN del TESTDOMAIN del ejercicio y la VLAN 60 con las mismas bocas que la vlan 50 de TESTDOMAIN. De esta manera, estas VLANs también se crearán en el switch que recibe el nombre de 'CLIENTE'.

Finalmente, conectaremos mediante un cable el cual será configurado en ambos switches (**SERVER y VTP SERVER**) como troncal dejando la red de la siguiente manera:

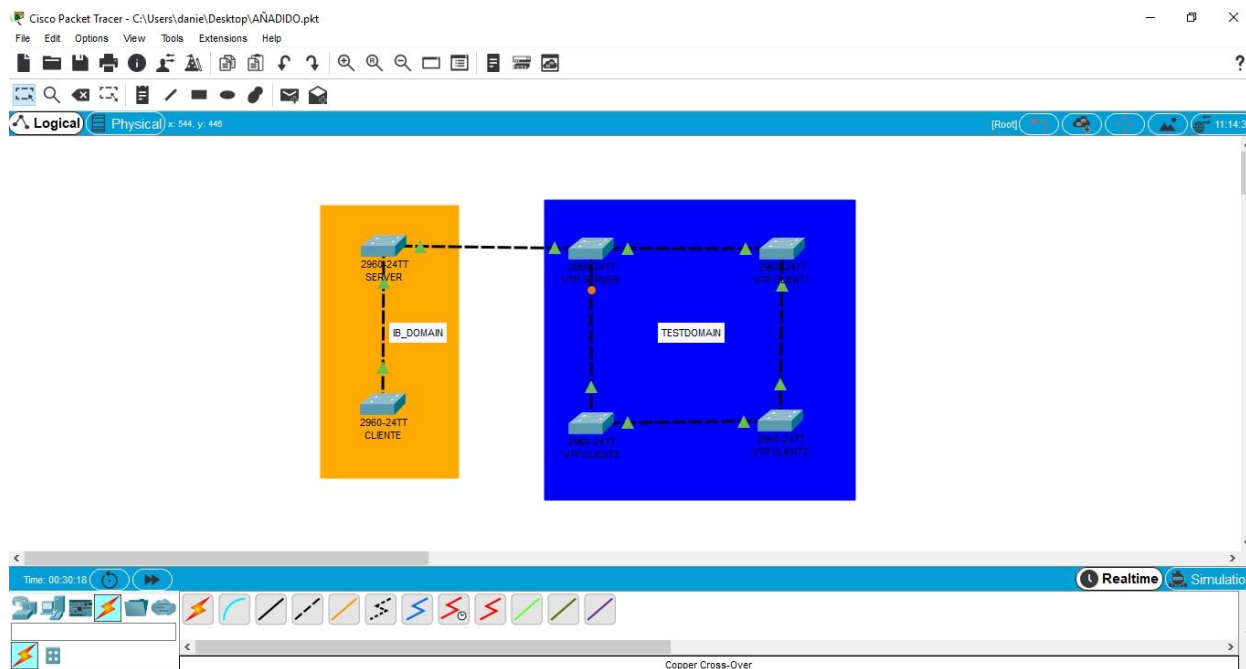


Figura 3.3.A4.A. Red con varios dominios en una misma red.

Visualmente realizando todas las configuraciones pertinentes no se ha observado ninguna anomalía por lo tanto se deduce que pueden convivir varios dominios en una misma red.

3.3.A
4

Añadido 5

5. ¿Hay conectividad entre los dominios?

1. Para ello, conecta un PC a la VLAN 10 en el TESTDOMAIN y un PC a la VLAN 10 en el IB_DOMAIN

2. ¿Hay conectividad entre ellos?

3.3.A5

Tenemos el siguiente esquema:

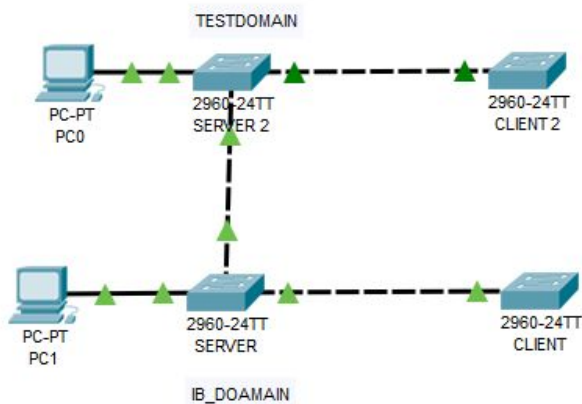


Figura 3.3.a5 esquema de prueba de conexión

El PC 1 y 0 están conectados a la misma vlan (10) en los distintos switch al realizar un ping entre los PC nos dice que ha fallado por lo tanto **no hay conexión**.

Añadido 6 (I)

6. ¿Qué ocurre si le cambiamos la clave VTP al servidor? ¿Se pierden las VLAN de los clientes?

En primer lugar, mostraremos las VLAN que tiene uno de los Switches (en este caso hemos escogido el "VTP-CLIENT1") establecidos como clientes con el comando "show vlan brief".

```
VTP-CLIENT1#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
10 STUDENTS	active	
50 SERVERS	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

3.3.A6

Figura 3.3.A6.a. Comprobación de VLAN en Switch VTP-CLIENT1 antes de cambiar clave.

Una vez hecho esto, iremos al Switch maestro (VTP-SERVER) y cambiaremos la clave VTP usando el comando "vtp password".

```
VTP-SERVER(config)#vtp password 1234  
Setting device VLAN database password to 1234
```

Figura 3.3.A6.b. Cambio de clave VTP en Switch maestro.

Ahora mostraremos las VLAN que tiene el Switch maestro para comprobar si hay cambios.

```
VTP-SERVER#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
10 STUDENTS	active	
50 SERVERS	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Figura 3.3.A6.c. Comprobación de VLAN en Switch maestro.

Añadido 6 (II)

6. ¿Qué ocurre si le cambiamos la clave VTP al servidor? ¿Se pierden las VLAN de los clientes?

Volvemos al Switch VTP-CLIENT1 para ver si han cambiado o no las VLAN.

```
VTP-CLIENT1#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
10	STUDENTS	active	
50	SERVERS	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

3.3.A6

Figura 3.3.A6.d. Comprobación de VLAN en Switch VTP-CLIENT1 al cambiar clave.

Como podemos comprobar, las VLAN que tienen los clientes **no** se borran.

Al cambiar la clave VTP todo lo que modifiques posteriormente en el Switch establecido como maestro **no** llegará a los demás, puesto que para que se cumpla VTP deben tener el mismo nombre de dominio, la misma versión de VTP y lo que nos concierne en este caso, **la misma contraseña**.

Añadido 7

7. ¿Está VTP descatalogado o está vigente en la actualidad? De estar descatalogado, ¿cuál es el protocolo que lo sustituye?

Actualmente VTP se encuentra en activo con su versión 3. Esto se puede confirmar gracias a que en la última gama de routers de CISCO ([Routers CISCO de 3º Generación: Serie 4000](#))

En el siguiente enlace se puede apreciar como CISCO sigue trabajando con VTP tanto en los switches como en sus routers antiguos como en los de última generación.

https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html?referring_site=RE&pos=2&page=https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98155-tshoot-vlan.html

3.3.A7

The screenshot shows a web browser window displaying the Cisco support page titled "Configuring VLAN Trunk Protocol (VTP)". The browser's address bar shows the URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html?referring_site=RE&pos=2&page=https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98155-tshoot-vlan.html. The page content includes a breadcrumb trail: "Support / Technology Support / LAN Switching / Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) / Configuration Examples and TechNotes /". Below the title, there are "Translations" and "Print" icons. The document is dated "Updated: September 24, 2014" with "Document ID: 98154". A "Contents" section lists various topics such as "Introduction", "Prerequisites" (Requirements, Components Used, Conventions), "Understand VTP", "VTP Configuration Guidelines", and "VTP Configuration on Catalyst Switches" (listing various Catalyst series like 6500/6000, 4500/4000, 2950, 3550, 2900XL, 3500XL, and Express 500). On the right side, there is a "Was this Document Helpful?" section with "Yes" and "No" buttons, a "Feedback" link, and a "Viewers of This Document Also Viewed" section listing related documents like "Configuring VTP", "Understanding VLAN Trunk Protocol (VTP)", and "Troubleshooting VLAN Trunk Protocol (VTP)".

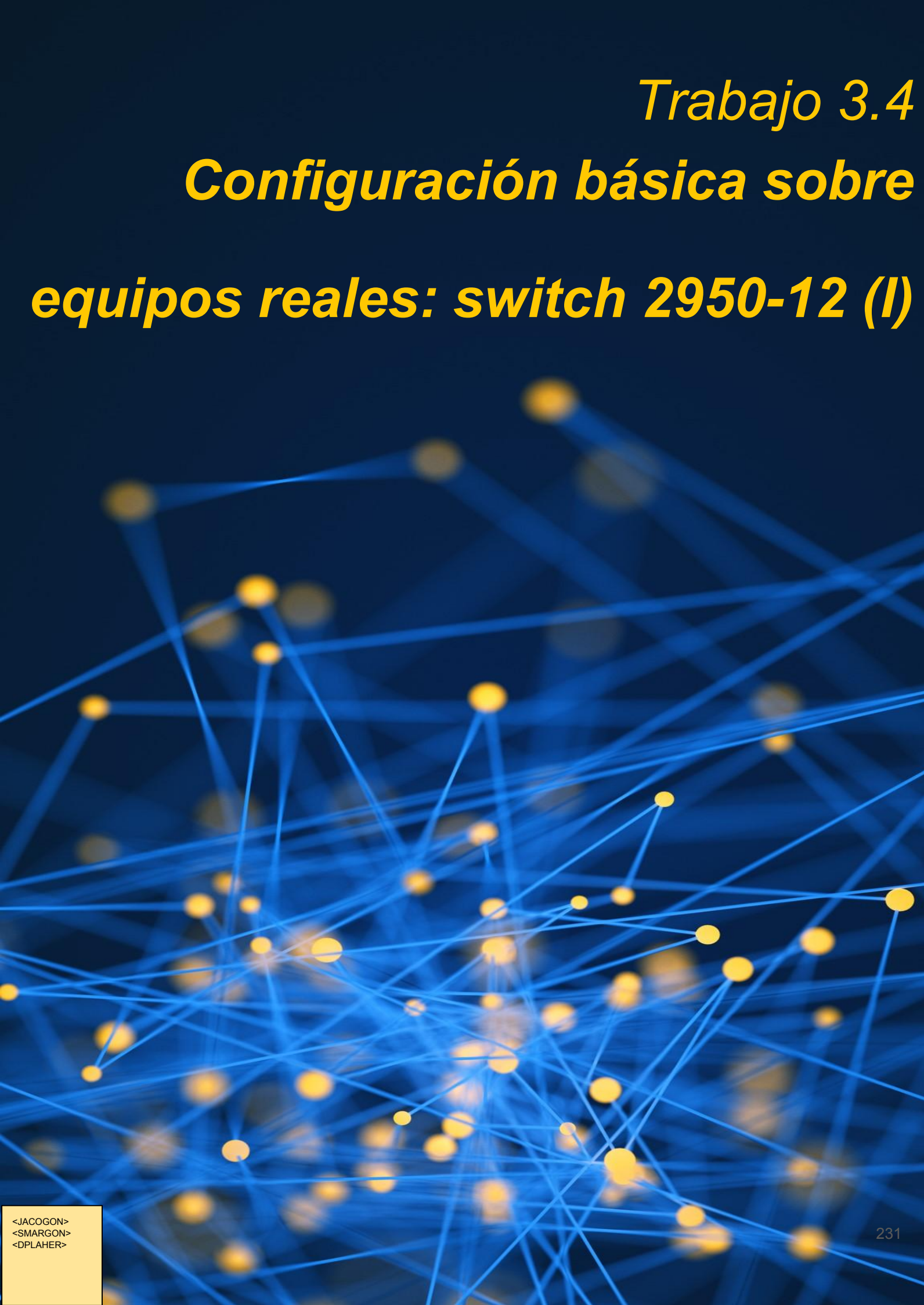
Figura 3.3.A7.a Página CISCO Configurando VTP

Añadido 8

8. ¿Hay alguna forma de que VTP se repliquen no solo las VLAN, su ID y su nombre, sino también las bocas asociadas?

Por VTP se replican sólo las distintas tantos IDs como nombres, pero no se propagan las bocas asociadas, por tanto habrá que asignar en cada switch las bocas correspondientes a cada VLAN, no se ha encontrado ninguna manera de replicar esa información mediante VTP, por tanto esto no es posible ?

3.3.A8



Trabajo 3.4
***Configuración básica sobre
equipos reales: switch 2950-12 (I)***

Trabajo 3.4. Configuración básica sobre equipos reales: switch 2950-12 (I)

Hasta ahora todos los trabajos los hemos realizado sobre el simulador de redes de datos Cisco Packet Tracer.

En esta ocasión vamos a utilizar los equipos de redes telemáticas que tenemos en clase.

Utilizando los switch 2950-12 del fabricante Cisco, los PCs de clase y la red de datos del aula, realizar las siguientes tareas:

1. **Serial.** Utiliza los adaptadores de USB a serial. Indica cómo se realiza su instalación, su conexión y su configuración.
2. **Putty.** Instala Putty en tu PC. Configura Putty y conéctate al switch desde tu PC utilizando un cable de conexión a la consola.
3. **Nombre del switch.** Cambia el nombre del switch y pon tu propio nombre.
4. **Telnet.** Habilita la conexión por telnet al switch. Conéctate desde un PC al switch vía telnet
5. **Guarda la configuración** que has creado del switch en la memoria no volátil, de modo que cuando arranque NO se pierdan los cambios que has hecho.
6. **VLAN.** Crea una nueva VLAN en el switch. Realiza una conexión física de varios equipos del aula a diferentes bocas del switch que estén en diferentes VLAN y demuestra que hay conectividad entre los equipos de la misma VLAN y que no hay conectividad entre los equipos de diferente VLAN
7. **SSH.** Habilita la conexión por SSH al switch. Prueba a conectarte desde un PC por ssh utilizando Putty. Por último, prueba a conectarte por SSH activando el cliente ssh desde la consola del CMD de Windows.
8. **VTP.** Utilizando dos switches, monta una red VTP con un servidor y un cliente. Demuestra que la red VTP está funcionando sencillamente comprobando que las VLAN del cliente están sincronizadas con las VLAN del servidor.

Apartado 1

1. **Serial.** Utiliza los adaptadores de USB a serial. Indica cómo se realiza su instalación, su conexión y su configuración.

Para poder usar los adaptadores necesitamos descargar el driver correspondiente para que puedan funcionar correctamente, en este caso el adaptador del que disponemos en clase es el convertidor de USB a serial TU-S9 de Trendnet.



Figura 3.4.1 a: Adaptador USB a Serial.

3.4.1.

Para ello nos iremos a la página web del fabricante y buscaremos este adaptador una vez allí nos descargamos los drivers correspondientes, el link que lleva a la página es el siguiente: http://www.trendnet.com/langsp/support/support-detail.asp?prod=265_TU-S9.

Luego pasaremos al proceso de instalación del software el cual es muy sencillo, simplemente usaremos el ejecutable que nos descarguemos, para el sistema operativo correcto ya sea Mac o Windows y seguiremos los pasos que nos indica el instalador, le daremos a next para continuar con la instalación.

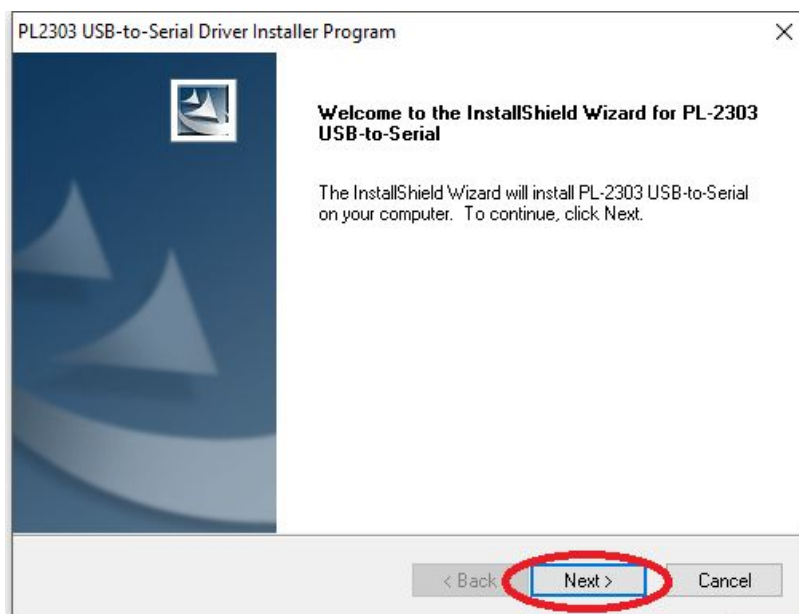
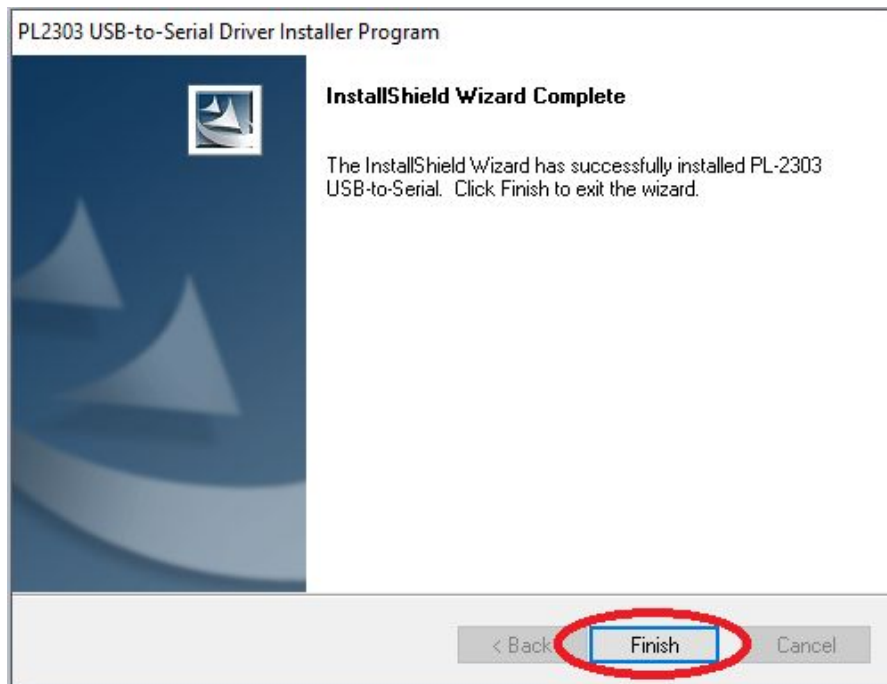


Figura 3.4.1 b: Instalador del Driver del adaptador.

Apartado 1

1. **Serial.** Utiliza los adaptadores de USB a serial. Indica cómo se realiza su instalación, su conexión y su configuración.

Cuando haya terminado el proceso de instalación daremos a finalizar en el instalador y reiniciamos el pc para que los cambios se apliquen.



3.4.1.

Figura 3.4.1 c: Finalización de Instalación del driver

Una vez hecho esto conectaremos nuestro adaptador al puerto USB del PC y conectaremos el cable de consola al adaptador y al puerto de consola del Switch y ya deberían funcionar correctamente.



Figura 3.4.1 d: Boca consola del switch

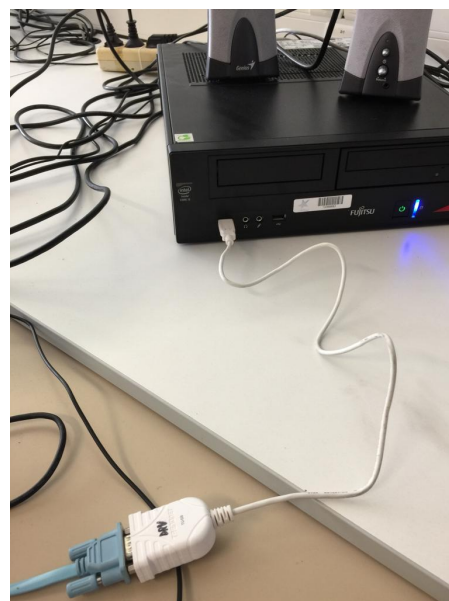


Figura 3.4.1 e: adaptador conectado

Apartado 2

2. Putty. Instala Putty en tu PC. Configura Putty y conéctate al switch desde tu PC utilizando un cable de conexión a la consola.

Para comenzar entraremos en la página de Putty: <https://www.putty.org/> y clicamos en **here**. **Figura 3.4.2.a**



Download PuTTY

PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is available with source code and is developed and supported by a group of volunteers.

You can download PuTTY [here](#).

Below suggestions are independent of the authors of PuTTY. They are not to be seen as endorsements by the PuTTY project.



Bitvise SSH Client

Bitvise SSH Client is an SSH and SFTP client for Windows. It is developed and supported professionally by Bitvise. The SSH Client is robust, easy to install, easy to use, and supports all features supported by PuTTY, as well as the following:

- graphical SFTP file transfer;
- single-click Remote Desktop tunneling;
- auto-reconnecting capability;
- dynamic port forwarding through an integrated proxy;
- an FTP-to-SFTP protocol bridge.

Bitvise SSH Client is **free to use**. You can [download it here](#).



Bitvise SSH Server

Bitvise SSH Server is an SSH, SFTP and SCP server for Windows. It is robust, easy to install, easy to use, and works well with a variety of SSH clients, including Bitvise SSH Client, OpenSSH, and PuTTY. The SSH Server is developed and supported professionally by Bitvise.

You can [download Bitvise SSH Server here](#).

[FAQ](#)

Figura 3.4.2.a: Descargando Putty.

Seleccionamos la opción 64-bit o 32-bit según nuestro equipo. **Figura 3.4.2.b**

Download PuTTY: latest release (0.70)

[Home](#) | [FAQ](#) | [Feedback](#) | [Licence](#) | [Updates](#) | [Mirrors](#) | [Keys](#) | [Links](#) | [Team](#)
[Download Stable](#) - [Snapshot](#) | [Docs](#) | [Changes](#) | [Wishlist](#)

This page contains download links for the latest released version of PuTTY. Currently this is 0.70, released on 2017-07-08.

When new releases come out, this page will up-date to contain the latest, so this is a good page to bookmark or link to. Alternatively, here is a [permanent link to the 0.70 release](#).

Release versions of PuTTY are versions we think are reasonably likely to work well. However, they are often not the most up-to-date version of the code available. If you have a problem with this release, then it might be worth trying out the [development snapshots](#), to see if the problem has already been fixed in those versions.

Package files

You probably want one of these. They include all the PuTTY utilities.

(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

MSI ("Windows Installer")

32-bit: [putty-0.70-installer.msi](#) (or by FTP) (signature)

64-bit: [putty-64bit-0.70-installer.msi](#) (or by FTP) (signature)

Unix source archive

.tar.gz: [putty-0.70.tar.gz](#) (or by FTP) (signature)

Alternative binary files

The installer packages above will provide all of these (except PuTTYtel), but you can download them one by one if you prefer.

(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

putty.exe (the SSH and Telnet client itself)

32-bit: [putty.exe](#) (or by FTP) (signature)

64-bit: [putty.exe](#) (or by FTP) (signature)

pscp.exe (an SCP client, i.e. command-line secure file copy)

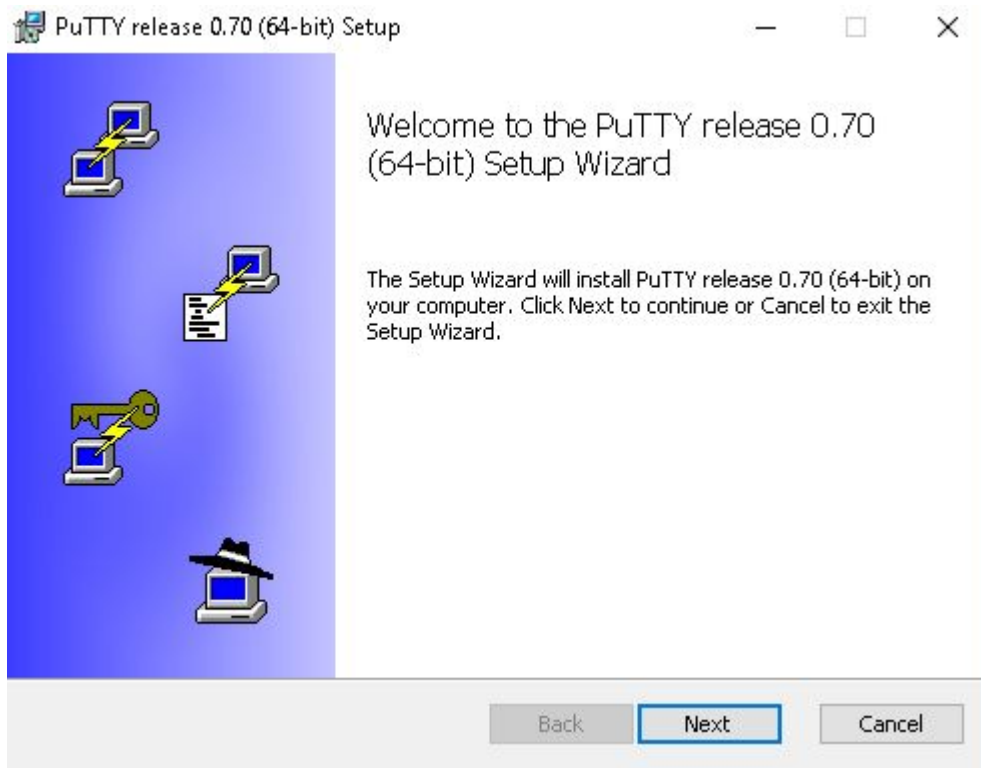
32-bit: [pscp.exe](#) (or by FTP) (signature)

Figura 3.4.2.b: Descargando Putty.

3.4.2

Apartado 2

Una vez descargamos el programa lo instalaremos siguiendo estos pasos:



3.4.2

Figura 3.4.2.c: Instalando Putty.

Seleccionamos el destino donde se instalará el programa. *Figura 3.4.2.d*

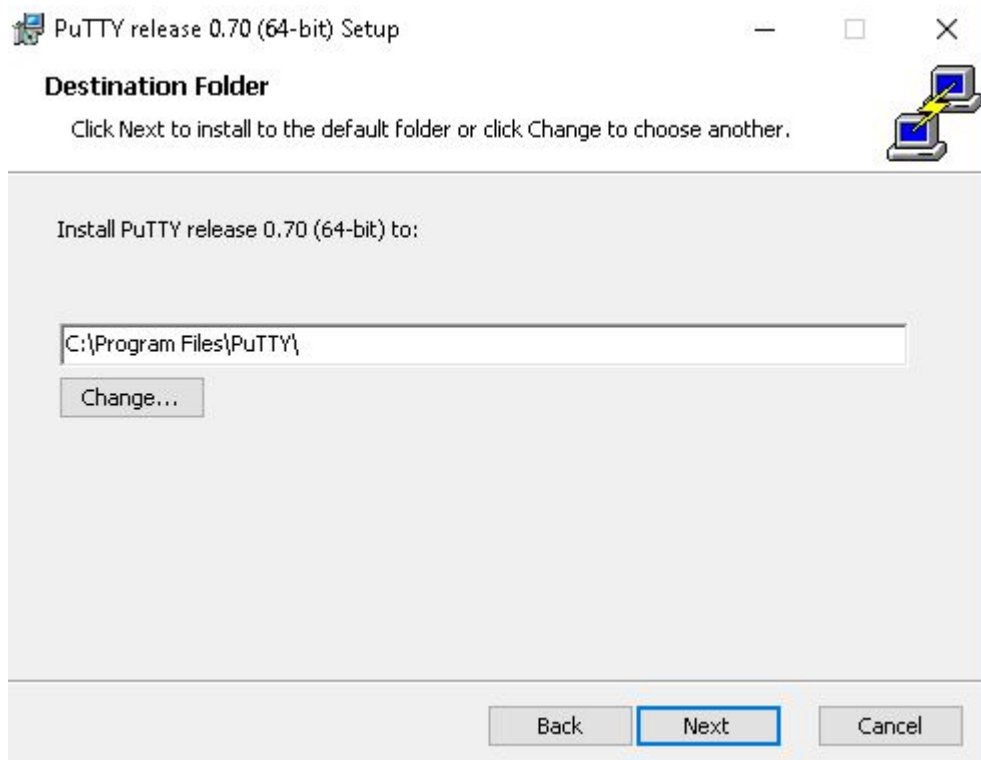
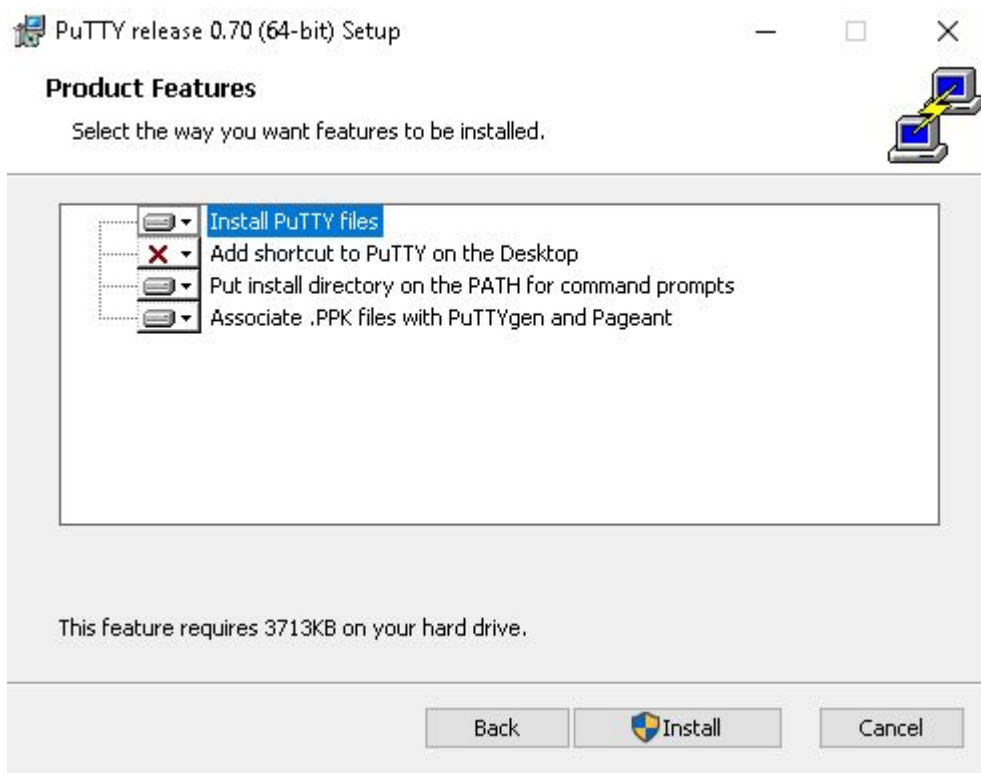


Figura 3.4.2.d: Instalando Putty.

Apartado 2

Elegimos esta configuración. **Figura 3.4.2.e**



3.4.2

Figura 3.4.2.e: Instalando Putty.

Finalizamos instalación. **Figura 3.4.2.e**

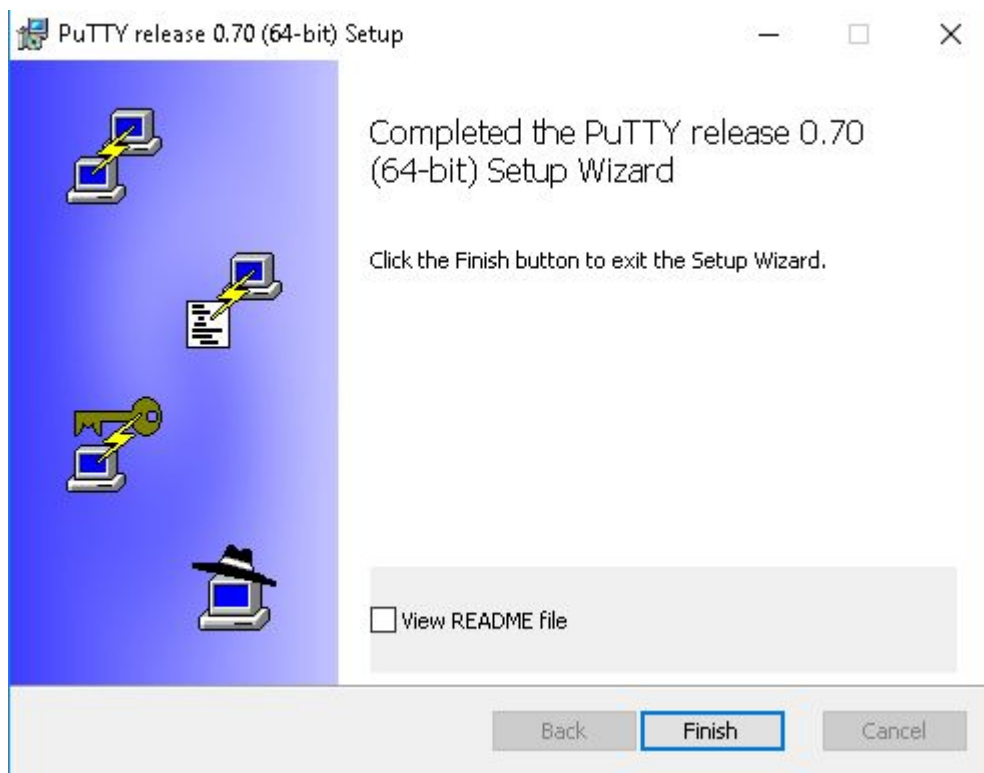
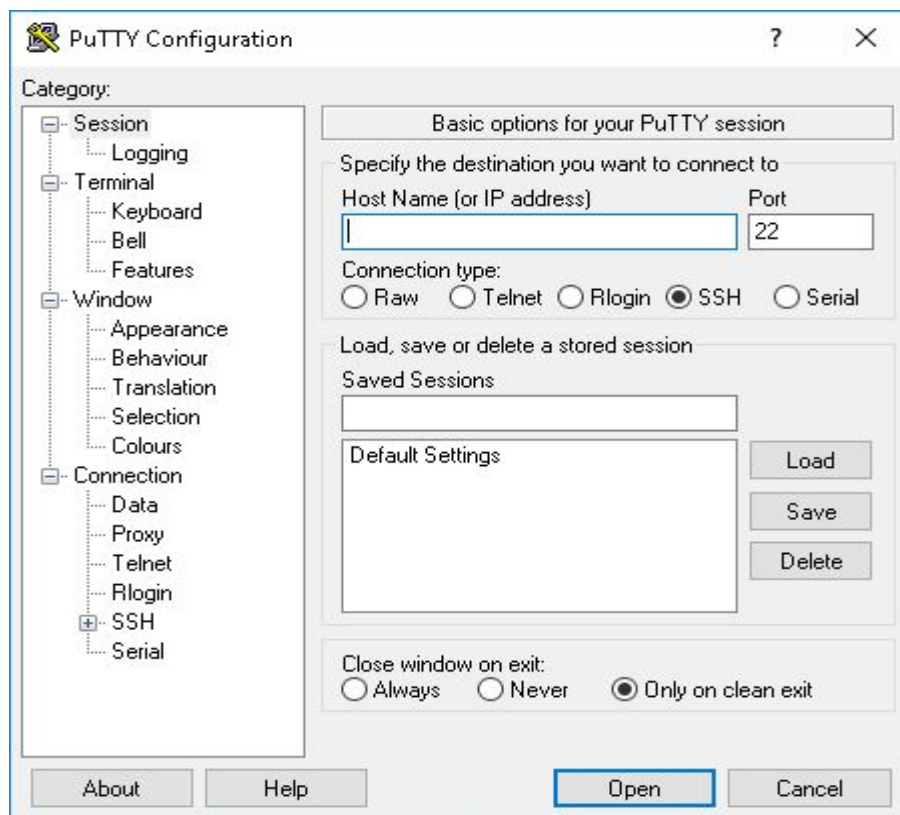


Figura 3.4.2.f: Instalando Putty.

Apartado 2

Abrimos el programa. **Figura 3.4.2.g**



3.4.2

Figura 3.4.2.g: Configurando Putty.

Conectamos el switch al PC con el adaptador de usb y serial como se explicó en el apartado 1. Una vez lo conectamos buscaremos cuál es el puerto al que se encuentra ligado. Para ello Iremos a Administración de dispositivos. Para ello hacemos click derecho en el símbolo de inicio y seleccionamos **Administración de dispositivos**. **Figura 3.4.2.h**

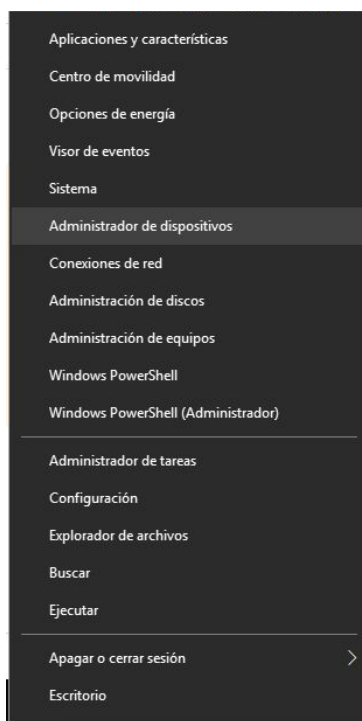
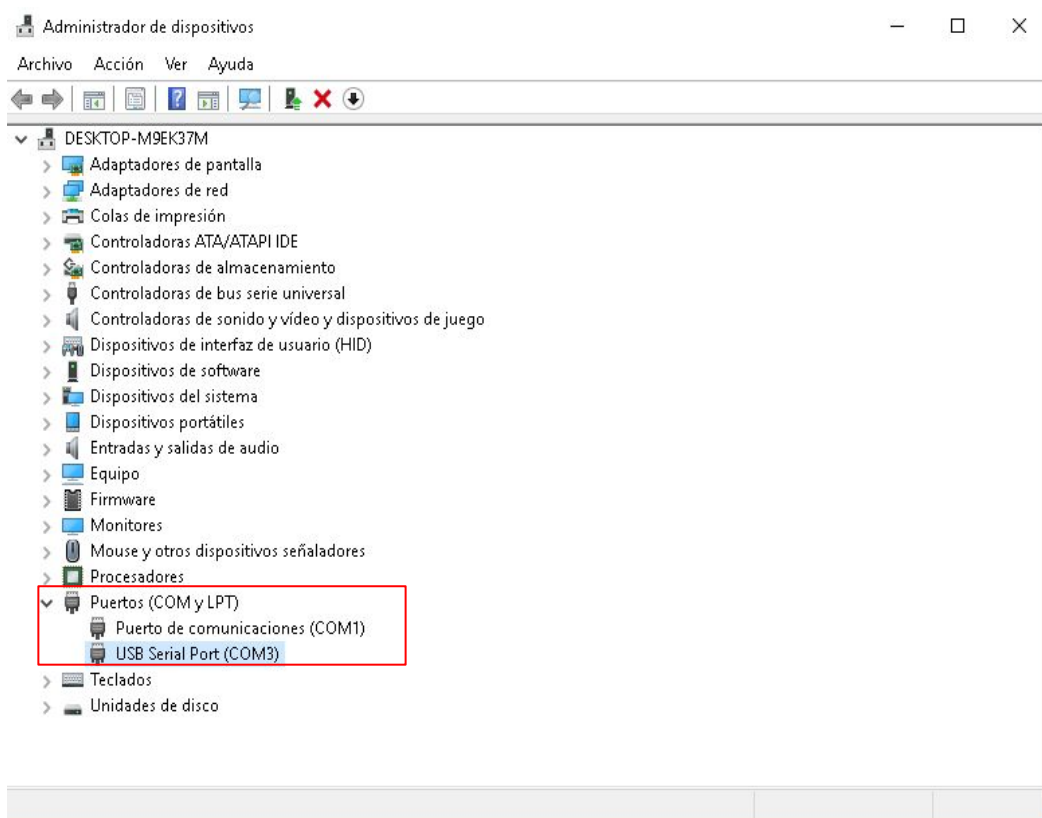


Figura 3.4.2.h: Puerto COM.

Apartado 2

Abrimos la pestaña “**Puerto (COM y LPT)**” y encontramos en nuestro caso que el adaptador es el llamado puerto **COM**.



3.4.2

Figura 3.4.2.i: Puerto COM.

En el menú que nos encontramos al abrir el programa seleccionamos el apartado Serial. En serial line escribimos **COM3** y no modificamos nada más. **Figura 3.4.2.j**

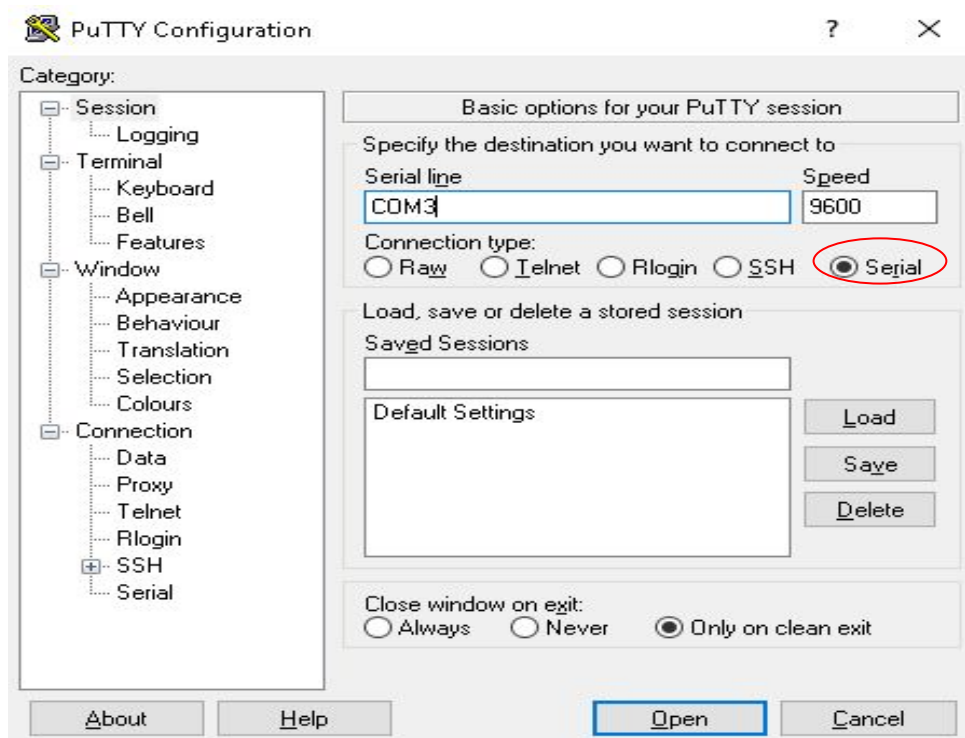
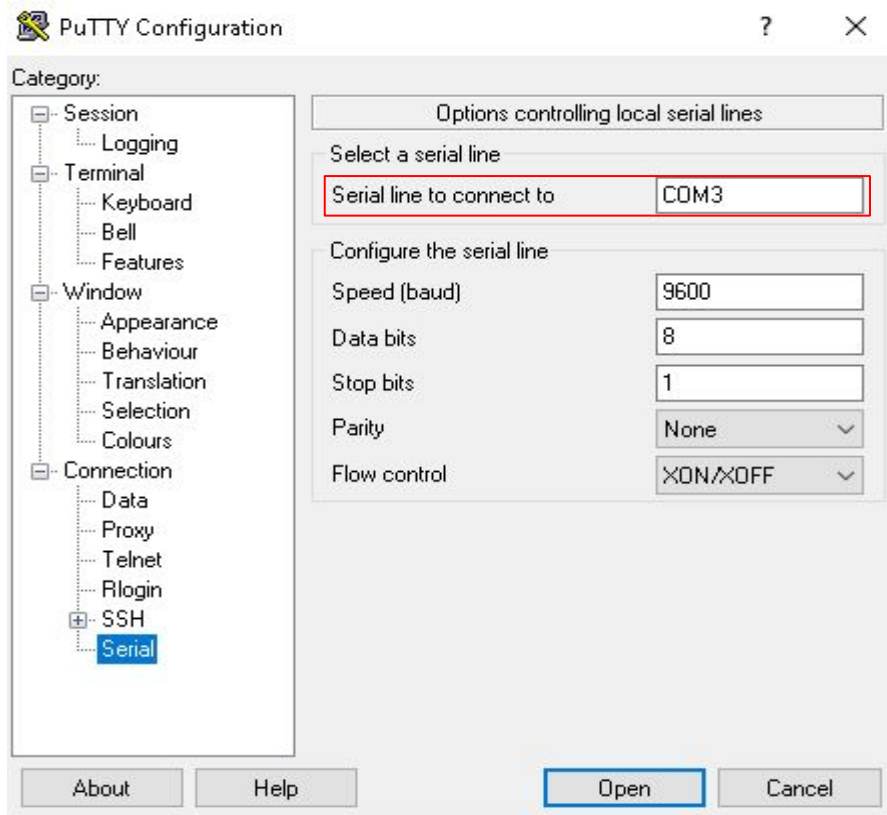


Figura 3.4.2.j: Configurando Putty.

Apartado 2

Lo siguiente será ir al apartado Connection-SSH-Serial. Dejaremos la configuración predeterminada y serial line pondremos **COM3**. **Figura 3.4.2.k**



3.4.2

Figura 3.4.2.k: Configurando Putty.

Clicamos en Open y ya estaríamos dentro del switch. **Figura 3.4.2.l**



Figura 3.4.2.l: Configurando Putty.

Apartado 3

2. **Nombre del switch.** Cambia el nombre del switch y pon tu propio nombre.

Para cambiarle el nombre al switch, lo que deberemos hacer será aplicar el comando "hostname NOMBRE" tras haber ingresado a la configuración del terminal con el comando "configure terminal".

Esto queda probado en la **Figura 3.4.3**.



Figura 3.4.3. Aplicación del comando "hostname" con switch real.

Apartado 4

4. Telnet. Habilita la conexión por telnet al switch. Conéctate desde un PC al switch vía telnet

Bueno, en este apartado de la configuración básica de equipos reales vamos a explicar como hacer una conexión vía telnet desde un PC para entrar a la **consola** de un switch, en este caso real. Pues para comenzar, vamos a empezar por el primer paso el cuál sería como conectar nuestro switch y nuestro PC para que pueda realizarse esta conexión.

De esta manera, lo primero sería coger un **Switch Real** y conectarlo la corriente mediante un cable de corriente, obviamente, para que directamente este se encienda y poder empezar a usarlo en condiciones. Seguidamente, el siguiente paso será conectar nuestro Switch al PC para lo cual debemos usar **un cable de consola**, y debido a que los ordenadores que disponemos en el aula no tienen puerto serie también utilizaremos un **adaptador Serial a USB**. El cable de consola irá conectado al puerto de consola del **Switch Real**, el otro extremo del cable irá al adaptador **Serial a USB** y el **USB** irá conectado a uno de los puertos USB de nuestro PC.

3.4.4



Figura 3.4.4.1. Conexión Switch Real al PC.



Figura 3.4.4.2. Adaptador Serial a USB.



Figura 3.4.4.3. Conexión adaptador USB a Serial al PC.

El segundo paso será conectar el otro extremo del cable Ethernet que se encuentra conectado al puerto FastEthernet de nuestro PC a una de las bocas de nuestro **Switch Real** para que haya conexión entre ambos, en nuestro caso lo conectaremos al puerto 1.



3.4.4

Figura 3.4.4.4. Conexión Cable Ethernet del PC al Switch.

Seguidamente, el tercer paso sería conocer en qué **Puerto COM** del PC tenemos conectado nuestro **Switch Real** para introducirlo después en el programa **PuTTY**. Para conocer en qué **puerto COM** tenemos conectado nuestro Switch Real debemos escribir en nuestra barra de búsqueda de nuestro sistema de operativo '**Administrador de dispositivos**' y haremos click sobre él.

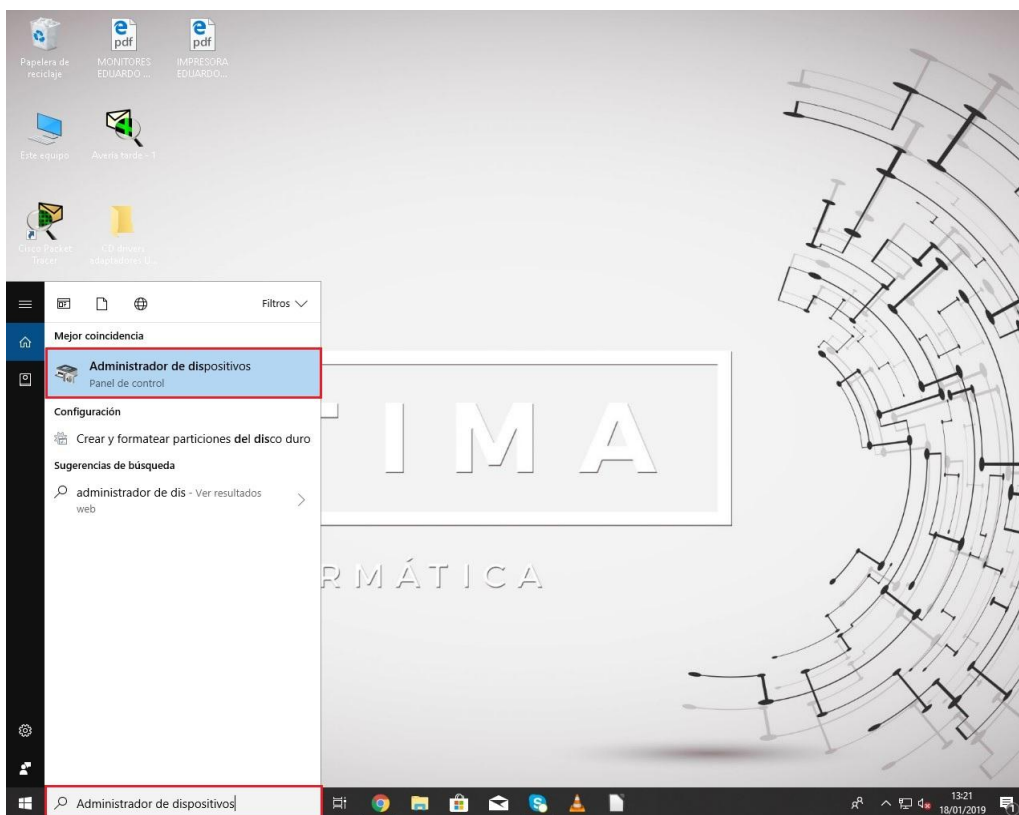
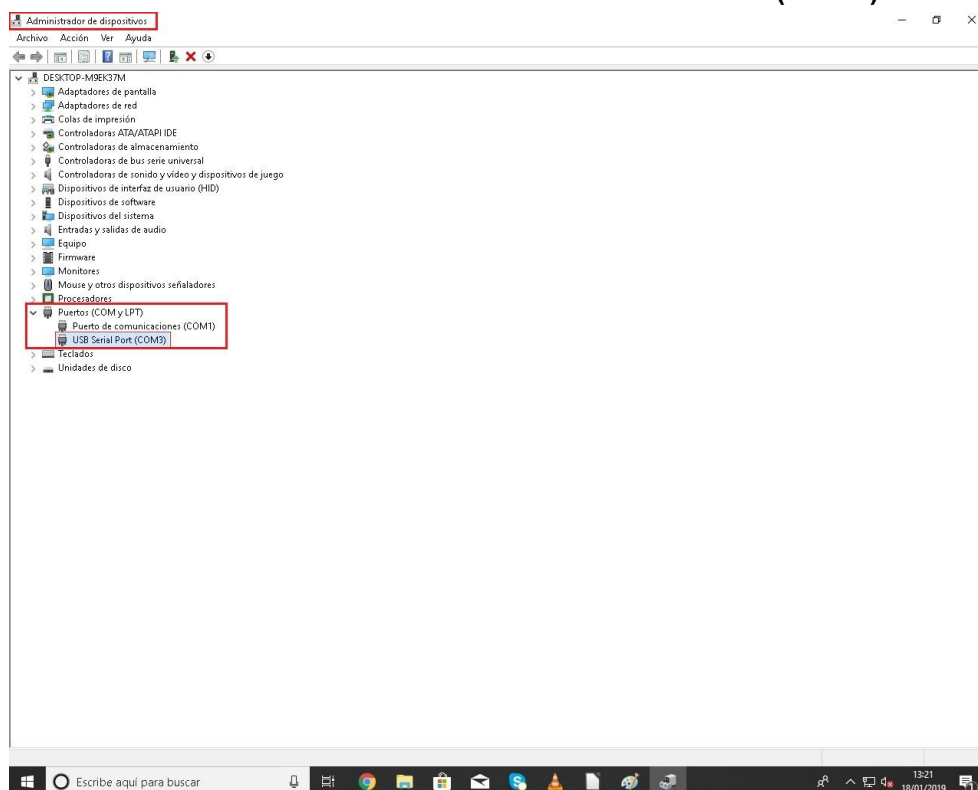


Figura 3.4.4.5. Acceso al Administrador de dispositivos.

<DPLAHER>

Una vez dentro de él dentro de la pestaña ‘Puertos (COM y LPT)’ podemos observar como nuestro Switch Real se encuentra conectado en el ‘USB Serial Port (COM3)’.



3.4.4

Figura 3.4.4.6. Comprobación Puerto COM del Switch Real.

El cuarto paso será entrar a la consola de nuestro **Switch Real** para introducir los comandos adecuados para poder realizar la conexión por telnet desde nuestro PC. Para ello utilizaremos el programa **PuTTY**, el cual ya fue explicada su instalación anteriormente. Para acceder al programa ya instalado, accederemos a él desde la barra de búsqueda de nuestro sistema operativo y haremos click sobre él.

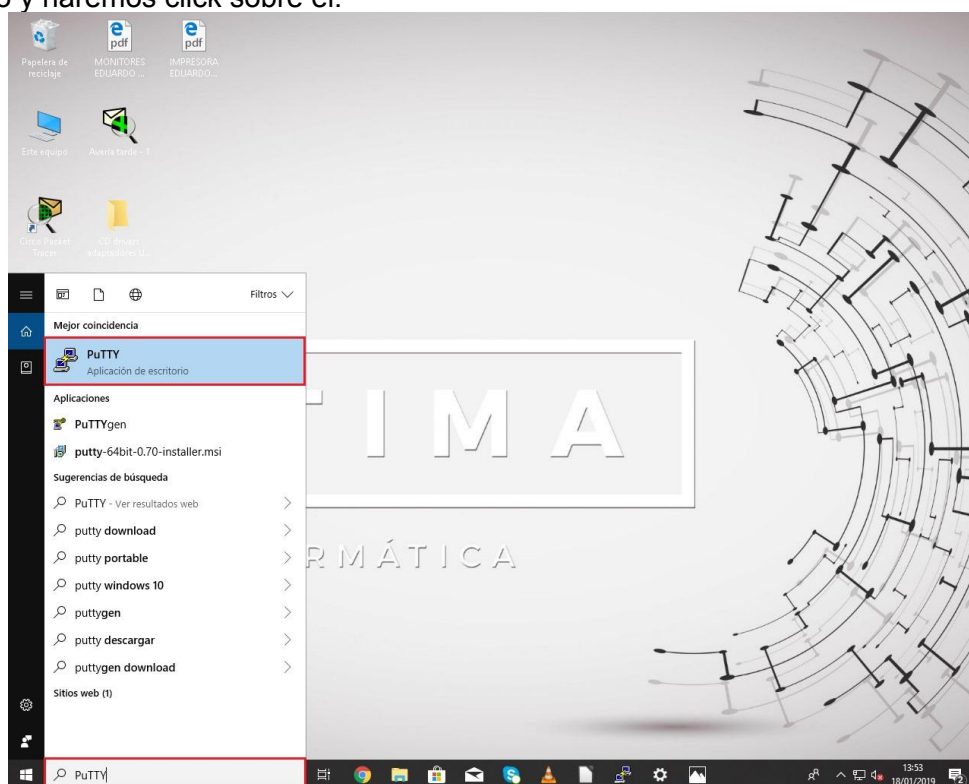
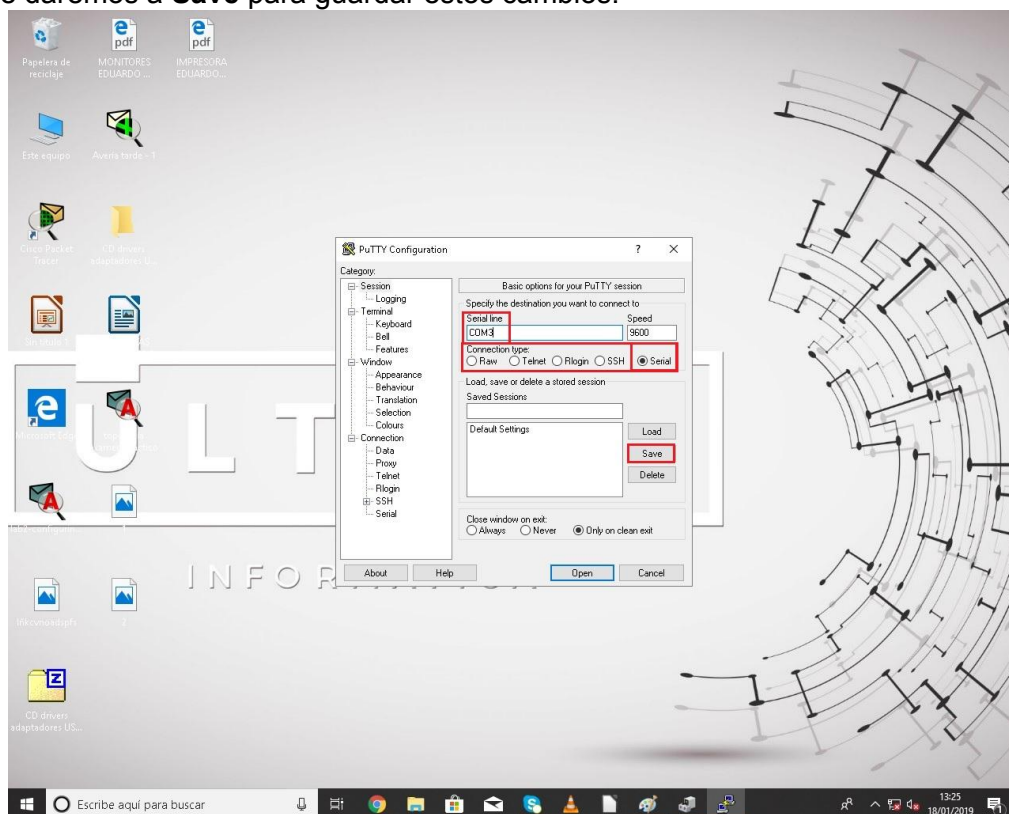


Figura 3.4.4.7. Acceso al programa PuTTY.

<DPLAHER>

Una vez dentro del programa **PuTTY** elegiremos la conexión tipo **Serial** y en el **Serial line** colocaremos **COM3**, el cual es el Puerto COM en que tenemos conectado nuestro Switch Real al PC, y le daremos a **Save** para guardar estos cambios.



3.4.4

Figura 3.4.4.8. Configuración PuTTY 1.

Tras esto, en las pestañas de la izquierda accederemos a la llamada **'Serial'** donde el único parámetro que debemos cambiar es el llamada **'Serial line to connect to'** y ponerlo en ese caso **'COM3'**, de resto **NO** cambiaremos ningún otro parámetro. Por último, haciendo click sobre **'OPEN'** accederemos a la consola del switch real.

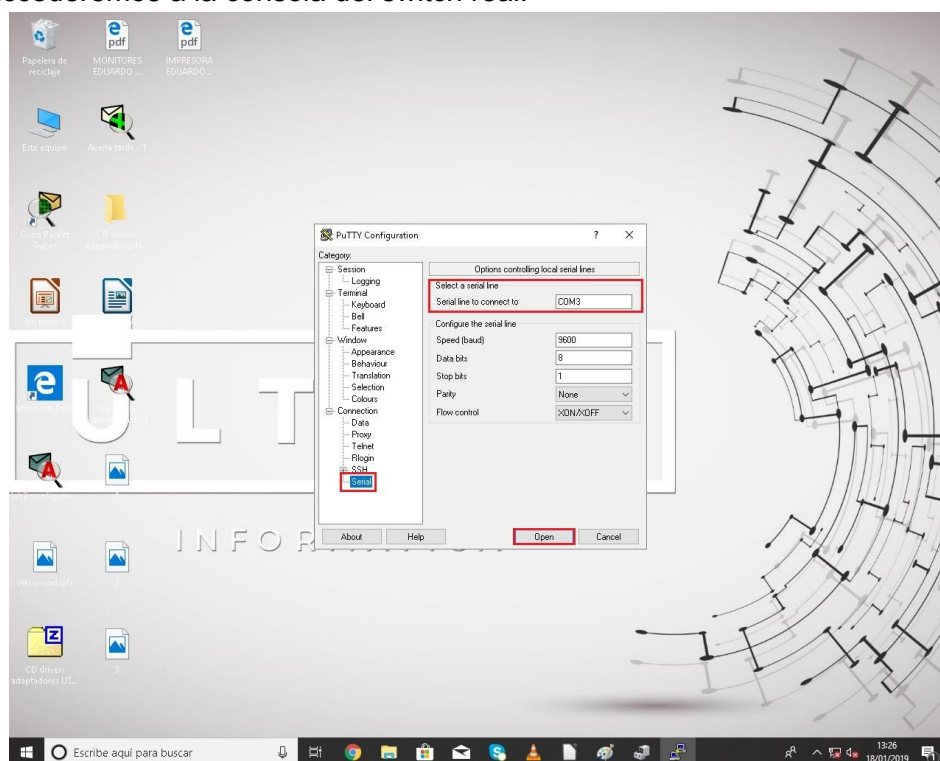


Figura 3.4.4.9. Configuración PuTTY 2.

El quinto paso, una vez ya dentro de la consola del **Switch Real** introduciremos los siguientes comandos para poder hacer la conexión vía telnet desde el PC:

```
enable
configure terminal
line vty 0 15
no login
login local
username dani password dani
username moi privilege 15
exit
```

Establecemos IP para el Switch Real:

```
configure terminal
interface vlan 1
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
exit
```

3.4.4

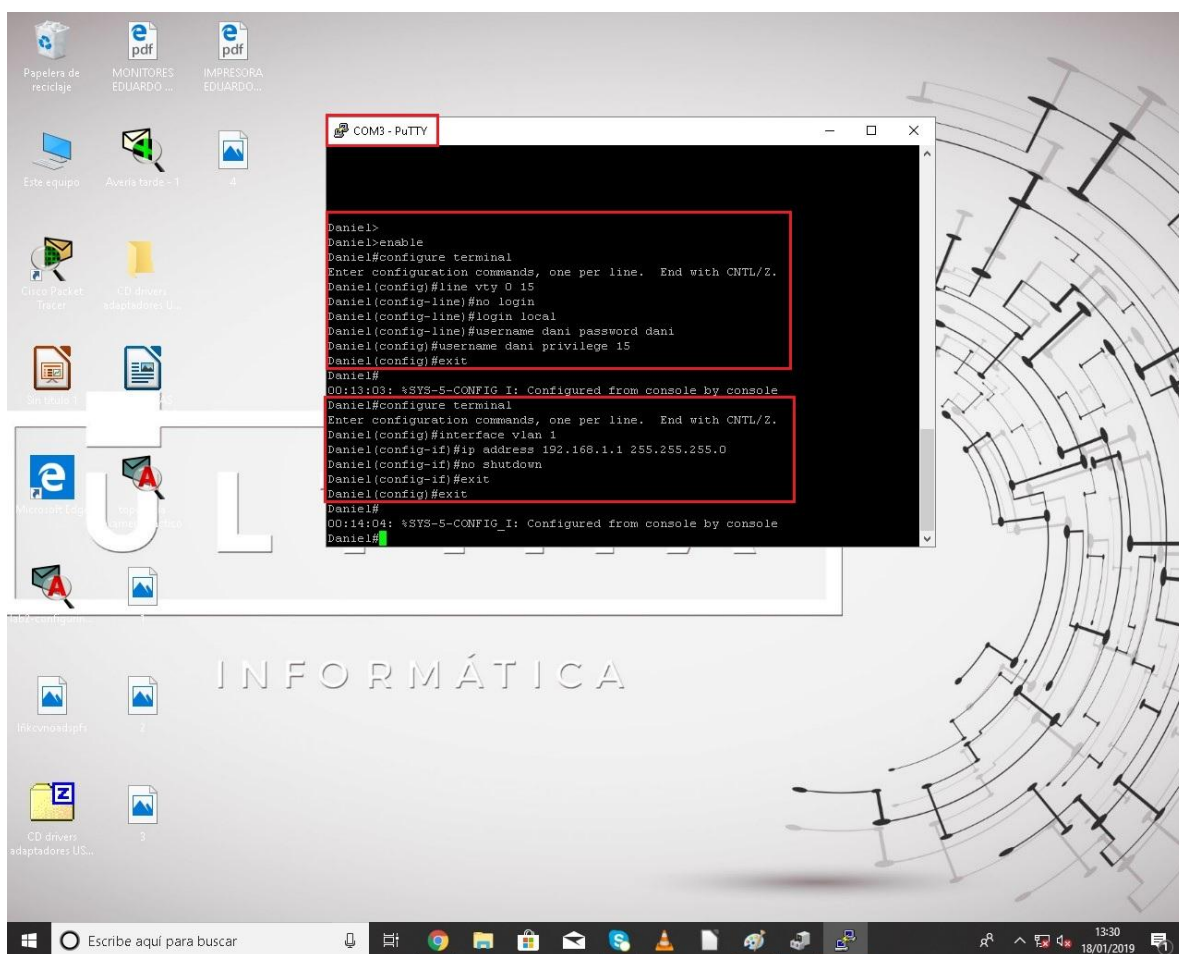


Figura 3.4.4.10. Configuración Switch.

El sexto paso será cambiar la IP de nuestro PC para que se encuentre en el mismo rango que la IP que le hemos puesto a nuestro Switch Real. Para ello escribiremos en nuestra barra de búsqueda de nuestro sistema operativo **'Estado de Red'**, desde la página que se nos abre haremos click en **'Cambiar opciones del adaptador'**, desde la siguiente página que se nos va a abrir haremos click con el botón derecho en el que pone **'Ethernet'** y haremos click sobre la opción llamada **'Propiedades'**. En la siguiente ventana que se nos va a abrir para poder cambiar la IP de nuestro PC haremos doble click sobre la opción llamada **'Protocolo de Internet versión 4 (TCP/IPv4)'**. Por último, en esta última ventana que se nos va a abrir podremos cambiar tanto la IP como la máscara a nuestro PC para que se encuentre en el mismo rango que nuestro **Switch Real**.

3.4.4

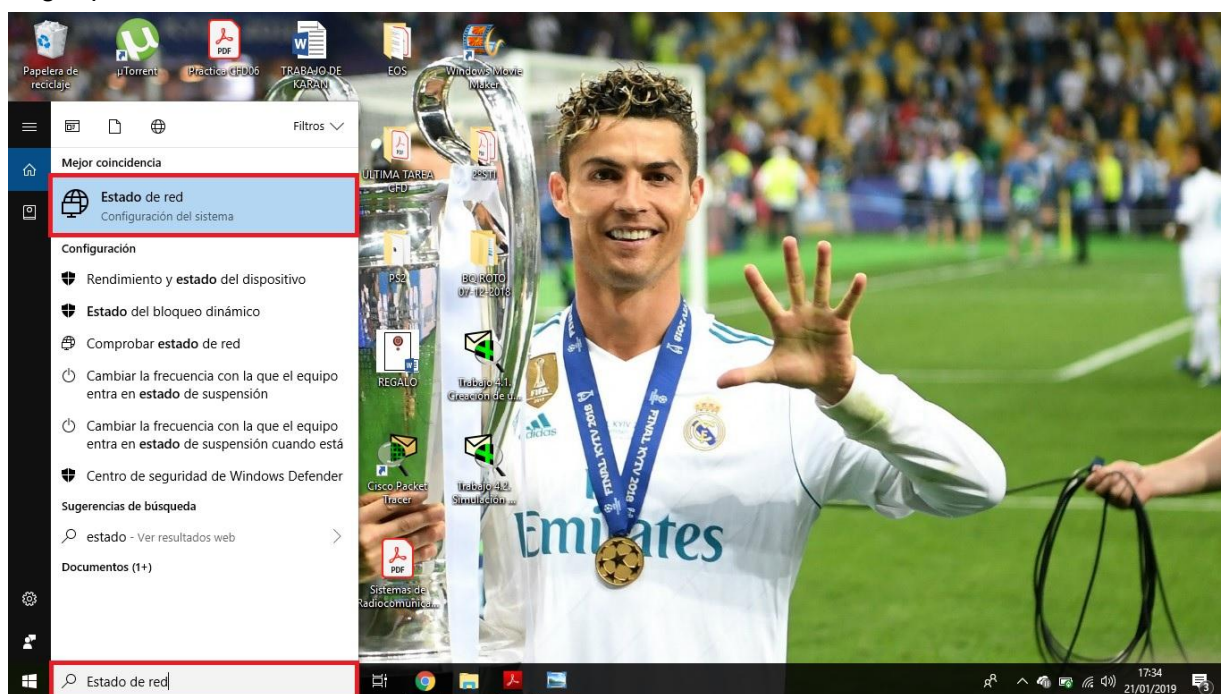


Figura 3.4.4.11. Acceso Estado de Red.

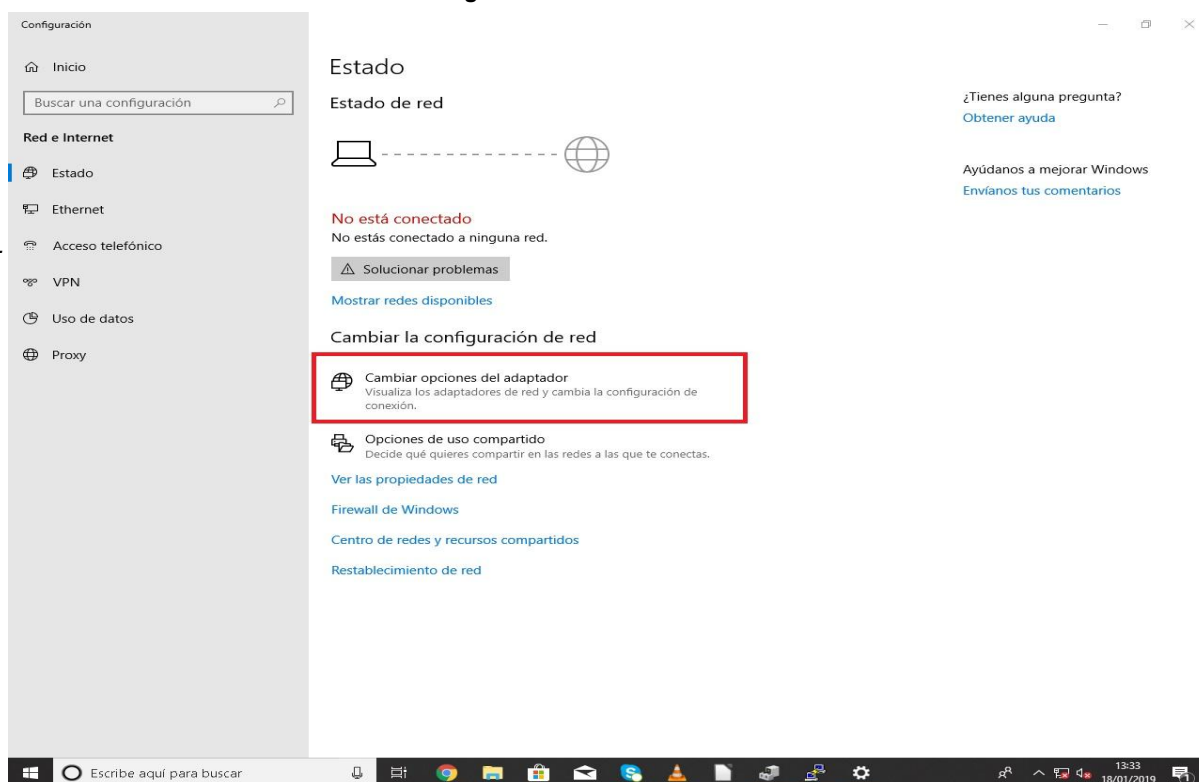
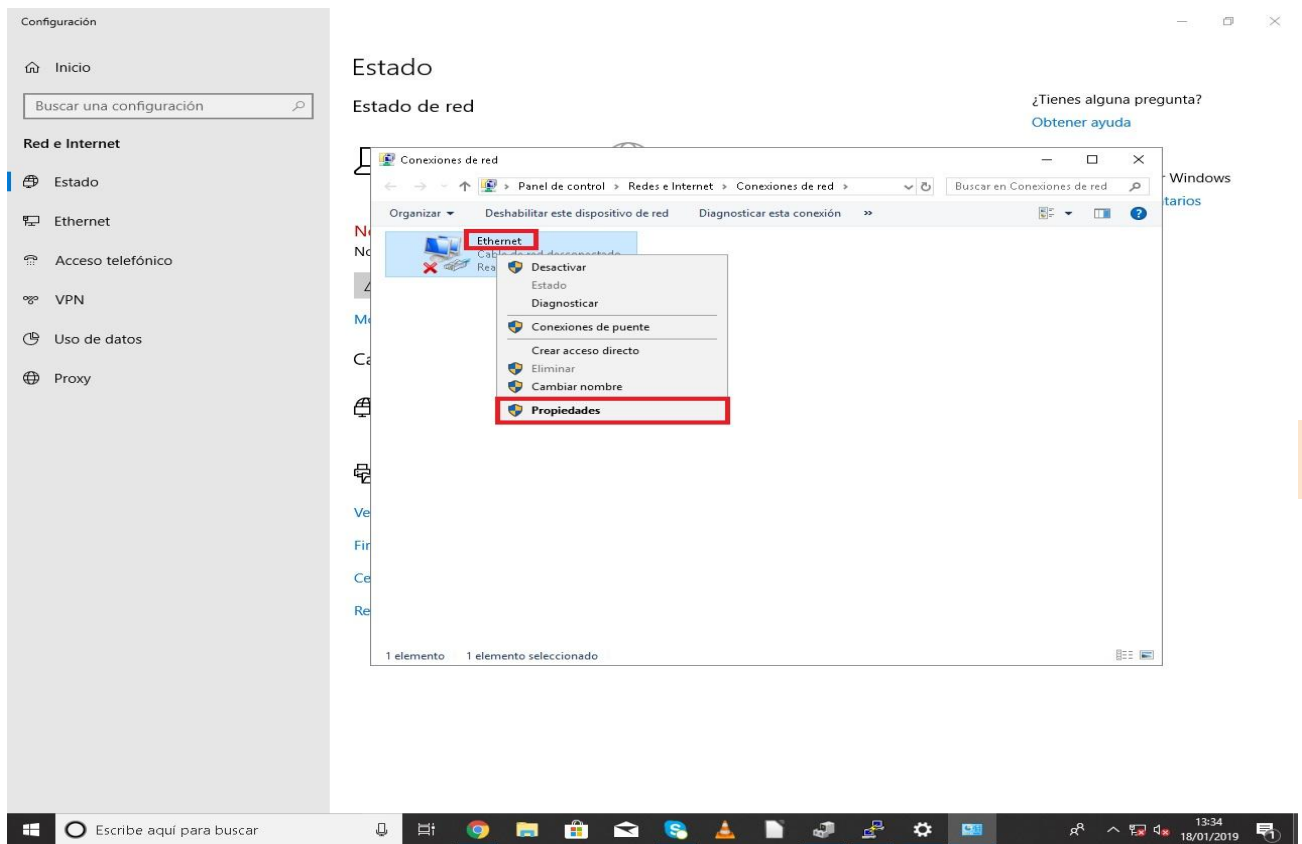


Figura 3.4.4.12. Acceso opciones del adaptador.



3.4.4

Figura 3.4.4.13. Ethernet y Propiedades.

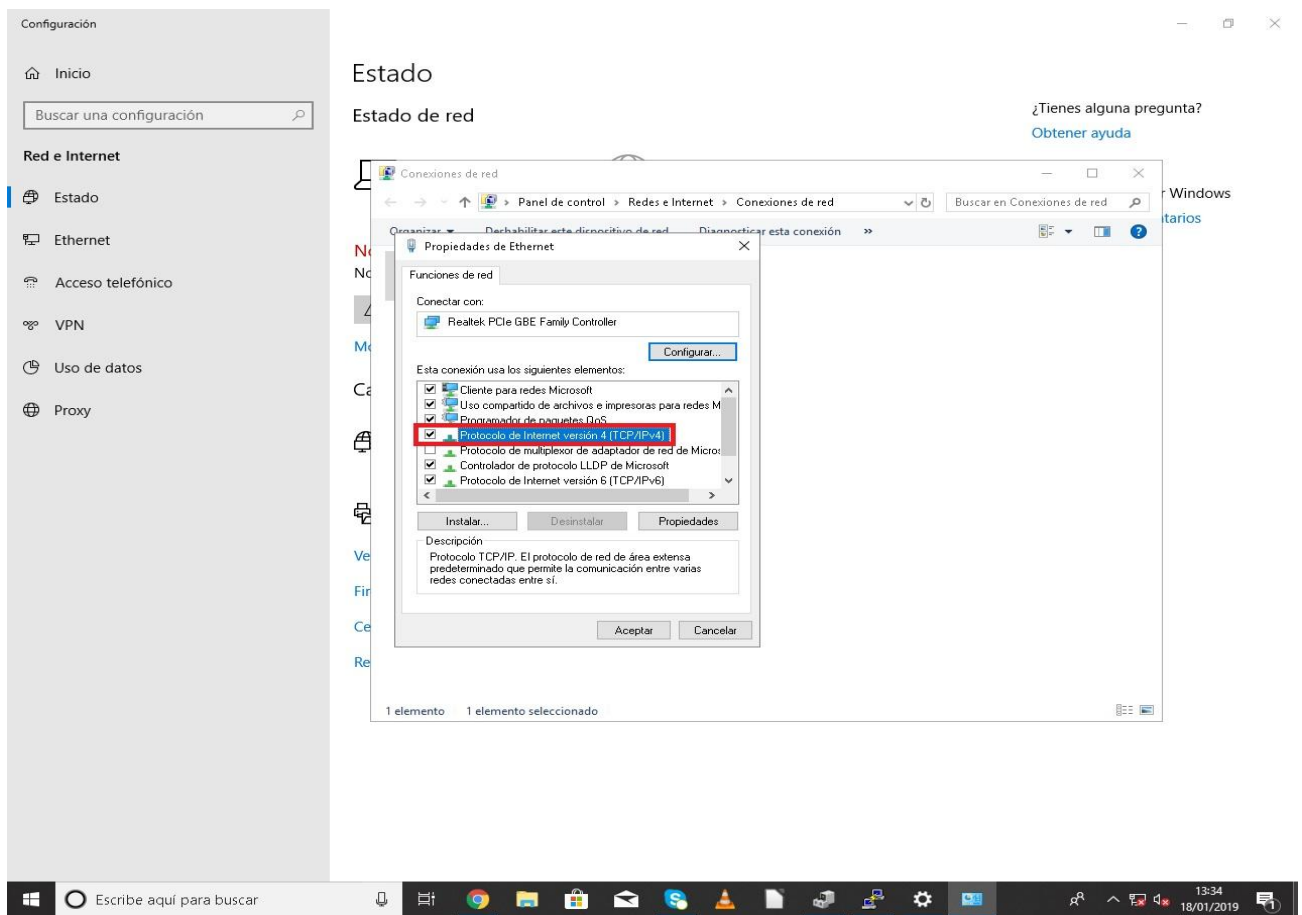


Figura 3.4.4.14. Acceso Protocolo de Internet versión 4 (TCP/IPv4).

<DPLAHER>

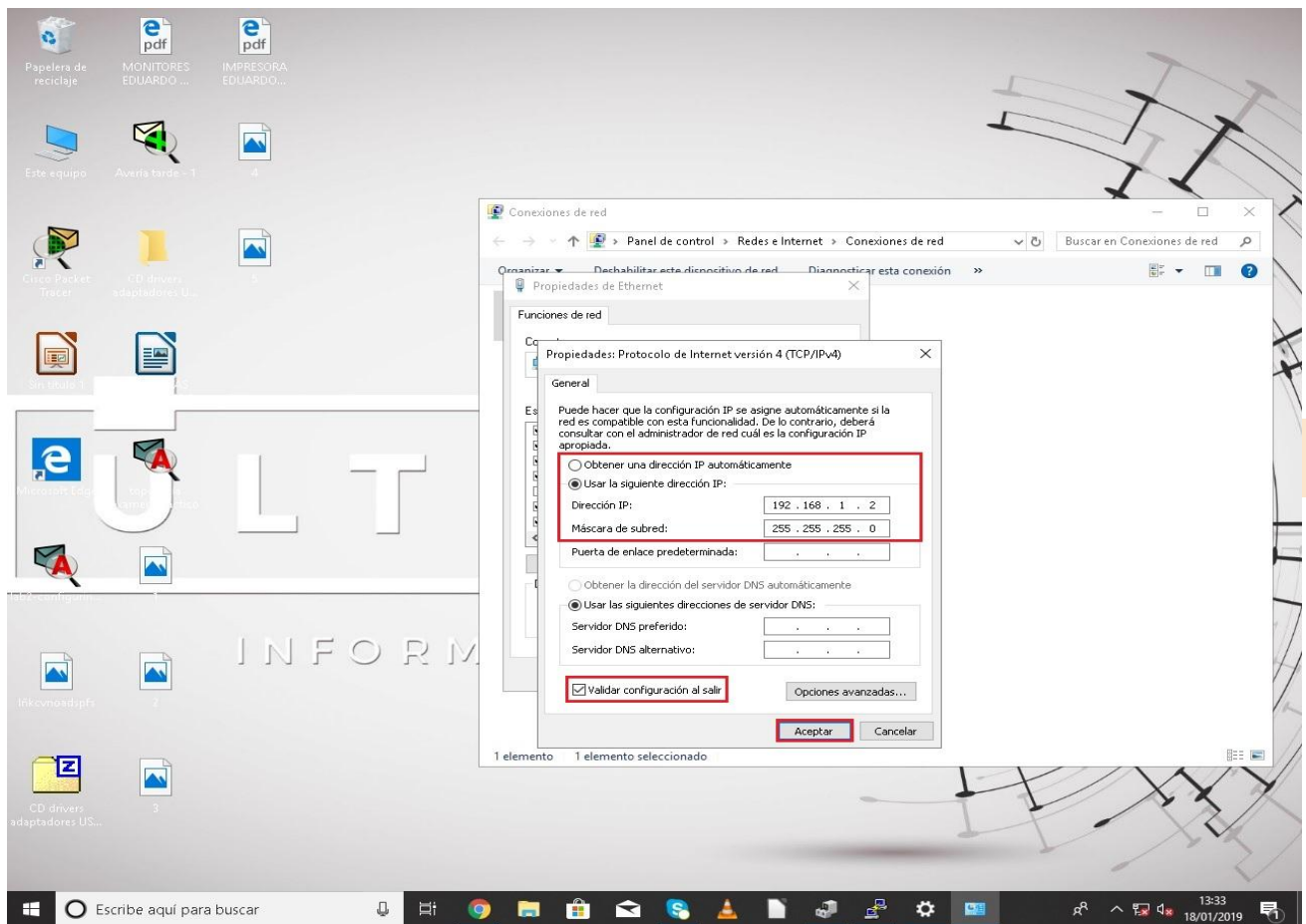


Figura 3.4.4.15. Cambio de IP al PC..

En nuestro caso le hemos puesto al PC la IP 192.168.1.2 - 255.255.255.0 debido a que al Switch Real le hemos puesto la 192.168.1.1 - 255.255.255.0 y deben encontrarse ambas en el mismo rango. Una vez hayamos puesto la IP correctamente haremos click en la opción **'Validar configuración al salir'** y a **'Aceptar'**.

El séptimo paso será activar la característica de Windows de telnet para poder realizar la conexión vía telnet con el Switch Real desde el CMD de Windows, porque esta viene por defecto desactivada en todos los equipos. Para activarla escribiremos en la barra de búsqueda **'Activar o desactivar las características de Windows'**, y tras acceder a ellas activaremos haciendo click en la opción llamada **'Cliente Telnet'**, y le damos a **'Aceptar'**.

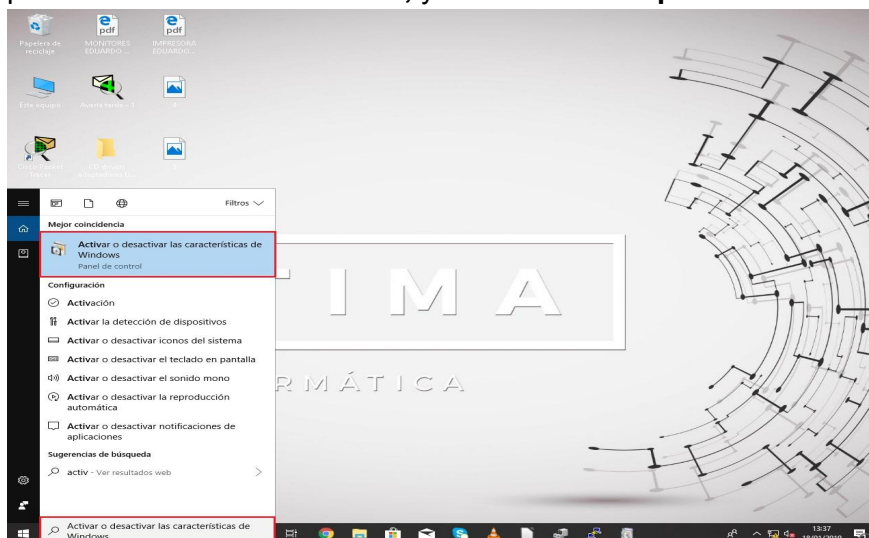
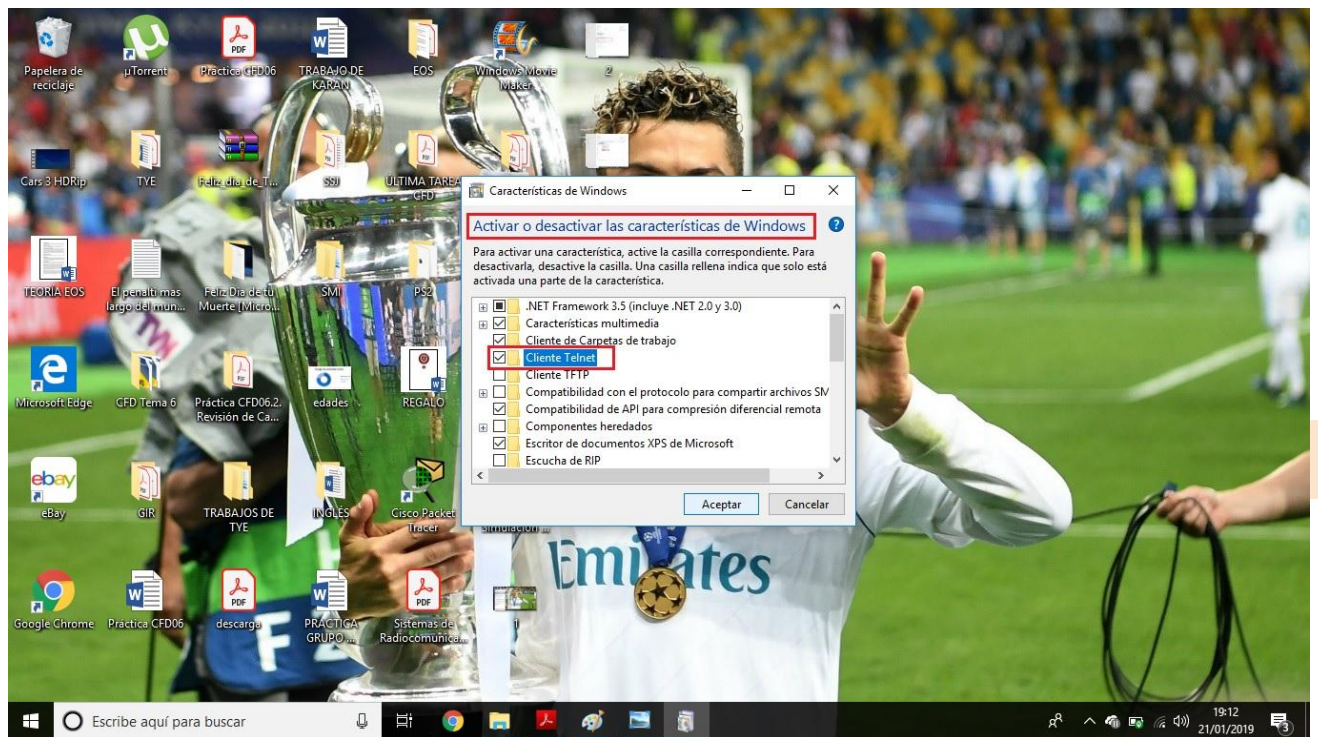


Figura 3.4.4.16. Activar o desactivar las características de Windows en la barra de búsqueda.



3.4.4

Figura 3.4.4.17. Activar Cliente Telnet.

Por último el octavo y último paso será acceder al **CMD** de nuestro PC, el cual lo llama Símbolo del sistema, y escribir en este caso el siguiente comando:

```
telnet 192.168.1.1
```

Una vez dentro nos va a pedir tanto el usuario como la contraseña que le pusimos anteriormente al Switch que en este caso es 'dani'.

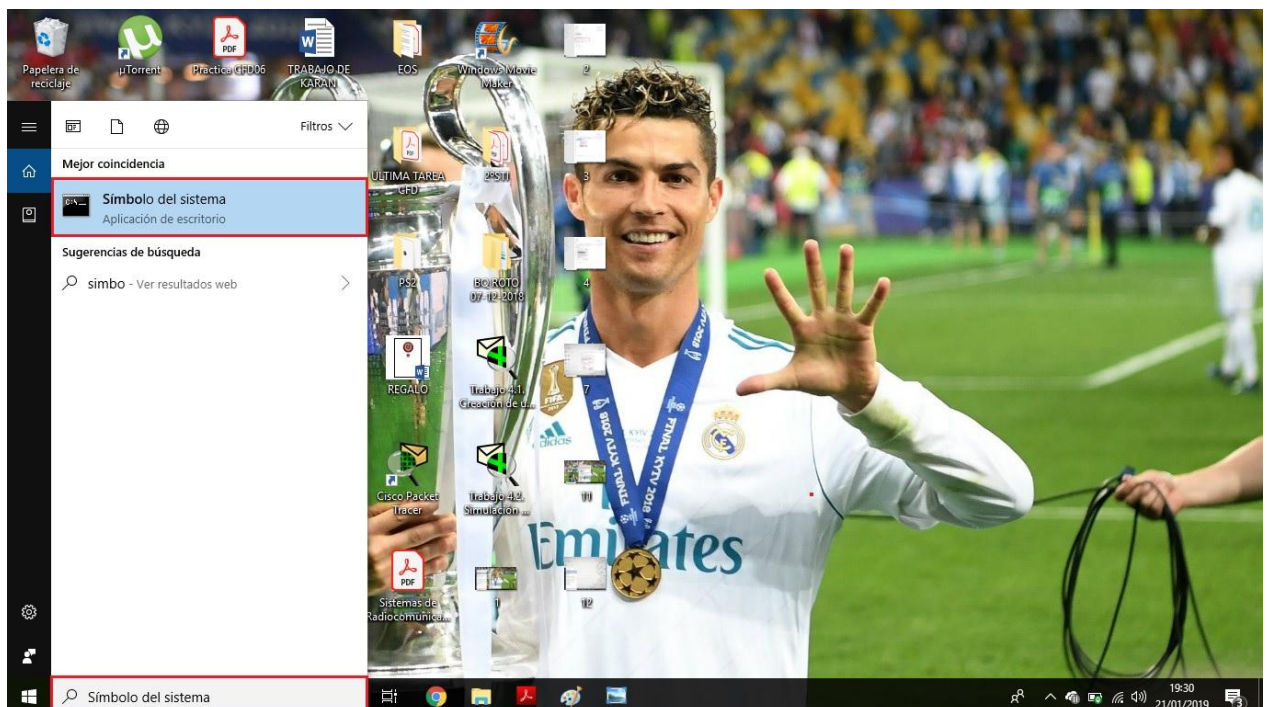


Figura 3.4.4.18. Acceso Símbolo del Sistema.

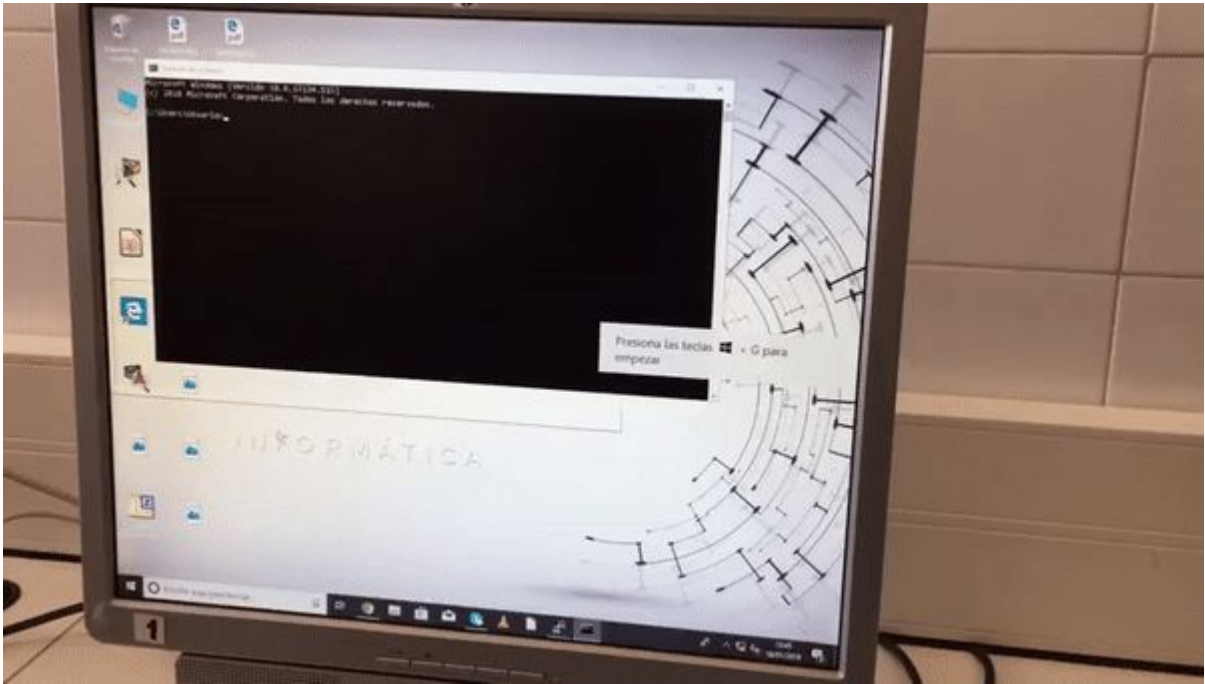


Figura 3.4.4.19. Acceso Switch Real desde el CMD del PC.

En el gif superior se puede observar el final de todo el proceso y como todo funciona incluyendo un **'show running-config'** mostrando toda información sobre el Switch Real.

Apartado 5

5. **Guarda la configuración** que has creado del switch en la memoria no volátil, de modo que cuando arranque NO se pierdan los cambios que has hecho.

En los switch de Cisco, hay dos tipos de archivos de configuración: la configuración en ejecución (funcionamiento actual) y la configuración de inicio. La configuración en ejecución se almacena en la memoria RAM, mientras que la configuración de inicio se almacena en la NVRAM (memoria no volátil).

Para guardar la configuración actual en ejecución en el archivo de configuración de inicio en la NVRAM, deberemos aplicar el comando “copy running-config startup-config” tras haber accedido al modo privilegiado o administrador del switch (#enable).

3.4.5

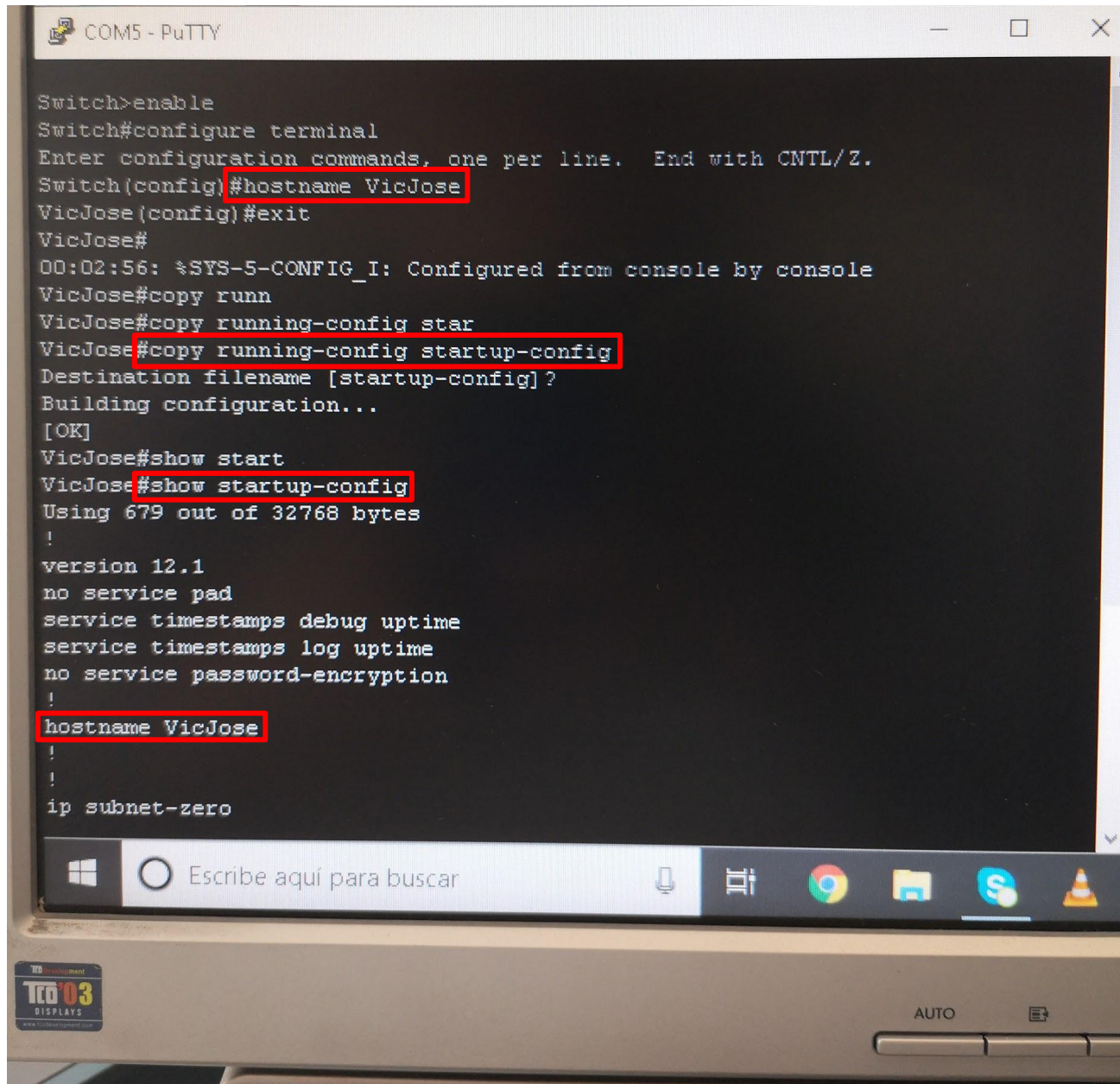


Figura 3.4.5.A. Aplicación del comando “copy running-config startup-config” con switch real.

En la **Figura 3.4.5.A** podemos observar la aplicación de dicho comando para copiar en la memoria no volátil la configuración actual, tras haberle cambiado previamente el nombre al switch.

Apartado 5

Para comprobar que hemos copiado la configuración en ejecución del switch en la memoria NVRAM, deberemos aplicar el comando "show startup-config", como se puede apreciar en la **Figura 3.4.5.B**. En dicha figura, podemos apreciar la aplicación de los comandos comentados anteriormente tras haber procedido al cambio de nombre del switch.



```
COM5 - PuTTY
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname VicJose
VicJose(config)#exit
VicJose#
00:02:56: %SYS-5-CONFIG_I: Configured from console by console
VicJose#copy runn
VicJose#copy running-config star
VicJose#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
VicJose#show start
VicJose#show startup-config
Using 679 out of 32768 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname VicJose
!
!
ip subnet-zero
```

3.4.5

Figura 3.4.5.B. Aplicación del comando "show startup-config" con switch real.

Apartado 6

6. VLAN. Crea una nueva VLAN en el switch. Realiza una conexión física de varios equipos del aula a diferentes bocas del switch que estén en diferentes VLAN y demuestra que hay conectividad entre los equipos de la misma VLAN y que no hay conectividad entre los equipos de diferente VLAN

Entramos en la consola del switch, entramos en la configuración crearemos las VLAN y les asignamos algunos puertos del switch tal como se explicó anteriormente en: [Trabajo 1.6. Seguridad básica. VLAN y trunking](#). Creamos la Vlan 2 con el nombre “vicjose” y le asignamos la boca fastEthernet 0/1 y 0/2. Por otro lado creamos la Vlan 3 con el nombre “jacosergio” y le asignamos la boca fastEthernet 0/11.

```
COM3 - PuTTY
WTP VLAN configuration not allowed when device is in CLIENT mode.
jacosergio(config)#vtp mode server
Setting device to VTP SERVER mode
jacosergio(config)#vlan 2
jacosergio(config-vlan)#name vicjose
jacosergio(config-vlan)#exit
jacosergio(config)#vlan 3
jacosergio(config-vlan)#name jacosergio
jacosergio(config-vlan)#exit
jacosergio(config)#interface fas
jacosergio(config)#interface fastEthernet 0/1
jacosergio(config-if)#switchport access vlan 2
jacosergio(config-if)#exit
jacosergio(config)#in
jacosergio(config)#interface fastEthernet 0/11
jacosergio(config-if)#switchport access vlan 3
jacosergio(config-if)#exit
jacosergio(config)#exit
jacosergio#sho
00:09:18: %SYS-5-CONFIG_I: Configured from console by cons
```

3.4.6

Figura 3.4.6.a: Crear VLAN.

Comprobamos que se ha creado correctamente las Vlan y sus asignaciones con el comando “show vlan brief”

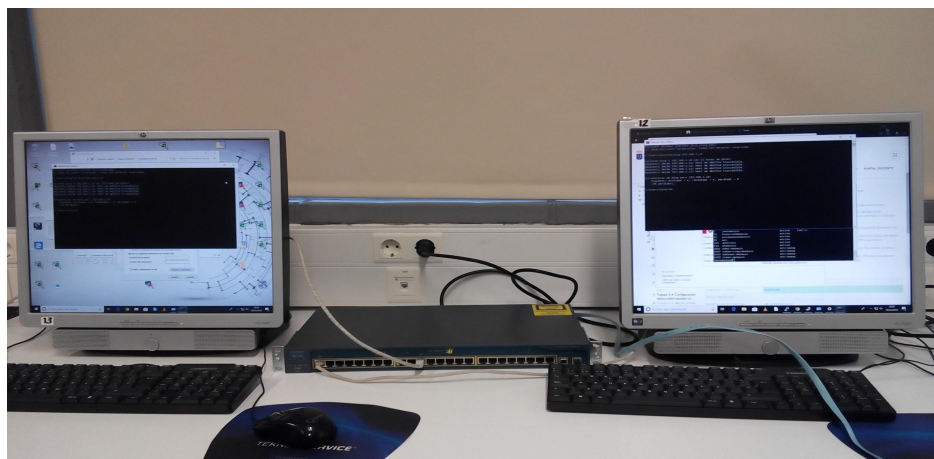
```
COM3 - PuTTY
jacosergio(config)#interface f
jacosergio(config)#interface fastEthernet 0/2
jacosergio(config-if)#switchport access vlan 2
jacosergio(config-if)#exit
jacosergio(config)#show vlan brief
^
% Invalid input detected at '^' marker.
jacosergio(config)#exit
jacosergio#show
00:16:08: %SYS-5-CONFIG_I: Configured from console by consolevlan brief

VLAN Name                Status    Ports
-----
1    default                 active    Fa0/9, Fa0/10, 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, Fa0/25
                                           Fa0/26
2    vicjose                 active    Fa0/1, Fa0/2
3    jacosergio              active    Fa0/11
70   Pountickdehecho         active
90   miraquenoseborra       active
99   moi                     active
```

Figura 3.4.6.b: Comprobando VLAN.

Apartado 6

Conectamos un PC a la boca fastEthernet 0/1 y otro a la boca fastEthernet 0/11 y realizamos un ping para verificar que entre distinta VLAN no hay visibilidad. EL PC de la VLAN 2 tendra la IP 192.168.1.10 y el de la VLAN 3 192.168.1.12. Fig 3.4.6.c, 3.4.6.d y 3.4.6.e



3.4.6

Figura 3.4.6.c: Distintas VLAN.

```
Microsoft Windows [Versión 10.0.17134.523]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ping 192.168.1.12

Haciendo ping a 192.168.1.12 con 32 bytes de datos:
Respuesta desde 192.168.1.10: Host de destino inaccesible.
Respuesta desde 192.168.1.10: Host de destino inaccesible.
Respuesta desde 192.168.1.10: Host de destino inaccesible.
Respuesta desde 192.168.1.10: Host de destino inaccesible.

Estadísticas de ping para 192.168.1.12:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),

C:\Users\Usuario>
```

Figura 3.4.6.d: PC VLAN 2.

```
Microsoft Windows [Versión 10.0.17134.523]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ping 192.168.1.10

Haciendo ping a 192.168.1.10 con 32 bytes de datos:
Respuesta desde 192.168.1.12: Host de destino inaccesible.
Respuesta desde 192.168.1.12: Host de destino inaccesible.
Respuesta desde 192.168.1.12: Host de destino inaccesible.
Respuesta desde 192.168.1.12: Host de destino inaccesible.

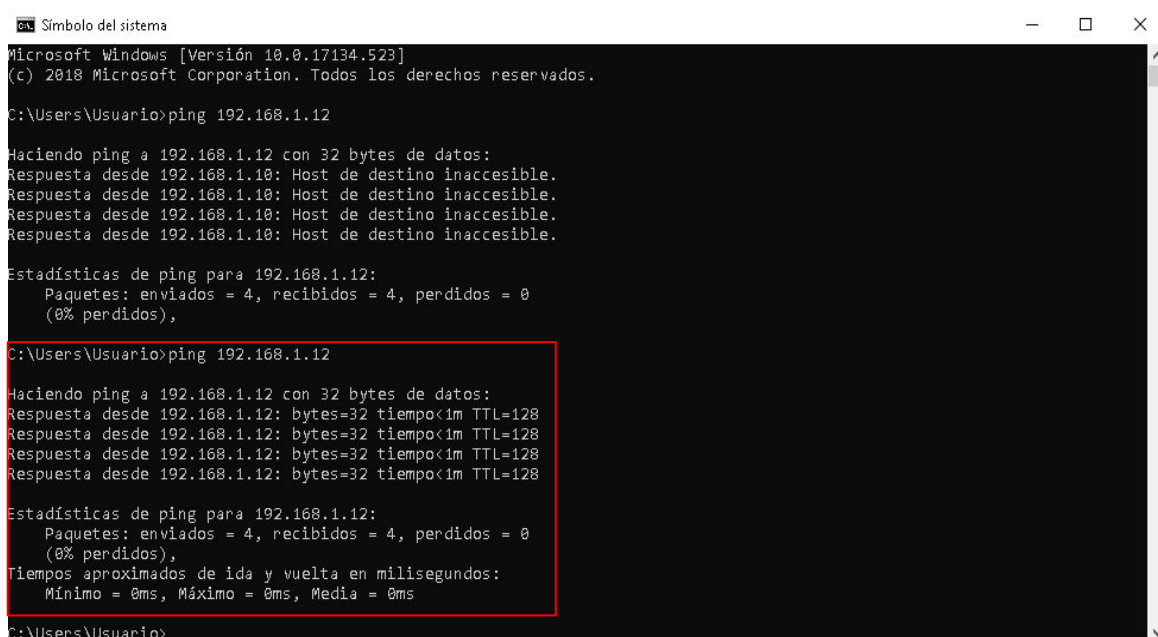
Estadísticas de ping para 192.168.1.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),

C:\Users\Usuario>
```

Figura 3.4.6.e: PC VLAN 3.

Apartado 6

Ahora Conectamos un PC a la boca fastEthernet 0/1 y otro a la boca fastEthernet 0/2 y realizamos un ping para verificar que en la misma VLAN si existe visibilidad. Utilizamos las mismas IP que en el paso anterior. **Fig 3.4.6.f y 3.4.6.g**



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.17134.523]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ping 192.168.1.12

Haciendo ping a 192.168.1.12 con 32 bytes de datos:
Respuesta desde 192.168.1.10: Host de destino inaccesible.
Respuesta desde 192.168.1.10: Host de destino inaccesible.
Respuesta desde 192.168.1.10: Host de destino inaccesible.
Respuesta desde 192.168.1.10: Host de destino inaccesible.

Estadísticas de ping para 192.168.1.12:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),

C:\Users\Usuario>ping 192.168.1.12

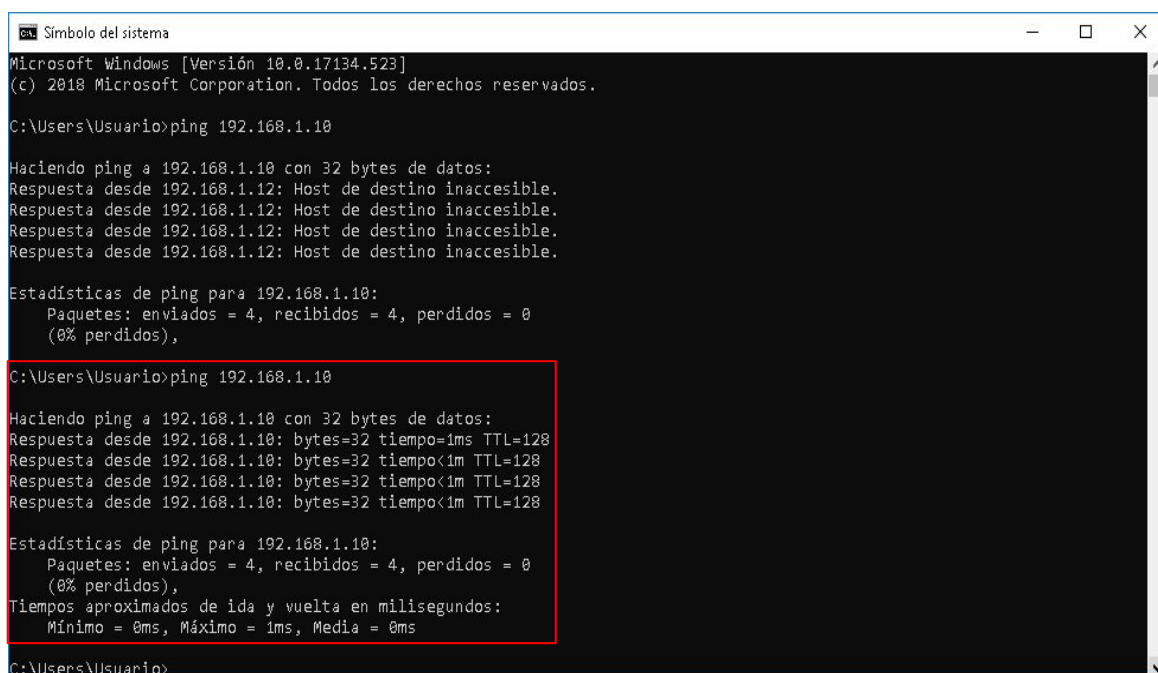
Haciendo ping a 192.168.1.12 con 32 bytes de datos:
Respuesta desde 192.168.1.12: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.12: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.12: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.12: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.12:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Usuario>
```

3.4.6

Figura 3.4.6.f: PC VLAN 2.



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.17134.523]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ping 192.168.1.10

Haciendo ping a 192.168.1.10 con 32 bytes de datos:
Respuesta desde 192.168.1.12: Host de destino inaccesible.
Respuesta desde 192.168.1.12: Host de destino inaccesible.
Respuesta desde 192.168.1.12: Host de destino inaccesible.
Respuesta desde 192.168.1.12: Host de destino inaccesible.

Estadísticas de ping para 192.168.1.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),

C:\Users\Usuario>ping 192.168.1.10

Haciendo ping a 192.168.1.10 con 32 bytes de datos:
Respuesta desde 192.168.1.10: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Usuario>
```

Figura 3.4.6.g: PC VLAN 3.

Apartado 7

7. Activar SSH en PUTTY, en Windows 10 y comprobar su correcto funcionamiento

Para configurar SSH en nuestro switch debemos entrar en su configuración a través de telnet o por cable serial.

1. Entrar en la configuración.
2. Nombramos al dominio.
3. Establecemos el número de bits que queremos utilizar para el cifrado de la key.
4. Seleccionamos el tiempo que tenemos para loguearnos antes de que se cierre la pestaña de SSH.
5. ehe
6. Configuramos el SSH con la version 2
7. Elegimos un nombre para el usuario.

```
#enable
#configure terminal
#ip domain-name jacoysergio
#crypto key generate rsa
How many bits in the modulus [512]: 1024

#ip ssh time-out 30 (tiempo de espera para logearse)
#ip ssh authentication-retries 3
#ip ssh version 2
#username jacosergio privilege 15
#line vty 0 4
#transport input ssh
#login local
```

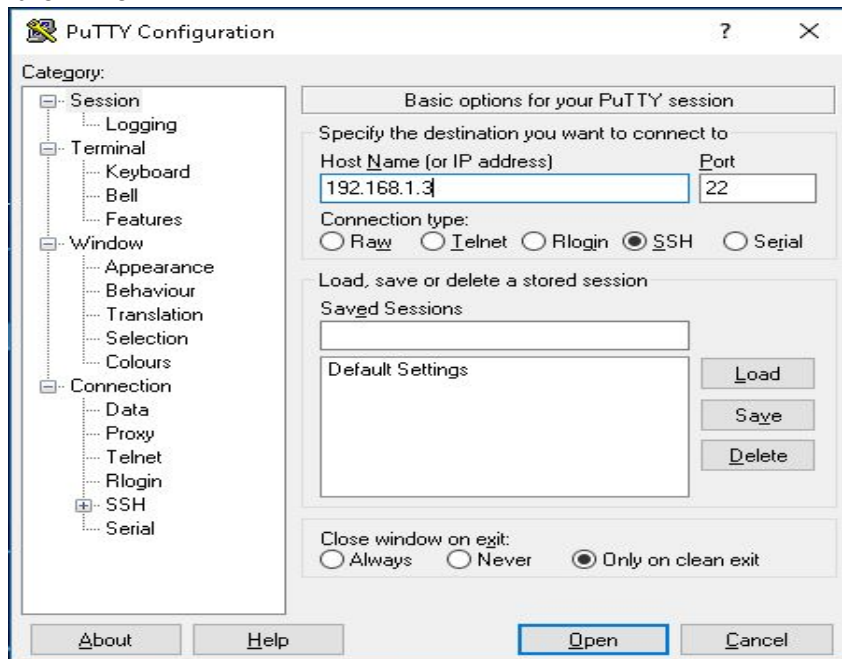
3.4.7

```
192.168.1.3 - PuTTY
Fa0/16, Fa0/17, Fa0/18, Fa0/19
Fa0/20, Fa0/21, Fa0/22, Fa0/23
Fa0/24
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
JACOSERGIO#configur
JACOSERGIO#configure term
JACOSERGIO#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
JACOSERGIO(config)#ip doma
JACOSERGIO(config)#ip domain-nam
JACOSERGIO(config)#ip domain-name jacoysergio
JACOSERGIO(config)#crypt
JACOSERGIO(config)#crypto key gen
JACOSERGIO(config)#crypto key generate rsa 1024
JACOSERGIO(config)#crypto key generate rsa
^
% Invalid input detected at '^' marker.
JACOSERGIO(config)#crypto key generate rsa ?
modulus Provide number of modulus bits on the command line
usage-keys Generate separate RSA keys for signing and encryption
<cr>
JACOSERGIO(config)#crypto key generate rsa 1024
^
% Invalid input detected at '^' marker.
JACOSERGIO(config)#crypto key generate rsa
The name for the keys will be: JACOSERGIO.jacoysergio
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
Generating RSA Keys ...
[OK]
JACOSERGIO(config)#ip ss
JACOSERGIO(config)#ip ssh ti
JACOSERGIO(config)#ip ssh time-out 30
JACOSERGIO(config)#ip ss
JACOSERGIO(config)#ip ssh au
JACOSERGIO(config)#ip ssh authentication-retries 3
JACOSERGIO(config)#ip ss
JACOSERGIO(config)#ip ssh ver
JACOSERGIO(config)#ip ssh version 2
JACOSERGIO(config)#usern
JACOSERGIO(config)#username jacosergio pri
JACOSERGIO(config)#username jacosergio privilege 15 pas
JACOSERGIO(config)#username jacosergio privilege 15 password cisco
JACOSERGIO(config)#line vty 0 4
JACOSERGIO(config-line)#trna
JACOSERGIO(config-line)#tr
JACOSERGIO(config-line)#transport i
JACOSERGIO(config-line)#transport input ss
JACOSERGIO(config-line)#transport input ssh
JACOSERGIO(config-line)#login local
JACOSERGIO(config-line)#
```

Figura 3.4.7.a. Configuración SSH en PUTTY

Apartado 7

A continuación utilizaremos el programa PUTTY para entrar a la configuración del switch y con esto comprobamos que el SSH está bien configurado. Para ello ponemos la IP del switch y no cambiaremos ninguna otra pestaña, con las predeterminadas ya podríamos entrar. **Figura 3.4.7.b y Figura 3.4.7.c**



3.4.7

Figura 3.4.7.b Conexión SSH via PUTTY



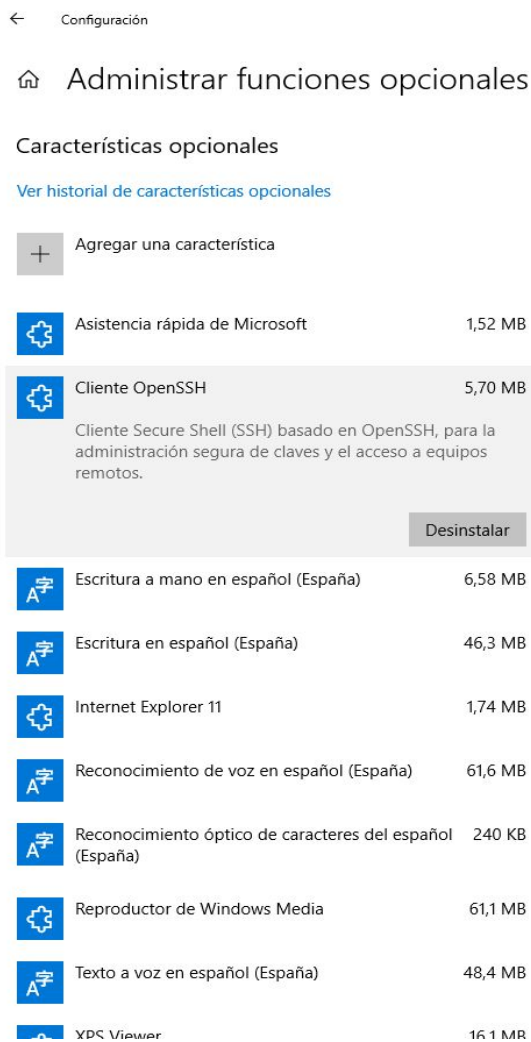
Figura 3.4.7.c Conexión SSH via PUTTY

Apartado 7

Para realizar la conexión a SSH en Windows 10, primero necesitamos activar el SSH ya que Windows trae desactivada esta opción.

Para ello buscaremos “**Administrar funciones opcionales**” en Windows.

Seleccionamos Cliente OpenSSH y deberemos instalarlo, en caso de no estar, buscaremos en “**Agregar una característica**”. **Figura 3.4.9.d**



3.4.7

Figura 3.4.7.d Activando SSH en Windows 10

Apartado 7

Luego entramos en la consola del PC y deberemos escribir los comandos mostrados en la Fig.3.4.7.e

```
OpenSSH SSH client
C:\Users\Usuario>ssh -help
unknown option --h
usage: ssh [-46AaCfGgKkMnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
          [-D [bind_address:]port] [-E log_file] [-e escape_char]
          [-F configfile] [-I pkcs11] [-i identity_file]
          [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]
          [-O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]
          [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
          destination [command]

C:\Users\Usuario>ssh -J jacosergio@192.168.1.3
usage: ssh [-46AaCfGgKkMnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
          [-D [bind_address:]port] [-E log_file] [-e escape_char]
          [-F configfile] [-I pkcs11] [-i identity_file]
          [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]
          [-O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]
          [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
          destination [command]

C:\Users\Usuario>ssh jacosergio@192.168.1.3
Unable to negotiate with 192.168.1.3 port 22: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1

C:\Users\Usuario>ssh -oKexAlgorithms+=diffie-hellman-group1-sha1 jacosergio@192.168.1.3
Unable to negotiate with 192.168.1.3 port 22: no matching cipher found. Their offer: 3des-cbc

C:\Users\Usuario>ssh -oKexAlgorithms+=diffie-hellman-group1-sha1 jacosergio@192.168.1.3
Unable to negotiate with 192.168.1.3 port 22: no matching cipher found. Their offer: 3des-cbc

C:\Users\Usuario>ssh -c 3des.cbc -oKexAlgorithms+=diffie-hellman-group1-sha1 jacosergio@192.168.1.3
Unknown cipher type '3des.cbc'

C:\Users\Usuario>ssh -c -oKexAlgorithms+=diffie-hellman-group1-sha1 jacosergio@192.168.1.3
Unknown cipher type '-oKexAlgorithms+=diffie-hellman-group1-sha1'

C:\Users\Usuario>ssh -c -oKexAlgorithms+=diffie-hellman-group1-sha1 jacosergio@192.168.1.3
Unknown cipher type '-oKexAlgorithms+=diffie-hellman-group1-sha1'

C:\Users\Usuario>ssh -c 3des-cbc jacosergio@192.168.1.3
Unable to negotiate with 192.168.1.3 port 22: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1

C:\Users\Usuario>ssh -c 3des-cbc -oKexAlgorithms+=diffie-hellman-group1-sha1 jacosergio@192.168.1.3
The authenticity of host '192.168.1.3 (192.168.1.3)' can't be established.
RSA key fingerprint is SHA256:78Hoed1Yb2kXvk2j2ds9Ph0CpvlNxxw3cp6y6/6ycuUk.
Are you sure you want to continue connecting (yes/no)?
Host key verification failed.

C:\Users\Usuario>ssh -c 3des-cbc -oKexAlgorithms+=diffie-hellman-group1-sha1 jacosergio@192.168.1.3
The authenticity of host '192.168.1.3 (192.168.1.3)' can't be established.
RSA key fingerprint is SHA256:78Hoed1Yb2kXvk2j2ds9Ph0CpvlNxxw3cp6y6/6ycuUk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.3' (RSA) to the list of known hosts.
jacosergio@192.168.1.3's password:
Permission denied, please try again.
jacosergio@192.168.1.3's password:

JACOSERGIO#
```

3.4.7

Figura 3.4.7.e Activando SSH en Windows 10

Apartado 8

8. VTP. Utilizando dos switches, monta una red VTP con un servidor y un cliente. Demuestra que la red VTP está funcionando sencillamente comprobando que las VLAN del cliente están sincronizadas con las VLAN del servidor.

Bueno en este apartado vamos a realizar una práctica en la cual con dos Switches reales vamos a realizar una conexión VTP entre ambos configurando uno como servidor y el otro como cliente. Para ello vamos a dividir el apartado en tres: primero la conexión entre ambos Switches Reales, segundo la configuración del Switch Real el cual va a ejecutar de **Server**, y por último la configuración del Switch Real el cual va a ejecutar de **Client**.

CONEXIÓN ENTRE AMBOS SWITCHES REALES:

Para realizar la conexión entre ambos Switches Reales debemos conectar un cable Ethernet '**CRUZADO**' a cualquiera de las bocas de cada uno de los Switches, aunque lo normal es conectarlos en la boca 1 de cada Switch. Es muy **IMPORTANTE** que el cable que conecte ambos Switches sea **CRUZADO** porque sino la práctica no va salir.

3.4.8

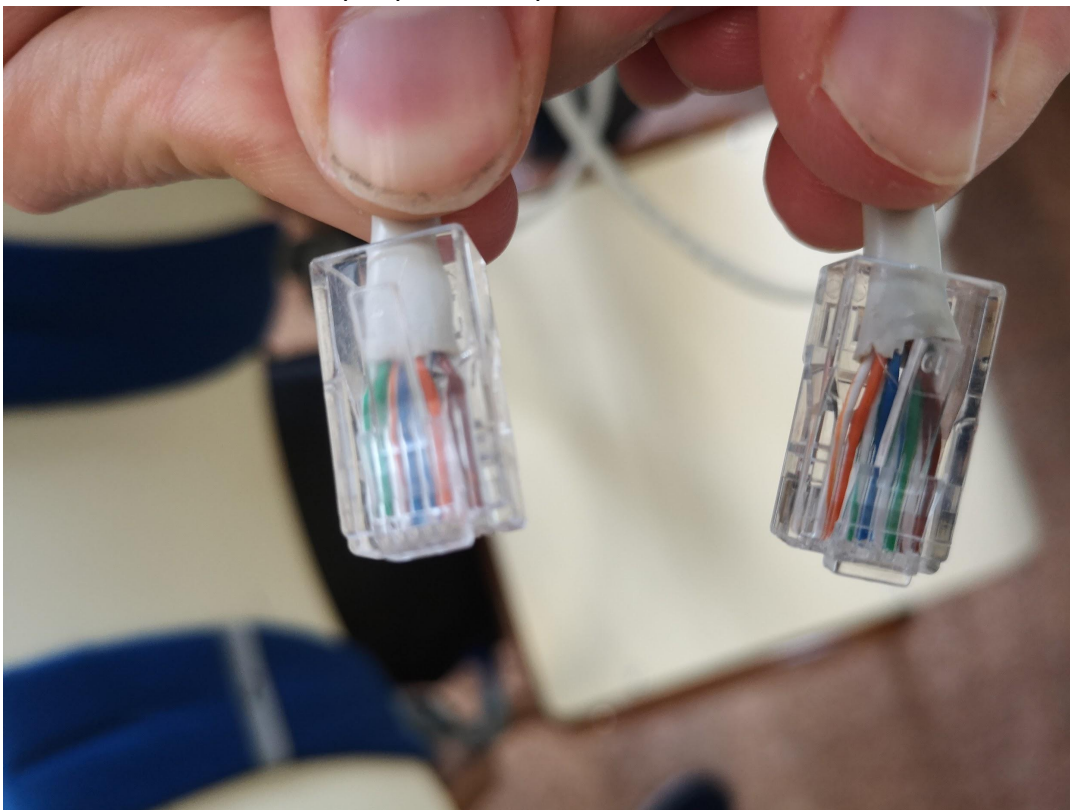


Figura 3.4.8.1. Cable Cruzado.



3.4.8

Figura 3.4.8.2. Comprobación Cable Cruzado.



Figura 3.4.8.3. Switch Server y Switch Client conectados mediante cable cruzado.

En la Figura 3.8.3 no sale Switch Server en la imagen por dificultad de longitud del cable de corriente.

CONFIGURACIÓN SWITCH SERVER

En el Switch server debemos configurar la boca la cual tengamos conectado nuestro cable Ethernet **CRUZADO**, en nuestro caso la FastEthernet0/1, cómo **'trunk'** para que se puedan pasar las VLAN al Switch Client. Esto se hace con los siguientes comandos:

```
enable
configure terminal
interface fastEthernet 0/1
switchport mode trunk
exit
```

El siguiente paso es configurar el switch en modo **server** y introducir un **'domain'** el cual en este caso será **'MANRIQUEDOMAIN'** y una **'password'** que en este caso será **'cisco'**, pero podeis poner la que quieran. Para ello utilizaremos los siguientes comandos:

3.4.8

```
enable
configure terminal
vtp mode server
vtp domain MANRIQUEDOMAIN
vtp password cisco
```

Tras la realización de estos comandos crearemos dos VLANs en este Switch para ver después en el Switch Client como se ven reflejadas. Para la creación de las VLANs utilizaremos los siguientes comandos:

```
enable
configure terminal
vlan 2
name VICJOSEDANI
exit
vlan 3
name CESAR
exit
```

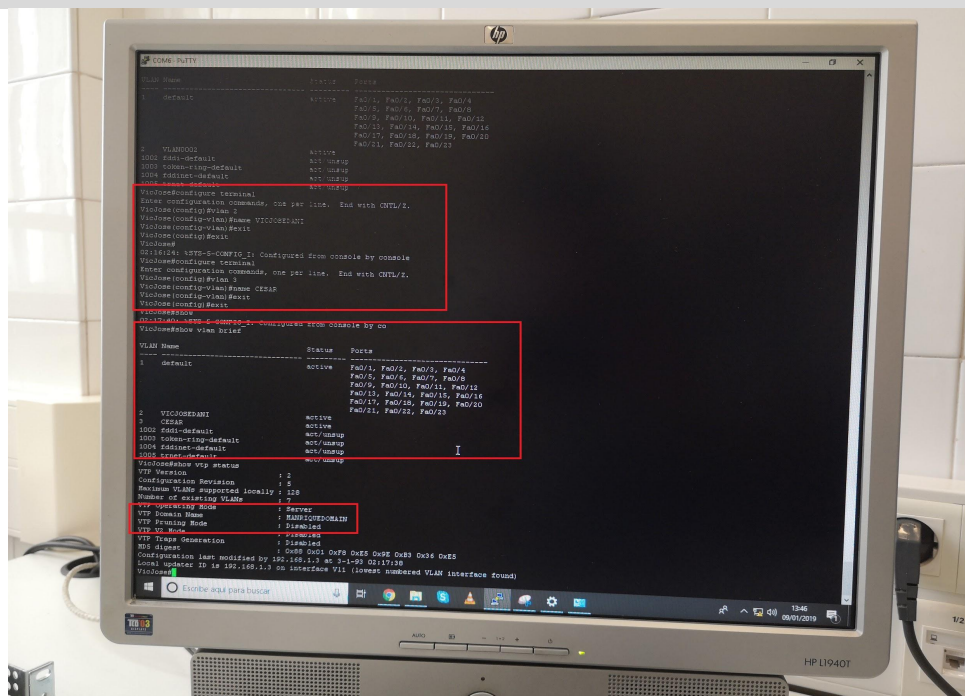


Figura 3.4.8.4. Estado Switch Server.

CONFIGURACIÓN SWITCH CLIENT

En el Switch cliente debemos configurar la boca la cual tengamos conectado nuestro cable Ethernet **CRUZADO**, en nuestro caso la FastEthernet0/1, cómo **'trunk'** para que nos puedan llegar las VLAN al Switch Client. Esto se hace con los siguientes comandos:

```
enable
configure terminal
interface fastEthernet 0/1
switchport mode trunk
exit
```

El siguiente paso es configurar el switch en modo **client** y introducir el **'domain'** el cual se puso en el switch server, que era **'MANRIQUEDOMAIN'** y la **'password'** la cual fue puesta en el Switch server, que era **'cisco'**. Para ello utilizaremos los siguientes comandos:

3.4.8

```
enable
configure terminal
vtp mode client
vtp domain MANRIQUEDOMAIN
vtp password cisco
```

Tras la realización de estos comandos podemos realizar un **'show vlan brief'** en el Switch Client para comprobar que realmente las dos VLANs creadas en el Switch Server aparecen por arte de magia en nuestro Switch.

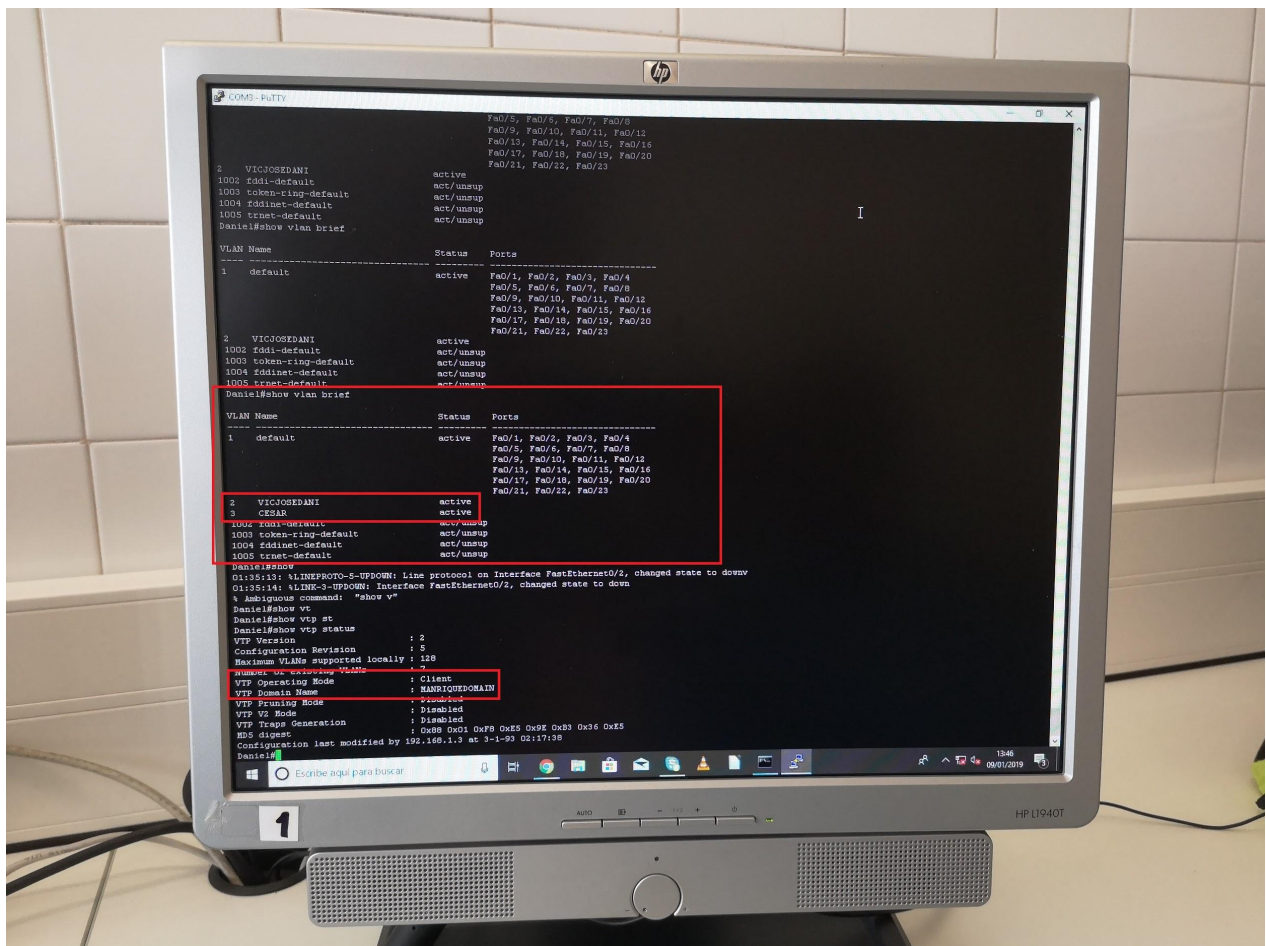


Figura 3.4.8.5. Estado Switch Client.

Preguntas de repaso (I)

3.4.1: (JACOGON)

- ¿Por qué razón hemos usado adaptadores TS-901?
- ¿Cómo se consulta el puerto COM en el que está conectado? (Mostrar empíricamente)
- ¿Cuántos pines tiene el puerto serial?
- ¿Cuál es el símbolo normalizado del puerto serial?

3.4.2: Instalación de Putty (IMARMEN)

- Comprueba que está conectado el PC al Switch desde el Administrador de dispositivos.
- Cuando realizamos una conexión desde Putty al puerto de consola de un router o switch corporativo debemos configurar algunos parámetros como el puerto COM o los bits paridad de la comunicación. Hay otros 5 parámetros que deben configurarse. Indica uno más.
- Además de comunicaciones serie (puerto serie COM), ¿qué otros 3 tipos de conexiones/comunicaciones soporta?

3.4.3: Cambiar nombre del switch (APLAFLE)

- ¿Qué comando debemos usar para poder cambiarle el nombre al Switch?
- ¿Debemos estar en el modo de configuración del switch para aplicar el comando para cambiar el nombre al switch?
- ¿Con qué comando del switch corporativo 2960 se puede consultar el nombre que tiene asignado?

3.4.3: (DPLAHER)

- ¿Cuál es el comando para poder cambiar el nombre a un switch?

3.4.4: Telnet (JDOMDAR)

- ¿Qué se necesita para conectar un switch al PC para configurarlo mediante PuTTY?
- Comando esencial de inicio para configurar Telnet.
- ¿Cómo se activa Telnet en Windows?

3.4.5: (APLAFLE)

- ¿Qué comando debemos usar para guardar la configuración del router?
- ¿Qué comando debemos usar para saber si los cambios se han aplicado correctamente?
- ¿En qué modo debemos de introducir el comando para guardar la configuración del router?

3.4.6: (IMARMEN)

- ¿Cómo se cambia el nombre de una VLAN?
- ¿Cómo se comprueba que varios PCs están en la misma VLAN?
- ¿Donde se modifica la dirección IP de un PC?

3.4.7: (IMARMEN)

- ¿Cómo se entra a SSH desde Putty?
- ¿Cuál es el número de bits que queremos utilizar para el cifrado de la key?
- ¿Qué cliente se debe instalar para acceder a SSH desde Windows?

3.4.8: (JDOMDAR)

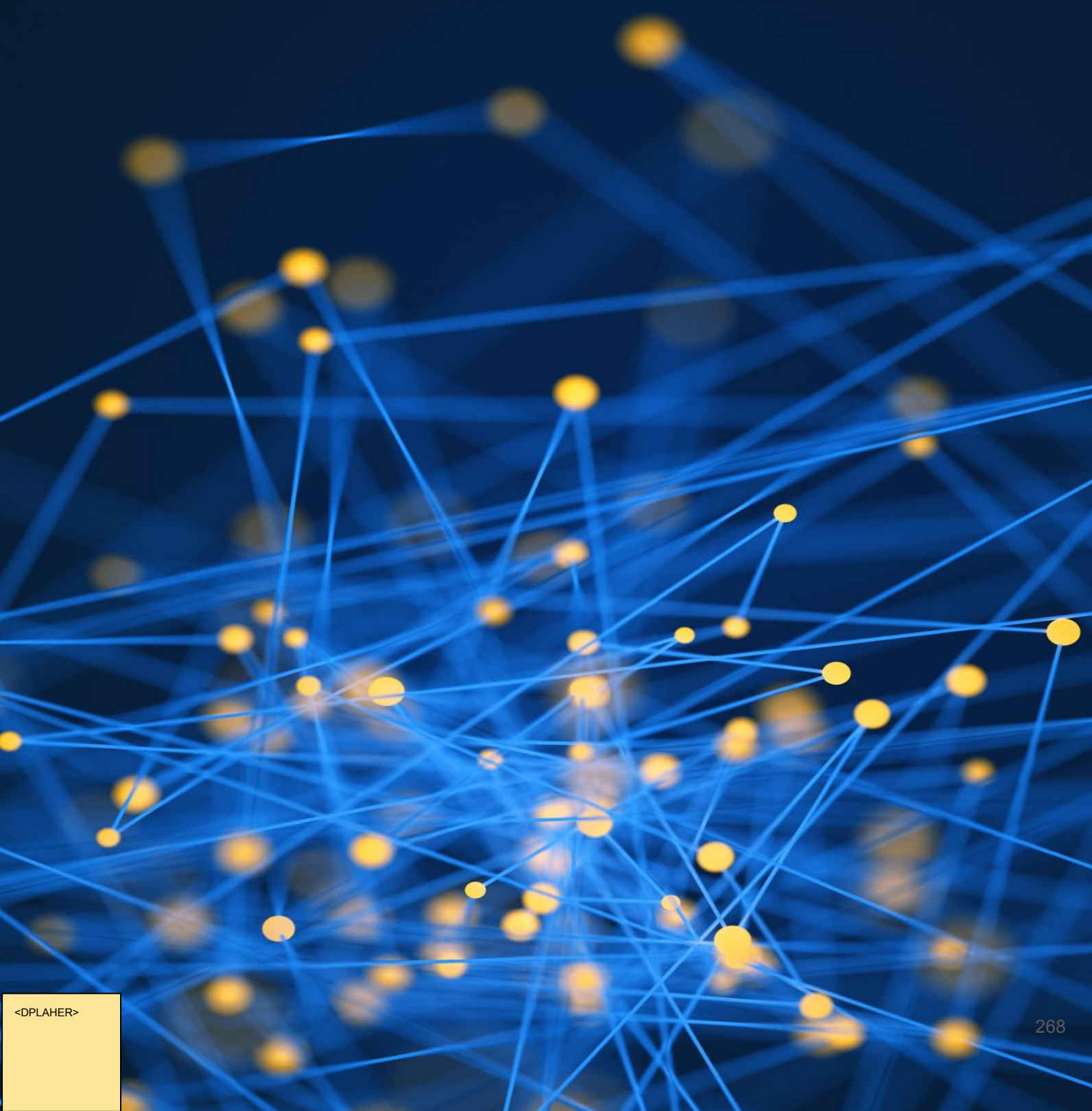
- ¿Qué tipo de cable es necesario usar para conectar dos switches y configurar VTP?
- En la configuración de VTP, servidor y cliente deben "emparejarse" en dos campos, ¿cuáles?
- En un switch cliente, ¿qué comando utilizamos para configurar las VLAN para VTP?

Preguntas de repaso (II)

Preguntas DPLAHER sobre 3.4.5:

- ¿Cuántos tipos de archivos de configuración tienen los switches de Cisco y como se llaman cada uno de ellos?
- ¿Donde se almacena cada uno de los tipos de archivos de configuración?
- ¿Cuál es el comando para guardar la configuración actual en ejecución de un switch?
- ¿Cuál es el comando para comprobar que hemos copiado la configuración en ejecución del switch?

Trabajo 3.5
Routers Cisco de 3ª Generación:
Serie 4000



Trabajo 3.5. Routers Cisco de 3ª Generación: serie 4000

Si bien el Router 2901 está realmente muy muy extendido por las redes corporativas, pertenece a la electrónica de red del gigante americano de 2ª generación.

En este trabajo se pretende hacer un prospección tecnológica sobre la Serie Cisco 4000 enmarcada en la 3ª generación de routers.

Para ello, se trata de responder a las siguientes preguntas:

1. Cuál es el precio en la actualidad del router 2901.
2. Comprobar que Cisco lo tiene descatálogo.
3. Qué routers se enmarcan en la serie 4000, ordenados desde la gama más básica hasta altas prestaciones.
4. Qué rango de precios tienen los equipos de esta serie.
5. Qué router de 3ª generación es equiparable en prestaciones y precio al 2901.
6. Qué ventajas incorporan los equipos de la Serie 4000 con respecto a los routers de segunda generación. Explicar de forma clara y razonada cada una de ellas.

Para cada una de estas preguntas deberá acompañarse con pruebas y evidencias que demuestren cada una de las afirmaciones.

Apartado 1

1. Cuál es el precio en la actualidad del router 2901

Después de indagar sobre los precios en el mercado y visitar varias webs he establecido un baremo entre dos.

Por ejemplo en Amazon podemos encontrarlo:



Precio: EUR 1.084,22

3.5.1

En Router-Switch:



USD ~ \$1,378.00

En conclusión los router 2901 de cisco tienen un precio elevado para el uso doméstico a parte que desempeñan unas tareas y poseen unos protocolos preparados para mayor envergadura que la de un hogar.

Apartado 2

2. Comprobar que Cisco lo tiene descatalogado (2091).

El router 2091 se encuentra descatalogado por Cisco, lo cual se puede comprobar tras realizar una búsqueda del mismo desde la página oficial de Cisco (<https://www.cisco.com>), y como queda corroborado en la **Figura 3.5.2**.

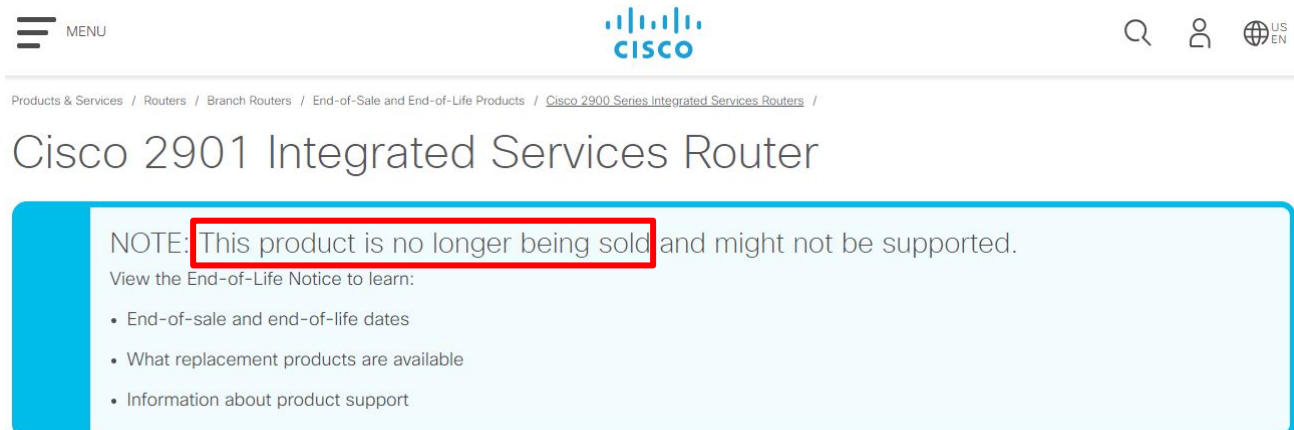


Figura 3.5.2. Captura realizada a la página oficial de Cisco referida al router 2091.

Como vemos en la imagen anterior, en el recuadro de color rojo se nos informa que “Este producto ya no se vende”.

En el siguiente enlace tenemos la página exacta donde Cisco nos informa de que se encuentra descatalogado:

<https://www.cisco.com/c/en/us/products/routers/2901-integrated-services-router-isr/index.html>

Apartado 3

3. Qué routers se enmarcan en la serie 4000, ordenados desde la gama más básica hasta altas prestaciones.

Si acudimos a la página web de Cisco, como se puede observar en la **Figura 3.5.3**, podemos observar el listado de routers Cisco de la serie 4000, ordenados de menor a mayor prestación.

<https://www.cisco.com/c/en/us/products/routers/4000-series-integrated-services-routers-isr/index.html#~:stickynav=1>

Products Software Features Deployment Services Resources Support For Partners Contact Cisco

ISR 4221	ISR 4321	ISR 4331	ISR 4351
<ul style="list-style-type: none">• GE/SFP integrated WAN ports• 1.2-Gbps performance• 75-Mbps encrypted throughput• Full IOS XE SD-WAN support• Cyberthreat protection through Trustworthy Systems framework	<ul style="list-style-type: none">• GE/SFP integrated WAN ports• 2-Gbps+ performance• 100-Mbps encrypted throughput• Full IOS XE SD-WAN support• Cyberthreat protection through Trustworthy Systems framework	<ul style="list-style-type: none">• GE/SFP integrated WAN ports• 2-Gbps+ performance• 500-Mbps encrypted throughput• Full IOS XE SD-WAN support• Cyberthreat protection through Trustworthy Systems framework	<ul style="list-style-type: none">• PoE GE/SFP, GE/SFP integrated WAN ports• 2-Gbps+ performance• 500-Mbps encrypted throughput• Full IOS XE SD-WAN support• Cyberthreat protection through Trustworthy Systems framework
ISR 4431	ISR 4451	ISR 4461	
<ul style="list-style-type: none">• PoE GE/SFP, GE/SFP integrated WAN ports• 4-Gbps+ performance• 900-Mbps encrypted throughput• Cyberthreat protection through Trustworthy Systems framework	<ul style="list-style-type: none">• PoE GE/SFP, GE/SFP integrated WAN ports• 4-Gbps+ performance• 1.6-Gbps encrypted throughput• Cyberthreat protection through Trustworthy Systems framework	<ul style="list-style-type: none">• 10 GE SFP+, PoE GE/SFP, GE/SFP integrated WAN ports• 10-Gbps+ performance• 7-Gbps encrypted throughput• Cyberthreat protection through Trustworthy Systems framework	

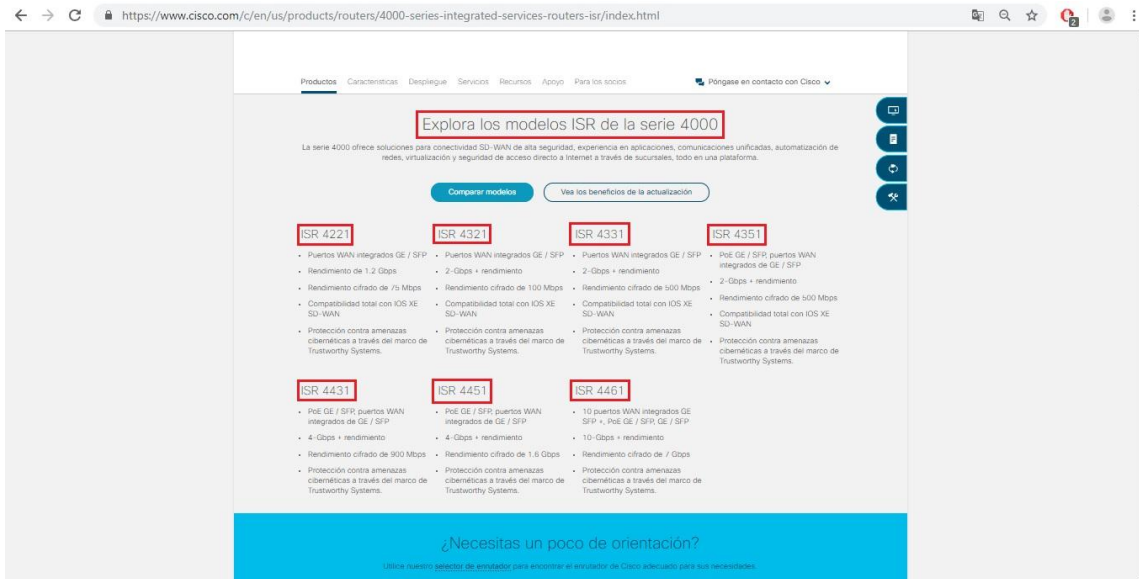
3.5.3

Figura 3.5.3. Captura de la página web de Cisco

<https://www.cisco.com/c/en/us/products/routers/4000-series-integrated-services-routers-isr/index.html#~:stickynav=1>

4. Qué rango de precios tienen los equipos de esta serie.

En cuanto al rango de precios de la Serie 4000 de Routers de Cisco se debe saber primero los modelos disponibles hasta el momento de esta gama de routers. Los **ISR (routers de servicios integrados)** de la serie 4000 de Cisco están disponibles en estos modelos : **4221 ISR, 4321 ISR, 4331 ISR, 4351 ISR, 4431 ISR, 4451 ISR, 4461 ISR.**



3.5.4

Figura 3.5.4.A. Modelos Serie 4000 Cisco.

Sabiendo esto y apoyándonos sobre la página web <http://www.router-switch.com>, los cuales son el 'Proveedor Líder de Hardware de Red' podemos observar en las siguientes imágenes el precio de cada uno de estos modelos extraídos de dicha página web.

ISR 4221:

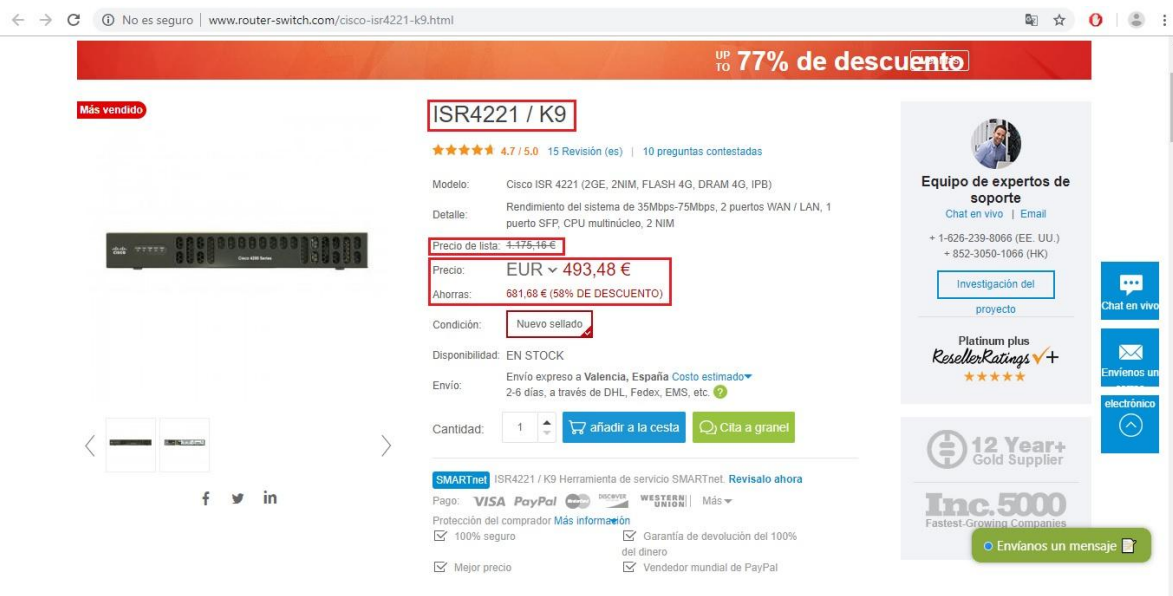


Figura 3.5.4.B. Precio Modelo ISR 4221.

<DPLAHER>


ISR 4321:

← → ↻ No es seguro | www.router-switch.com/cisco-isr4321-k9-p-16545.html

Inicio / Cisco / Enrutadores Cisco / Cisco Router ISR 4000 / ISR4321 / K9

UP TO 77% de descuento

Compra



ISR4321 / K9

★★★★★ 4.4 / 5.0 17 Revisión (s) | 10 preguntas contestadas

Modelo: Cisco ISR 4321 (2GE, 2NIM, 4G FLASH, 4G DRAM, IP Base)
Rendimiento del sistema de 50Mbps-100Mbps, 2 puertos WAN / LAN, 1 puerto SFP, CPU multinúcleo, 2 NIM, seguridad, voz, WAAS, WAN inteligente, OnePK, AVC

Detalle: **Precio de lista: ~~4.922,50 €~~**
Precio: EUR ~ 686,19 €
Ahorras: € 1.236,40 (64% DE DESCUENTO)

Condición: **Nuevo sellado**

Disponibilidad: EN STOCK

Envío: Envío expreso a Valencia, España Costo estimado 2-6 días, a través de DHL, FedEx, EMS, etc.

Cantidad: 1 **añadir a la cesta** **Cita a granel**

SMARTnet Herramienta de servicio SMARTnet ISR4321 / K9. **Revisalo ahora**

Pago: **VISA PayPal** **DISCOVER WESTERN UNION** Más ▾

Protección del comprador **Más información**

100% seguro Garantía de devolución del 100%

Equipo de expertos de soporte
Chat en vivo | Email
+ 1-626-239-8066 (EE. UU.)
+ 852-3050-1066 (HK)

Investigación del proyecto

Platinum plus ResellerRatings ✓+
★★★★★

12 Year+ Gold Supplier

Inc.5000 Fastest-Growing Companies

Envíanos un mensaje

Chat en vivo

Envíanos un mensaje electrónico

f t in

Figura 3.5.4.C. Precio Modelo ISR 4321.


ISR 4331:

← → ↻ No es seguro | www.router-switch.com/cisco-isr4331-k9-p-16544.html

Inicio / Cisco / Enrutadores Cisco / Cisco Router ISR 4000 / ISR4331 / K9

UP TO 77% de descuento

Compra



ISR4331 / K9

★★★★★ 4.4 / 5.0 14 Revisión (es) | 10 preguntas contestadas

Modelo: Cisco 4000 Router ISR4331 (2GE, 2NIM, 1SM, 4G FLASH, 4G DRAM, IP Base)
Cisco 4000 Router, rendimiento del sistema 100Mbps-300Mbps, 2 puertos WAN / LAN, 2 puertos SFP, CPU multinúcleo, 1 ranuras de módulo de servicio, seguridad, voz, WAAS, Intelligent WAN, OnePK, AVC

Detalle: **Precio de lista: ~~3.147,28 €~~**
Precio: EUR ~ 1.090,52 €
Ahorras: € 2.056,76 (65% DE DESCUENTO)

Condición: **Nuevo sellado**

Disponibilidad: EN STOCK

Envío: Envío expreso a Valencia, España Costo estimado 2-6 días, a través de DHL, FedEx, EMS, etc.

Cantidad: 1 **añadir a la cesta** **Cita a granel**

SMARTnet ISR4331 / K9 Herramienta de servicio SMARTnet. **Revisalo ahora**

Pago: **VISA PayPal** **DISCOVER WESTERN UNION** Más ▾

Protección del comprador **Más información**

100% seguro Garantía de devolución del 100% del dinero

Equipo de expertos de soporte
Chat en vivo | Email
+ 1-626-239-8066 (EE. UU.)
+ 852-3050-1066 (HK)

Investigación del proyecto

Platinum plus ResellerRatings ✓+
★★★★★

12 Year+ Gold Supplier

Inc.5000 Fastest-Growing Companies

Envíanos un mensaje

Chat en vivo

Envíanos un mensaje electrónico

f t in

Figura 3.5.4.D. Precio Modelo ISR 4331.

3.5.4

<DPLAHER>

ISR 4351:

UP TO **77% de descuento**

ISR4351 / K9

★★★★★ 4.8 / 5.0 26 Revisión (s) | 11 preguntas contestadas

Modelo: Cisco ISR 4351 (3GE, 3NIM, 2SM, 4G FLASH, 4G DRAM, IP Base)
Detalle: Rendimiento del sistema de 200Mbps-400Mbps, 2 puertos WAN / LAN, 3 puertos SFP, CPU multinúcleo, 2 ranuras de módulo de servicio, Seguridad, Voz, WAAS, Intellignt WAN, OnePK, AVC

Precio de lista: ~~€ 7.599,78~~
Precio: **EUR ~ 2.787,97 €**
Ahorras: € 4.798.81 (63% DE DESCUENTO)

Condición: **Nuevo sellado**

Disponibilidad: EN STOCK

Envío: Envío expreso a Valencia, España Costo estimado▼
2-6 días, a través de DHL, FedEx, EMS, etc. ?

Cantidad: 1 [añadir a la cesta](#) [Cita a granel](#)

SMARTnet Herramienta de servicio SMARTnet ISR4351 / K9. [Revisalo ahora](#)

Pago: **VISA PayPal** Más ▼

Protección del comprador [Más información](#)

100% seguro Garantía de devolución del 100% del dinero Mejor precio Vendedor mundial de PayPal

Equipo de expertos de soporte
Chat en vivo | Email
+ 1-626-239-8066 (EE. UU.)
+ 852-3050-1066 (HK)

[Investigación del proyecto](#)

Platinum plus ResellerRatings +★★★★★

12 Year+ Gold Supplier

Inc.500
Fastest-Growing Companies

[Envíanos un mensaje](#)

Chat en vivo

Envíanos un mensaje electrónico

Figura 3.5.4.E. Precio Modelo ISR 4351.

ISR 4431:

UP TO **77% de descuento**

Comprar

ISR4431 / K9

★★★★★ 4.8 / 5.0 31 Revisión (es) | 10 preguntas contestadas

Modelo: Cisco ISR 4431 (4GE, 3NIM, 8G FLASH, 4G DRAM, IP Base)
Detalle: Rendimiento del sistema 500Mbps-1Gbps, 4 puertos WAN / LAN, 4 puertos SFP, CPU multinúcleo, alimentación dual, seguridad, voz, WAAS, Intellignt WAN, OnePK, AVC, CPU de datos y servicios de control por separado

Precio de lista: ~~€ 10.319,83 €~~
Precio: **EUR ~ 4.767,29 €**
Ahorras: € 5.552.53 (54% DE DESCUENTO)

Condición: **Nuevo sellado**

Disponibilidad: EN STOCK

Envío: Envío expreso a Valencia, España Costo estimado▼
2-6 días, a través de DHL, FedEx, EMS, etc. ?

Cantidad: 1 [añadir a la cesta](#) [Cita a granel](#)

SMARTnet ISR4431 / K9 Herramienta de servicio SMARTnet. [Revisalo ahora](#)

Pago: **VISA PayPal** Más ▼

Protección del comprador [Más información](#)

100% seguro Garantía de devolución del 100% del dinero

Equipo de expertos de soporte
Chat en vivo | Email
+ 1-626-239-8066 (EE. UU.)
+ 852-3050-1066 (HK)

[Investigación del proyecto](#)

Platinum plus ResellerRatings +★★★★★

12 Year+ Gold Supplier

Inc.500
Fastest-Growing Companies

[Envíanos un mensaje](#)

Chat en vivo

Envíanos un mensaje electrónico

Figura 3.5.4.F. Precio Modelo ISR 4431.

3.5.4

ISR 4451:

Inicio / Cisco / Enrutadores Cisco / Cisco Router ISR 4000 / ISR4451-X / K9

UP TO **77% de descuento**

Más vendido

ISR4451-X / K9

★★★★★ 4.9 / 5.0 13 Comentario (s) | 10 preguntas contestadas

Modelo: Cisco ISR 4451 (4GE, 3NIM, 2SM, 8G FLASH, 4G DRAM)
Rendimiento del sistema 1-2G, 4 puertos WAN / LAN, 4 puertos SFP, 10 Core CPU, Seguridad, Voz, WAAS, Intelligent WAN, OnePK, AVC, CPU de datos y servicios de control por separado

Detalle: Rendimiento del sistema 1-2G, 4 puertos WAN / LAN, 4 puertos SFP, 10 Core CPU, Seguridad, Voz, WAAS, Intelligent WAN, OnePK, AVC, CPU de datos y servicios de control por separado

Precio de lista: ~~16.988,10€~~

Precio: EUR **8.562,03 €**

Ahorras: 8.426,07 € (50% DE DESCUENTO)

Condición: **Nuevo sellado**

Disponibilidad: EN STOCK

Envío: Envío expreso a Valencia, España Costo estimado 2-6 días, a través de DHL, FedEx, EMS, etc.

Cantidad: 1 [añadir a la cesta](#) [Cita a granel](#)

SMARTnet Herramienta de servicio SMARTnet ISR4451-X / K9. [Revisalo ahora](#)

Pago: **VISA** **PayPal** **Discover** **WESTERN UNION** Más

Protección del comprador [Más información](#)

100% seguro Garantía de devolución del 100% del dinero

Equipo de expertos de soporte
Chat en vivo | Email
+ 1-626-239-8066 (EE. UU.)
+ 852-3050-1066 (HK)

Investigación del proyecto

Platinum plus ResellerRatings **✓+**
★★★★★

12 Year+ Gold Supplier

In 5000 Fastest-Growing

Envíanos un mensaje

Figura 3.5.4.G. Precio Modelo ISR 4451.

El precio de todos los Switches en este momento en esta página se encuentran rebajados pero el precio real es el señalado en el recuadro llamado '**Precio de lista**'. También decir que el router ISR 4461 no aparece su precio en esta página por lo que no se encuentra su imagen con el precio. Pasando por alto este último Router (**ISR 4461**) y centrándonos en el resto podemos observar sin tener en cuenta el descuento de esta página en este momento como el precio oscila entre **1.000€ y 17.000€**, más o menos.

3.5.4

Apartado 5

5. Qué router de 3ª generación es equiparable en prestaciones y precio al 2901.

Si acudimos a la página web de Cisco, tenemos un documento oficial por parte de la compañía en el que se nos recomienda el router 4321 de la serie 4000 para saltar desde un router 2091, o, incluso, desde un router 1941. Esto queda confirmado en las siguientes Figuras:



3.5.5

Figura 3.5.5.A. Documento oficial de Cisco.

https://www.cisco.com/c/dam/global/es_es/assets/pdf/en_06_4k_architecture_wp_pte_cte_es.pdf


Apartado 5

← → ↻ https://www.cisco.com/c/dam/global/es_es/assets/pdf/en_06_4k_architecture_wp_pte_cte_es.pdf 🔍 ☆

en_06_4k_architecture_wp_pte_cte_es.pdf 7 / 7

La figura 7 muestra el router de servicios integrados Cisco 4321.

Figura 7. Cisco 4321



El Cisco 4321 se recomienda para migrar desde los actuales routers **Cisco 2901 y 1941**. Ofrece una velocidad de 50 Mb/s, actualizable hasta 100 Gb/s, con un formato de 1 RU con 2 ranuras NIM y sin ranuras SM.

- CPU de 4 núcleos con 2 núcleos para el plano de datos, 1 núcleo para el plano de control y 1 núcleo dedicado para servicios
- Memoria de control y servicios de hasta 8 GB

Conclusión

El router Cisco serie 4000 está diseñado para ayudar a las sucursales y oficinas remotas a hacer más con menos. Estos routers ofrecen más ancho de banda y gestión WAN inteligente, además de más máquinas virtuales, más servidores de categoría de Data Center y más flexibilidad para actualizaciones. Además, necesitan menos espacio en el rack; suponen menores costes de mantenimiento, electricidad y refrigeración; y requieren una menor administración por parte del personal técnico.

El router Cisco serie 4000 ya está a la venta. Para obtener más información, póngase en contacto con su distribuidor de Cisco.

Si desea obtener más información, visite: cisco.com/go/4000.

CISCO

Sede central en América
Cisco Systems, Inc.
San José, CA

Sede central en Asia-Pacífico
Cisco Systems (USA) Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV
Amsterdam, Países Bajos

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, números de teléfono y fax se encuentran en la Web de Cisco en www.cisco.com/go/offices.

Cisco y el logotipo de Cisco son marcas comerciales o registradas de Cisco y/o sus entidades filiales en Estados Unidos y otros países. Si desea consultar una lista de las marcas comerciales de Cisco, visite: www.cisco.com/go/trademarks. Todas las marcas comerciales de terceros mencionadas en este documento pertenecen a sus respectivos propietarios. El uso de la palabra "partner" no implica la existencia de una asociación entre Cisco y cualquier otra empresa. (11102)

Impreso en EE. UU. C11-732909-00 08/14

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco. Página 7 de 7

3.5.5

Figura 3.5.5.B. Referencia al router 4321 desde Cisco.

La figura 7 muestra el router de servicios integrados Cisco 4321.

Figura 7. Cisco 4321



El Cisco 4321 se recomienda para migrar desde los actuales routers Cisco 2901 y 1941. Ofrece una velocidad de 50 Mb/s, actualizable hasta 100 Gb/s, con un formato de 1 RU con 2 ranuras NIM y sin ranuras SM.

- CPU de 4 núcleos con 2 núcleos para el plano de datos, 1 núcleo para el plano de control y 1 núcleo dedicado para servicios
- Memoria de control y servicios de hasta 8 GB

Figura 3.5.5.C. Recomendación explícita de Cisco.

Apartado 6

6. Qué ventajas incorporan los equipos de la Serie 4000 con respecto a los routers de segunda generación. Explicar de forma clara y razonada cada una de ellas.

1. Enterprise Network Functions Virtualization (Virtualización de funciones de red empresarial).

Aproveche los servicios de red de confianza de Cisco como software: enrutamiento, firewall, aceleración de aplicaciones y controlador de LAN inalámbrica, así como servicios de terceros. Simplifique las operaciones y despliegue nuevos servicios de red virtual en minutos en cualquier plataforma.

2. Cisco IOS XE open operating system

Cisco IOS XE es un sistema operativo abierto y flexible optimizado para una nueva era de redes empresariales.

Sus interfaces programables basadas en estándares automatizan las operaciones de red y le brindan una gran visibilidad de los comportamientos de los usuarios, las aplicaciones y los dispositivos.

Se basa en linux y proporciona una arquitectura de software distribuida que elimina muchas de las responsabilidades del sistema operativo del proceso de IOS. IOS XE ejecuta una copia de IOS lo que permite que los comandos CLI sean los mismos entre Cisco IOS e IOS XE, en contraste con IOS XR, que tiene una base de código completamente diferente y sus desarrolladores implementaron un conjunto de comandos de CLI bastante diferente.

3. Native Application Hosting (Alojamiento de aplicaciones nativas).

No necesita dispositivos de red adicionales en la sucursal. Permite tener una plataforma para usar las propias herramientas y utilidades que se quieran, es decir, facilita al Sistema Operativo para que se ajuste a las herramientas existentes (desarrolladas mediante Linux). Por último, puedes tener todas estas aplicaciones en un dispositivo de red.

4. Cisco DNA Center centralized management (Sistema de control centralizado).

Permite:

- Simplificar la gestión de la red.
- Gestiona tu red empresarial sobre un tablero centralizado.
- Implementar redes en minutos, no días. Utilizando flujos de trabajo intuitivos, Centro de DNA hace que sea fácil Diseño, provisión y aplicación de políticas a través de su red.
- Costos más bajos. Impulsado por la política aprovisionamiento y guiado red de incremento de remediación tiempo de actividad y tiempo de reducción gastado en la gestión simple operaciones de red.
- Transforma tu red con servicios y aplicaciones en la nube que se benefician de este inteligente optimización de la red.

3.5.6

Apartado 6

5. Cisco SD-WAN

Las WAN tradicionales no pueden mantener el ritmo de aplicaciones que se están moviendo a la nube ni el creciente número de dispositivos que se conectan, siendo cada vez más complejas y costosas de operar. La WAN definida por software (SD-WAN) constituye un nuevo enfoque para la conectividad de red que reduce los costes operativos y mejora la experiencia de uso de las aplicaciones.

SD-WAN de Cisco:

- Permite establecer transportes independientes que permiten reducir los costes e incrementar el ancho de banda
- Ofrece una experiencia de usuario óptima para las aplicaciones SaaS y se extiende de forma infalible en la nube pública
- Proporciona una segmentación de extremo a extremo para proteger recursos informáticos vitales para las empresas
- Hace posible cumplir los SLA en aplicaciones empresariales críticas

3.5.6



Figura 3.5.6.A. Características de SD-WAN.

6. Pay-as-you-grow performance and services

Tienes la posibilidad de comprar el equipamiento necesario actual para después poder actualizar cuando quieras sin tener que realizar un cambio de equipamiento completo.

7. Trustworthy System (Sistemas de confianza).

En lo que a seguridad se refiere, los **Trustworthy Systems** de Cisco son sistemas que nos proporcionan cifrado de futuras generaciones y verificación de la integridad.

Sellos de confianza de los Trustworthy Systems:

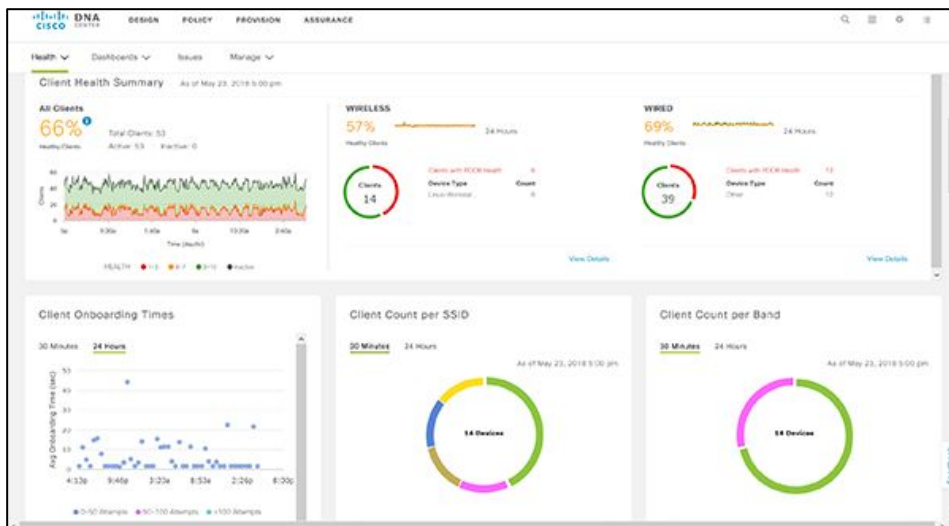
- Los proveedores de confianza se esfuerzan por garantizar que un producto se diseñe, se desarrolle, se fabrique, se venda y se repare según lo establecido en los manuales.
- Los proveedores de confianza toman medidas para asegurar su fabricación y distribución en cadenas de suministro contra la falsificación y manipulación, y para prevenir la instalación de características no autorizadas tales como "puertas traseras".
- Productos confiables que cumplen con las normas de seguridad de la industria y del gobierno relevante para los requerimientos del negocio del cliente.

Apartado 6

8. DNA Assurance network monitoring (monitoreo de red de seguridad).

Cisco DNA Center permite:

- Gestión:
 - Control total desde un panel de único
 - Vistas granulares de redes, servicios y dispositivos
 - Gestión del ciclo de vida del dispositivo
 - Importe mapas y configuraciones para Cisco Prime o APIC-EM



3.5.6

Figura 3.5.6.B. Pestaña de gestión de Cisco DNA Center.

- Automatización
 - Descubrimiento automatizado de dispositivos
 - Creación de políticas drag-and-drop
 - Implementación de dispositivos sin intervención
 - Calidad del servicio (QoS) automatizada

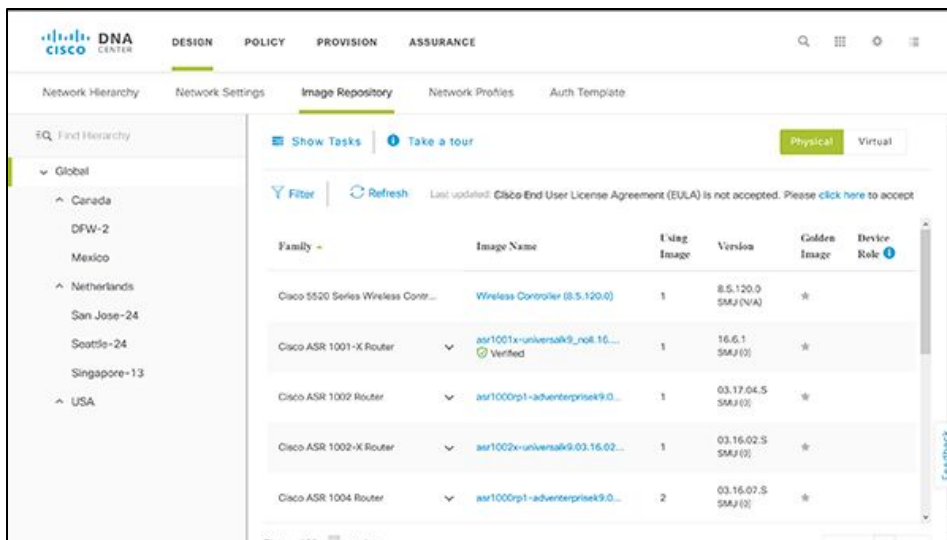
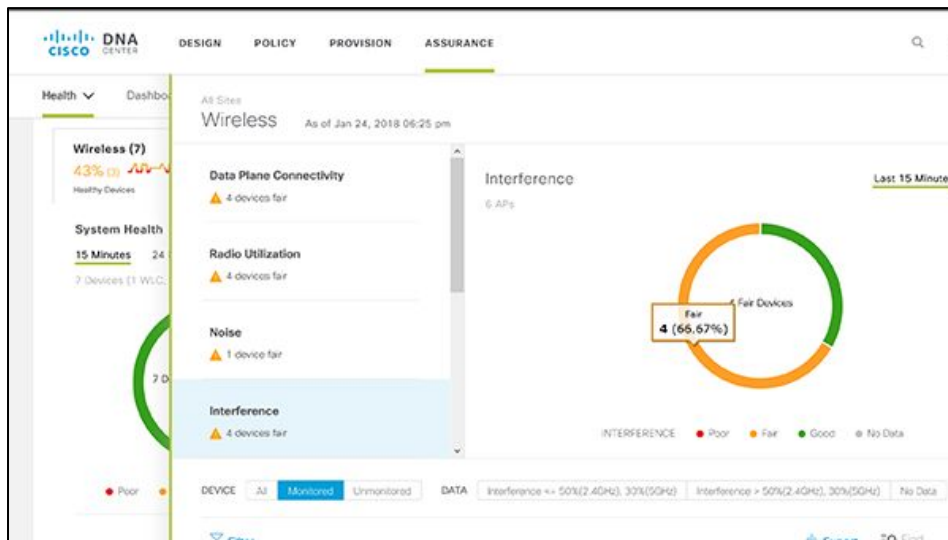


Figura 3.5.6.C. Pestaña de automatización de Cisco DNA Center.

Apartado 6

- Análisis
 - Todo como sensor
 - Análisis guiados por el contexto
 - Más de 150 datos procesables
 - Remediación guiada



3.5.6

Figura 3.5.6.D. Pestaña de análisis de Cisco DNA Center.

- Seguridad
 - Detección y respuesta ante amenazas
 - Integración de ISE y *Stealthwatch*
 - Análisis de tráfico encriptado
 - Segmentación muy segura

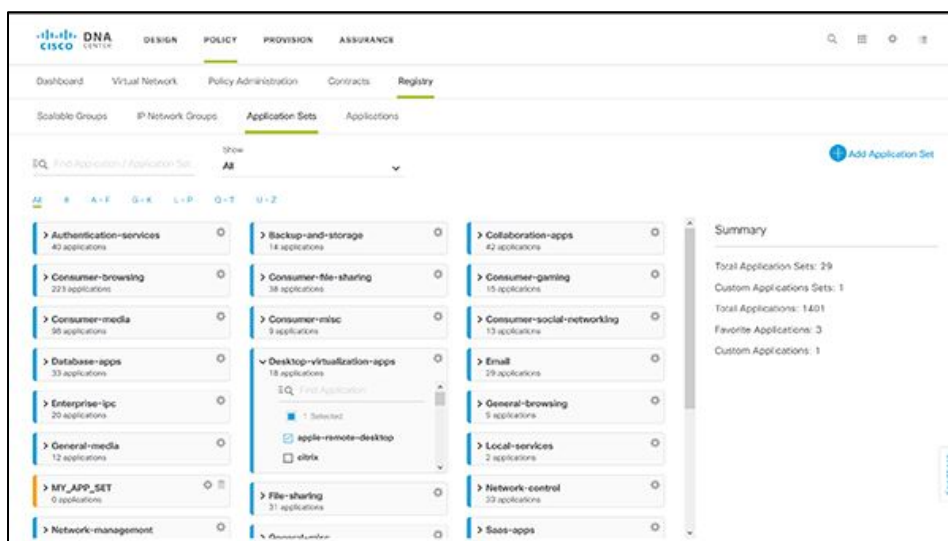


Figura 3.5.6.E. Pestaña de automatización de Cisco DNA Center.

Apartado 6

9. Cisco Umbrella (OpenDNS)

Cisco Umbrella es una plataforma de seguridad en la nube que proporciona una primera línea de defensa contra las amenazas en Internet donde sea que vayan los usuarios, es decir, desde un PC, un portátil, un smartphone...

Umbrella usa DNS para detener las amenazas en todos los puertos y protocolos, incluso en las conexiones directas a IP, con el fin de detener el malware antes de que llegue a sus puntos finales o red.

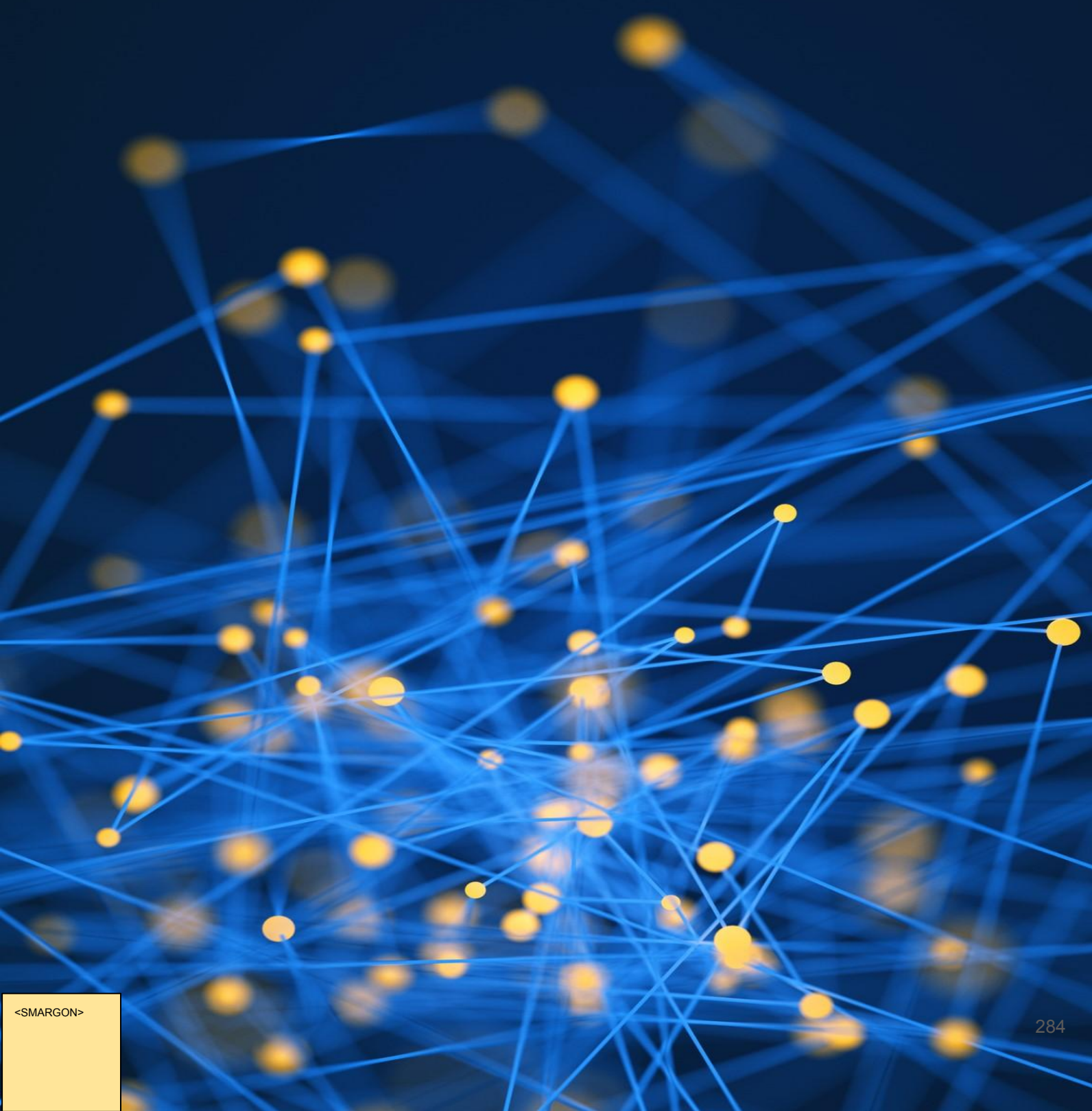
10. Encrypted Traffic Analytics

Es la capacidad de hacer 'Análisis de tráfico cifrado': Aprovechar las últimas capacidades de red de Cisco para evitar, detener o mitigar las amenazas más rápido que nunca. Cisco Digital Network Architecture (DNA) es la primera red de la industria con la capacidad de encontrar amenazas en el tráfico cifrado.

3.5.6

Trabajo 4.1

Creación de una conexión WAN por xDSL



Vamos a crear una conexión WAN desde dos sedes simulando la conexión al servidor de un ISP por medio de xDSL

Pasos a seguir:

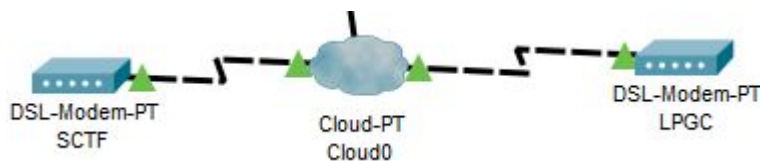
1. Crear una nube a la que conectaremos por Ethernet un servidor.

- Poner ip al servidor 192.168.1.1
- Activar servicio DHCP
- Conectar al puerto ethernet de la nube



4.1

2. Dar de alta un módems xDSL para cada sede.



- Conectar mediante cable telefónico cada módem a la nube
- La conexión debe realizarse a un puerto módem
- En la nube, asociar cada módems xDSL con el puerto Ethernet que conecta con el servidor del ISP

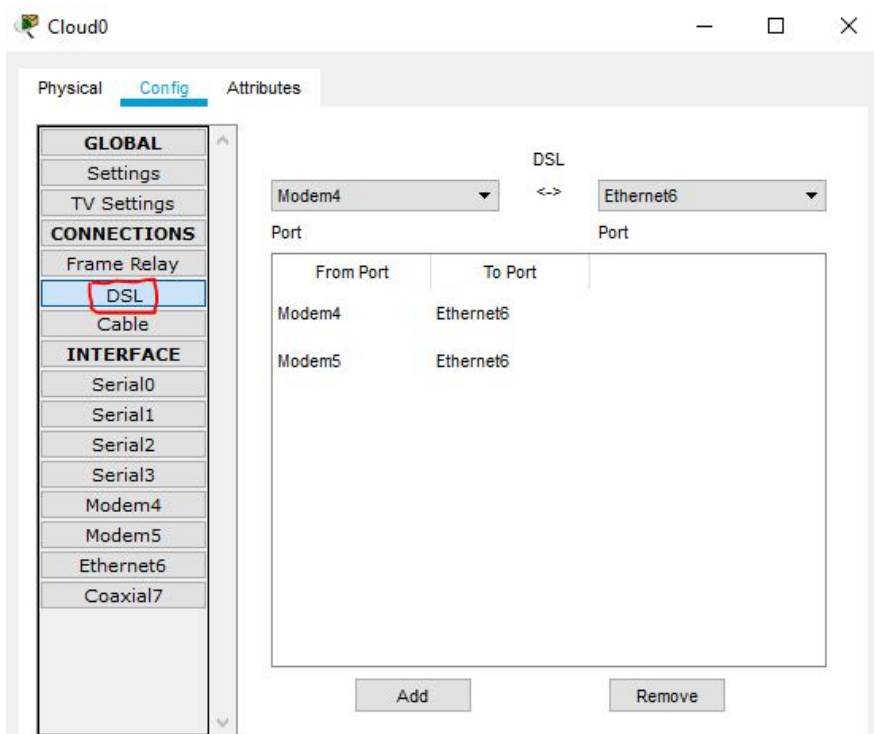
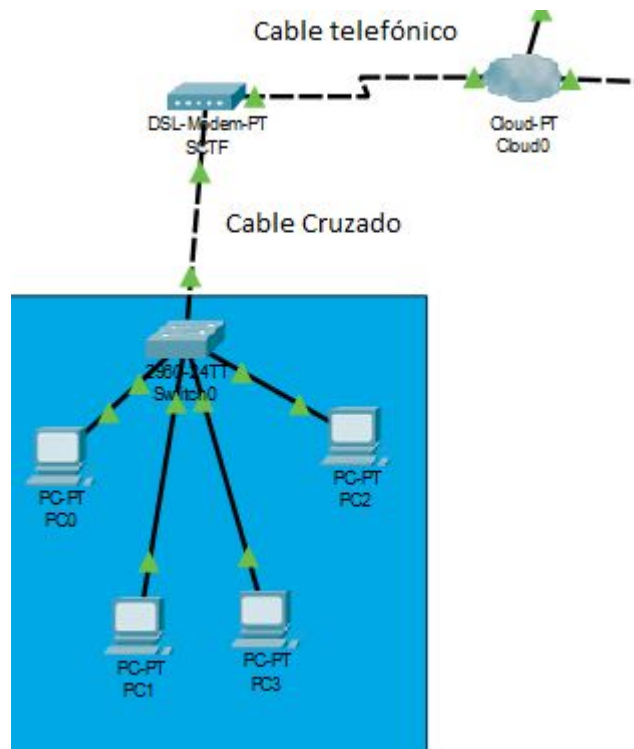


Figura 4.1.A. Asociar Modem xDSL a la nube

3. En cada sede, asignar un switch y 4 Pcs para que tengan conexión al módem.

- La conexión del módem a cada switch mediante cable cruzado
- La conexión del switch a la nube mediante cable telefónico
- La IP de los Pcs vía DHCP



4.1

Figura 4.1.B. Asignación de Pcs y switch de cada sede

Topología de la red

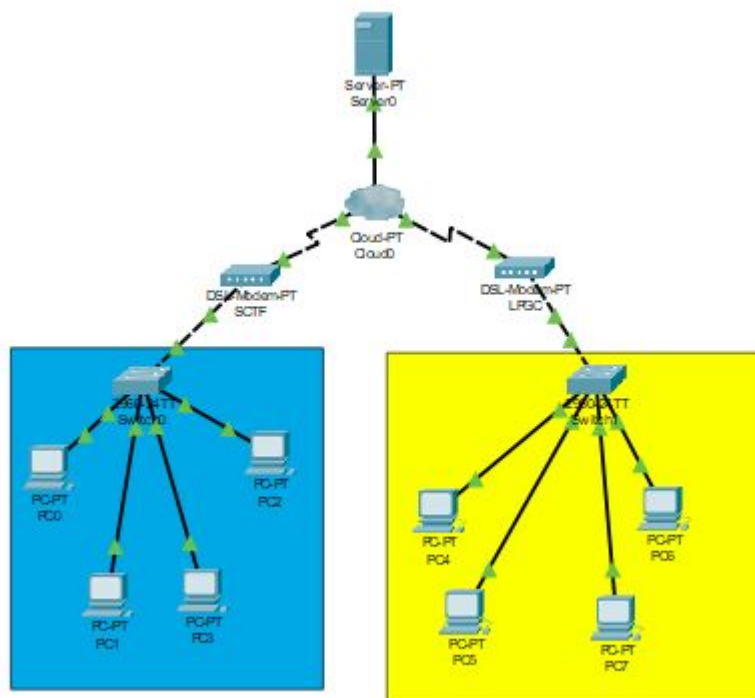


Figura 4.1.C. Topología de la red

Trabajo 4.2
Simulación de conexión ISP - Cable
y xDSL

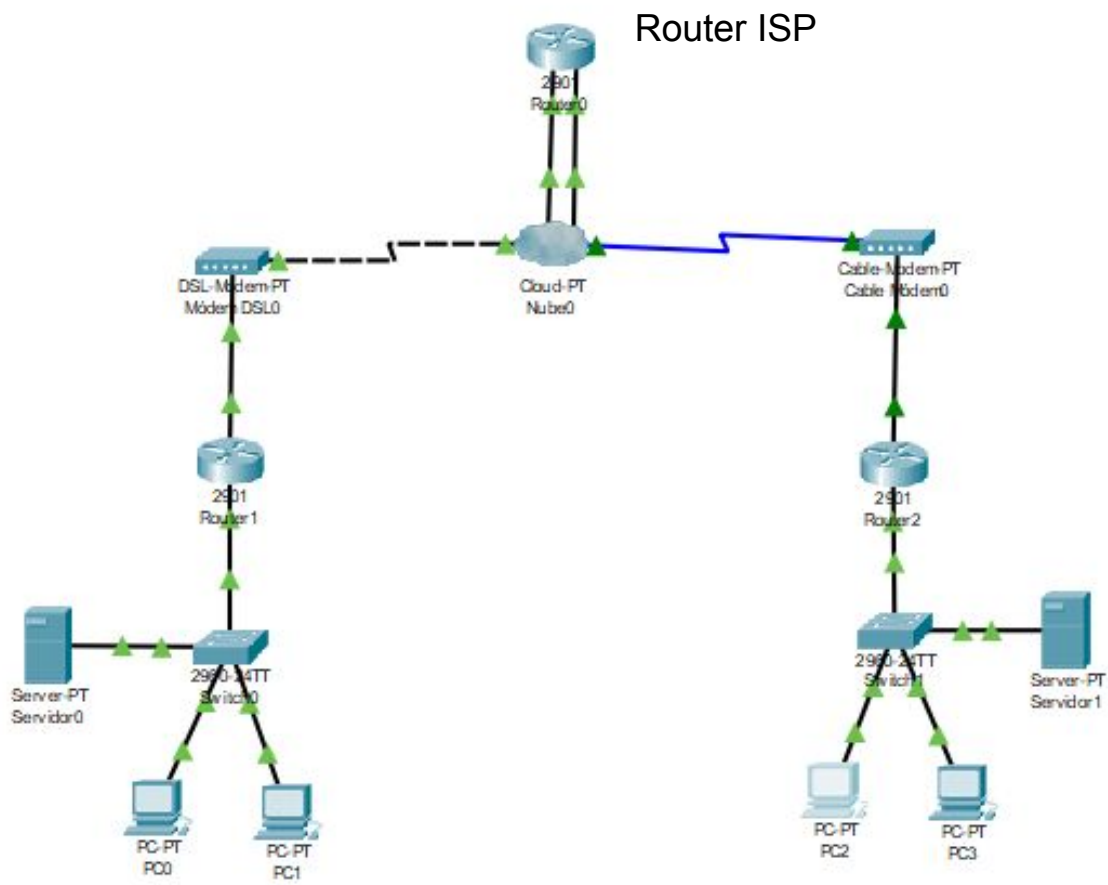


Trabajo 4.2. Simulación de conexión ISP - cable y xDSL

- Vamos a diseñar una red que simule la conexión WAN de varios domicilios a un ISP
- Representaremos toda la conexión mediante una nube
- Representaremos dos domicilios, uno en SCTF y otro en LPGC
- El ISP lo representaremos mediante un simple router
- Cada domicilio tendrá en su interior un router y un módem xDSL para SCTF y cable para LPGC
- Todos los routers se conectarán a la nube mediante una IP pública de clase A • Internamente, los routers domiciliarios tendrán la IP 192.168.1.1
- A nivel domiciliario, conectaremos varios PC por DHCP
- Situar dentro de cada domicilio un servidor DHCP con las siguientes características – IP: 192.168.1.2 – Dirección IP de inicio para DHCP: 192.168.1.50 – Número máximo de equipos: 50
- Probar que hay conectividad entre cualquiera de los routers de abonado entre sí y con el ISP
- Recuerda que: – El módem de SCTF debe conectarse mediante cable telefónico – El módem de LPGC debe conectarse mediante cable coaxial – Realiza la conexión en la nube de los módems al router del ISP.

4.3

- Vamos a diseñar una red que simule la conexión WAN de varios domicilios a un ISP



4.2

Figura 4.2.a. Topología de la red

- Representaremos toda la conexión mediante una nube

Toda la conexión se representará mediante una nube

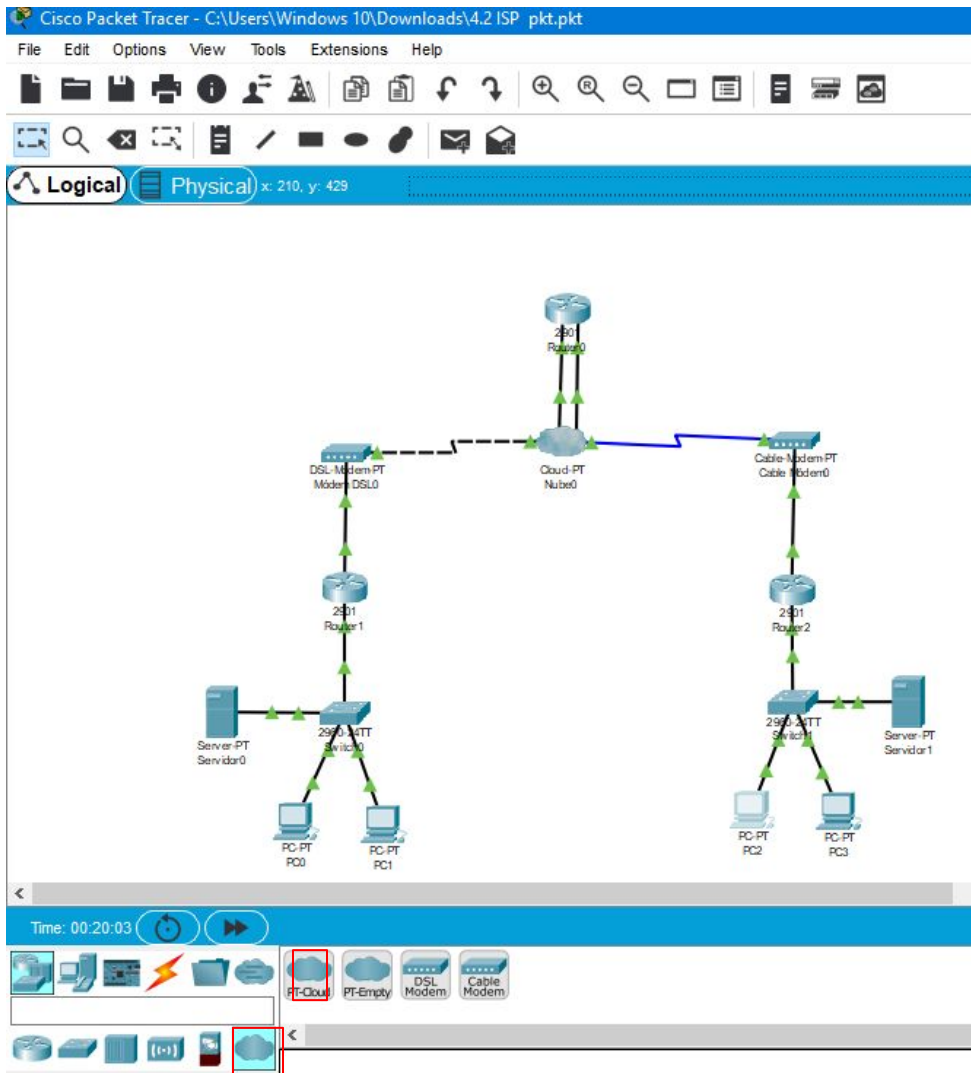
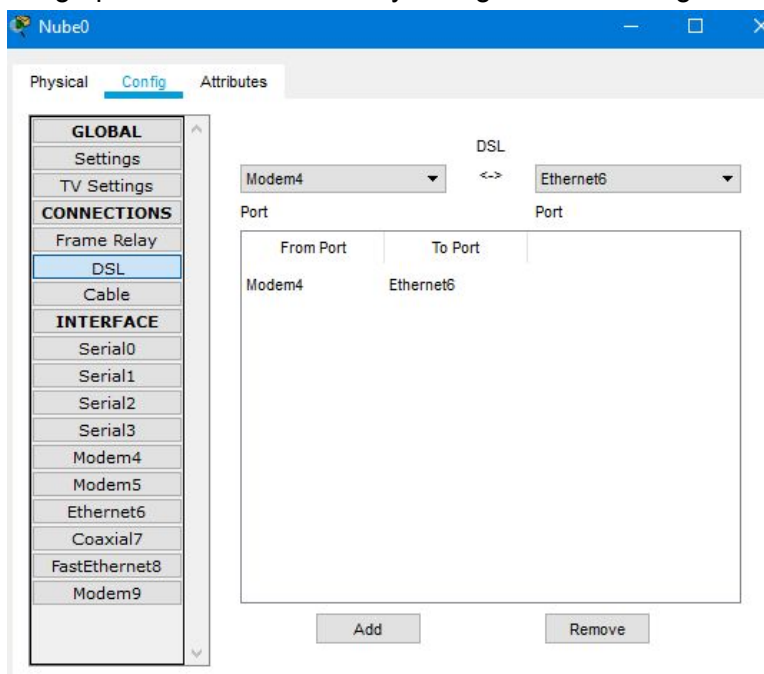


Figura 4.2.b Localización de la nube Packet tracer

Conectaremos el abonado de SCTF al módem DSL con cable telefónico



Luego pinchamos en la nube y configuraremos lo siguiente



4.2

Figura 4.2.d Conexión de la nube al módem DSL

Conectamos el abonado de LPGC al módem de cable con coaxial

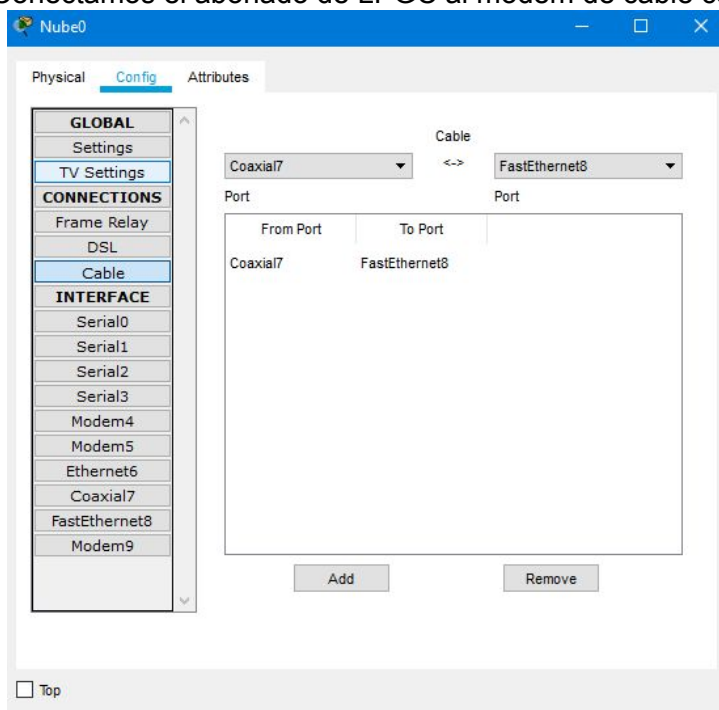
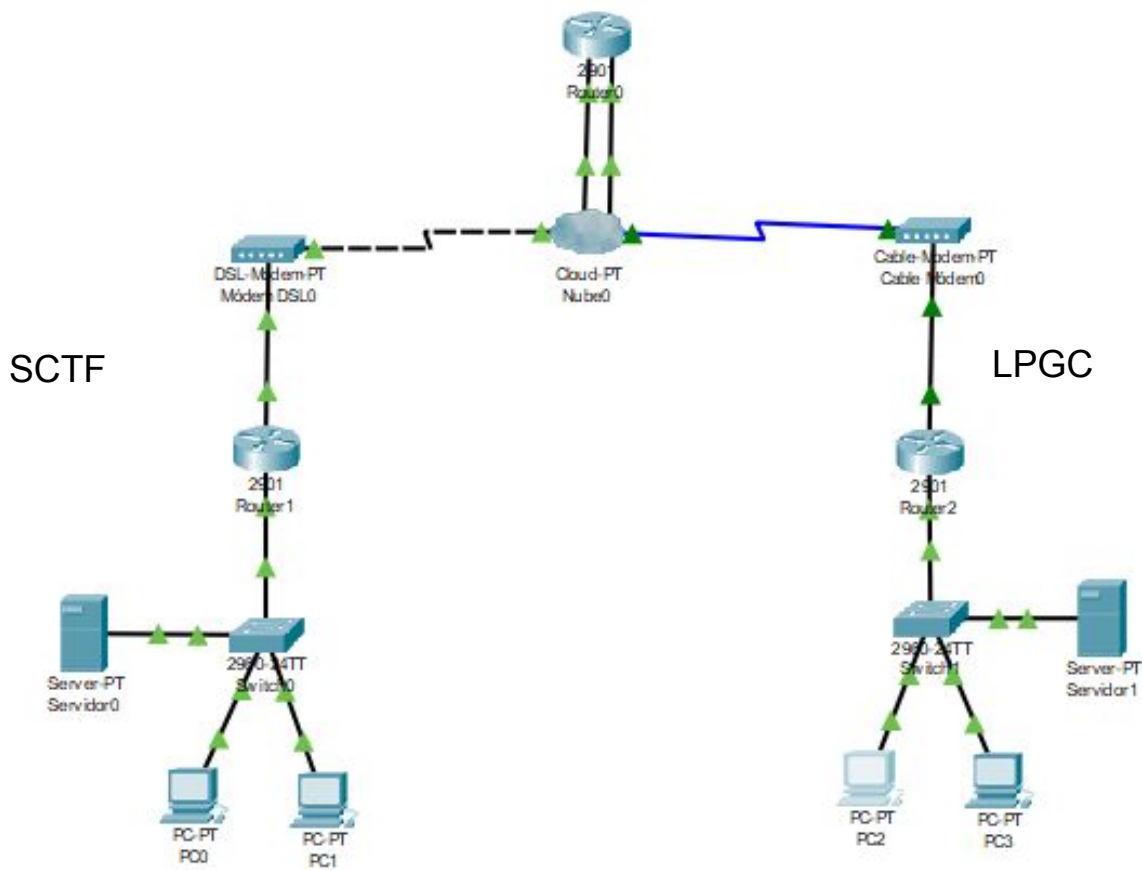


Figura 4.2.e Conexión de la nube al módem por cable

- Representaremos dos domicilios, uno en SCTF y otro en LPGC

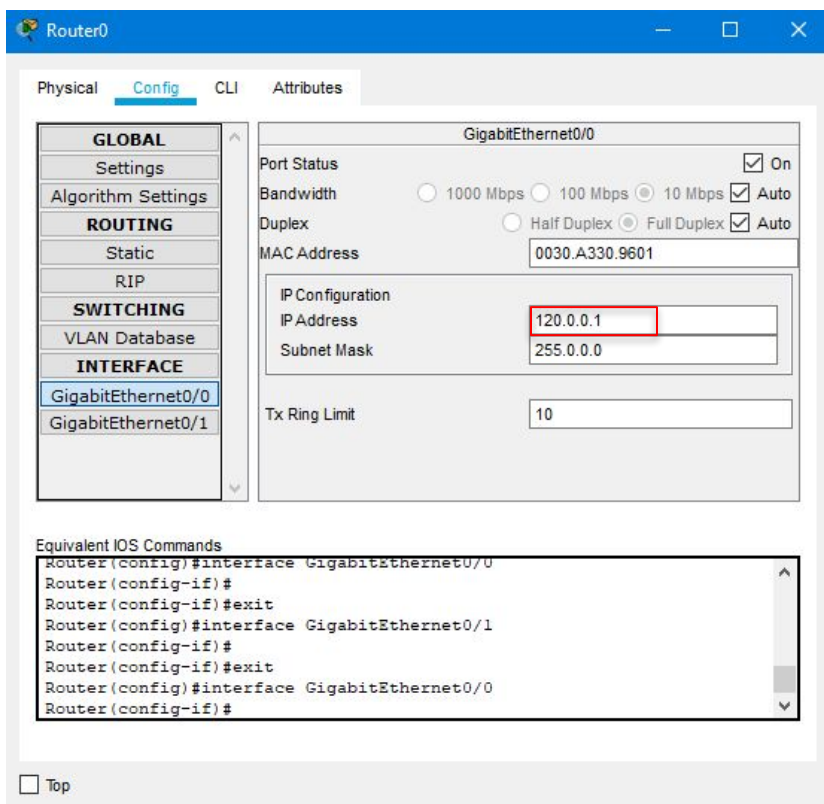


4.2

Figura 4.2.f. Topología de la red con sus respectivas sedes

- El ISP lo representaremos mediante un simple router

Le pondremos 2 tarjetas gigabitEthernet una para la conexión de cable y otra para la conexión telefónica y sus IP (120.0.0.1 y 121.0.0.1).



4.2

Figura 4.2.g Configuración puerto G0/0 router ISP

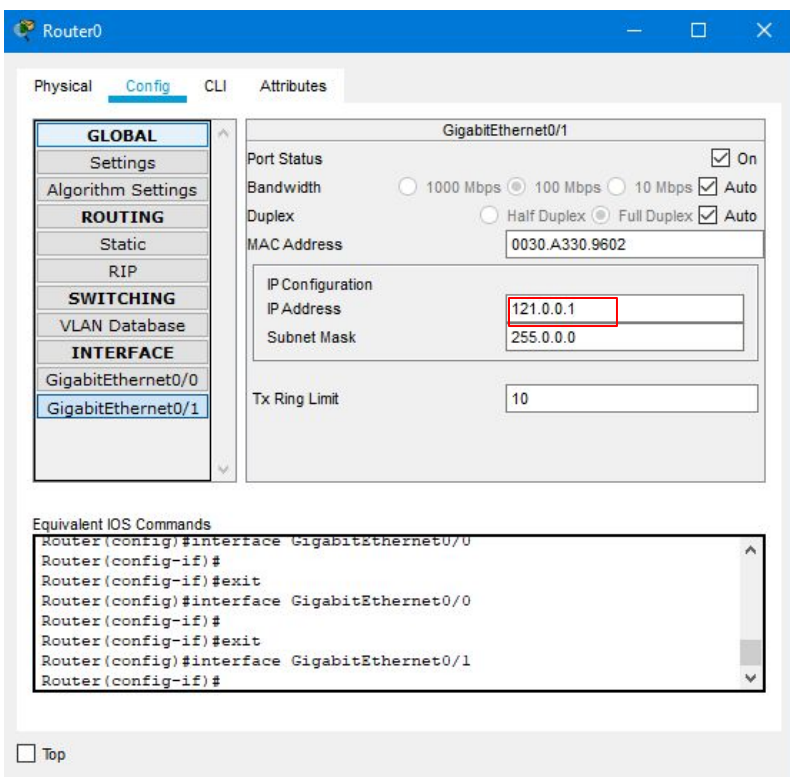


Figura 4.2.h Configuración puerto G0/1 router ISP

- Cada domicilio tendrá en su interior un router y un módem xDSL para SCTF y cable para LPGC

En el apartado número 3 se pueden ver los domicilios con sus respectivos routers y módems

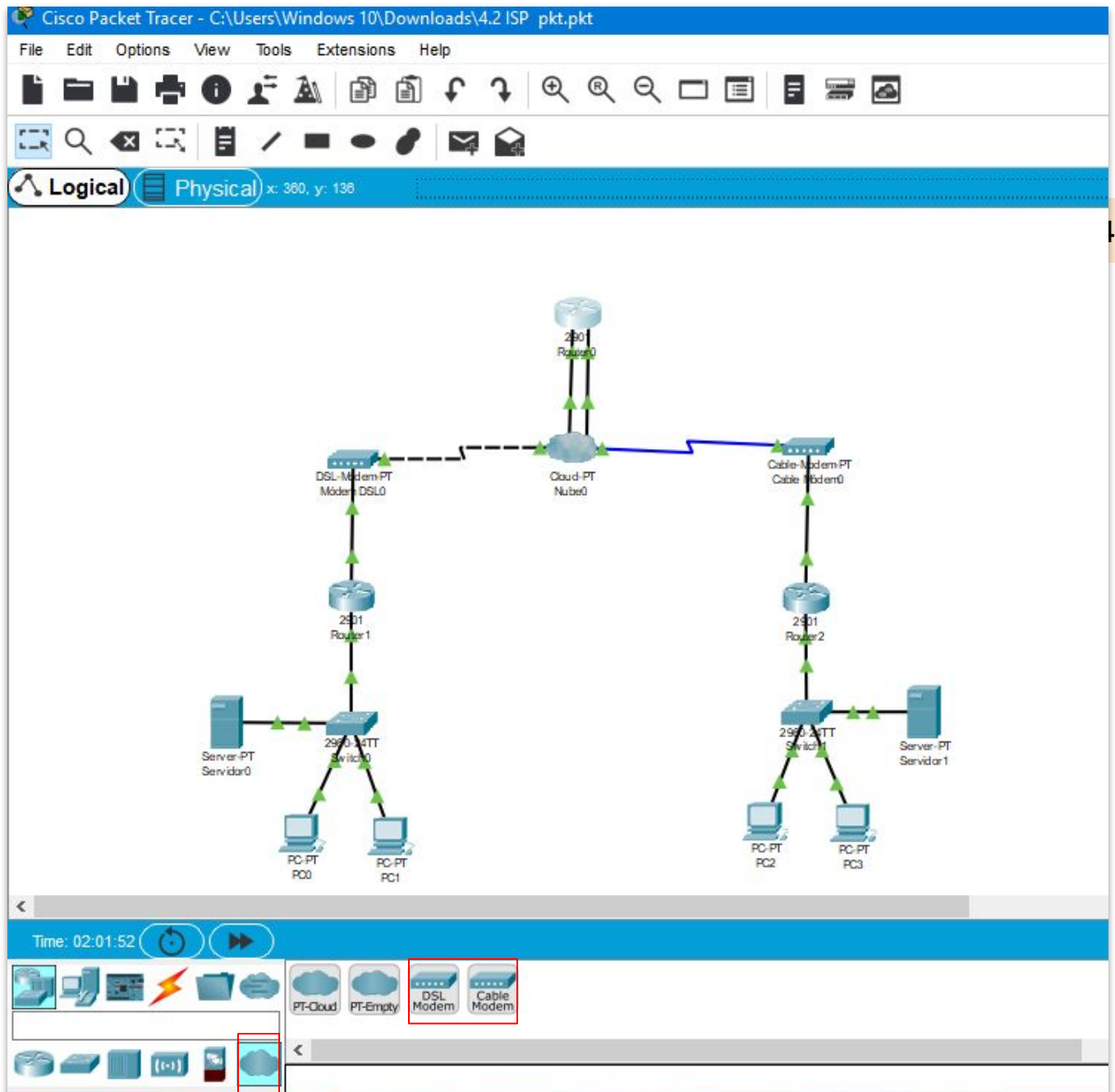


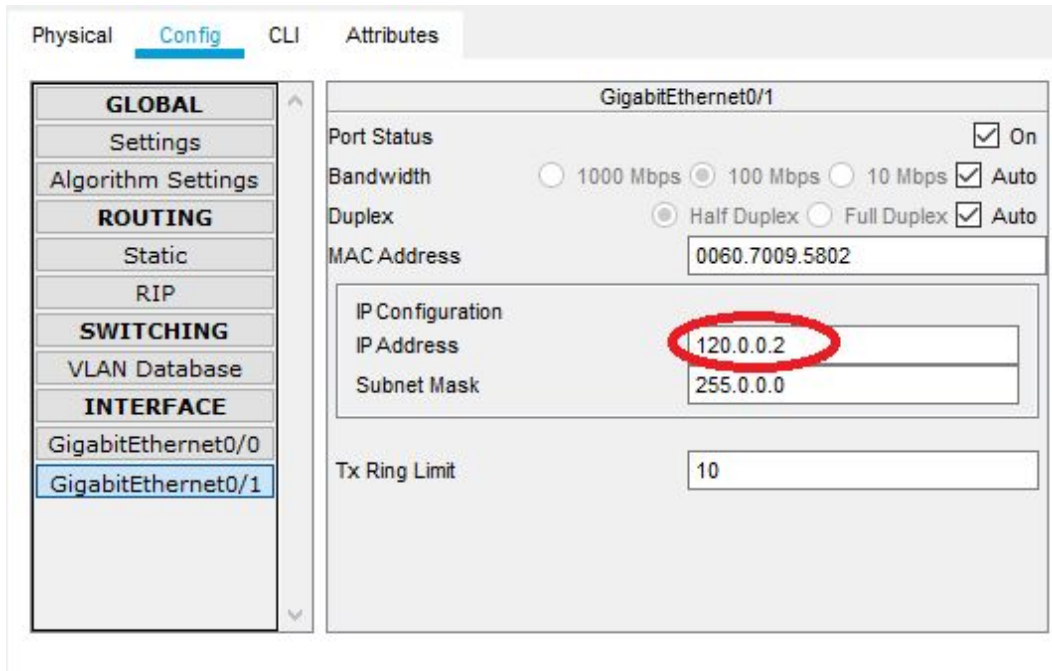
Figura 4.2.i Localización de los módems DSL y de Cable en Packet Tracer

4.2

<APLAFLE>
<VCARLEO>

- Todos los routers se conectarán a la nube mediante una IP pública de clase A
- Internamente, los routers domiciliarios tendrán la IP 192.168.1.1.

En la boca externa que irá conectada al modem de la red de S/C de Tenerife ponemos la ip de clase A 120.0.0.1 y en la que irá conectada al modem de la red de Las Palmas de GC.



4.2

Figura 4.2.x. Ejemplo IP de Red Exterior.

Ponemos en las bocas internas de los routers de cada red S/C de Tenerife y Las Palmas de GC, la IP 192.168.1.1.

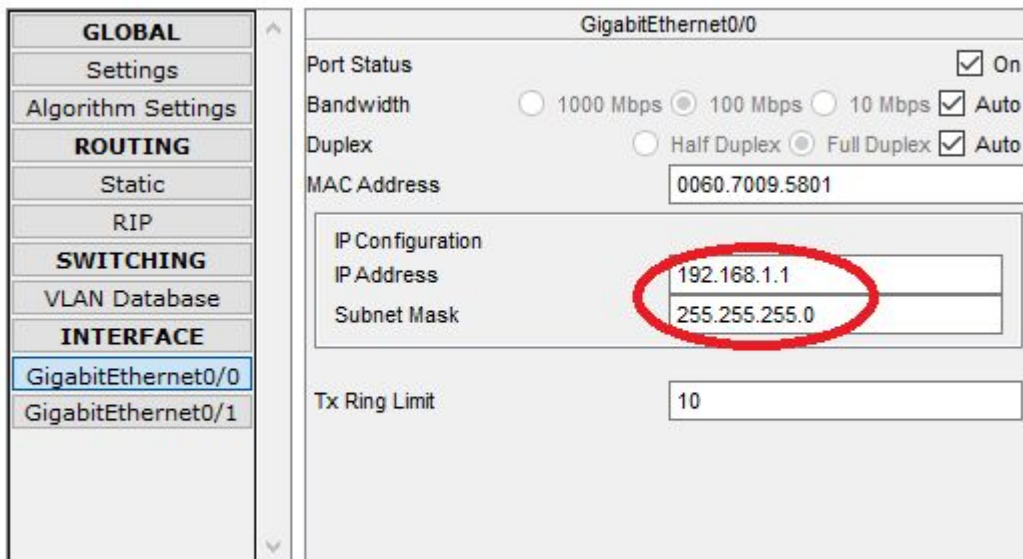
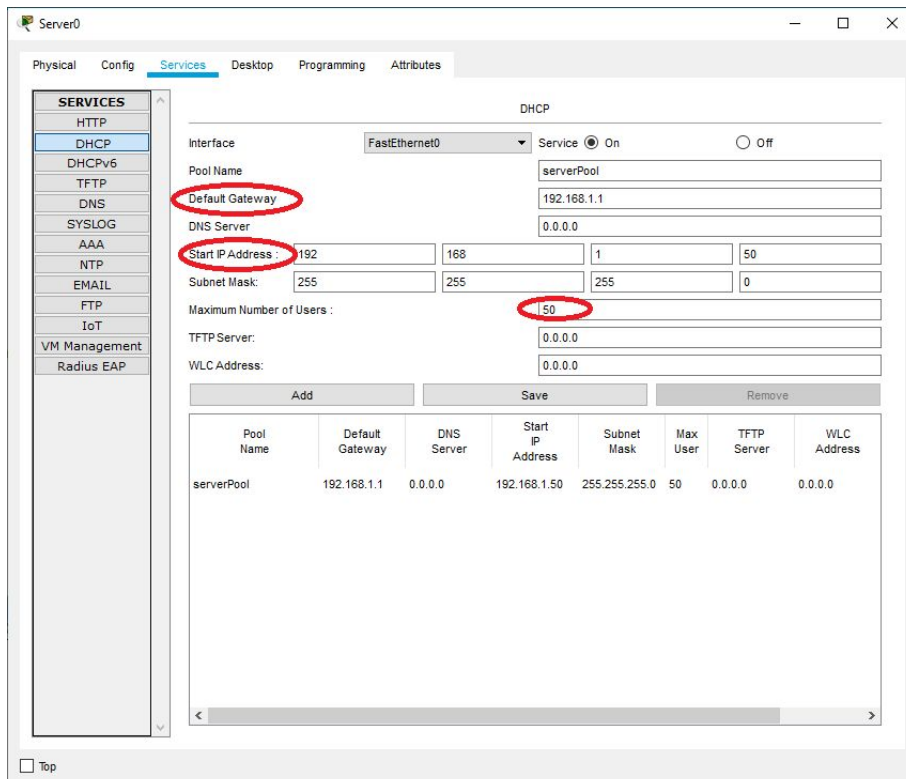


Figura 4.2.x. Ejemplo IP de Red Interior.

- A nivel domiciliario, conectaremos varios PC por DHCP
- Situar dentro de cada domicilio un servidor DHCP con las siguientes características – IP: 192.168.1.2 – Dirección IP de inicio para DHCP: 192.168.1.50 – Número máximo de equipos: 50

En cada uno de las redes conectamos los Pc mediante DHCP con las siguiente configuración:
 IP: 192.168.1.2 – Dirección IP de inicio para DHCP: 192.168.1.50 – Número máx de equipos: 50



4.2

Figura 4.2.x. Configuración Servidor DHCP.

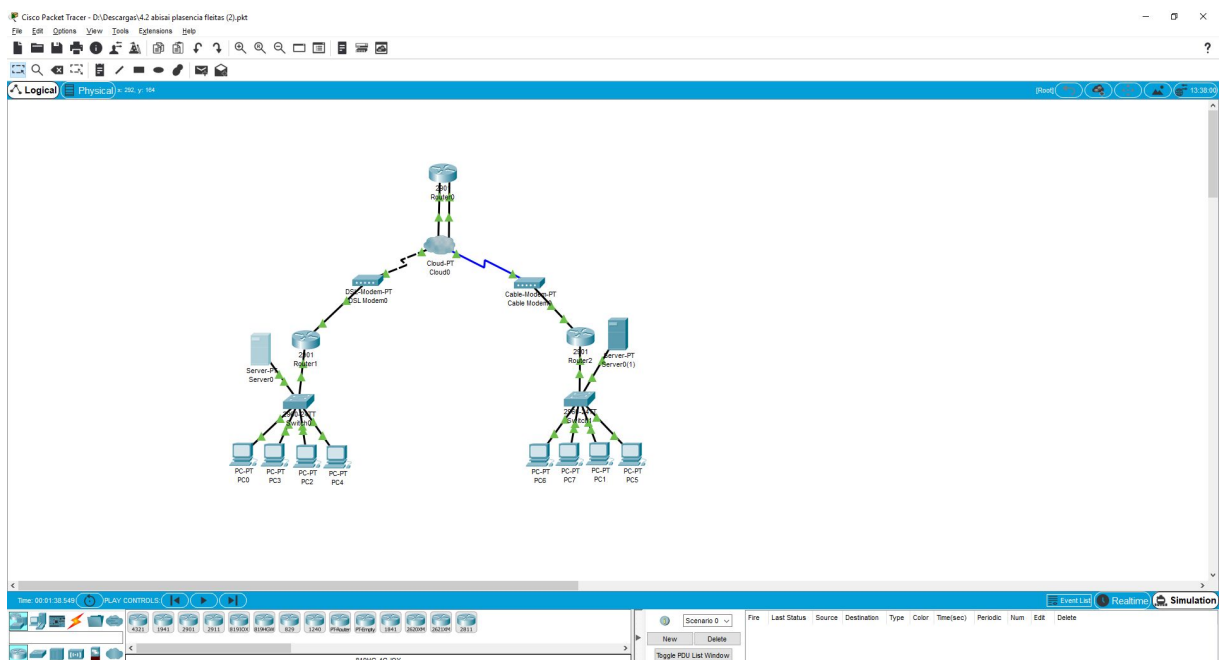


Figura 4.2.x. Topología finalizada

- Probar que hay conectividad entre cualquiera de los routers de abonado entre sí y con el ISP

Finalmente comprobaremos que la topología esté correctamente configurada para ello usaremos la herramienta complex PDU en ella rellenamos los datos de la siguiente manera, en IP ponemos la IP a la que queremos ir en este caso 121.0.0.2, en sequence number ponemos y finalmente en One shot y ponemos 0 los demás campos los dejamos por defecto.

4.2

Figura 4.2.x. Herramienta Complex PDU

Finalmente en este GIF se demuestra como los routers de abonados tienen conexión entre sí y que los equipos de cada red tienen conexión con el ISP pero no al revés porque no está NAT configurado.

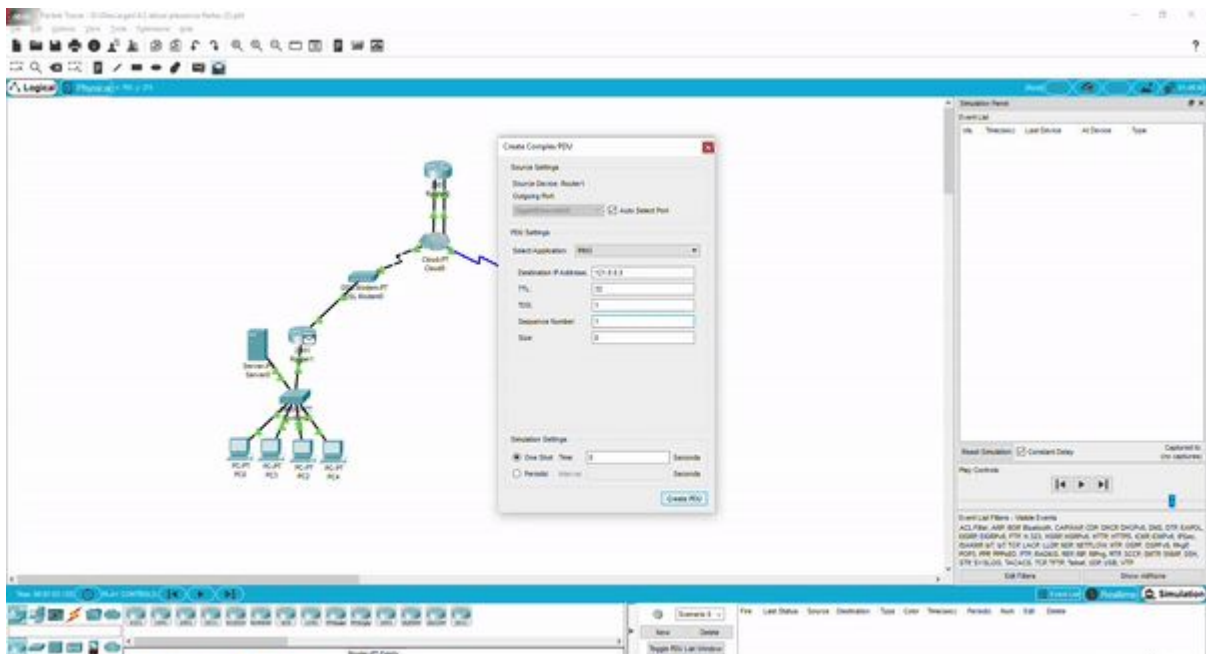
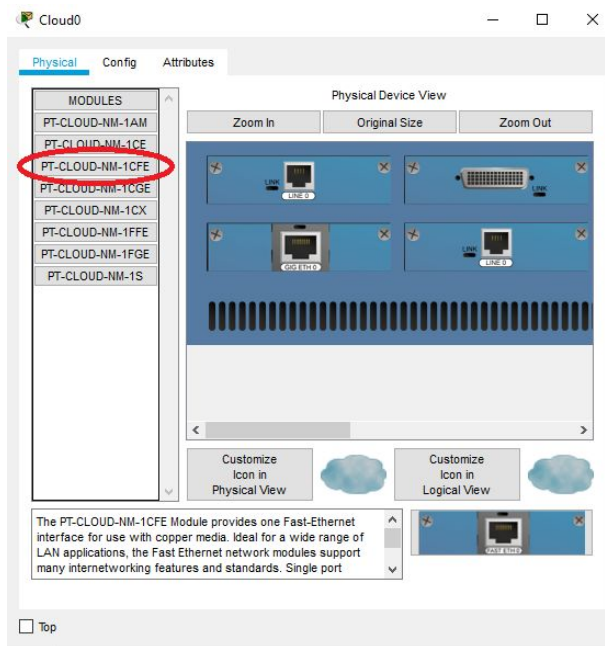


Figura 4.2.x. GIF comprobación de la red

- Recuerda que: – El módem de SCTF debe conectarse mediante cable telefónico – El módem de LPGC debe conectarse mediante cable coaxial – Realiza la conexión en la nube de los módems al router del ISP.

La conexión del módem de S/C de Tenerife se hará mediante cable telefónico y la de las Palmas de GC por cable coaxial. para ello en la nube necesitaremos conectar una tarjeta para dar cobertura al módem con cable en concreto usaremos la PT-CLOUD-NM-CFE.



4.2

Figura 4.2.x. Conexión de tarjeta PT-CLOUD-NM-CFE

Recordemos que para el módem de telefonía debemos usar cable telefónico  y para el módem de cable debemos usar cable coaxial 

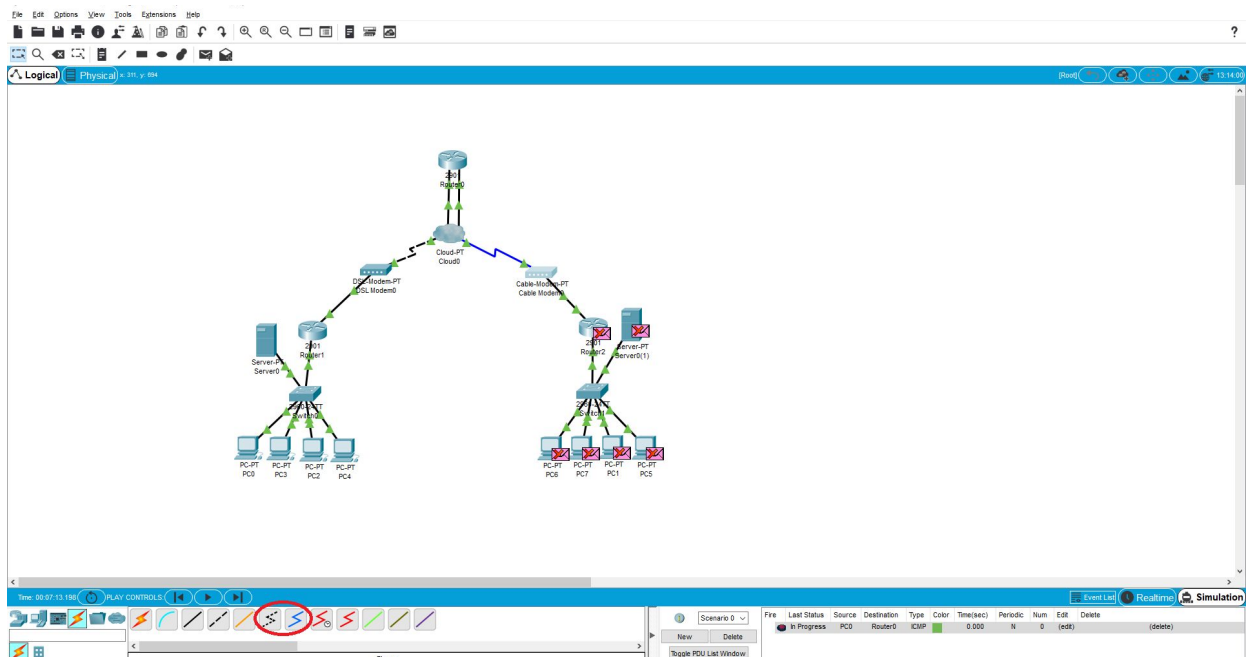


Figura 4.2.x. Botón para cable telefónico/coaxial en packet tracer

Trabajo 4.3
Simulación de conexión ISP - cable
y xDSL utilizando NAT



Trabajo 4.3. Simulación de conexión ISP - cable y xDSL utilizando NAT

- Partimos de la red anterior.
- Hay conectividad desde los PC de SCTF/LPGC hacia el ISP pero **NO** a la inversa.
- El ISP **NO** puede responder a un paquete cuya IP es 192.168.1.51.
- Nos falta configurar NAT para que se complete la conectividad.
- Los PCs de cada domicilio usarán la IP pública de su router.

Partiendo de la red anterior, configurar NAT para que se complete la conectividad. Los PCs de cada domicilio usarán la IP pública de su router.

- **¿Qué es NAT?**

La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés Network Address Translation), es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

Mientras que el servidor de DHCP asigna direcciones IP dinámicas a los dispositivos que se encuentran dentro de la red, los routers habilitados para NAT retienen una o varias direcciones IP de Internet válidas fuera de la red. Cuando el cliente envía paquetes fuera de la red, NAT traduce la dirección IP interna del cliente a una dirección externa. Para los usuarios externos, todo el tráfico que entra a la red y sale de ella tiene la misma dirección IP o proviene del mismo conjunto de direcciones.

Su uso más común es permitir utilizar direcciones privadas (definidas en el RFC 1918) para acceder a Internet. Existen rangos de direcciones privadas que pueden usarse libremente y en la cantidad que se quiera dentro de una red privada. Si el número de direcciones privadas es muy grande puede usarse solo una parte de direcciones públicas para salir a Internet desde la red privada. De esta manera simultáneamente sólo pueden salir a Internet con una dirección IP tantos equipos como direcciones públicas se hayan contratado. Esto es necesario debido al progresivo agotamiento de las direcciones IPv4. Se espera que con el advenimiento de IPv6 no sea necesario continuar con esta práctica.

Sabiendo qué es NAT, procederemos a finalizar el ejercicio de nuestra red creada anteriormente (**Figura 4.3.A**).

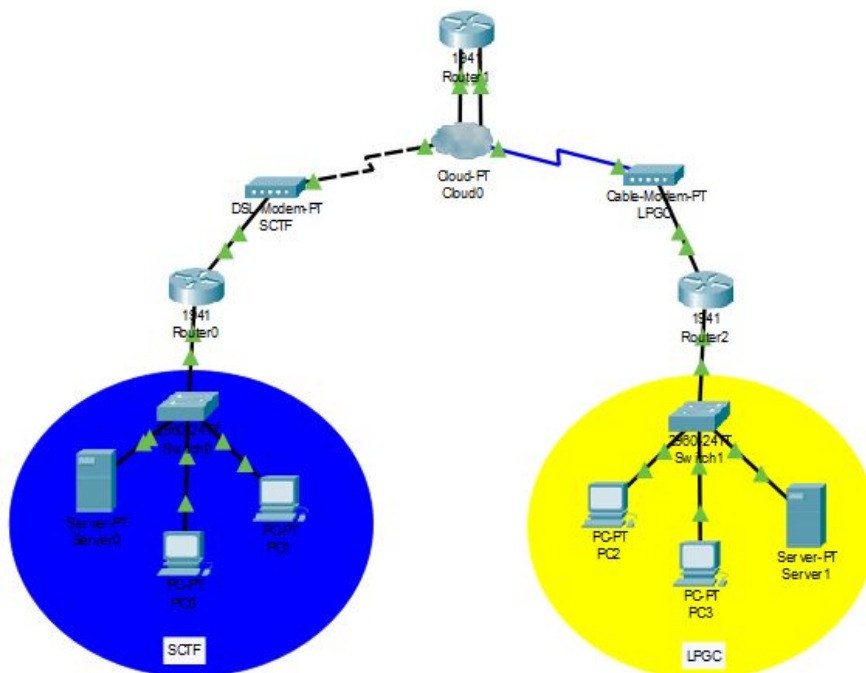


Figura 4.3.A. Red con conexión a ISP.

Para que los paquetes vengan de vuelta desde el ISP a la red debemos configurar el NAT en los router “domésticos”.

Seguiremos los siguientes pasos desde la configuración de la consola de comandos, configurando ambos router de cada delegación.

1º. Definiremos la lista de equipos que podrán salir.

```
“access-list 1 permit 192.168.1.0 0.0.0.255”
```

2º. Declaramos a la lista anterior la interfaz por la que utilizarán PAT.

```
“ip nat inside source list 1 interface GigabitEthernet0/1 overload”
```

3º. Definiremos la IP pública que se va a utilizar.

```
“ip nat pool my_public_ip 120.0.0.1 120.0.0.1 netmask 255.0.0.0”
```

4º. Asociamos la IP pública a la lista de acceso 1.

```
“ip nat inside source list 1 pool my_public_ip overload”
```

5º. Establecemos la interfaz que está en el lado interior de la red.

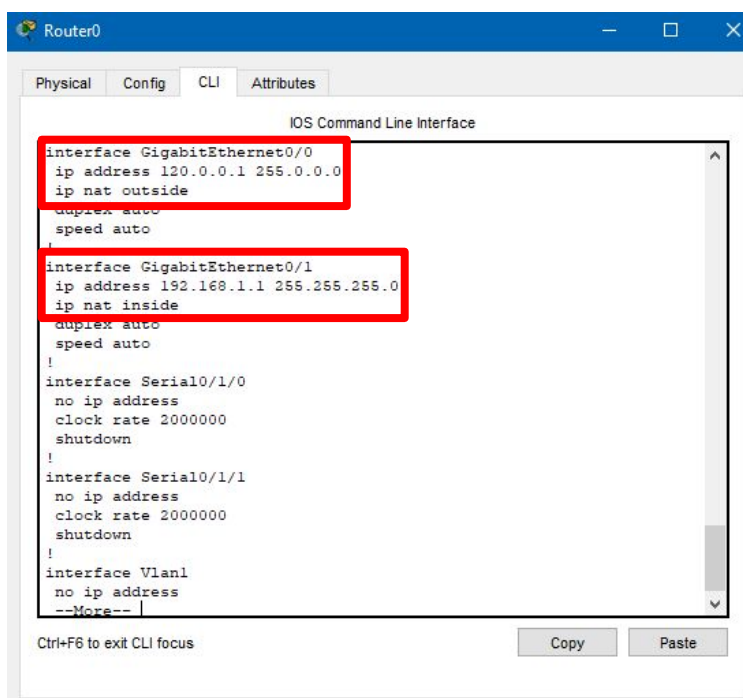
```
(config)#interface GigabitEthernet0/1          *(puerto interno)*
(config-if)#ip nat inside
(config-if)#exit
```

6º. Establecemos la interfaz que está en el lado exterior de la red.

```
(config)#interface GigabitEthernet0/0          *(puerto externo)*
(config-if)#ip nat outside
(config-if)#exit
```

Deberemos repetir el mismo proceso con el otro router, debiendo cambiar la IP pública con la asociada a dicha delegación (121.0.0.1).

Podemos verificar la configuración con el comando “show running-config”.



The screenshot shows the CLI of a router named Router0. The configuration is displayed in the 'IOS Command Line Interface' window. Two sections are highlighted with red boxes:

```
interface GigabitEthernet0/0
ip address 120.0.0.1 255.0.0.0
ip nat outside
duplex auto
speed auto
!

interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
```

The rest of the configuration includes Serial10/1/0 and Serial10/1/1 interfaces (both with no IP address, clock rate 2000000, and shutdown) and a Vlan1 interface (with no IP address). The window also shows 'Ctrl+F6 to exit CLI focus', 'Copy', and 'Paste' buttons.

Figura 4.3.B. Puertos del router de SCTF configurados con NAT.

Por último, con el comando “show ip nat translations” podemos observar la tabla de traducción de NAT, mientras que con el comando “clear ip nat translation” podremos borrar la tabla de traducción de NAT.

```
Router#show ip nat translations
Pro Inside global      Inside local      Outside local     Outside global
icmp 121.0.0.1:1      192.168.1.50:1   120.0.0.1:1      120.0.0.1:1
icmp 121.0.0.1:13     192.168.1.51:13  120.0.0.1:13     120.0.0.1:13

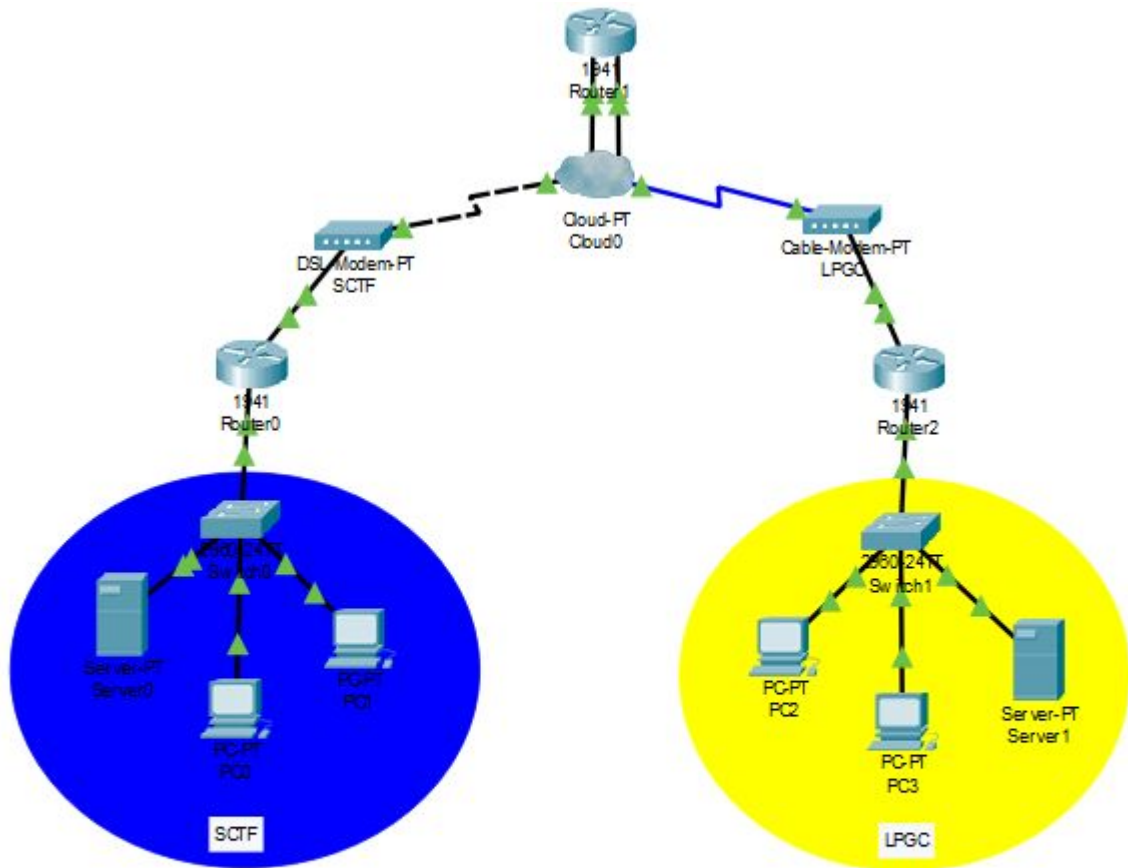
Router#clear ip nat trans
Router#clear ip nat translation *
Router#show ip nat translation
Router#
```

Figura 4.3.C. Tabla de traducción NAT y borrado de la misma.

Cisco define estos términos como:

- **Inside local address:** la dirección IP asignada a un host en la red interna. Esta es la dirección configurada como un parámetro del sistema operativo de la computadora o recibida a través de protocolos de asignación de direcciones dinámicas, como DHCP. Es probable que la dirección no sea una dirección IP legítima asignada por el Centro de información de red (NIC) o el proveedor de servicios.
- **Inside global address:** una dirección IP legítima asignada por la NIC o el proveedor de servicios que representa una o más direcciones IP locales dentro del mundo exterior.
- **Outside local address:** la dirección IP de un host externo tal como aparece en la red interna. No necesariamente una dirección legítima, se asigna desde un espacio de direcciones enrutable en el interior.
- **Outside global address:** la dirección IP asignada a un host en la red externa por el propietario del host. La dirección se asigna desde una dirección enrutable globalmente o espacio de red.

Con la imagen adjuntada (**Figura 4.3.D**), podemos ver como se ha efectuado correctamente un ping entre un PC de Santa Cruz de Tenerife (SCTF) y Las Palmas de Gran Canaria (LPGC), y entre el mismo PC de SCTF y el ISP.



4.3

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC1	PC2	ICMP	Blue	0.000	N	0	(edit)
	Successful	PC1	Router1	ICMP	Green	0.000	N	1	(edit)

Figura 4.3.D. Pings exitosos SCTF - LPGC + SCTF - ISP.

*Trabajo 5.1.
Puesta en servicios de redes.
Protocolos de enrutamiento:
RIP, OSPF, IS-IS, EIGRP*



Trabajo 5.1. Puesta en servicio de redes. Protocolos dinámicos

1. Configuración básica de OSPF
2. OSPF. Ciclos y ruta más corta
3. RIP básico
4. RIP con bucles
5. OSPF con diferentes enlaces. Comando bandwidth
6. OSPF con diferentes enlaces. Consultar tabla de ruteo
7. OSPF con diferentes enlaces. Comprobar ancho de banda
8. Eliminar restricciones de ancho de banda
9. Comprobar de bandwidth NO tiene efecto en RIP
10. Forzando una ruta en RIP y en OSPF
11. Ruta estática de último recurso

Añadido 1. Red con EIGRP

Añade a tu diseño PT una tercera red configurada con EIGRP. Incluye en tu memoria cómo se configura e incluye pruebas y evidencias de su correcto funcionamiento.

Añadido 2. Red con IS-IS y con IGRP

Se trata de dos protocolos que supuestamente NO soporta PT. Si consigues configurarlos, Procede como en el extra anterior

Por el contrario, si no consigues configurarlos, incluye en tu memoria pruebas y evidencias fiables que demuestren que no se puede realizar.

Añadido 3. Macro-red con múltiples algoritmos de ruteo

Crea una macro red en la que convivan RIP, EIGRP y OSPF

Así, algunos routers estarán configurados con RIP, otros con EIGRP y otros con OSPF

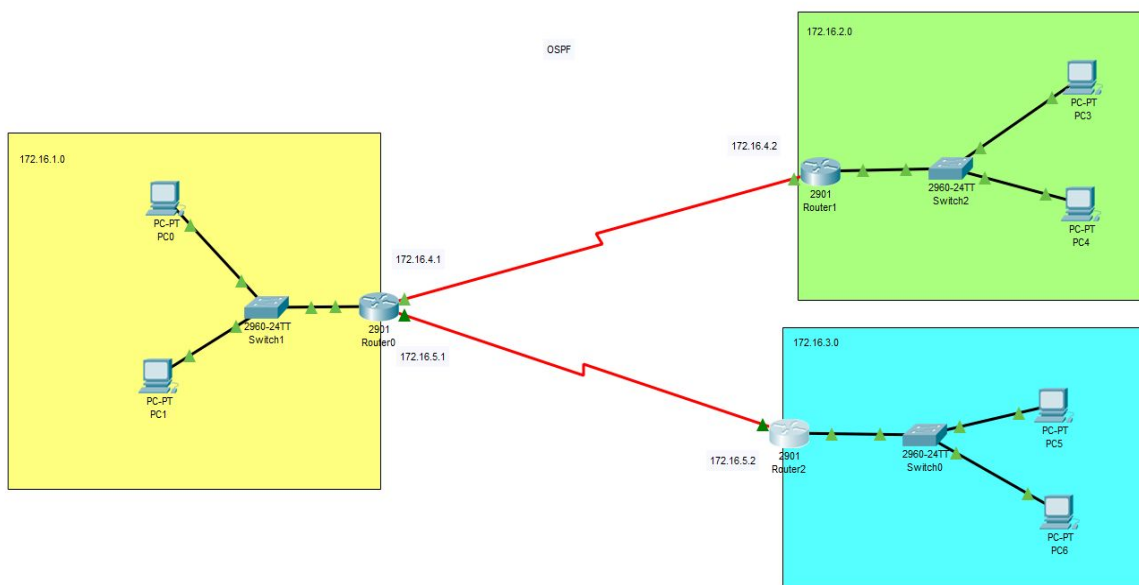
Mostrar la tabla de enrutamiento y explicar/razonar las rutas y la distancia administrativa

Añadido 4. Modificar la frecuencia con la que se envían los mensajes Hello

1. Configuración básica de OSPF

Open Shortest Path First (OSPF), Primer Camino Más Corto, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

Montamos la red. Fig 5.1.1a



5.1.1

Figura 5.1.1.a Topología de la red

A continuación entraremos en la CLI de los router y configuraremos OSPF. Para ello pondremos los siguientes comandos: Fig 5.1.1.b

```
Router>enable
Router #configure terminal
Router(config)#router ospf 1
Switch(config-router)#network 0.0.0.0 255.255.255.255 area 0
```

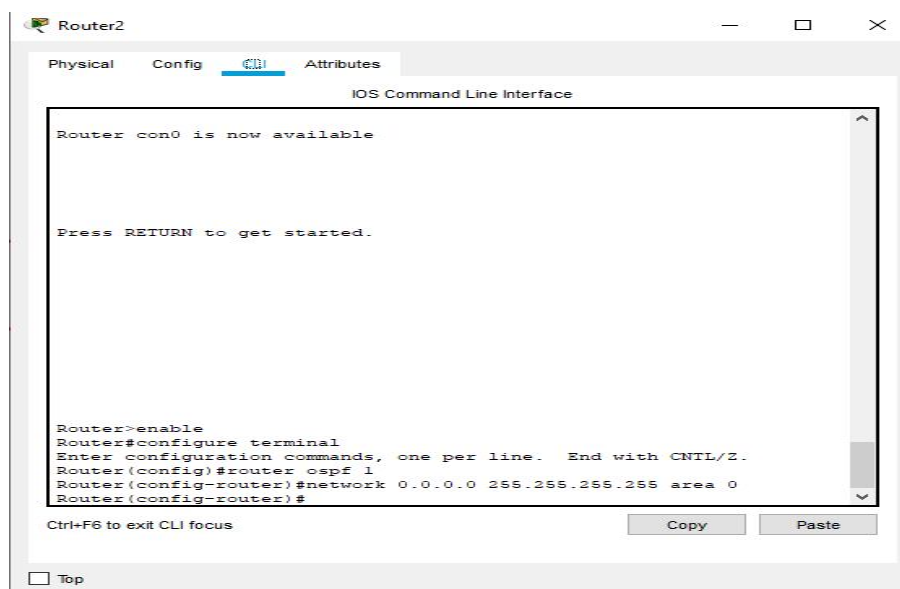
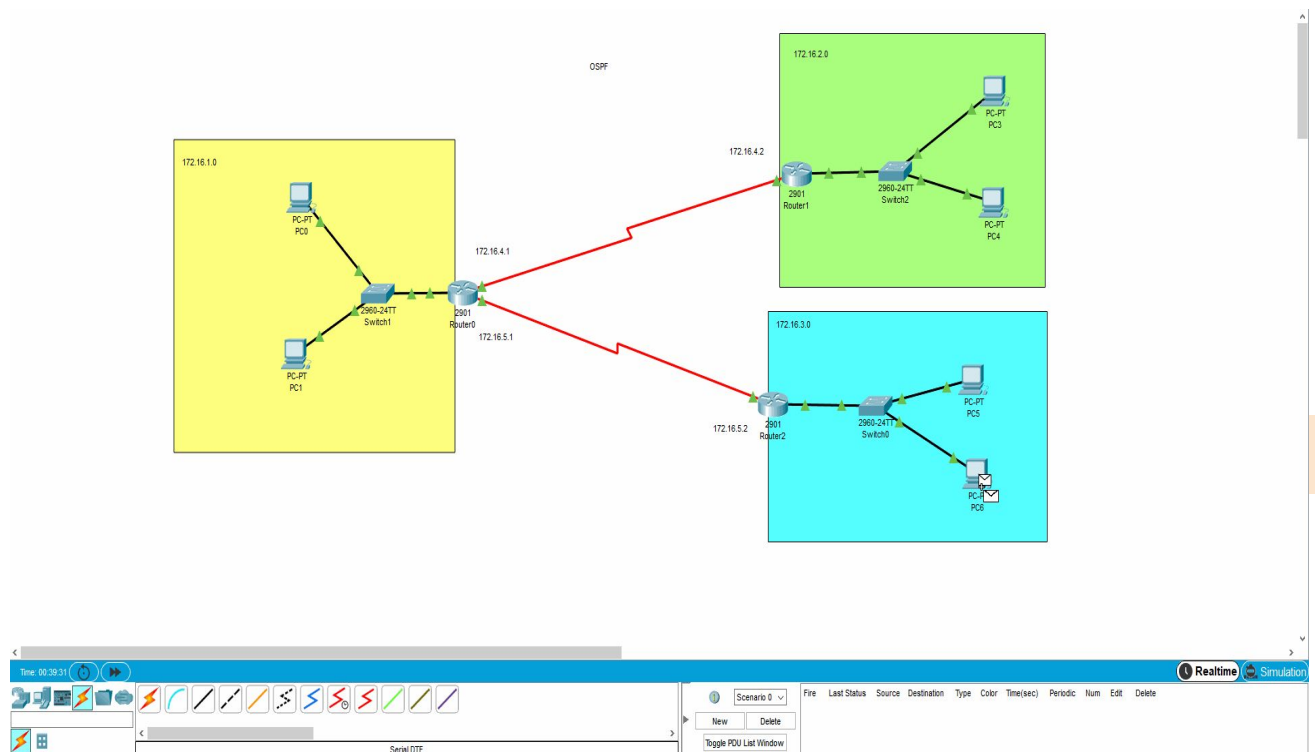


Figura 5.1.1.b Configurando OSPF

Ahora comprobamos que funciona la configuración realizando pings entre PC de distinto router
Fig.5.1.1.c

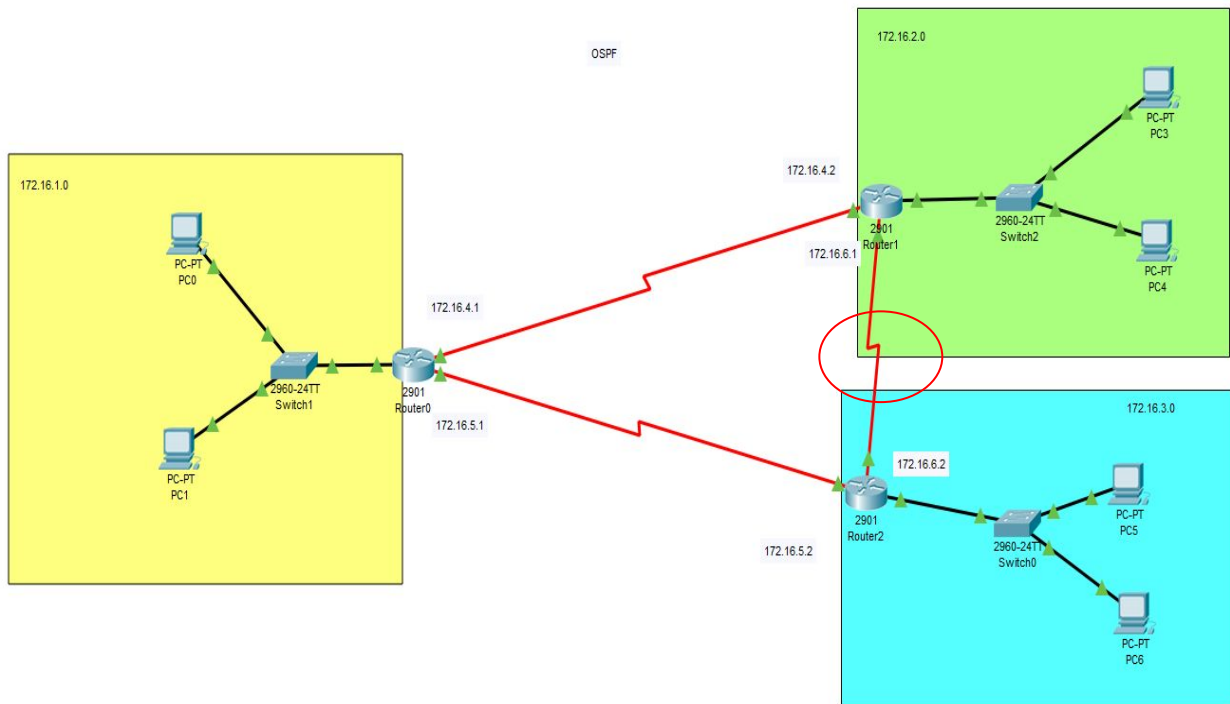


5.1.1

Figura 5.1.1.c Comprobando OSPF

2. OSPF. Ciclos y ruta más corta

En este apartado colocamos un nuevo enlace que unirá la red verde con la azul, con el objetivo de comprobar que OSPF al no existir una diferencia entre los enlaces escogerá la ruta que menos saltos deba pasar. Fig. 5.1.2.a



5.1.2

Figura 5.1.2.a Red con nuevo enlace

Comprobamos que escoge la ruta con menos saltos. Fig 5.1.2.b

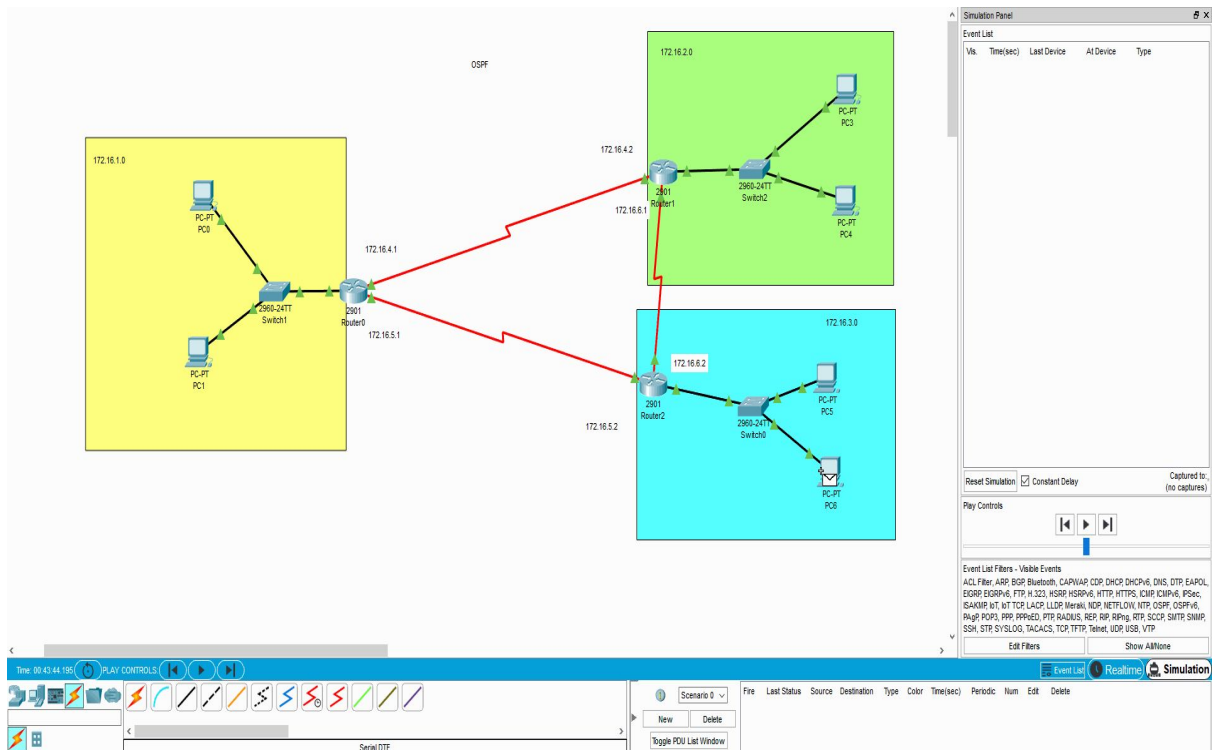
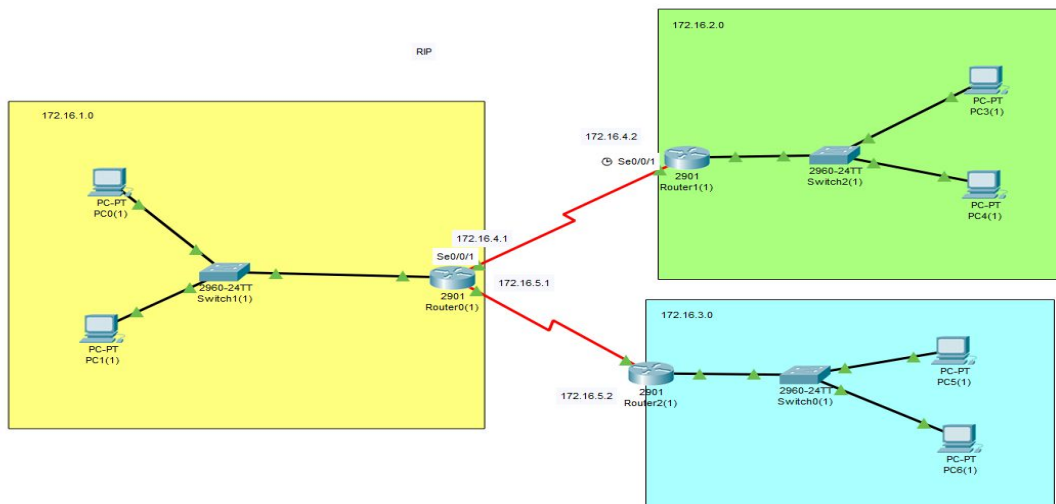


Figura 5.1.2.b Comprobando OSPF

3. RIP básico

Establecemos la red para a continuación configurar RIP en los routers. Fig 5.1.3.a



5.1.3

Figura 5.1.3.a Topología de la red

Entramos en la configuración de los router y entramos al apartado RIP y establecemos la red a la que pertenece. Con ello los router sabrán a la red que pertenecen y podrán generar su tabla de ruteo. Fig 5.1.3.b

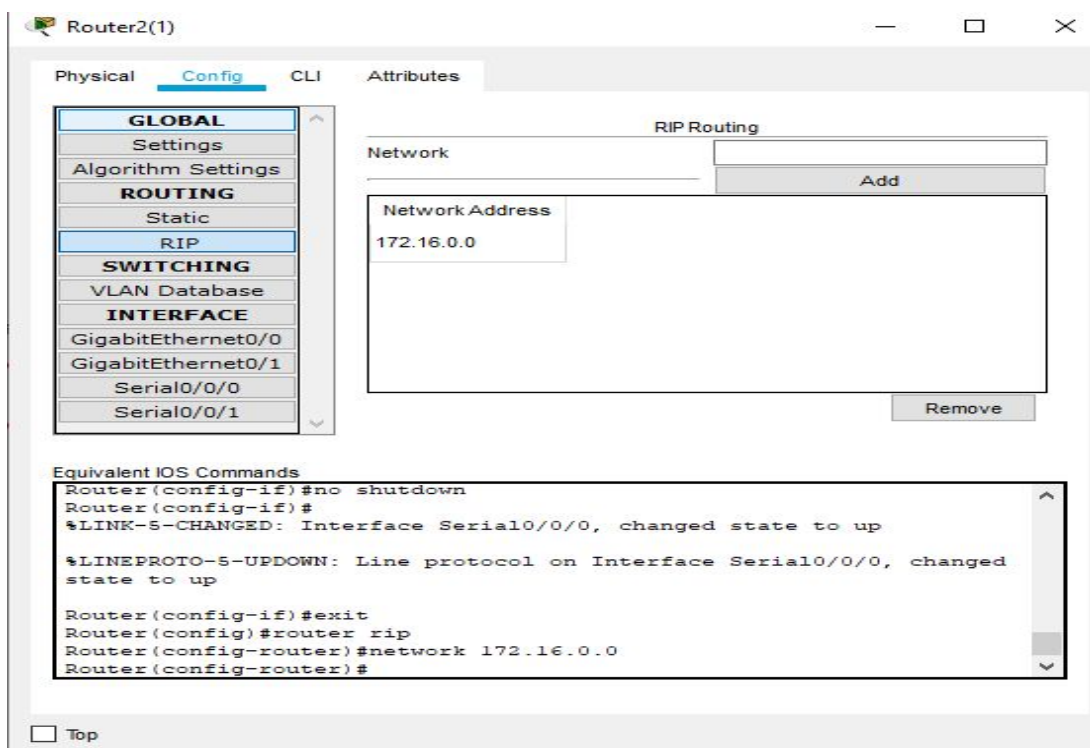
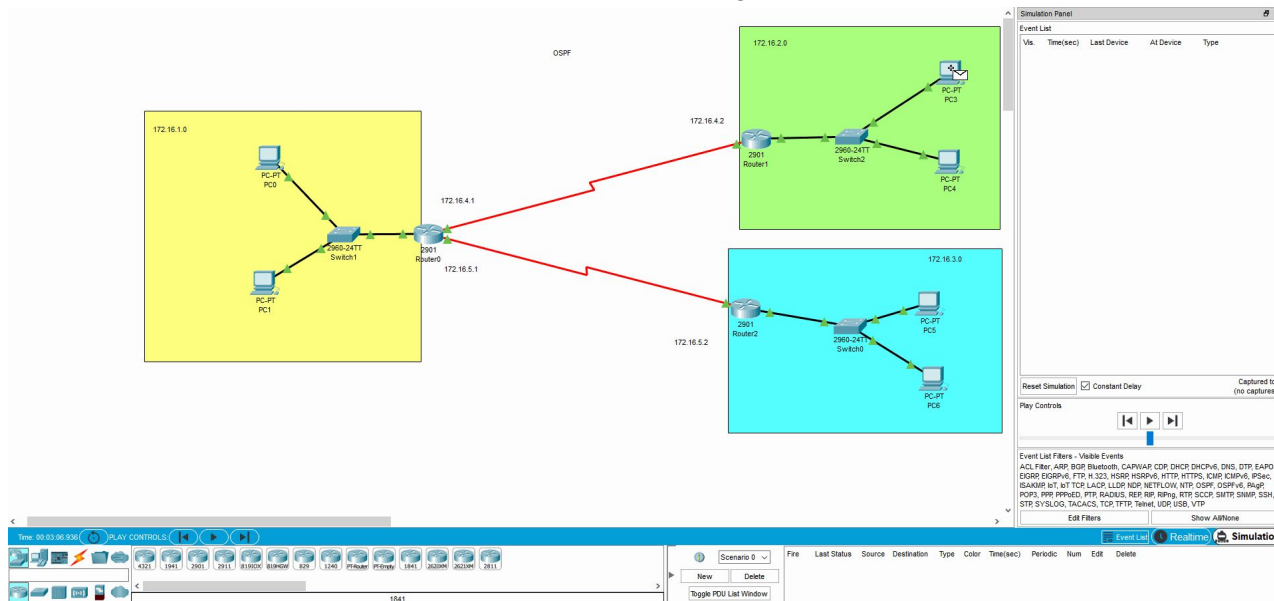


Figura 5.1.3.b Configurando RIP

Comprobamos el correcto funcionamiento de la red. Fig 5.1.3.c

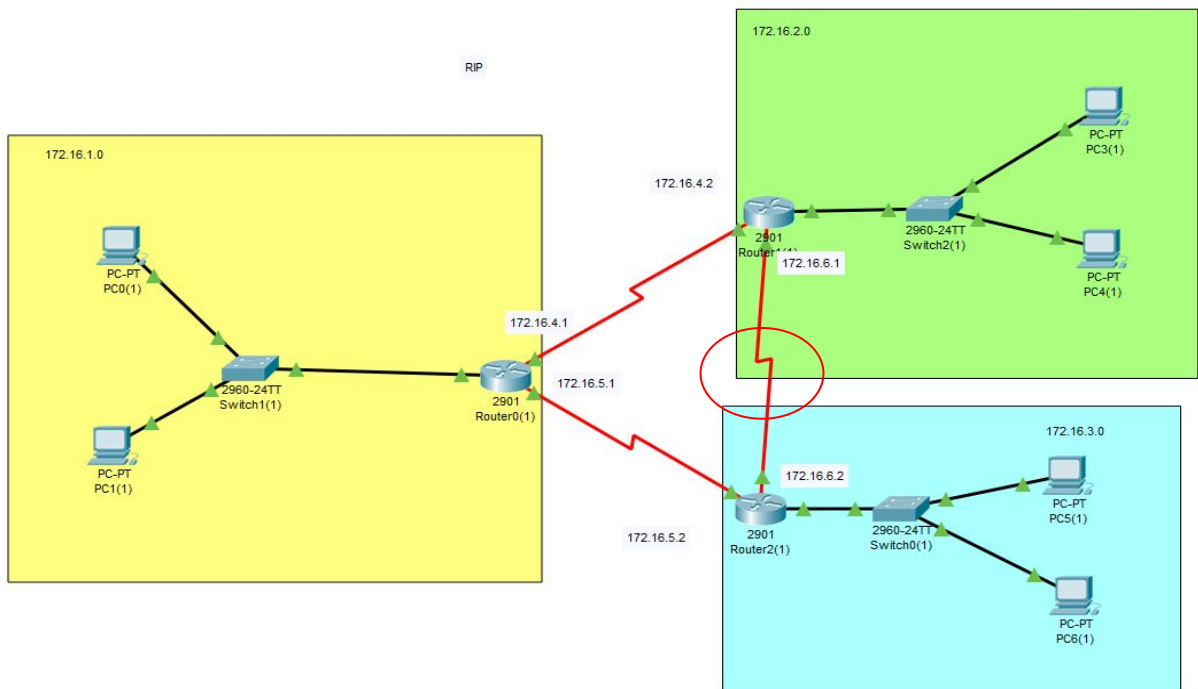


5.1.3

Figura 5.1.3.c Comprobando funcionamiento RIP

4. RIP con bucles

Creamos un nuevo enlace para comprobar si la red sigue funcionando y cómo actúa RIP. Fig 5.1.4.a



5.1.4

Figura 5.1.4.a Conectando un nuevo enlace

Una vez creamos el nuevo enlace entre la red verde y azul comprobamos como RIP utiliza la nueva ruta para enviar paquetes entre estas redes. Fig.5.1.4.b

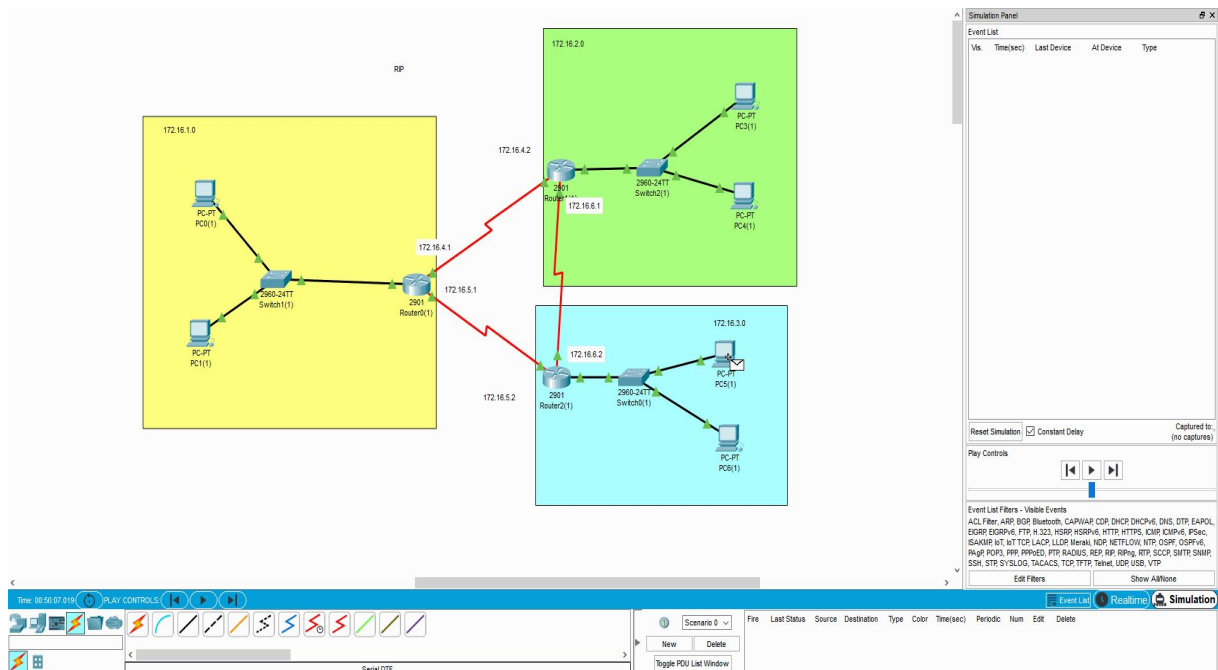


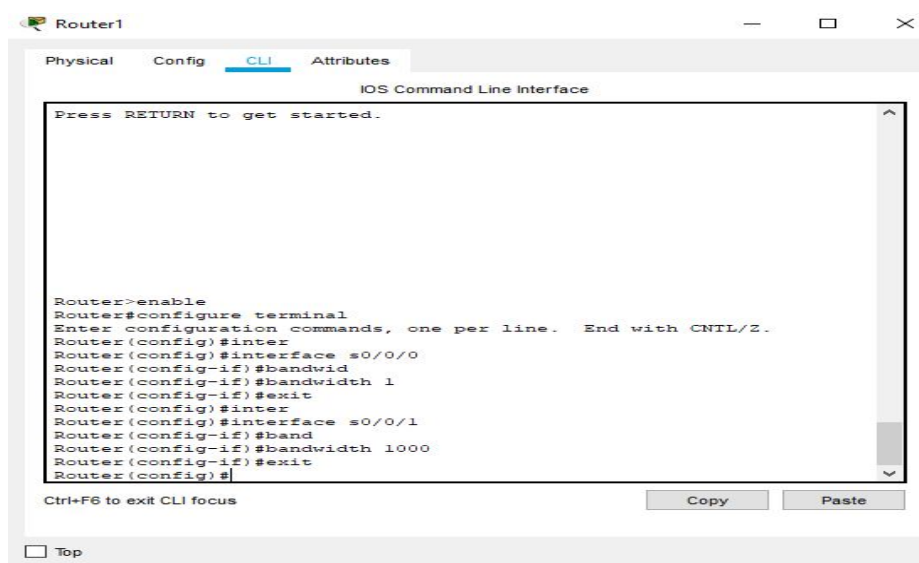
Figura 5.1.4.b Comprobando la ruta de RIP

5. OSPF con diferentes enlaces. Comando bandwidth

En este apartado comprobaremos como OSPF siempre elegirá la ruta con las mejores características par enviar el paquete para ello reducimos el ancho de banda que pasa por una boca del enlace con el comando "Bandwidth"

El comando Bandwidth nos permite establecer el valor de ancho de banda real para los enlaces seriales. Cambiaremos el ancho de banda de la boca del router 1 (zona verde) que conecta directamente con la red azul en este caso la serial 0/0/0 con la velocidad mínima. Y en el serial 0/0/1 pondremos mayor velocidad y el paquete debería usar esta vía para ir de la red verde a la azul y volver por el enlace corto.

Entramos en la interfaz de los seriales y escribiremos bandwidth y el valor que deseemos. Poniendo 1 estableceremos 1Kbp/s y con 1000 - 1Mb/s. Fig 5.1.5.a



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#inter
Router(config)#interface s0/0/0
Router(config-if)#bandwidth
Router(config-if)#bandwidth 1
Router(config-if)#exit
Router(config)#inter
Router(config)#interface s0/0/1
Router(config-if)#band
Router(config-if)#bandwidth 1000
Router(config-if)#exit
Router(config)#
```

5.1.5

Figura 5.1.5.a Cambiando el ancho de banda de los seriales

Ahora comprobamos que el paquete enviado de verde a azul escoge la ruta que se nombró anteriormente.

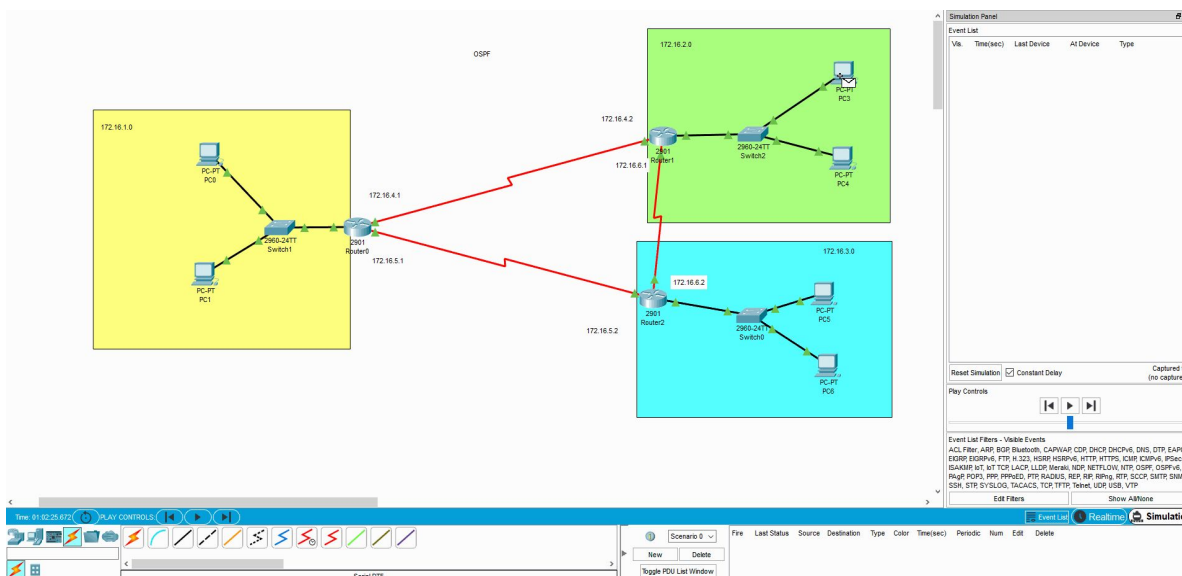
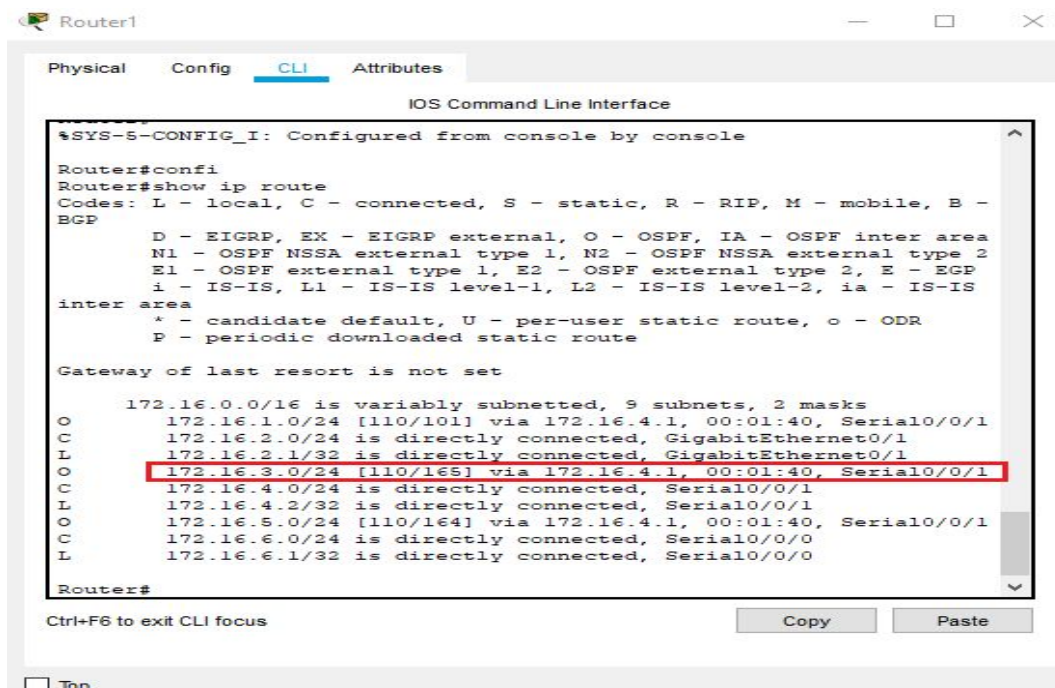


Figura 5.1.5.b Comprobando la ruta de OSPF con los cambios de ancho de banda.

<IMARMEN>
<JACOGON>

6. OSPF con diferentes enlaces. Consultar tabla de ruteo

Para consultar la tabla de ruteo utilizaremos el comando "show ip route". Con este podremos comprobar las rutas que siguió el paquete en el apartado anterior. Para el router 1 (zona verde) la ruta para ir a la zona azul se observa cómo utiliza la ruta hacia el router 0. Fig.5.1.6.a

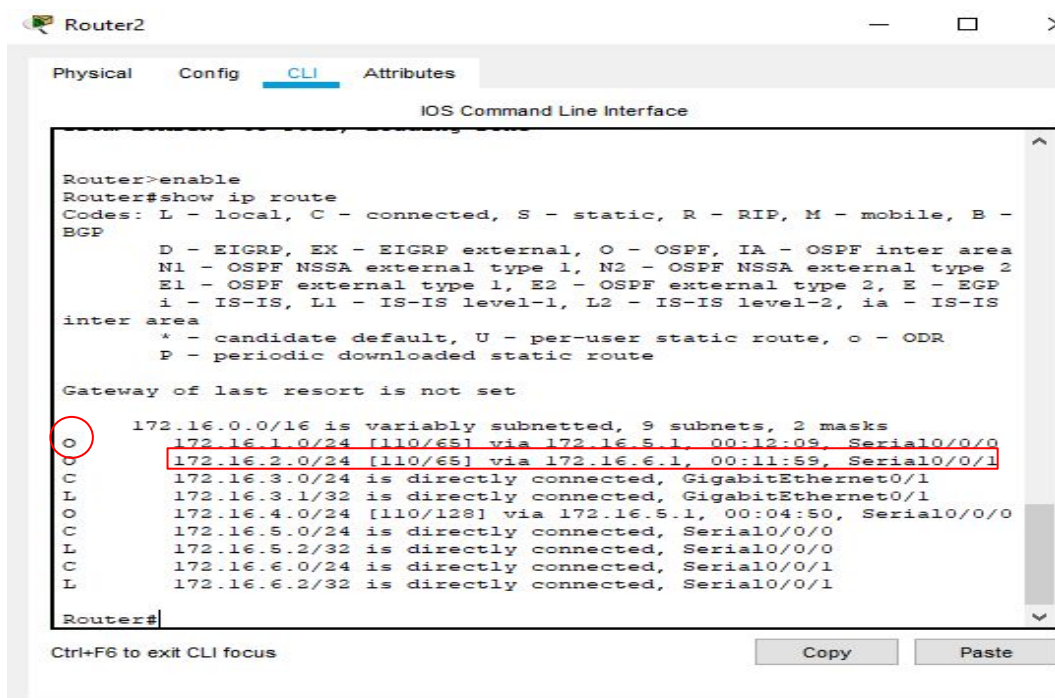


```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
%SYS-5-CONFIG_I: Configured from console by console
Router#confi
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 9 subnets, 2 masks
O 172.16.1.0/24 [110/101] via 172.16.4.1, 00:01:40, Serial0/0/1
C 172.16.2.0/24 is directly connected, GigabitEthernet0/1
L 172.16.2.1/32 is directly connected, GigabitEthernet0/1
O 172.16.3.0/24 [110/165] via 172.16.4.1, 00:01:40, Serial0/0/1
C 172.16.4.0/24 is directly connected, Serial0/0/1
L 172.16.4.2/32 is directly connected, Serial0/0/1
O 172.16.5.0/24 [110/164] via 172.16.4.1, 00:01:40, Serial0/0/1
C 172.16.6.0/24 is directly connected, Serial0/0/0
L 172.16.6.1/32 is directly connected, Serial0/0/0
Router#
```

5.1.6

Figura 5.1.6.a Comprobando la ruta Router 1

A continuación se muestra la tabla de ruteo del router 3 (zona azul) el cual no cambiamos el bandwidth y la ruta establecida para ir a la zona verde es vía el enlace directo entre ellas. Además a la izquierda de esta ruta se ve una letra O que identifica que se estableció siguiendo el protocolo OSPF. Fig 5.1.6.b



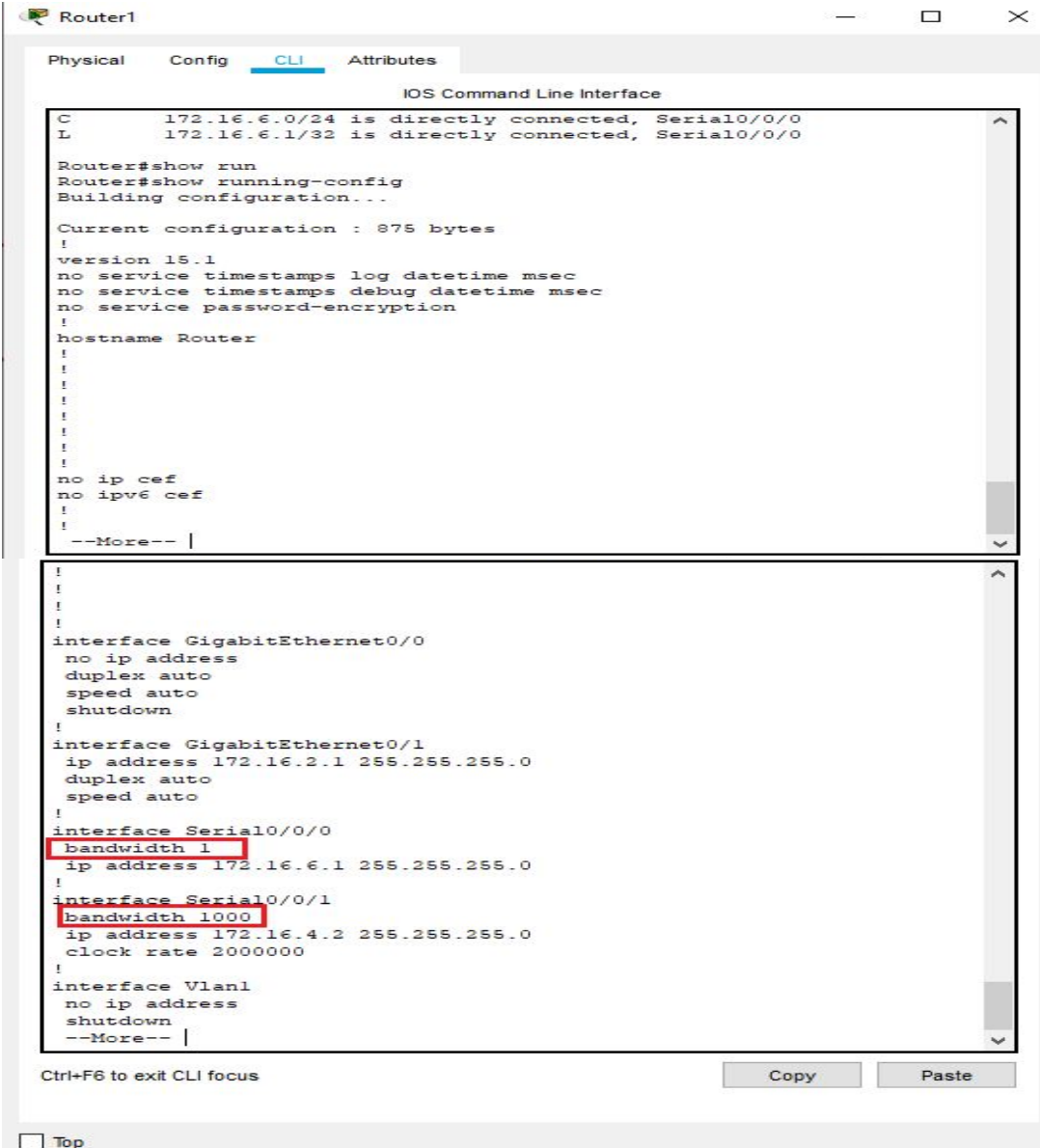
```
Router2
Physical Config CLI Attributes
IOS Command Line Interface
Router>enable
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
O 172.16.0.0/16 is variably subnetted, 9 subnets, 2 masks
O 172.16.1.0/24 [110/65] via 172.16.5.1, 00:12:09, Serial0/0/0
O 172.16.2.0/24 [110/65] via 172.16.6.1, 00:11:59, Serial0/0/1
C 172.16.3.0/24 is directly connected, GigabitEthernet0/1
L 172.16.3.1/32 is directly connected, GigabitEthernet0/1
O 172.16.4.0/24 [110/128] via 172.16.5.1, 00:04:50, Serial0/0/0
C 172.16.5.0/24 is directly connected, Serial0/0/0
L 172.16.5.2/32 is directly connected, Serial0/0/0
C 172.16.6.0/24 is directly connected, Serial0/0/1
L 172.16.6.2/32 is directly connected, Serial0/0/1
Router#
```

Figura 5.1.6.b Comprobando la ruta Router 2

7. OSPF con diferentes enlaces. Comprobar ancho de banda

En este apartado comprobaremos los cambios en los anchos de banda de las bocas seriales de los routers de los apartados anteriores. Para ello utilizamos el comando "show running-config" y cuando lleguemos a la información de las bocas seriales aparecerán sus anchos de banda.

Como solo realizamos cambios en el router 1 haremos la comprobación en este. Fig 5.1.7



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
C 172.16.6.0/24 is directly connected, Serial0/0/0
L 172.16.6.1/32 is directly connected, Serial0/0/0

Router#show run
Router#show running-config
Building configuration...

Current configuration : 875 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
--More-- |

!
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
ip address 172.16.2.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
bandwidth 1
ip address 172.16.6.1 255.255.255.0
!
interface Serial0/0/1
bandwidth 1000
ip address 172.16.4.2 255.255.255.0
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
--More-- |

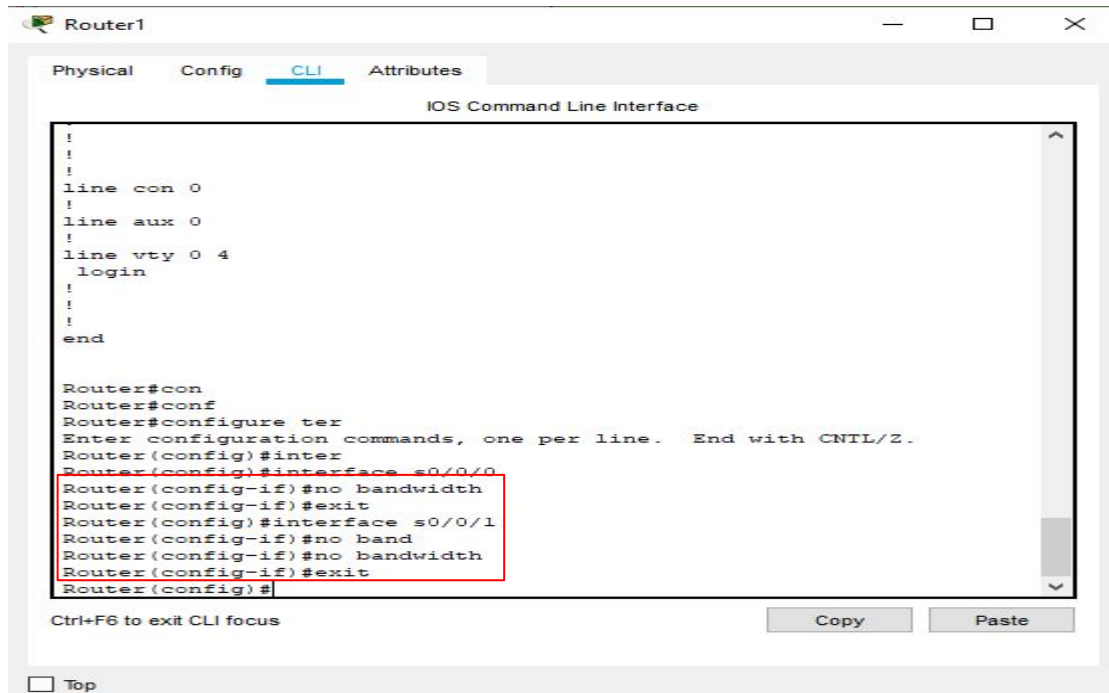
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

5.1.7

Figura 5.1.7 Comprobando los nuevos anchos de banda

8. Eliminar restricciones de ancho de banda

Para eliminar las restricciones de ancho de banda basta con ir al router afectado entrar en sus bocas y como en muchos comandos de Cisco Packet Tracer escribimos el comando que queremos revocar y antes de este ponemos no. En este caso quedaría "no bandwidth" Fig 5.1.8.a



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end

Router#con
Router#conf
Router#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#inter
Router(config)#interface s0/0/0
Router(config-if)#no bandwidth
Router(config-if)#exit
Router(config)#interface s0/0/1
Router(config-if)#no band
Router(config-if)#no bandwidth
Router(config-if)#exit
Router(config)#
```

5.1.8

Figura 5.1.8.a Eliminando restricciones de anchos de banda

Quedaría comprobar que al eliminar las restricciones los paquetes utilizan las rutas de antes de las modificaciones. Fig.5.1.8.b

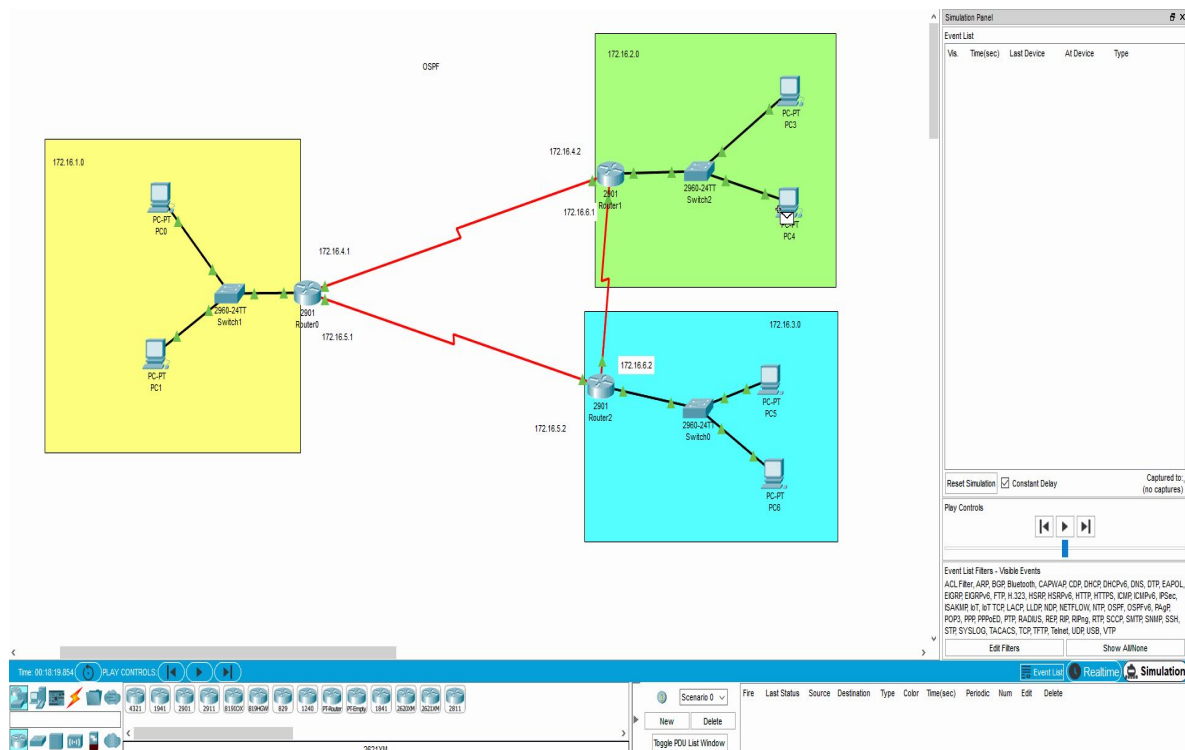


Figura 5.1.8.b Comprobando que se restablece el funcionamiento inicial

9. Comprobar de bandwidth NO tiene efecto en RIP

Para comprobar que el protocolo RIP siempre coge la ruta con menos saltos da igual el ancho de banda de esa línea, cambiaremos los anchos de banda del router de la zona verde de la misma manera que para OSPF. Utilizaremos la red creada para el apartada 3 y 4. Fig.5.1.9.a

```
Router1(1)
Physical Config CLI Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed
state to up

Router>enable
Router#conf t
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface s0/0/0
Router(config-if)#bandwidth 1
Router(config-if)#exit
Router(config)#interface s0/0/1
Router(config-if)#bandwidth 1000
Router(config-if)#exit
Router(config)#

Ctrl+F6 to exit CLI focus
```

5.1.9

Figura 5.1.9.a Cambiando anchos de banda en RIP

A continuación comprobamos como ignora los cambios y sigue usando la ruta más corta. Fig 5.1.9.b

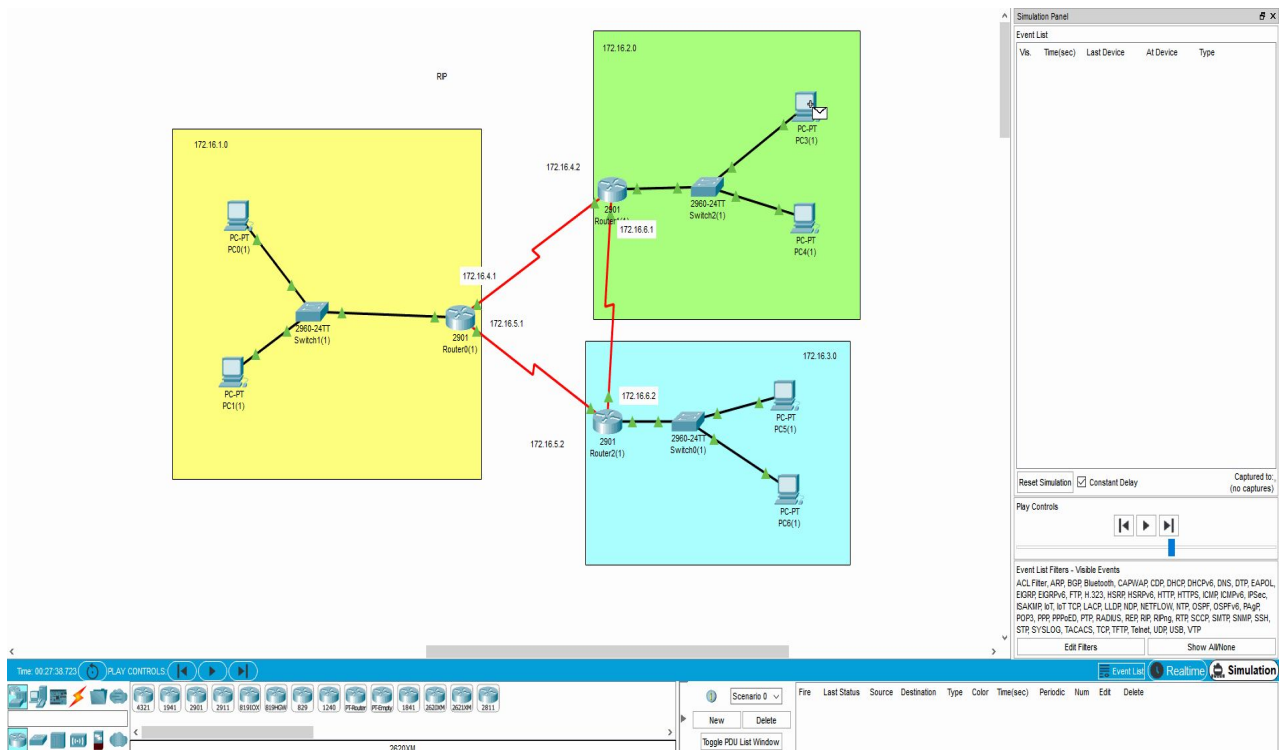
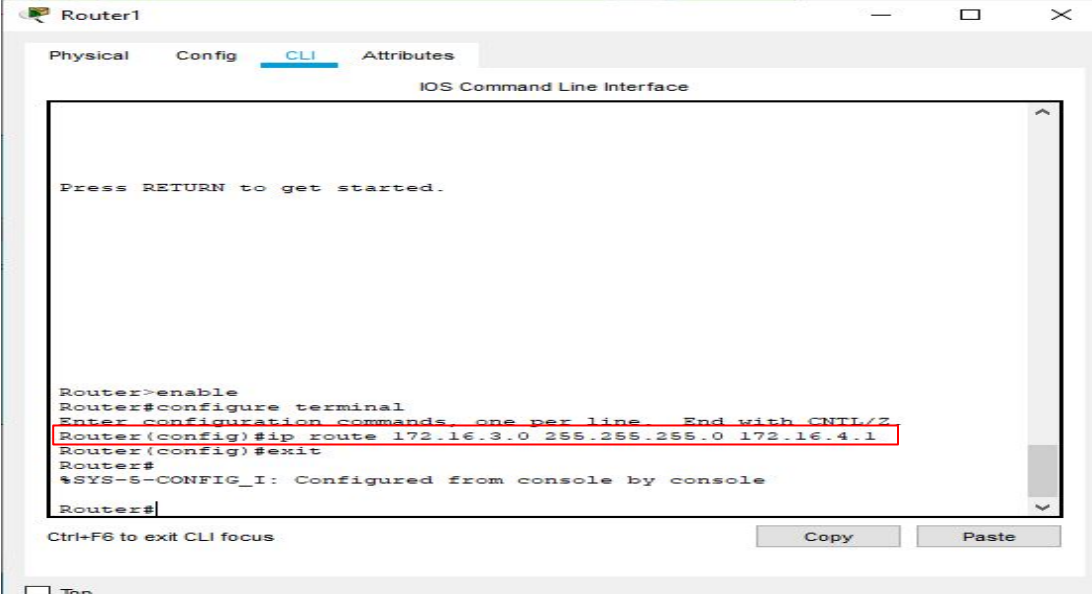


Figura 5.1.9.b Comprobando los cambios RIP

10. Forzando una ruta en RIP y en OSPF

Vamos a establecer en la red con OSPF y RIP una ruta estática que tiene más prioridad que las creadas por el protocolo. Esto hará que ignore la ruta creada por OSPF o RIP y el paquete viaje por la ruta establecida de manera estática.

OSPF: Router (zona verde). La ruta que establecemos será para ir a la zona azul pero pasando primero por el router de la zona amarilla. Fig 5.1.10.a Comprobamos que se crea la ruta en la tabla de ruteo. Fig 5.1.10.b



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

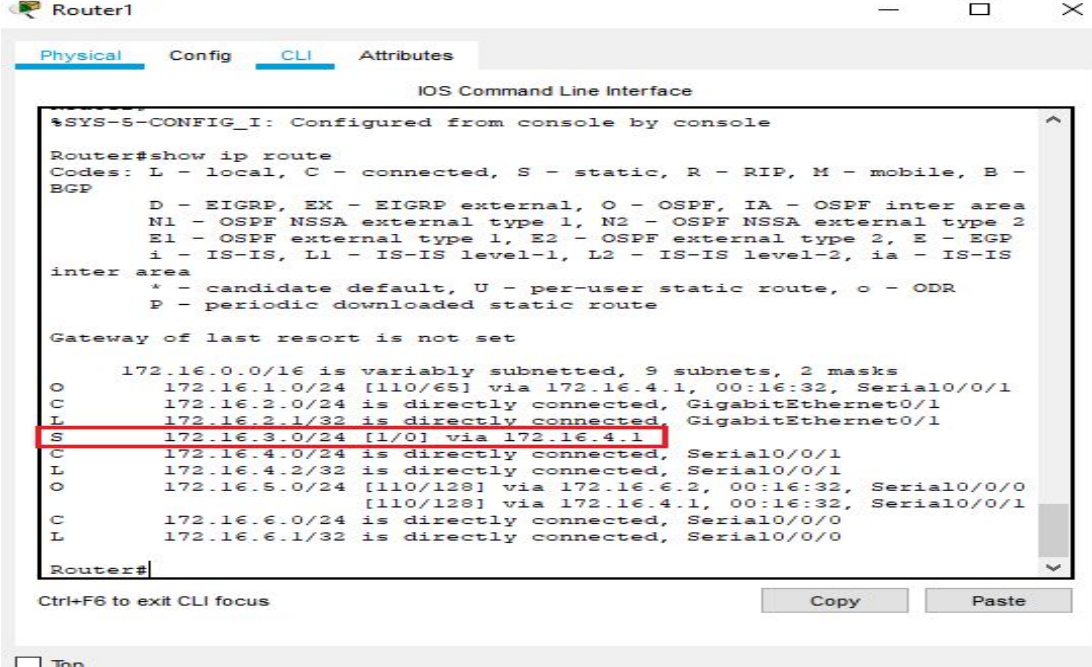
Press RETURN to get started.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)#ip route 172.16.3.0 255.255.255.0 172.16.4.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

5.1.10

Figura 5.1.10.a Creando la ruta estática



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

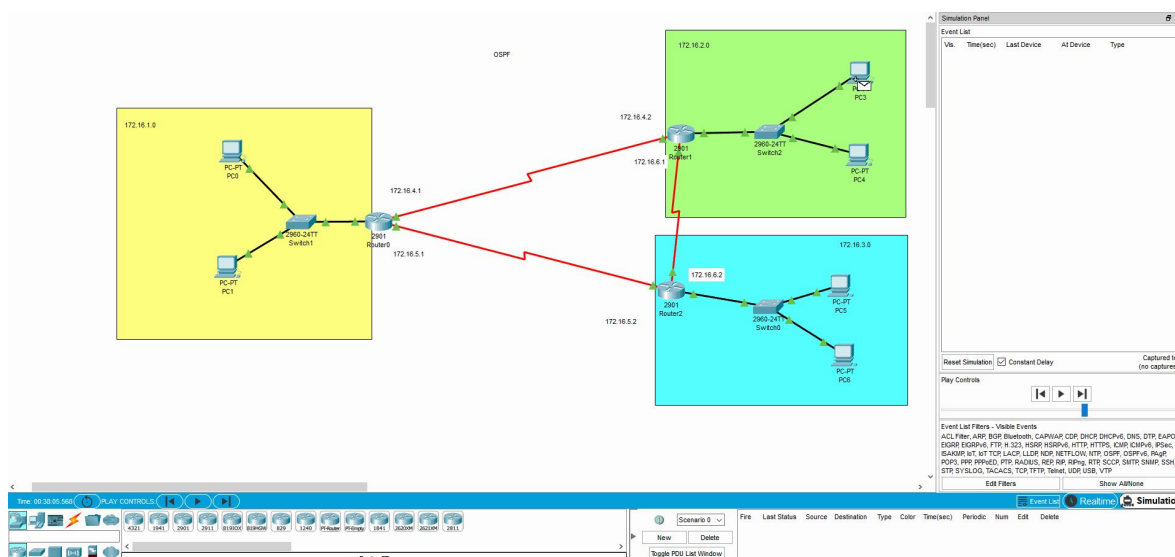
Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 9 subnets, 2 masks
O       172.16.1.0/24 [110/65] via 172.16.4.1, 00:16:32, Serial0/0/1
C       172.16.2.0/24 is directly connected, GigabitEthernet0/1
L       172.16.2.1/32 is directly connected, GigabitEthernet0/1
S       172.16.3.0/24 [1/0] via 172.16.4.1
C       172.16.4.0/24 is directly connected, Serial0/0/1
L       172.16.4.2/32 is directly connected, Serial0/0/1
O       172.16.5.0/24 [110/128] via 172.16.6.2, 00:16:32, Serial0/0/0
       [110/128] via 172.16.4.1, 00:16:32, Serial0/0/1
C       172.16.6.0/24 is directly connected, Serial0/0/0
L       172.16.6.1/32 is directly connected, Serial0/0/0

Router#
```

Figura 5.1.10.b Comprobando que se creó la ruta

Comprobamos que los paquetes viajan a través de la ruta estática ignorando a OSPF. Fig 5.1.10.c



5.1.10

Figura 5.1.10.c Comprobando el trayecto del paquete

Realizamos los mismos pasos para la red con RIP. Fig 5.1.10.d-e-f

```

Router1(1)
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 172.16.3.0 255.255.255.0 172.16.4.1
Router(config)#exit
Router#
*SYS-5-CONFIG_I: Configured from console by console

Router#
    
```

Figura 5.1.10.d Creando ruta estática

```

Router1(1)
Physical Config CLI Attributes
IOS Command Line Interface

*SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, SE -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

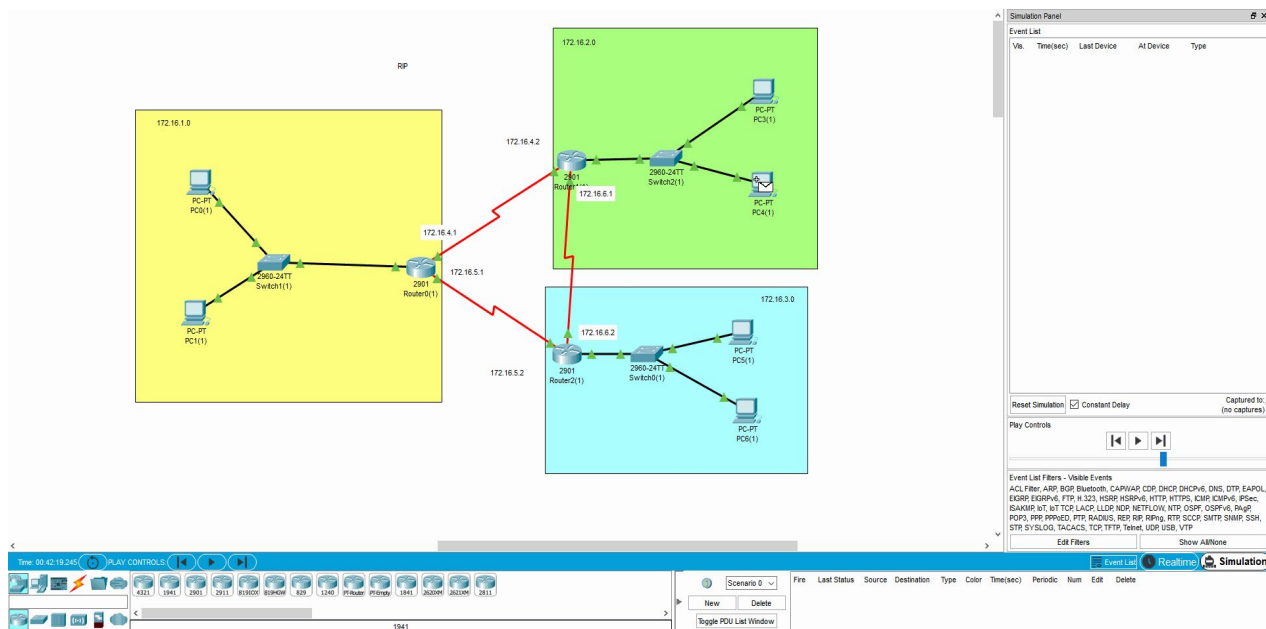
Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 9 subnets, 2 masks
R 172.16.1.0/24 [120/1] via 172.16.4.1, 00:00:14, Serial0/0/1
C 172.16.2.1/32 is directly connected, GigabitEthernet0/1
S 172.16.3.0/24 [1/0] via 172.16.4.1
R 172.16.4.0/24 is directly connected, Serial0/0/1
L 172.16.4.3/32 is directly connected, Serial0/0/1
R 172.16.5.0/24 [120/1] via 172.16.4.1, 00:00:03, Serial0/0/0
C 172.16.6.0/24 [120/1] via 172.16.4.1, 00:00:14, Serial0/0/1
L 172.16.6.1/32 is directly connected, Serial0/0/0
    
```

Figura 5.1.10.e Comprobando que se creó la ruta

<IMARMEN>
<JACOGON>

Comprobamos que los paquetes viajan a través de la ruta estática ignorando a RIP. Fig 5.1.10.f



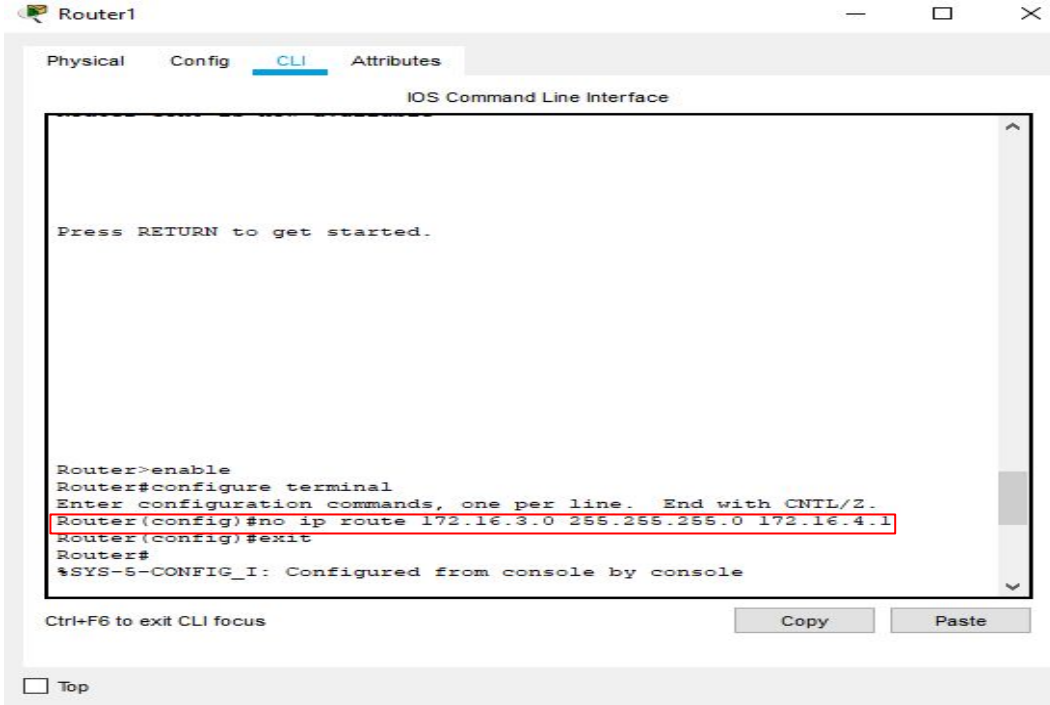
5.1.10

Figura 5.1.10.f Comprobando el trayecto del paquete

11.Ruta estática de último recurso

En este punto creamos una ruta estática sin prioridad añadiendo al final del comando de creación un número de distancia más alto 210

Primero con la red de OSPF: Quitamos la ruta creada anteriormente y la volvemos a crear poniendo 210 al final del comando. Flg 5.1.11.a y b



The screenshot shows the CLI of Router1. The command `no ip route 172.16.3.0 255.255.255.0 172.16.4.1` is entered and highlighted with a red box. The output shows the route being removed from the routing table.

```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

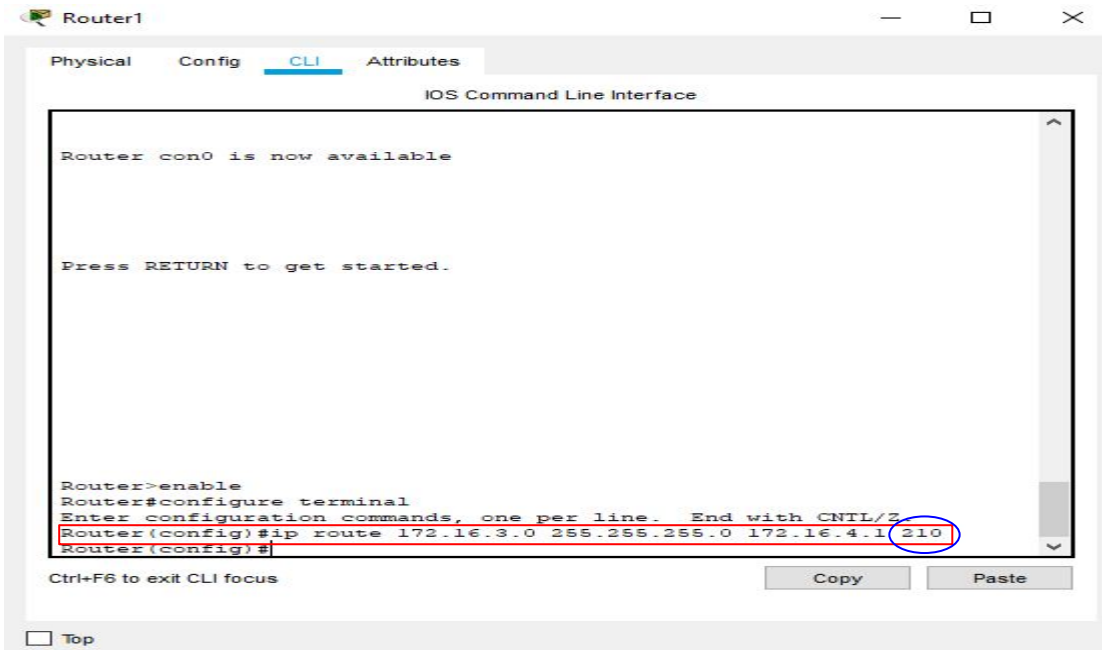
Press RETURN to get started.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip route 172.16.3.0 255.255.255.0 172.16.4.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Ctrl+F6 to exit CLI focus
```

5.1.11

Figura 5.1.11.a Eliminando la ruta estática prioritaria



The screenshot shows the CLI of Router1. The command `ip route 172.16.3.0 255.255.255.0 172.16.4.1 210` is entered and highlighted with a red box. The number 210 is circled in blue. The output shows the route being added to the routing table.

```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

Router con0 is now available

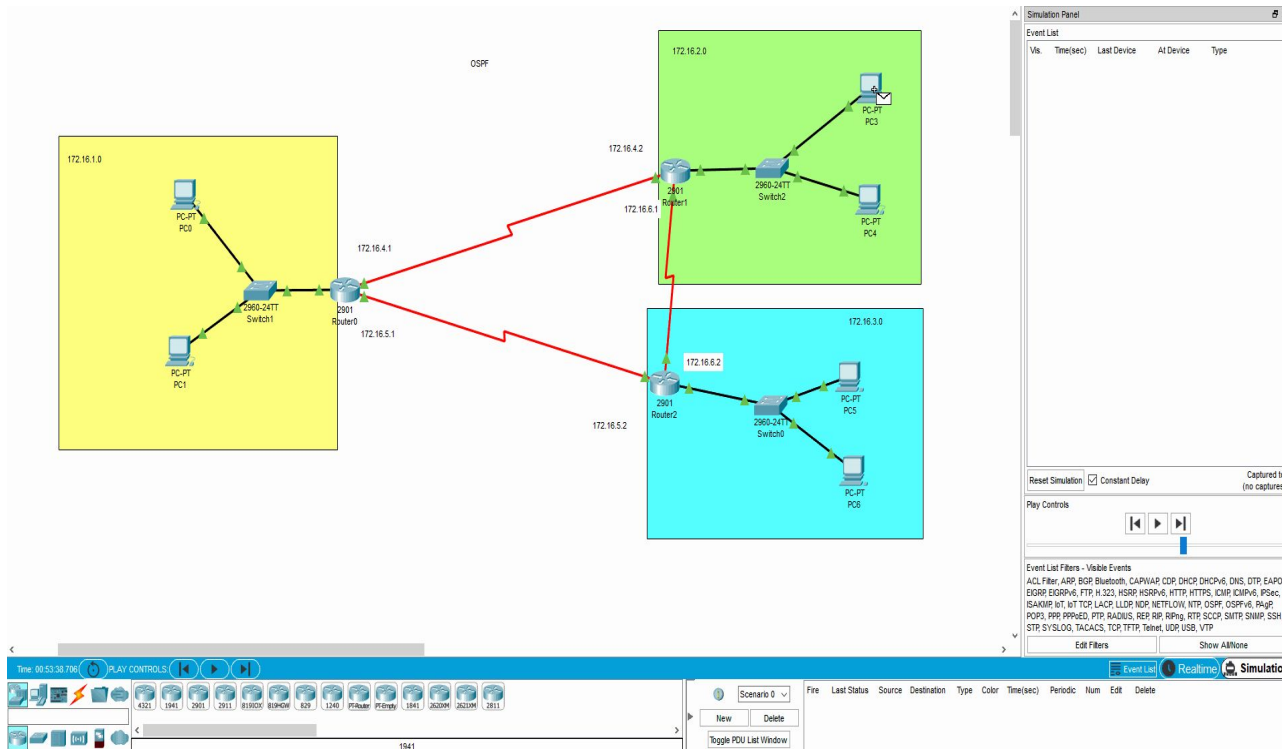
Press RETURN to get started.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 172.16.3.0 255.255.255.0 172.16.4.1 210
Router(config)#

Ctrl+F6 to exit CLI focus
```

Figura 5.1.11.b Creando la ruta estática no prioritaria

Comprobamos si funciona como debería. En condiciones normales ignora la ruta estática y sigue la ruta del protocolo OSPF (Fig 5.1.11.c). En caso de que la ruta de OSPF fallará condiciones normales:



5.1.11

Figura 5.1.11.c Ignorando la ruta no prioritaria

Hacemos lo mismo con la red de RIP y comprobamos que ignora la ruta. Fig 5.1.11.d

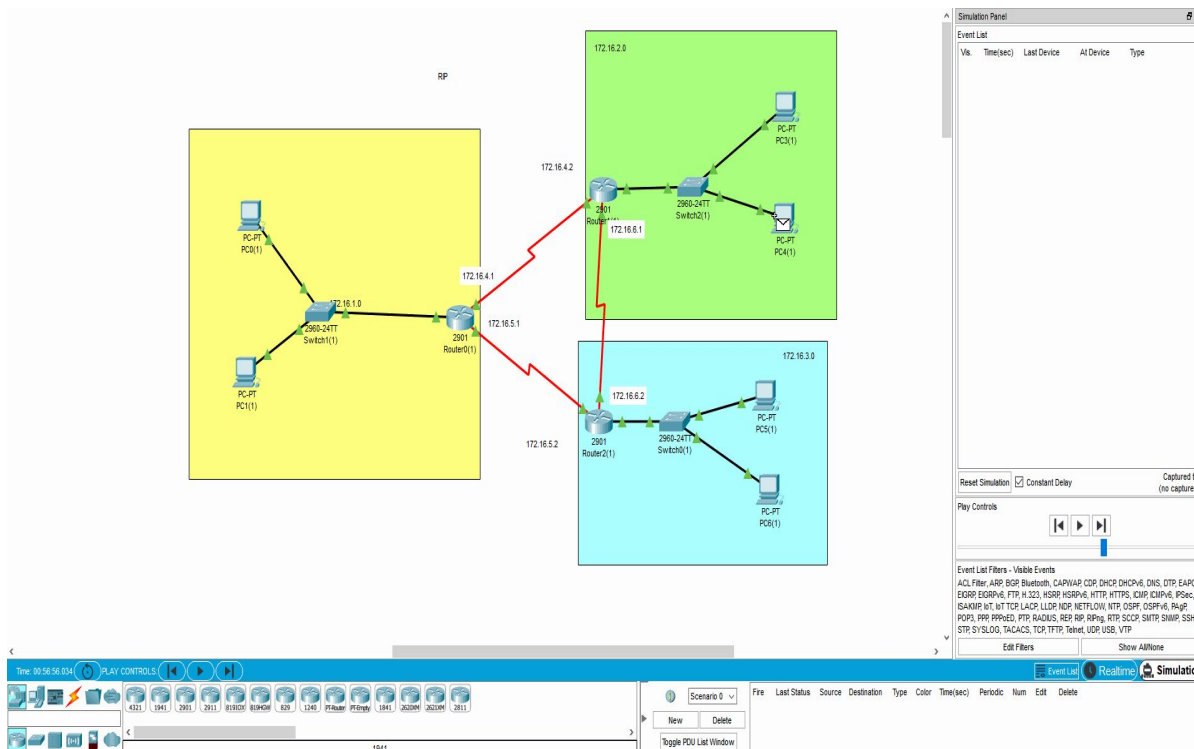


Figura 5.1.11.d Ignorando la ruta no prioritaria

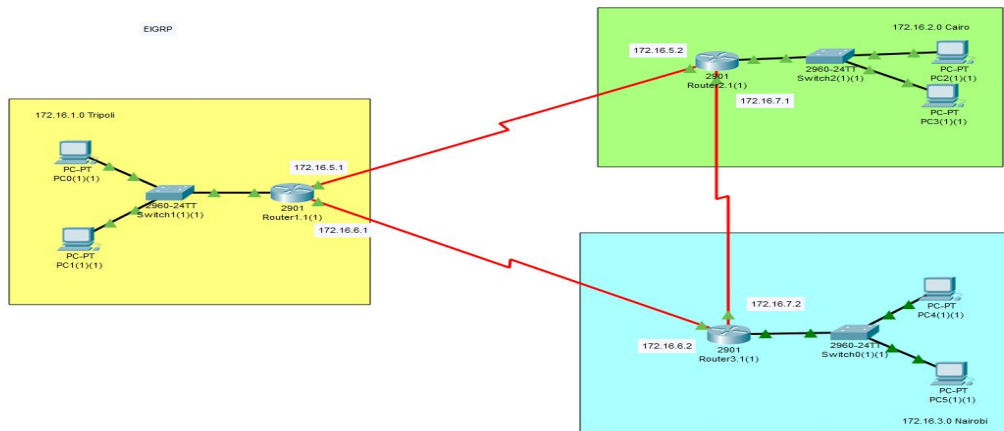
<IMARMEN>
<JACOGON>

Añadido 1. Red con EIGRP

Añade a tu diseño PT una tercera red configurada con EIGRP. Incluye en tu memoria cómo se configura e incluye pruebas y evidencias de su correcto funcionamiento.

EIGRP (Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español) es un protocolo de encaminamiento de estado de enlace, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace.

Montamos la misma red que en los apartados anteriores. Fig 5.1.A1.a



5.1.A1

Figura 5.1.A1.a. Red EIGRP

Los comandos para configurar EIGRP son similares a los utilizados con OSPF:

```
Router>enable
Router #configure terminal
Router (config)#router EIGRP 1
Switch(config-router)#network 0.0.0.0 255.255.255.255
```

A continuación vemos cómo se han creado las rutas en uno de los routers: Fig.5.1.A1.b

Router3.1(1)

```
Physical Config CLI Attributes
IOS Command Line Interface
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

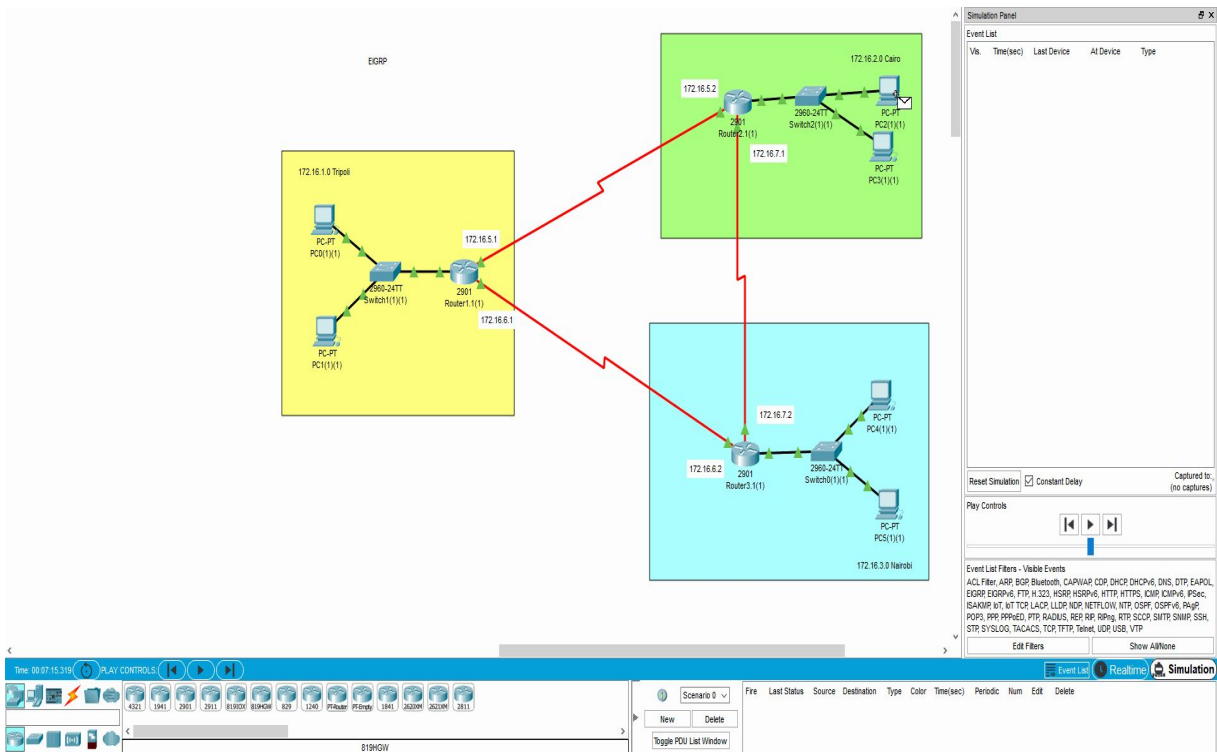
Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 9 subnets, 2 masks
D 172.16.1.0/24 [90/2170112] via 172.16.6.1, 00:02:03,
Serial0/3/1
D 172.16.2.0/24 [90/2170112] via 172.16.7.1, 00:02:03,
Serial0/3/0
C 172.16.3.0/24 is directly connected, GigabitEthernet0/1
L 172.16.3.1/32 is directly connected, GigabitEthernet0/1
D 172.16.5.0/24 [90/2681856] via 172.16.6.1, 00:02:03,
Serial0/3/1
C 172.16.6.0/24 is directly connected, Serial0/3/1
L 172.16.6.2/32 is directly connected, Serial0/3/1
C 172.16.7.0/24 is directly connected, Serial0/3/0
L 172.16.7.2/32 is directly connected, Serial0/3/0

Router#
```

Figura 5.1.A1.b. Rutas EIGRP

Realizamos comprobaciones para ver que todo está bien configurado y conectado: Fig 5.1.A1.c



5.1.A1

Figura 5.1.A1.c. Red EIGRP

Cambiamos bandwidth de router el cairo a nairobi (s0/3/1) a 1 de el cairo a tripoli (s0/3/0) a 1000 y coge el otro recorrido:

```

Router2.1(1)
Physical Config CLI Attributes
IOS Command Line Interface
Router(config-if)#exit
Router(config)#serial 0/3/1
% Invalid input detected at '^' marker.
Router(config)#interface serial 0/3/1
Router(config-if)#no band
Router(config-if)#no bandwidth
Router(config-if)#exit
Router(config)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.5.1 (Serial0/3/0) is
down: interface down
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.7.2 (Serial0/3/1) is
down: interface down
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.5.1 (Serial0/3/0) is
up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.7.2 (Serial0/3/1) is
up: new adjacency
Router(config)#interface s0/3/1
Router(config-if)#bandwidth 1
Router(config-if)#exit
Router(config)#interface s0/3/0
Router(config-if)#bandwidth 1000
Router(config-if)#exit
    
```

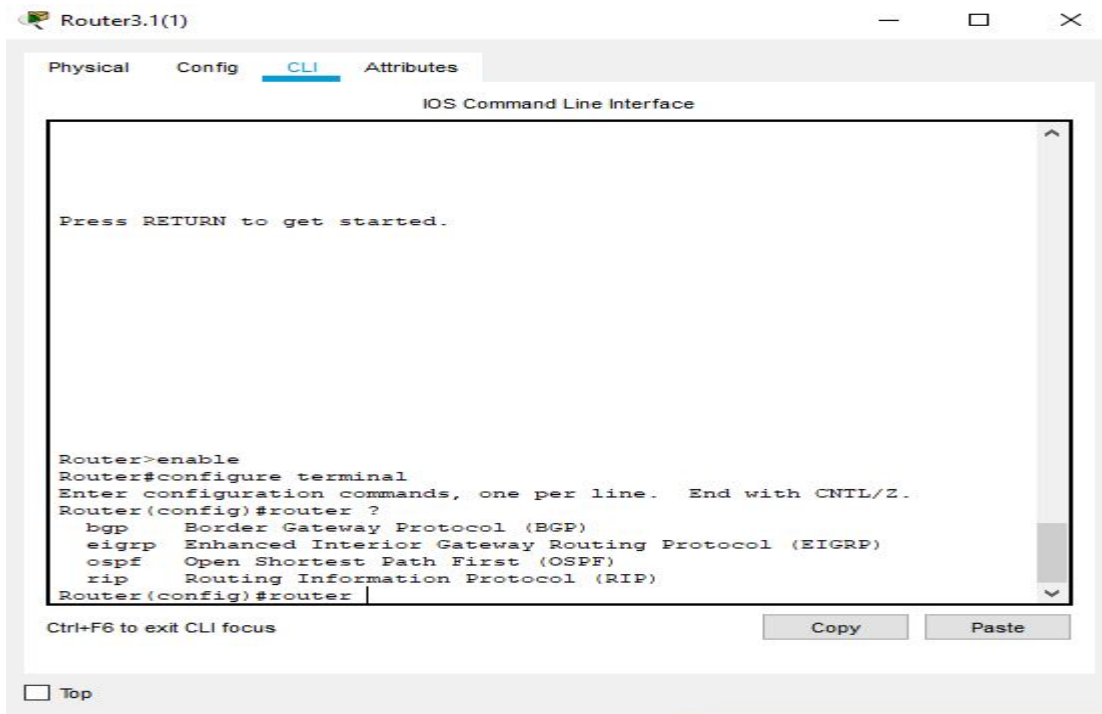
Figura 5.1.A1.d. Cambio bandwidth

Añadido 2. Red con IS-IS y con IGRP

Se trata de dos protocolos que supuestamente NO soporta PT. Si consigues configurarlos, Procede como en el extra anterior

Por el contrario, si no consigues configurarlos, incluye en tu memoria pruebas y evidencias fiables que demuestren que no se puede realizar.

Entramos a la configuración del router y escribimos router ? para ver las opciones de ruteo de cisco packet tracer 7.2 y no aparece IS-IS ni IGRP por lo que no está preparado para su configuración. Fig. 5.1.A2



```
Router3.1(1)
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ?
  bgp      Border Gateway Protocol (BGP)
  eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
  ospf     Open Shortest Path First (OSPF)
  rip      Routing Information Protocol (RIP)
Router(config)#router
```

5.1.A2

Figura 5.1.A2.a. No IS-IS no IGRP

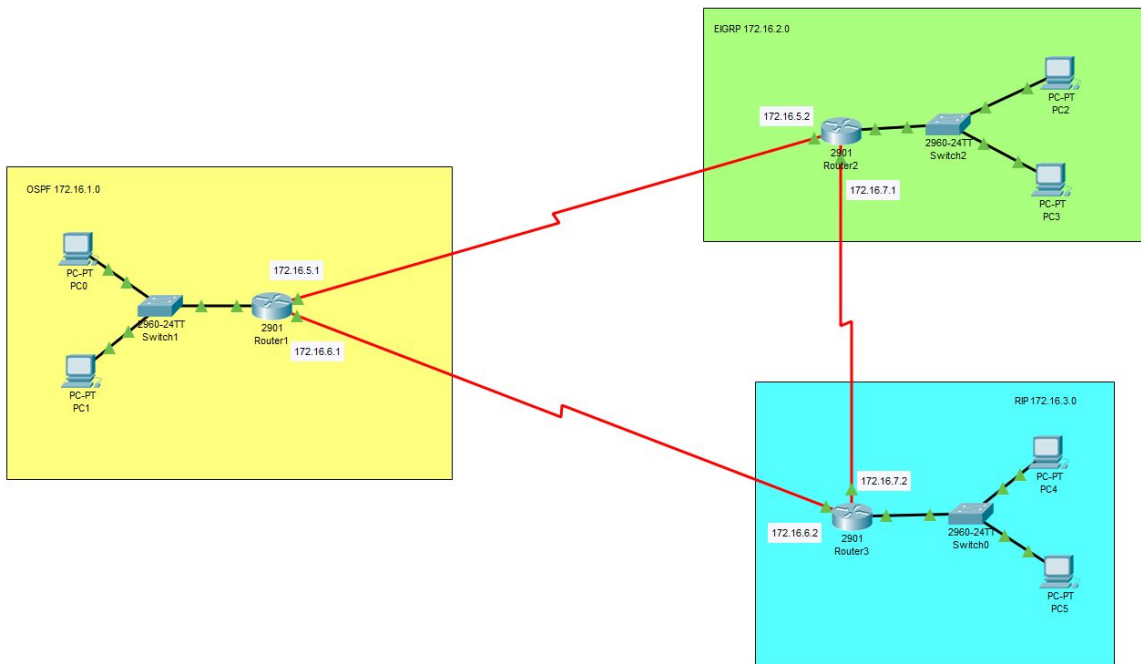
Añadido 3. Macro-red con múltiples algoritmos de ruteo

Crea una macro red en la que convivan RIP, EIGRP y OSPF

Así, algunos routers están configurados con RIP, otros con EIGRP y otros con OSPF

Mostrar la tabla de enrutamiento y explicar/razonar las rutas y la distancia administrativa

Existe la posibilidad de compatibilizar estas tres algoritmos de ruteo pero es bastante rebuscado. Si solo configuramos los routers cada uno con un algoritmo de ruteo distinto no funciona, red: Fig.5.1.A3.a



5.1.A3

Figura 5.1.A3.a. Red EIGRP,RIP y OSPF

Configuramos los tres routers uno con cada algoritmo y mostrando la tabla de ruteo se ve que no existen rutas. Un ejemplo con el router configurado con RIP: Fig.5.1.A3.b

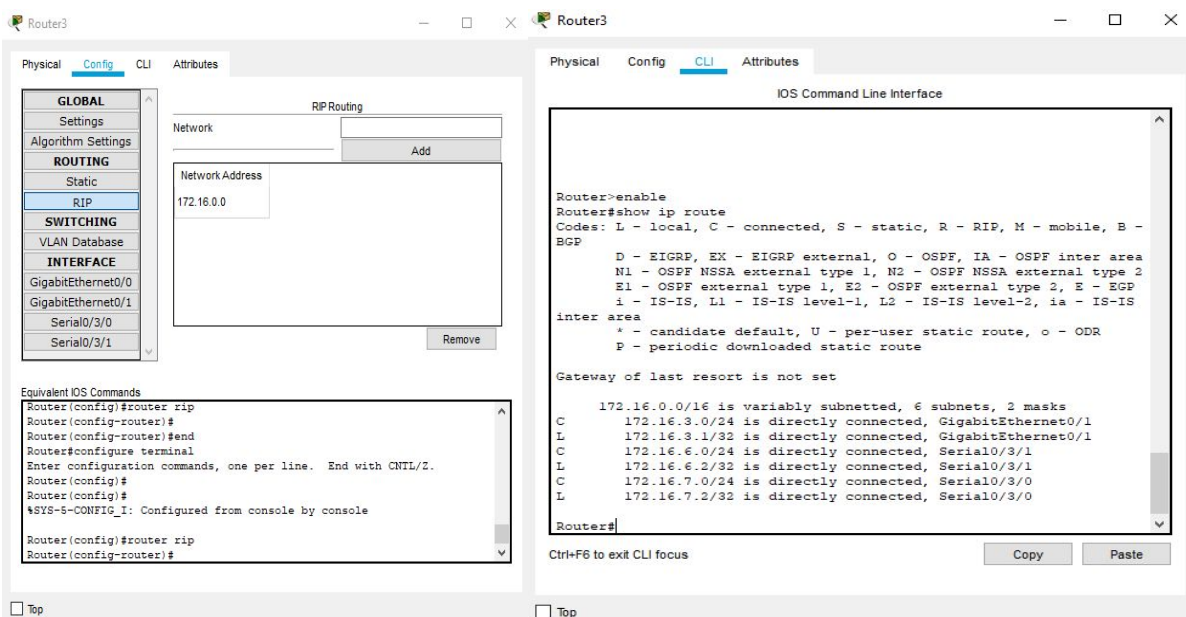
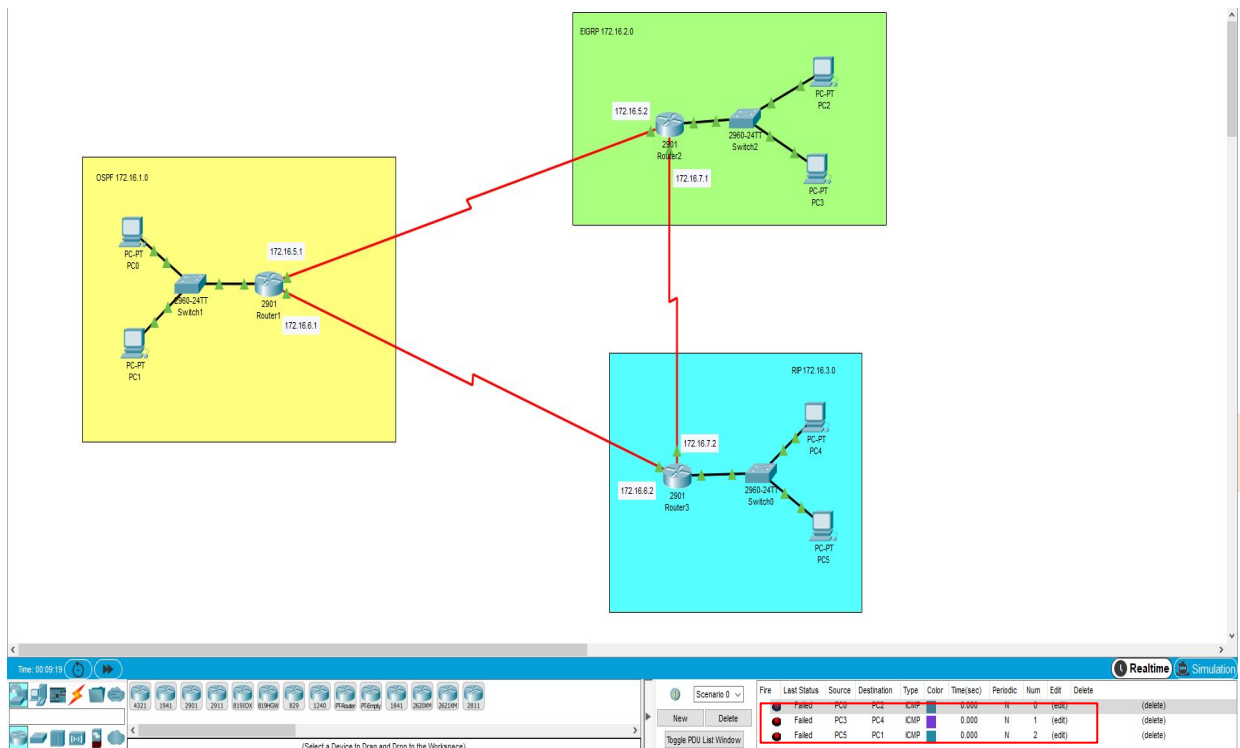


Figura 5.1.A3.b. No crea rutas

Probamos las conexiones haciendo ping entre las distintas redes y todas dan error. Flg.5.1.A3.c



5.1.A3

Figura 5.1.A3.c. No hay conexión

Añadido 4. Modificar la frecuencia con la que se envían los mensajes Hello

En una red que posea el protocolo OSPF es posible cambiarle a los routers la frecuencia con la que estos se mandan mensajes 'HELLO' entre ellos. Para ello se debe realizar el siguiente proceso de comandos para cambiar esta frecuencia en cada una de las bocas seriales que deseamos (en este caso se cambiará para la boca Serial 0/3/0):

```
enable
configure terminal
interface serial 0/3/0
ip ospf hello-interval x (x = número de segundos que deseamos)
exit
```

Una vez realizado estos comandos si queremos comprobar que efectivamente se realizó este cambio es tan fácil como realizar en la consola del router un:

5.1.A4

```
enable
configure terminal
show ip ospf interface serial 0/3/0
```

En las siguientes imágenes se muestra este proceso aquí mostrado.

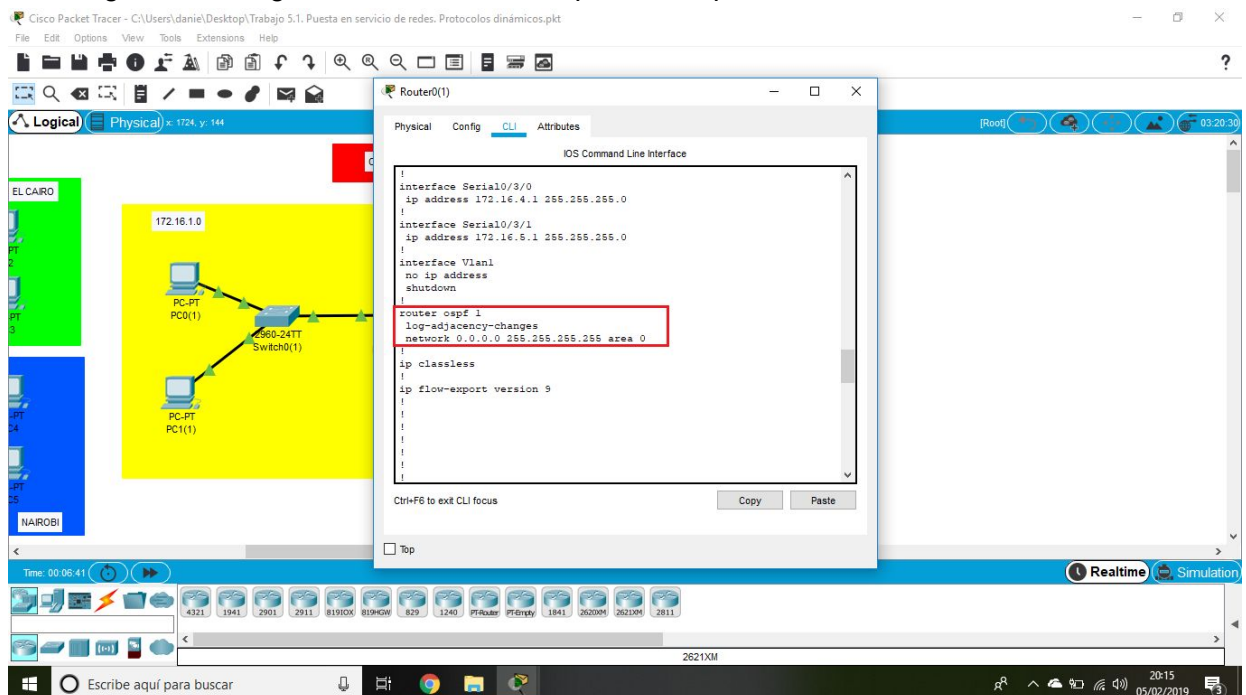
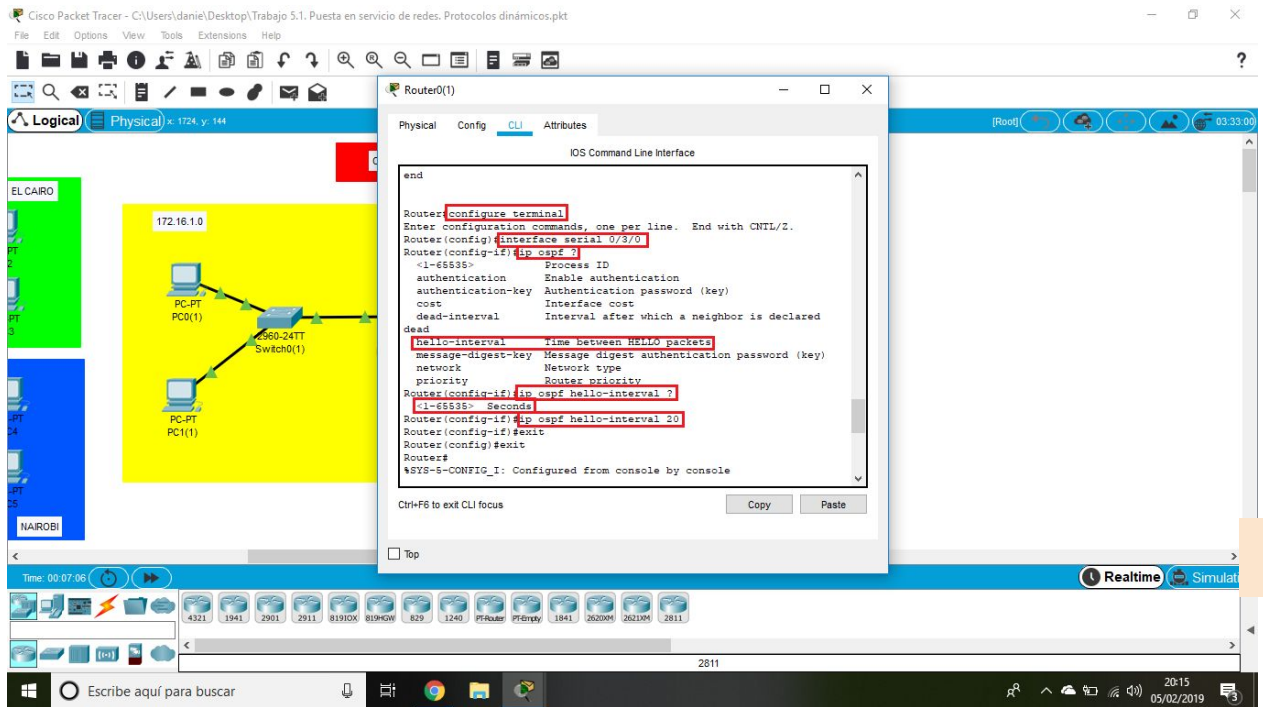


Figura 5.1.A4.a. Comprobación Router OSPF mediante show running-config.



5.1.A4

Figura 5.1.A4.b. Modificación frecuencia mensajes HELLO.

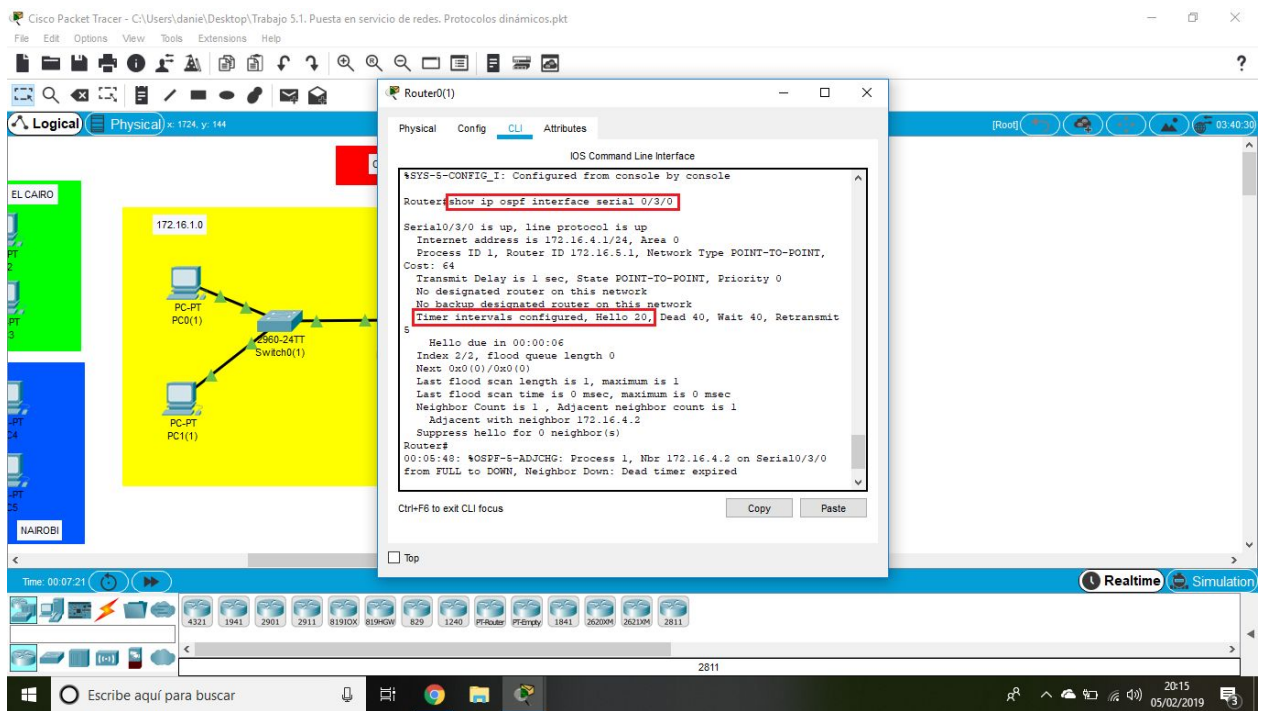


Figura 5.1.A4.c. Comprobación frecuencia mensajes HELLO.

<DPLAHER>
<IMARMEN>
<JACOGON>

Anexo I



BOOTP



BOOTP (V́ctor e Isaac)

- ¿Qué es BOOTP?

Es un protocolo de arranque utilizado por los clientes de red para obtener su direcci3n IP autom1ticamente.

Bootp

- ¿Para qu3 sirve?

Este protocolo permite a los ordenadores sin disco obtener una direcci3n IP antes de cargar un sistema operativo avanzado. Hist3ricamente ha sido utilizado por las estaciones de trabajo sin disco basadas en UNIX (las cuales tambi3n obtenían la localizaci3n de su imagen de arranque mediante este protocolo) y tambi3n por empresas para introducir una instalaci3n preconfigurada de Windows en PC reci3n comprados (típicamente en un entorno de red Windows NT).

- ¿Es anterior o posterior a DHCP?

Es anterior, DHCP est1 basado en BOOTP.

- ¿Qu3 diferencias existen entre uno y otro?

BOOTP	DHCP
Diseñado antes que DHCP.	Diseñado despu3s que BOOTP.
Pensado para configurar estaciones de trabajo sin disco con capacidades de arranque limitadas.	Pensado para configurar equipos conectados en red que cambian de ubicaci3n con frecuencia (como port1tiles) que disponen de discos duros locales y capacidades completas de arranque.
BOOTP dinámico tiene una expiraci3n predeterminada de 30 d1as para las concesiones de direcciones IP.	DHCP tiene una expiraci3n predeterminada de ocho d1as para las concesiones de direcciones IP.
Admite un n1mero limitado de par1metros de configuraci3n de clientes denominados <i>extensiones del proveedor</i> .	Admite un conjunto mayor y extensible de par1metros de configuraci3n de clientes denominados <i>opciones</i> .
Describe un proceso de configuraci3n de arranque en dos fases, de la manera siguiente: <ul style="list-style-type: none">• Los clientes se ponen en contacto con los servidores BOOTP para realizar la determinaci3n de las direcciones y la selecci3n del nombre del archivo de arranque.• Los clientes se ponen en contacto con los servidores del Protocolo trivial de transferencia de archivos (TFTP) para realizar la transferencia de archivos de su imagen de arranque.	Describe un proceso de configuraci3n de arranque de una sola fase donde un cliente DHCP negocia con un servidor DHCP para determinar su direcci3n IP y obtener cualquier otro detalle de configuraci3n inicial que se necesite para el funcionamiento de la red.
Los clientes BOOTP no reenlazan ni renuevan la configuraci3n con el servidor BOOTP salvo cuando se reinicia el sistema.	Los clientes DHCP no necesitan un reinicio del sistema para reenlazar o renovar la configuraci3n con el servidor DHCP. En su lugar, los clientes entran autom1ticamente en un estado de reenlace a intervalos establecidos para renovar la asignaci3n de sus direcciones concedidas con el servidor DHCP. Este proceso tiene lugar en segundo plano y es transparente para el usuario.

BOOTP (Víctor e Isaac)

- ¿Qué ventajas/desventajas incluye el uno frente al otro?

Bootp

BOOTP es más simple que DHCP de manera que DHCP es más eficiente a la hora de entregar direcciones IP. También, el DHCP nos muestra más información que el BOOTP como por ejemplo la máscara de la IP.

- ¿Cuál de los dos protocolos se usa en la actualidad?

DHCP.

BOOTP (Javier y Sergio)

- **¿Qué es BOOTP?**

Es un protocolo de arranque utilizado por los clientes de red para obtener su dirección IP automáticamente.

- **¿Para qué sirve?**

Este protocolo permite a los ordenadores sin disco obtener una dirección IP antes de cargar un sistema operativo avanzado. Históricamente ha sido utilizado por las estaciones de trabajo sin disco basadas en UNIX (las cuales también obtenían la localización de su imagen de arranque mediante este protocolo) y también por empresas para introducir una instalación preconfigurada de Windows en PC recién comprados.

- **¿Es anterior o posterior a DHCP?**

Es anterior, DHCP está basado en BOOTP. BOOTP es de 1985 y DHCP es de 1993.

- **¿Qué ventajas/desventajas incluye el uno frente al otro?**

Bootp da Ip estáticas, pero DHCP es dinámico (pero también puede ser estático).

DHCP es excelente cuando los dispositivos y las direcciones IP cambian.

- **¿Qué diferencias existen entre uno y otro?**

BOOTP	DHCP
Diseñado antes que DHCP.	Diseñado después que BOOTP.
Pensado para configurar estaciones de trabajo sin disco con capacidades de arranque limitadas.	Pensado para configurar equipos conectados en red que cambian de ubicación con frecuencia (como portátiles) que disponen de discos duros locales y capacidades completas de arranque.
BOOTP dinámico tiene una expiración predeterminada de 30 días para las concesiones de direcciones IP.	DHCP tiene una expiración predeterminada de ocho días para las concesiones de direcciones IP.
Admite un número limitado de parámetros de configuración de clientes denominados <i>extensiones del proveedor</i> .	Admite un conjunto mayor y extensible de parámetros de configuración de clientes denominados <i>opciones</i> .
Describe un proceso de configuración de arranque en dos fases, de la manera siguiente: <ul style="list-style-type: none">• Los clientes se ponen en contacto con los servidores BOOTP para realizar la determinación de las direcciones y la selección del nombre del archivo de arranque.• Los clientes se ponen en contacto con los servidores del Protocolo trivial de transferencia de archivos (TFTP) para realizar la transferencia de archivos de su imagen de arranque.	Describe un proceso de configuración de arranque de una sola fase donde un cliente DHCP negocia con un servidor DHCP para determinar su dirección IP y obtener cualquier otro detalle de configuración inicial que se necesite para el funcionamiento de la red.
Los clientes BOOTP no reenlazan ni renuevan la configuración con el servidor BOOTP salvo cuando se reinicia el sistema.	Los clientes DHCP no necesitan un reinicio del sistema para reenlazar o renovar la configuración con el servidor DHCP. En su lugar, los clientes entran automáticamente en un estado de reenlace a intervalos establecidos para renovar la asignación de sus direcciones concedidas con el servidor DHCP. Este proceso tiene lugar en segundo plano y es transparente para el usuario.

BOOTP (Javier y Sergio)

- ¿Cuál de los dos protocolos se usa en la actualidad?

DHCP

Bootp

BOOTP

¿Qué es BOOTP?

Es un protocolo de arranque utilizado por los clientes de red para obtener su dirección IP automáticamente.

Bootp

- ¿Para qué sirve?

Este protocolo permite a los ordenadores sin disco obtener una dirección IP antes de cargar un sistema operativo avanzado. Históricamente ha sido utilizado por las estaciones de trabajo sin disco basadas en UNIX (las cuales también obtenían la localización de su imagen de arranque mediante este protocolo) y también por empresas para introducir una instalación preconfigurada de Windows en PC recién comprados (típicamente en un entorno de red Windows NT).

- ¿Es anterior o posterior a DHCP?

Es anterior, DHCP está basado en BOOTP.

- ¿Qué diferencias existen entre uno y otro?

BOOTP requiere que el servidor esté preconfigurado manualmente con las asignaciones de dirección MAC a dirección IP para cada cliente, mientras que DHCP no necesita estas predefiniciones. En su lugar, DHCP asigna dinámicamente (y rastrea) direcciones IP de un grupo por solicitud de cliente durante el tiempo que el dispositivo necesita. Como se mencionó, BOOTP es un protocolo heredado. DHCP es su desarrollo y es ampliamente utilizado hoy en día.

- ¿Qué ventajas/desventajas incluye el uno frente al otro?

Con DHCP no es necesario preconfigurar manualmente el servidor con las direcciones MAC a IP para cada cliente.

- ¿Cuál de los dos protocolos se usa en la actualidad?

DHCP



<DPLAHER>
<JDOMDAR>
<IMARMEN>
<JACOGON>
<VCARLEO>
<SMARGON>

CIDR

Classless Inter-Domain Routing o **CIDR** se introdujo en 1993 por IETF y representa la última mejora en el modo de interpretar las direcciones IP. Su introducción permitió una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas. De esta manera permitió:

- La técnica VLSM para especificar prefijos de red de longitud variable. Una dirección CIDR se escribe con un sufijo que indica el número de bits de longitud de prefijo, p.ej. 192.168.0.0/16 que indica que la máscara de red tiene 16 bits (es decir, los primeros 16 bits de la máscara son 1 y el resto 0). Esto permite un uso más eficiente del cada vez más escaso espacio de direcciones IPv4.
- La agregación de múltiples prefijos contiguos en superredes, reduciendo el número de entradas en las tablas de ruta globales.

CIDR

CIDR reemplaza la sintaxis previa para nombrar direcciones IP, las clases de redes. En vez de asignar bloques de direcciones en los límites de los octetos, que implicaban prefijos «naturales» de 8, 16 y 24 bits, CIDR usa la técnica VLSM (*variable length subnet mask*, en español «máscara de subred de longitud variable»), para hacer posible la asignación de prefijos de longitud arbitraria.

CIDR fue creada para simplificar las tablas de ruteo pudiendo mandar todas las direcciones IP con octetos iguales por una determinada boca.

▪ Ejemplo

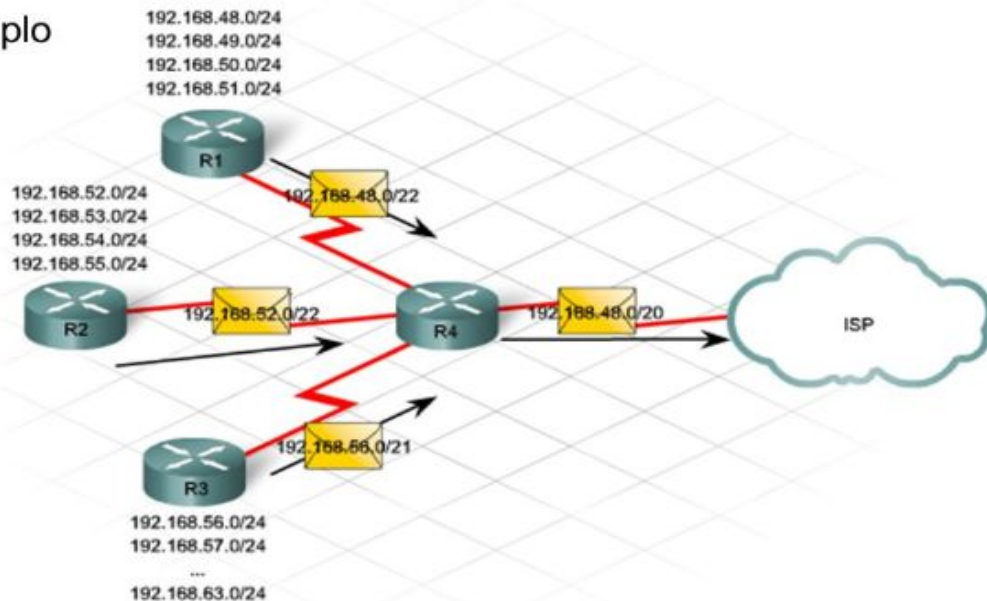


Figura CIDR 1.1. Ejemplo CIDR.

Beneficios de las mejoras en 3^a Generación. Routers Cisco Serie 4000



<DPLAHER>
<JDOMDAR>
<IMARMEN>
<JACOGON>
<VCARLEO>
<SMARGON>
<APLAFLE>

Benefits of Upgrading to Cisco 4000 Series Integrated Services Routers



Learn more at <https://www.cisco.com/go/isr4000>

Intent-based networking capabilities	Features	First-Generation (Cisco 1800, 2800, and 3800 Series [EOL Oct 2016])	Generation 2 (ISR G2) (Cisco 1900, 2900, and 3900 Series [EOS Dec 2017])	Cisco 4000 Series Integrated Services Routers	Benefits
Digital-ready infrastructure	Enterprise Network Functions Virtualization	×	×	✓	Simplified operations and deployment of virtual network services on any platform
	Cisco IOS® XE open operating system	×	×	✓	Multi-core processing increases network services performance and availability
Policy-based Automation	Native Application Hosting	×	×	✓	No need for additional network devices in the branch
	Integrated compute with Cisco UCS E-Series servers	×	✓	✓	Local compute resources for applications, data backup, and analytics
Analytics and Assurance	Cisco DNA Center centralized management	×	×	✓	Simplify network management, deploy networks in minutes, and predict problems before they happen
	Cisco SD-WAN	×	×	✓	Cloud-delivered, secure, flexible and rich services architecture that delivers the best user experience over any connection
Optimization	Pay-as-you-grow performance and services	×	×	✓	Ability to buy what you need today and upgrade anytime without a complete equipment upgrade
	DNA Assurance network monitoring	×	×	✓	Continuous verification, insights and visibility, and corrective actions
Security and Compliance	Cisco® Application Visibility and Control (AVC)	×	✓	✓	Visibility into 1000+ applications for capacity planning and prioritization

© 2018 Cisco and/or its affiliates. All rights reserved.

S4000

https://www.cisco.com/c/dam/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/aag_c83-731053.pdf

Benefits of Upgrading to Cisco 4000 Series Integrated Services Routers



Learn more at <https://www.cisco.com/go/isr4000>

Intent-based networking capabilities	Features	First-Generation (Cisco 1800, 2800, and 3800 Series [EOL Oct 2016])	Generation 2 (ISR G2) (Cisco 1900, 2900, and 3900 Series [EOS Dec 2017])	Cisco 4000 Series Integrated Services Routers	Benefits
Optimization	WAN optimization (Cisco WAAS with Akamai)	×	✓	✓	Improved application performance and WAN offload with Layer 4 through 7 optimization and intelligent caching
	Trustworthy Systems	×	×	✓	Security foundation that also provides next-generation encryption and integrity verification
Security and Compliance	Cisco Umbrella (OpenDNS)	×	×	✓	Protection from malware, botnets, phishing, and targeted online attacks using real-time threat intelligence
	Cisco Stealthwatch Enterprise	×	✓	✓	Branch network visibility and device-level incident response with packet capture and machine learning
	Encrypted Traffic Analytics	×	×	✓	Ability to find malicious activity in encrypted traffic without decryption

Cisco software subscription licenses for routing make it easy for IT to get started on their intent-based networking journey.

- Gain flexibility and investment protection
- License portability between on-prem and cloud management
- Access to ongoing routing innovations

Learn more about software subscription for routing at [cisco.com/go/dnawan](https://www.cisco.com/go/dnawan)

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) C83-731053-04 04/18

Victor:

Interfaz digital de inicio:

función de visualización de canal de empresa solo disponible en la serie 4000 de Cisco se encarga de simplificar operaciones y despliegue de los servicios de canales virtuales en cualquier plataforma.

S4000

Básicamente, esta función ahorra tiempo obteniéndose nuevos servicios de red virtual en minutos.

Organiza y administra los servicios para acelerar el mantenimiento y las respuestas.

Cisco IOS XE sistema operativo de interconexión de redes:

se basa en linux y proporciona una arquitectura de software distribuida que elimina muchas de las responsabilidades del sistema operativo del proceso de IOS. Este ejecuta una copia de IOS lo que permite que los comandos CLI sean los mismos entre Cisco IOS y IOS XE.

- **Native Application Hosting (Alojamiento de aplicaciones nativas):** No necesita dispositivos de red adicionales en la sucursal. Permite tener una plataforma para usar las propias herramientas y utilidades que se quieran, es decir, facilita al Sistema Operativo para que se ajuste a las herramientas existentes (desarrolladas mediante Linux). Por último, puedes tener todas estas aplicaciones en un dispositivo de red.
- **Integrated compute with Cisco UCS E-Series servers (Servidores con cálculo integrado con Cisco UCS E-Series):** Recursos de cálculos locales para aplicaciones, datos, restauración de datos de reserva y analíticas. Presenta el tipo de servidores Cisco UCS E-Series teniendo un centro de datos para la sucursal, lo que permite que no comprometas los servicios de red vitales.

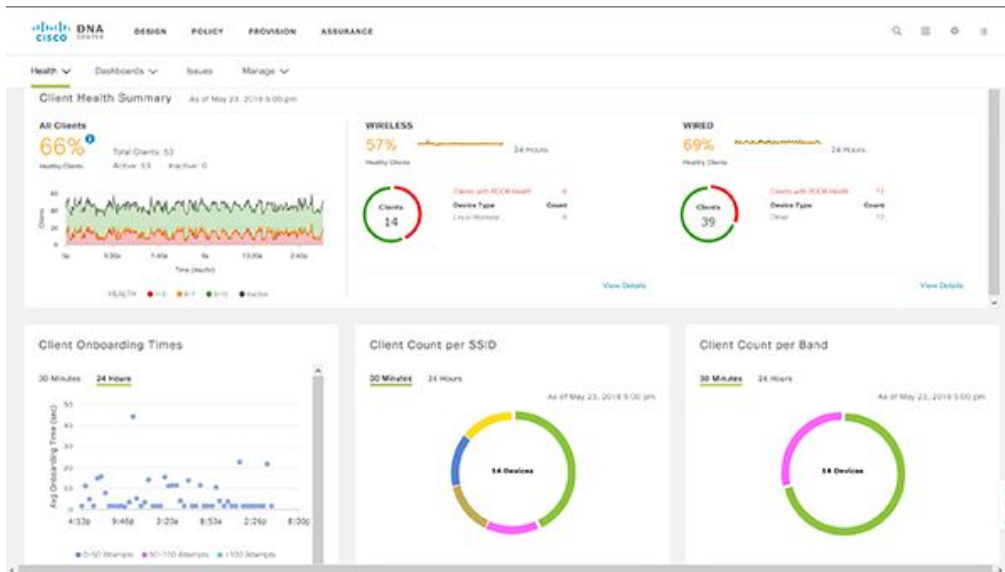
S4000

Cisco DNA Center:

Gestión

- Control total desde un panel de único
- Vistas granulares de redes, servicios y dispositivos
- Gestión del ciclo de vida del dispositivo
- Importe mapas y configuraciones para Cisco Prime o APIC-EM

S4000



Automatización

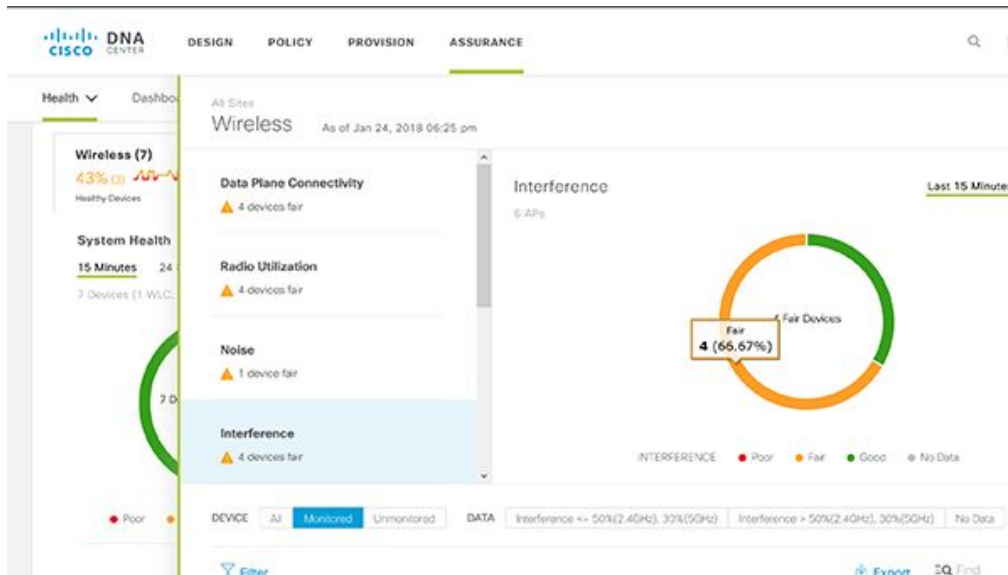
- Descubrimiento automatizado de dispositivos
- Creación de políticas drag-and-drop
- Implementación de dispositivos sin intervención
- Calidad del servicio (QoS) automatizada

The screenshot shows the Cisco DNA Center Image Repository page. It displays a table of network images with the following columns: Family, Image Name, End-User Image, Version, Golden Image, and Device Role. The table lists several Cisco devices and their corresponding images.

Family	Image Name	End-User Image	Version	Golden Image	Device Role
Cisco 5520 Series Wireless Contr...	Wireless Controller (8.5.120.0)	1	8.5.120.0 SMAJ (N/A)	*	
Cisco ASR 1001-X Router	asr1001x-universak9_nof... Verified	1	16.6.1 SMAJ (0)	*	
Cisco ASR 1002 Router	asr1000rpt-adventerprisek9.0...	1	03.17.04.5 SMAJ (0)	*	
Cisco ASR 1002-X Router	asr1002x-universak9.03.16.02...	1	03.16.02.5 SMAJ (0)	*	
Cisco ASR 1004 Router	asr1000rpt-adventerprisek9.0...	2	03.16.07.5 SMAJ (0)	*	

Análisis

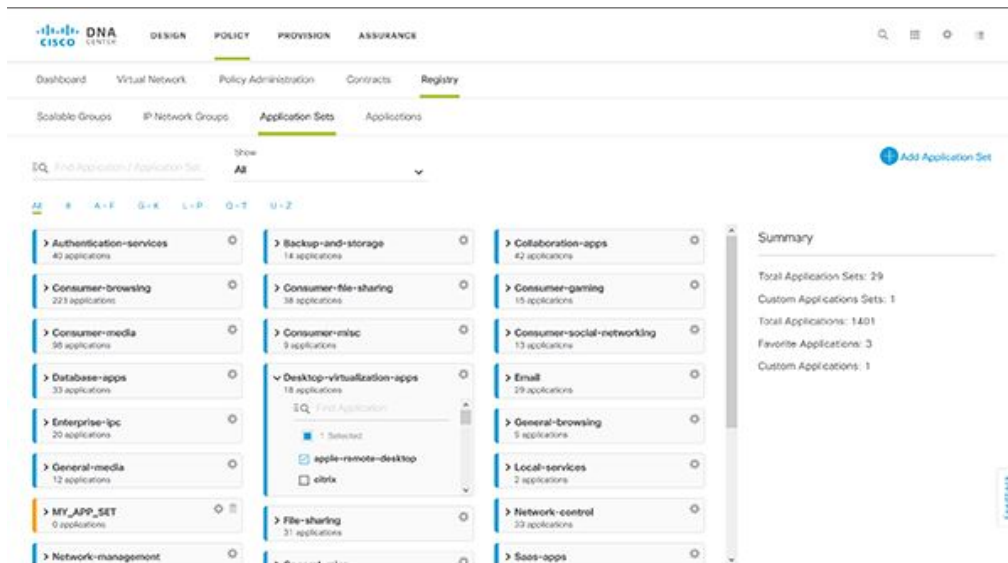
- Todo como sensor
- Análisis guiados por el contexto
- Más de 150 datos procesables
- Remediación guiada



S4000

Seguridad

- Detección y respuesta ante amenazas
- Integración de ISE y Stealthwatch
- Análisis de tráfico encriptado
- Segmentación muy segura



Pay as you grow performance and services: Tienes la posibilidad de comprar el equipamiento necesario actual para después poder actualizar cuando quieras sin tener que realizar un cambio de equipamiento completo.

- **CISCO DNA Center centralized management**

Sistema de control centralizado que permite:

- Simplificar la gestión de la red.
- Gestiona tu red empresarial sobre un tablero centralizado.
- Implementar redes en minutos, no días. Utilizando flujos de trabajo intuitivos, Centro de DNA hace que sea fácil Diseño, provisión y aplicación de políticas a través de su red.
- Costos más bajos. Impulsado por la política aprovisionamiento y guiado red de incremento de remediación tiempo de actividad y tiempo de reducción gastado en la gestión simple operaciones de red.
- Transforma tu red con servicios y aplicaciones en la nube que se benefician de este inteligente optimización de la red.

S4000

- **Cisco SD-WAN**

Las WAN tradicionales no pueden mantener el ritmo de aplicaciones que se están moviendo a la nube ni el creciente número de dispositivos que se conectan, siendo cada vez más complejas y costosas de operar. La WAN definida por software (SD-WAN) constituye un nuevo enfoque para la conectividad de red que reduce los costes operativos y mejora la experiencia de uso de las aplicaciones.

SD-WAN de Cisco ofrece:

- Permite establecer transportes independientes que permiten reducir los costes e incrementar el ancho de banda
- Ofrece una experiencia de usuario óptima para las aplicaciones SaaS y se extiende de forma infalible en la nube pública
- Proporciona una segmentación de extremo a extremo para proteger recursos informáticos vitales para las empresas
- Hace posible cumplir los SLA en aplicaciones empresariales críticas

SD-WAN de Cisco puede ayudarle.			
	Desafíos para las empresas	Funciones de SD-WAN de Cisco	Ventajas de la migración
Nube	<ul style="list-style-type: none"> >50 % del tráfico se produce en la nube, y aún así la red sigue sin estar preparada para la nube SaaS no funciona debidamente Flujos de trabajo complejos para AWS/Azure de la nube pública 	<ul style="list-style-type: none"> Una única superposición que se extiende al Data Center, a la nube y a la sucursal Optimización dinámica para QoS y para otros SaaS 	<ul style="list-style-type: none"> Optimizado para la nube pública y para SaaS Tiempo de respuesta de SaaS 4 veces más rápido Conectividad perfecta a la nube pública
Coste	<ul style="list-style-type: none"> Costes de ancho de banda inasequibles, de 100 USD/mbps El tráfico crece un 30 % cada año Una arquitectura rígida necesita entre 6 y 9 meses para llevar a cabo un cambio de política simple 	<ul style="list-style-type: none"> Combinación de MPLS con banda ancha de bajo coste/LTE Administración centralizada y visibilidad de aplicaciones 	<ul style="list-style-type: none"> Reducción de >50 % en los costes de la WAN Control de cambios de seis meses a dos días

Experiencia con las aplicaciones	<ul style="list-style-type: none"> La experiencia con las aplicaciones (SLA) es impredecible El 70 % de las interrupciones de aplicaciones se deben a problemas de red 	<ul style="list-style-type: none"> Enlaces híbridos activo-activo Políticas con reconocimiento de aplicaciones con ejecución en tiempo real 	<ul style="list-style-type: none"> SLA de aplicaciones predecible Sin interrupciones en las aplicaciones debido a las redes
Seguridad	<ul style="list-style-type: none"> Difícil de garantizar Activos fundamentales de la empresa, conexiones inalámbricas de invitados, partners empresariales Vulnerabilidades en las arquitecturas híbridas 	<ul style="list-style-type: none"> Segmentación de la WAN con políticas granulares Autenticación + cifrado + seguridad de la nube para redes híbridas 	<ul style="list-style-type: none"> Aislamiento de los activos fundamentales de la empresa, conexiones inalámbricas de invitados, partners empresariales Seguridad sólida para redes híbridas

Cisco® Application Visibility and Control (AVC) Configurar una red compatible con la aplicación

Tiene la capacidad de detectar cada aplicación en su red y optimizar el ancho de banda con políticas conscientes de la aplicación.

Cisco AVC supervisa el rendimiento de la aplicación y resuelve los problemas que surgen. Le ayuda a entregar políticas de intención comercial en toda la red. Y hace todo esto sin aparatos adicionales de una manera sencilla y potente.

S4000

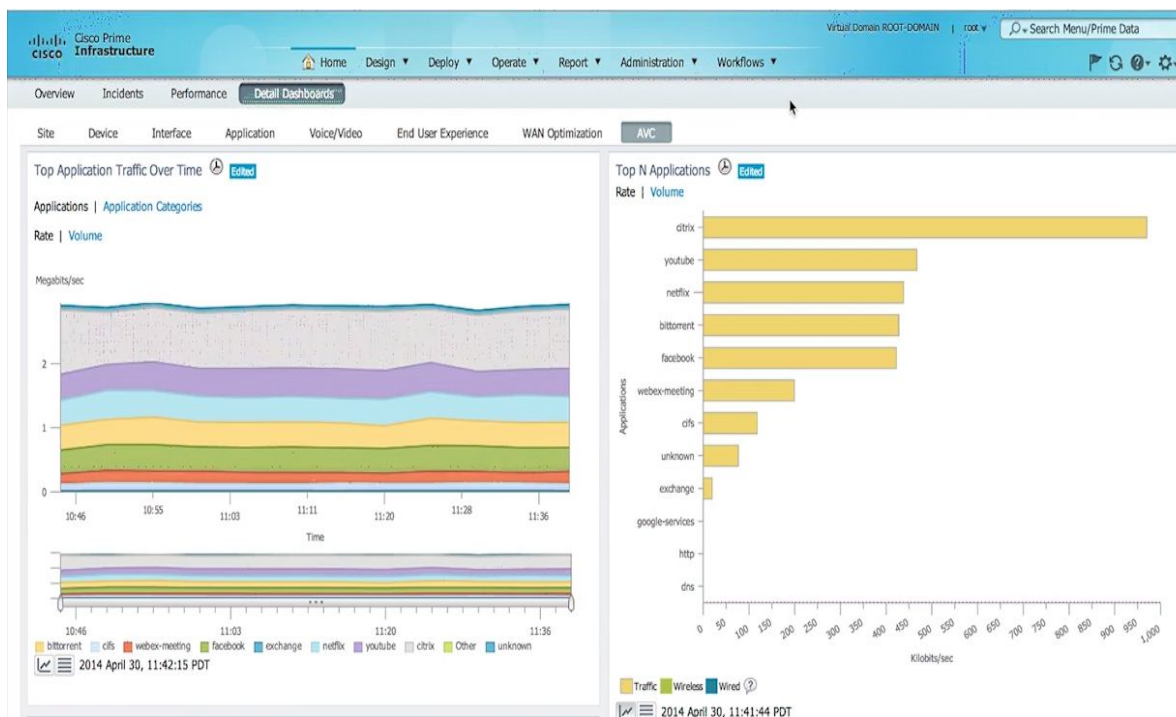


Figura Router. Ejemplo Aplicación AVC

WAN optimization (Cisco WAAS with Akamai)

- **Ahorrar dinero**

Use transporte alternativo como banda ancha o 4G LTE para aumentar el MPLS tradicional y para seleccionar dinámicamente la ruta más rentable para aplicaciones y datos.

- **Aumentar la productividad del usuario.**

La optimización WAN de próxima generación acelera las aplicaciones empresariales, SaaS e IaaS que se entregan desde infraestructuras privadas y virtuales privadas en la nube. Ayude a su empresa a ofrecer experiencias digitales de alta calidad.

- **Optimizar el ancho de banda**

Reduzca el consumo de ancho de banda con almacenamiento inteligente en caché, compresión y optimización de aplicaciones para aumentar el rendimiento.

DANIEL:

ISR 4000 Series Benefits
Cisco public



Benefits of Upgrading to Cisco 4000 Series Integrated Services Routers



Learn more at <https://www.cisco.com/go/isr4000>

S4000

Intent-based networking capabilities	Features	First-Generation (Cisco 1800, 2800, and 3800 Series [EOL Oct 2016])	Generation 2 (ISR G2) (Cisco 1900, 2900, and 3900 Series [EOS Dec 2017])	Cisco 4000 Series Integrated Services Routers	Benefits
Optimization	WAN optimization (Cisco WAAS with Akamai)	×	✓	✓	Improved application performance and WAN offload with Layer 4 through 7 optimization and intelligent caching
Security and Compliance	Trustworthy Systems	×	×	✓	Security foundation that also provides next-generation encryption and integrity verification
	Cisco Umbrella (OpenDNS)	×	×	✓	Protection from malware, botnets, phishing, and targeted online attacks using real-time threat intelligence
	Cisco Stealthwatch Enterprise	×	✓	✓	Branch network visibility and device-level incident response with packet capture and machine learning
	Encrypted Traffic Analytics	×	×	✓	Ability to find malicious activity in encrypted traffic without decryption

Cisco software subscription licenses for routing make it easy for IT to get started on their intent-based networking journey.

- Gain flexibility and investment protection
- License portability between on-prem and cloud management
- Access to ongoing routing innovations

Learn more about software subscription for routing at [cisco.com/go/dnawan](https://www.cisco.com/go/dnawan)

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (11159) C32-731053-04 04/18

En cuanto al apartado de seguridad podemos observar en la imagen superior como en el aspecto de **'Security and Compliance'**, el único apartado el cual incorpora tanto la segunda como la tercera generación de los routers de Cisco es el **'Cisco Stealthwatch Enterprise'**.

Dicho apartado gestiona lo siguiente:

Cisco Stealthwatch utiliza la telemetría en la infraestructura de la red existente para detectar amenazas avanzadas, realizar diagnósticos más exhaustivos y simplificar la segmentación de red. Gracias a sus sistemas de aprendizaje automático y modelado de comportamiento líderes en el sector, podrá adelantarse a las amenazas emergentes en su negocio digital.



Este apartado mejora la visibilidad de la red pudiendo detectar los ataques que traspasan las defensas del perímetro en el negocio digital, patrones maliciosos en el tráfico encriptado.

<DPLAHER>
<JDOMDAR>
<IMARMEN>
<JACOGON>
<VCARLEO>
<SMARGON>

DANIEL:

Por último, en cuanto al apartado de seguridad podemos observar en la imagen mostrada anteriormente como en el aspecto de **'Security and Compliance'**, el apartado el cual incorpora en este caso solamente la tercera generación de los routers de Cisco es **'Encrypted Traffic Analytics'**.

Dicho apartado que solamente incluye la tercera generación de routers de Cisco es la capacidad de hacer 'Análisis de tráfico cifrado':

Aprovechar las últimas capacidades de red de Cisco para evitar, detener o mitigar las amenazas más rápido que nunca. Cisco Digital Network Architecture (DNA) es la primera red de la industria con la capacidad de encontrar amenazas en el tráfico cifrado.

S4000

Aray:

- **TRUSTWORTHY SYSTEMS (Sistemas de confianza):** en lo que a seguridad se refiere, los **Trustworthy Systems** de Cisco son sistemas que nos proporcionan cifrado de futuras generaciones y verificación de la integridad.
 - **Sellos de confianza de los Trustworthy Systems:**
 - Los proveedores de confianza se esfuerzan por garantizar que un producto se diseñe, se desarrolle, se fabrique, se venda y se repare según lo establecido en los manuales.
 - Los proveedores de confianza toman medidas para asegurar su fabricación y distribución en cadenas de suministro contra la falsificación y manipulación, y para prevenir la instalación de características no autorizadas tales como "puertas traseras".
 - Productos confiables que cumplen con las normas de seguridad de la industria y del gobierno relevante para los requerimientos del negocio del cliente.

- **Cisco Umbrella (Open DNS):** Cisco Umbrella es una plataforma de seguridad en la nube que proporciona una primera línea de defensa contra las amenazas en Internet donde sea que vayan los usuarios, es decir, desde un PC, portátil, un smartphone...
 - Umbrella usa DNS para detener las amenazas en todos los puertos y protocolos, incluso en las conexiones directas a IP, con el fin de detener el malware antes de que llegue a sus puntos finales o red.

S4000

Cisco ISR 4000 Family I/O Design

Management Interface
out-of-band control plane
connection directly to a
management network

Front-Panel GE

- RJ45/SFP GE Interfaces
- PoE+ available on some models

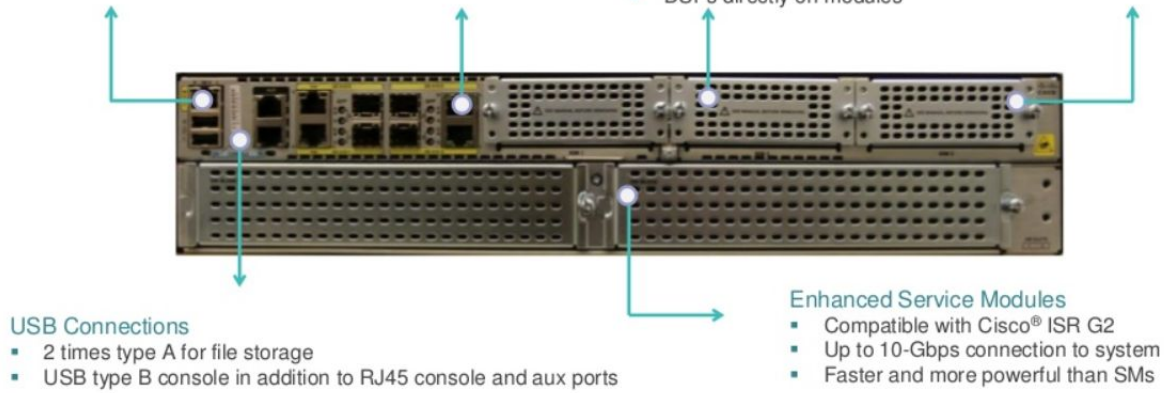
Network Interface Modules (NIMs)

- Larger and more powerful than EHWICs
- Up to 8 ports per module
- DSPs directly on modules

Optional Drive NIM for Embedded Applications

- RAID 1 for data protection
- Single HD (future) and dual SSD options

S4000



USB Connections

- 2 times type A for file storage
- USB type B console in addition to RJ45 console and aux ports

Enhanced Service Modules

- Compatible with Cisco® ISR G2
- Up to 10-Gbps connection to system
- Faster and more powerful than SMs

Glosario de comandos



- **Desactivar translating “xyz”:**

“no ip domain lookup”

- **Habilitar conexión vía telnet:**

```
configure terminal
line vty 0 15
no login
login local
username moi password moi
username moi privilege 15
```

IP para el Switch:

```
configure terminal
interface vlan 1
ip address (dirección IP) (máscara)
no shutdown
```

GDC

- **Guardar configuración:**

“copy running-config startup-config”

- **Ejecutar configuración de la memoria:**

“copy startup-config running-config”

- **Establecer red en RIP:**

```
router rip
network (ip)
```

- **Router on a stick:**

Configuración del switch:

```
interface (puerto)
switchport mode trunk
```

Router. Desactivar IP del puerto trunk:

```
interface (puerto)
no ip address
no shutdown
```

Configuración del router (subinterfaz 1 y 2):

```
interface (puerto).1
encapsulation dot1q 1 native
ip address (ip) (máscara)
exit
interface (puerto).2
encapsulation dot1q 2
ip address (ip) (máscara)
```

- **Configurar NAT:**

Lista de equipos que podrán “salir”

```
“access-list 1 permit (IP) 0.0.0.255”
```

Lista de equipos de la lista anterior que usan PAT a través del puerto:

```
“ip nat inside source list 1 interface (puerto interno) overload”
```

IP pública que vamos a usar:

```
“ip nat pool my_public_ip (ip pública) (misma ip pública) netmask (máscara)”
```

Asociamos la IP pública a la lista de acceso 1:

```
“ip nat inside source list 1 pool my_public_ip overload”
```

Establecemos que puerto va hacia la red interna:

```
interface (puerto interno)
ip nat inside
exit
```

GDC

Establecemos que puerto va hacia la red externa:

```
interface (puerto externo)
ip nat outside
exit
```

- **Activar OSPF:**

```
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
```

- **Activar RIP:**

```
router rip
network (IP)
```

- **Activar EIGRP:**

```
router eigrp 1
network 0.0.0.0 255.255.255.255
```

- **Configurar PC:**

Entramos en “Command Prompt”

```
ipconfig (IP) (máscara) (gateway)
```

- **SSH:**

```
enable
configure terminal
ip domain-name (nombre)
hostname (distinto de Router)
crypto key generate rsa
How many bits in the modulus [512]: 1024

ip ssh time-out 30
ip ssh authentication-retries 3
ip ssh version 2
username (nombre) privilege 15
line vty 0 4
transport input ssh
login local
```


Plantilla para crear nuevas páginas

Modo de uso

Simplemente copia esta página y pégala en el documento y con eso te aseguras que tu página cumple con la guía de estilos.

Fíjate que aquí tienes el título 1 de tu sección (en nuestro ejemplo “Plantilla para crear nuevas páginas”) y el subtítulo o título 2 (en nuestro caso, Modo de uso). Respetar el tamaño de fuente, las negritas,... los márgenes,... tal y como lo ves aquí.

Para ello, simplemente copia y pega esta página.

```
Configure terminal
Interface FastEthernet 0/1
```

Para resaltar un comando en un cuadro de texto, subrayar el comando de la siguiente manera:

“Comando”

Para hacer mención a una figura, escribir en cursiva y negrita la referencia de dicha figura, p.ej.: ***Figura X.Y***

