

Instituto Tecnológico y de Estudios Superiores de Monterrey  
Campus Santa Fe



Interconexión de dispositivos  
TC2006B.300

## Reporte final: Solución del reto

Andrea Serrano Diego	A01028728
Octavio Fenollosa Sosa	A01781042
Emilio Sibaja Villarreal	A01025139
Iwalani Amador Piaga	A01732251
Iván Díaz Lara	A01365801

09 de junio del 2022

# Resumen

Anualmente, se realiza el International Collegiate Programming Contest (ICPC), un concurso de programación y algoritmos, para dicho evento es necesario diseñar, configurar e interconectar una red local a la infraestructura de la red actual.

El Tec campus Santa Fe tiene que prepararse para ser la sede del concurso este año, por lo que se da una propuesta de la solución de la implementación y el diseño de la red misma conforme a las especificaciones proporcionadas.

En este reporte desglosamos el desarrollo de nuestra propuesta de diseño de red para el mencionado concurso, planteando las directrices en cuanto alcance, objetivos y definición de requerimientos. Desarrollamos la elección del espacio físico, diseño lógico y físico de la red con nuestra propuesta económica de los equipos requeridos. Posteriormente, se podrán observar las evaluaciones y simulaciones del correcto funcionamiento de la red. Al final concretamos el proyecto y mencionamos propuestas de valor para una mejora a futuro.

# Índice General

Índice de Figuras	4
Índice de Tablas	5
1. Introducción	1
1.1. Contexto del problema	1
1.2. Objetivos del reto	1
2. Planteamiento del problema	2
2.1. Problemática	2
2.2. Alcance del proyecto	2
2.3. Objetivos	2
2.5. Propuesta inicial de solución del reto	3
3. Propuesta de solución del reto	4
Dirección o subred que se debe de asignar, y requerimientos de conexión.	4
3.1. Espacios físicos propuestos	5
Figura 1 Figura de muestra para el índice de figuras	6
3.2. Equipo requerido y propuesta económica	6
Tabla 1 Tabla de muestra para el índice de tablas	7
3.3. Diseño lógico de la red	8
Tabla 2 Otra tabla de muestra para el índice de tablas	8
Figura 2 Otra figura de muestra para el índice de figuras	9
3.4. Diseño físico de la red	9
Figura 3 Otra figura de muestra para el índice de figuras	10
3.5. Configuración y pruebas de conectividad	11
4. Evaluación de resultados	23
4.1. Problemáticas enfrentadas durante la etapa de solución del reto	23
4.2. Evaluación de los objetivos planteados	23
4.3. Evaluación de la propuesta	23
5. Conclusiones y trabajo futuro	24
5.1. Conclusiones	24
5.2. Trabajo futuro	24
Apéndice	25
Glosario de términos	49
Bibliografía	52

## Índice de Figuras

<a href="#">Figura 1 Figura de muestra para el índice de figuras</a>	<a href="#">3</a>
<a href="#">Figura 2 Otra figura de muestra para el índice de figuras</a>	<a href="#">4</a>
<a href="#">Figura 3 Una figura más para muestra en el índice de figuras</a>	<a href="#">5</a>

## Índice de Tablas

<u>Tabla 1 Tabla de muestra para el índice de tablas</u>	<u>3</u>
<u>Tabla 2 Otra tabla de muestra para el índice de tablas</u>	<u>3</u>

# Capítulo 1

## 1. Introducción

### 1.1. Contexto del problema

Este año el campus Santa Fe será la sede del evento International Collegiate Programming Contest (ICPC), este concurso de programación y algoritmo requiere de la implementación de una red local interconectada a la red e infraestructura del campus Tec.

ICPC requiere de una infraestructura de red estable, segura y confiable para que el concurso se lleve a cabo de manera correcta, ya que en el caso de que surja cualquier problema, los participantes del concurso regional se podrían ver directamente afectados y quedaría en manos del director ejecutivo.

Para esta edición regional del ICPC participarán 8 equipos, cada uno conformado por 3 integrantes y 1 entrenador, donde cada equipo deberá tener un área de trabajo asignada y debido a las condiciones sanitarias actuales, se tendrá que respetar la sana distancia en la planeación del diseño físico del área del concurso.

Debido a las restricciones sanitarias, el Campus Santa Fe puede tener hasta 8 equipos repartidos en dos salones diferentes. Además, se ha definido que cada equipo debe tener un segmento de red diferente. Campus Santa Fe asignará un bloque de red, el cual se tiene que partir para poder atender hasta 8 equipos cada uno con 3 integrantes, así como otro segmento para 8 entrenadores y un administrador de sede. El campus configura un nodo específico donde se tendrá el equipo que proveerá conexión con el resto de la red del Tec y la salida a internet.

### 1.2. Objetivos del reto

Diseñar e implementar la interconexión de las redes locales necesarias para realizar con éxito, y con altos estándares de calidad, el evento del ICPC dentro de las instalaciones del Tecnológico de Monterrey campus Santa Fe.

# Capítulo 2

## 2. Planteamiento del problema

Habrán 8 equipos participando en esta edición regional del ICPC, cada equipo consta de 3 jugadores y 1 entrenador, cada equipo debe tener un área de trabajo designada, y debido a las condiciones sanitarias actuales, el diseño y la planificación deben respetar la distancia sanitaria en la zona de competición.

El buen funcionamiento de la competencia requiere una infraestructura de red estable, segura y confiable, ya que ante cualquier inconveniente, los participantes de la competencia regional pueden verse directamente afectados y estarán en manos del Director Ejecutivo.

En los requerimientos principales brindados para el evento, se menciona que participarán como máximo 8 equipos, 3 integrantes por equipo, dando como resultado 24 participantes, además debe existir un segmento de administración, uno para 8 entrenadores (1 por equipo), y por último un segmento de conexión a internet.

### 2.1. Problemática

Diseñar e implementar una red local segura y confiable, la cual se interconecte a la infraestructura del Tecnológico de Monterrey campus Santa Fe. Además de contar con las medidas de sana distancia por Covid-19.

La red tiene que ser una que cumpla con los más altos estándares internacionales, sin embargo, no puede ser un diseño excesivamente caro.

### 2.2. Alcance del proyecto

Propuesta de diseño de red para el socio formador sobre el concurso ICPC para implementarlo en las instalaciones e infraestructura del campus Santa Fe.

### 2.3. Objetivos

La red debe poder mantener 8 equipos de 3 personas, 8 coaches y un administrador, deben de estar aisladas las redes de los equipos entre sí. El administrador puede checar el estado de la red en todo momento. Y todas las redes deben poder conectarse a internet.

## 2.5. Propuesta inicial de solución del reto

Al principio consideramos usar hubs para cada equipo en un solo segmento independiente, sin embargo, por el tipo de datos y la rapidez del uso de datos de la competencia, la posibilidad de algún retraso o colisión no son viables, entonces decidimos utilizar switches de 5 puertos, teniendo suficientes espacios para los equipos.

Definido esto decidimos usar solamente 1 router, ya que cada router es muy costoso y no creemos que sea pertinente tener un costo tan exorbitante para una competencia que es relativamente pequeña (33 equipos conectados a la red local).

Debido a que se busca contar con un administrador que pueda tener acceso a todos los equipos de la red decidimos asignar un switch administrable, el cual será el enlace entre todas las redes y el router, para mitigar las fallas que pudieran ocurrir dentro de nuestra red decidimos implementar el diseño con usando una topología de red de tipo estrella.

Habrán 10 switches no administrables conectados al switch central, 8 para los participantes (1 por equipo), 1 para los coaches y 1 para el administrador. A cada puerto de este switch administrable se le asignará una VLAN.



# Capítulo 3

## 3. Propuesta de solución del reto

### **Identificación de la cantidad de segmentos de red necesarios.**

Con lo anterior se prevé tener 11 segmentos:

1. Participantes (8 segmentos)
2. Coaches
3. Administración
4. Conexión a internet

### **Protocolos y necesidades de comunicación en la red:**

Basándose en el modelo TCP/IP para la comunicación en la red:

Protocolos de internet:

- IP

Protocolos de enrutamiento de redes:

- Telnet
- SSH

### **Dirección o subred que se debe de asignar, y requerimientos de conexión.**

Para el evento, y con fines de demostración, en la propuesta se ha asignado una dirección privada “198.162...”, una dirección configurable en la red que los routers pueden usar para identificarse con otros dispositivos de la misma red, así como el reto requiere.

Se requiere que la red pueda dividirse en múltiples LAN's (nosotros las implementamos como VLANs) para así asignar una a cada conjunto de personas, 1 para los coaches, 8 para cada equipo de participantes y 1 para la administración. Esta asignación de IP's la hicimos de manera dinámica mediante el protocolo DHCP, sin embargo para que no haya conflictos de repetición de IPs para cada pool de DHCP se tuvo que excluir el gateway de cada una de las VLANs.

### **Propuesta de espacios físicos dentro del Tec que cumplen con los requerimientos:**

- Multicanchas
- Salón de congreso

Los elementos y equipos que son necesarios para la propuesta:

- Routers (1)
- Switch administrable (1)
- Switch No Administrable (1)
- Cables Ethernet UTP (Longitud Variable) (Bobina de Cable CAT5 200mts)

De acuerdo al estándar de cableado estructurado de la EIA/TIA 568, los cables UTP CAT 5 entre conexiones no exceden los 100 metros, además, estos mismos cables están acomodados contra la pared a fin de evitar accidentes (tropiezos y desconexión), y sobre todo la identificación de la conexión en caso de haber algún problema con un cable, para una solución óptima (cambiar un cable dañado por uno funcional).

### **3.1. Espacios físicos propuestos**

Siendo multicanchas la alternativa A, y el Salón de congreso la alternativa B, se argumenta la propuesta de acuerdo a lo observado:

#### **Multicanchas:**

Cuenta con un espacio cuadrado aproximado (aristas de piso-pared) de 37.5 x 37.5 metros, permitiendo la distribución de las mesas de equipos, coaches y administrador con sana distancia de 1.5 metros. Además de la posibilidad de incluir aproximadamente al menos 18 mesas adicionales y seguir cumpliendo con las normativas.

#### **Salón de congresos:**

Su espacio cuadrado es menor a diferencia de multicanchas (se especula que al menos 50%), por lo que cumple con el espacio para la correcta distribución de cada mesa de equipos, coaches y administrador, pero no tiene espacio adicional para incluir más mesas, incumpliendo con el requisito de sana distancia.

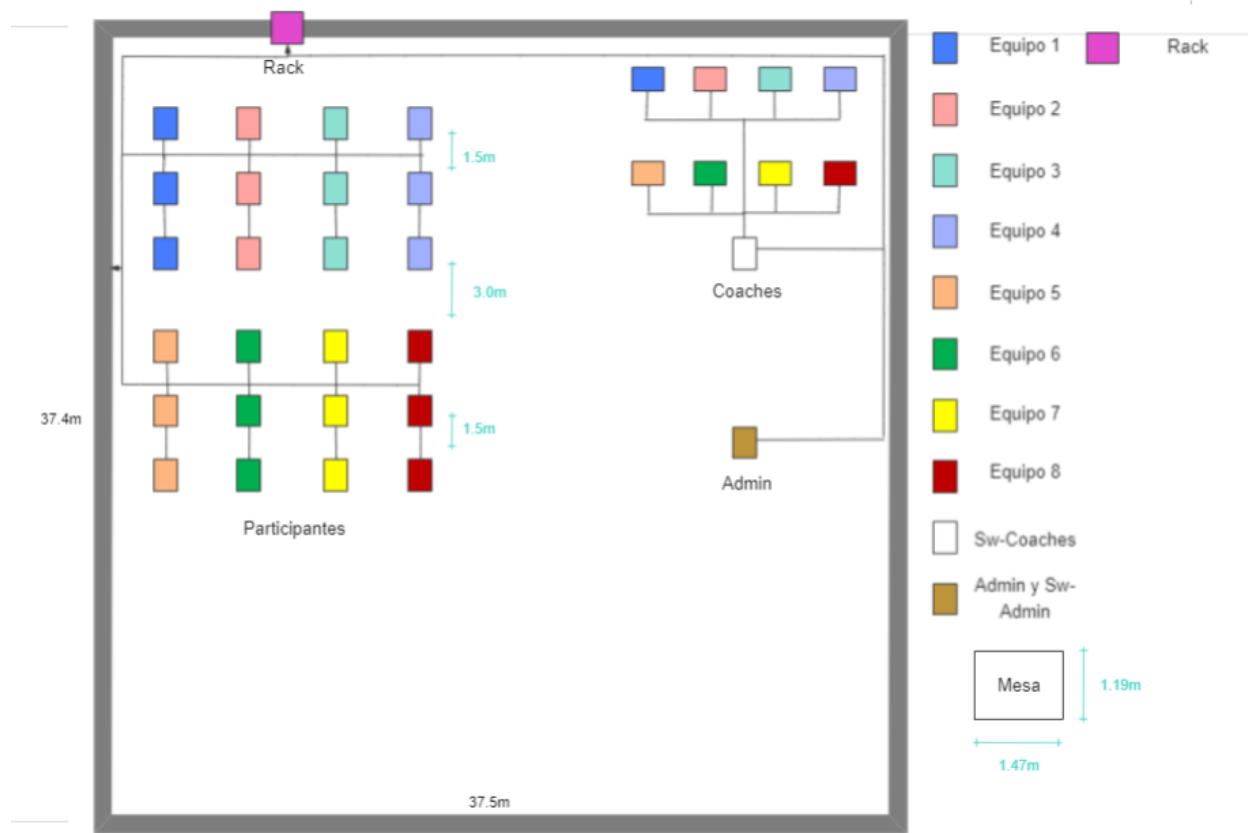


Figura 1 Figura de muestra para el índice de figuras

### 3.2. Equipo requerido y propuesta económica

Con respecto al beneficio estructural que proporciona Multicanchas a diferencia del Salón de Congresos, dentro de la propuesta se mantiene la decisión de implementar el evento y la conectividad dentro del espacio de Multicanchas.

Además de la distribución correcta de equipos y mesas, en el sketch se han optimizado los espacios para disminuir el uso de cableado que a su vez, disminuye el costo total.

**Instalación física de los equipos: Ver Apéndice 11.0**

De acuerdo al estándar de cableado estructurado de la EIA/TIA 568, los cables UTP CAT 5 entre conexiones no exceden los 100 metros, además, estos mismos cables están acomodados contra la pared a fin de evitar accidentes (tropiezos y desconexión), y sobre todo la identificación de la conexión en caso de haber algún problema con un cable, para una solución óptima (cambiar un cable dañado por uno funcional).

Es posible disminuir el costo final, sin embargo, eso significa que se deben usar equipos de otras marcas, abandonando la confiabilidad que ofrece cisco en sus equipos y sobre todo evitar problemas de compatibilidad, pues se toma en cuenta que la propuesta cuente con los más altos estándares, manteniendo la calidad del Tec.

Cantidad	Nombre.	Descripción/Justificación	Costo Unitario	Costo total
10	<a href="#">Switch-no-administrable</a>	<b>Cisco® Business CBS110-5T-D Switch no administrable de 5 puertos.</b> Se usarán para asignar una red a cada equipo de la competencia, para los participantes no es necesario administrar los switch, pues funcionarán como medio de conexión hacia fuera con switch main (que si administrara), además considerando que no se utilizarán todas las funciones que contiene un switch administrable, este tienen menor costo que los administrables. Siendo un costo por lo que se necesita, sin desperdiciar la operatividad.	1283	\$12.830,00
1	<a href="#">Switch-main</a>	<b>Switch Cisco Gigabit Ethernet CBS250, 16 Puertos, Administrable.</b> Para el switch main es necesario el uso de un dispositivo administrable porque funciona como medio de comunicación entre el administrador y los demás componentes (equipos, coaches y conexión al router main). Al ser administrable permitirá ajustar cada puerto del switch a una configuración especificada, monitorear y configurar la red. Además de tener el control sobre como viajan los datos en la red y quien tiene acceso a ellos.	5689	\$5.689,00
1	<a href="#">Router-main</a>	<b>Router Cisco Firewall Firepower 1010, Alámbrico, 1500Mbit/s, 8x RJ-45.</b> El router main es quien dará acceso a la conexión a internet (protocolo de internet) y analiza los datos que son enviados a través de la red (paquetes). Para el proyecto es necesario un router porque se necesitan conectar equipos a la red local del tec y a internet.	21559	\$21.559,00
2	<a href="#">Cableado UTP 5 (200 m)</a>	<b>BRobotix Bobina de Cable Cat5e UTP, 200 Metros.</b> Para lograr la interconexión entre dispositivos es necesario contar con cables UTP categoría 5, ya que este cable permite transmitir información de manera rápida y eficaz, con una velocidad de hasta 10000 Mbps a frecuencias de 100 Mhz. Normalmente es utilizada para conexiones cortas y para redes LAN, así como el reto demanda.	779	\$1.558,00
100	<a href="#">Plugs RJ-45</a>	<b>Intellinet Plugs Modulares RJ-45, Cat6</b> (para el reto serán necesarios 72 unidades de las 100 que incluye el paquete) Para disminuir el costo, los cables serán hechos a medida y desde cero, es por eso que se incluyen los plugs RJ-45 en esta misma propuesta económica.	4,43	\$443,00
<b>Total</b>				<b>\$42.079,00</b>

Tabla 1 Tabla de muestra para el índice de tablas

### 3.3. Diseño lógico de la red

Primero tuvimos que segmentar de manera correcta nuestras redes, tras analizar el problema de manera correcta y preguntando requerimientos a nuestro socio formador, pudimos crear un seccionamiento correcto de nuestras áreas tanto lógicas como físicas.

- LAN dedicada a los coaches
- LAN dedicada al administrador
- Optimización de routers
- División correcta de los equipos, 1 LAN por cada equipo.
- “Subnetting” adecuado a las necesidades de las competencias.
  - ◆ División de subredes, generando una para cada equipo.
  - ◆ Seguridad entre equipos.

Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast	Wildcard
14	14	0	192.168.1.0	/28	255.255.255.240	192.168.1.1 - 192.168.1.14	192.168.1.15	0.0.0.15
6	6	0	192.168.1.16	/29	255.255.255.248	192.168.1.17 - 192.168.1.22	192.168.1.23	0.0.0.7
6	6	0	192.168.1.24	/29	255.255.255.248	192.168.1.25 - 192.168.1.30	192.168.1.31	0.0.0.7
6	6	0	192.168.1.32	/29	255.255.255.248	192.168.1.33 - 192.168.1.38	192.168.1.39	0.0.0.7
6	6	0	192.168.1.40	/29	255.255.255.248	192.168.1.41 - 192.168.1.46	192.168.1.47	0.0.0.7
6	6	0	192.168.1.48	/29	255.255.255.248	192.168.1.49 - 192.168.1.54	192.168.1.55	0.0.0.7
6	6	0	192.168.1.56	/29	255.255.255.248	192.168.1.57 - 192.168.1.62	192.168.1.63	0.0.0.7
6	6	0	192.168.1.64	/29	255.255.255.248	192.168.1.65 - 192.168.1.70	192.168.1.71	0.0.0.7
6	6	0	192.168.1.72	/29	255.255.255.248	192.168.1.73 - 192.168.1.78	192.168.1.79	0.0.0.7
6	6	0	192.168.1.80	/29	255.255.255.248	192.168.1.81 - 192.168.1.86	192.168.1.87	0.0.0.7

Tabla 2 Otra tabla de muestra para el índice de tablas

Sin embargo, tener un buen diseño lógico no es suficiente para que una red funcione de manera adecuada, y fue sobre estos cambios donde implementamos los protocolos necesarios para poder llegar al diseño final de la red.

Primero se construyó lo que son las VLAN, con su debido encapsulamiento, para cada segmento formado por cada equipo dentro de la competencia (10 equipos en total).

Proseguimos configurando nuestro Router (RT-Main) con el protocolo DHCP, para ello comenzamos excluyendo las IP de los Gateways, (para que estas no sean asignadas a otros dispositivos por error) de los segmentos de Admin, Coach y de cada equipo, de la misma forma le asignamos un pool a cada segmento además de configurar la IP del DNS. Al terminar este proceso, a cada dispositivo de usuario final le cambiamos la configuración IP al modo de DHCP y así de manera automática se les asigna su dirección IP junto con la DNS anteriormente configurada.

Debido a que solamente contamos con un router local, decidimos conectarnos al router del segmento de internet a través de un protocolo de enrutado estático, ya que no contamos con algún tipo de variación en el camino que la conexión podría tomar.

Finalmente, terminamos asignando las contraseñas y un banner a todos nuestros dispositivos intermediarios. Al abrir el CLI en cada uno de los dispositivos, un mensaje de advertencia aparece indicando que se debe tener la debida autorización para tener acceso al dispositivo. En el modo EXEC de usuarios, privilegiado y para ingresar a las VTY se necesita ingresar una contraseña.

## Dirección IPv4 privada

### a.1.0/25

La red privada ha sido asignada por el docente a cargo, de acuerdo al número de equipo, donde a los equipos cuyo tercer octeto fuera impar, se asignó como cuarto octeto el 0.

Además de ello, se sabe que la dirección privada “198.162...” es una dirección que se puede configurar en una red. Es también, una IP privada que los routers pueden usar para identificarse con otros dispositivos de la misma red, así como el reto requiere.

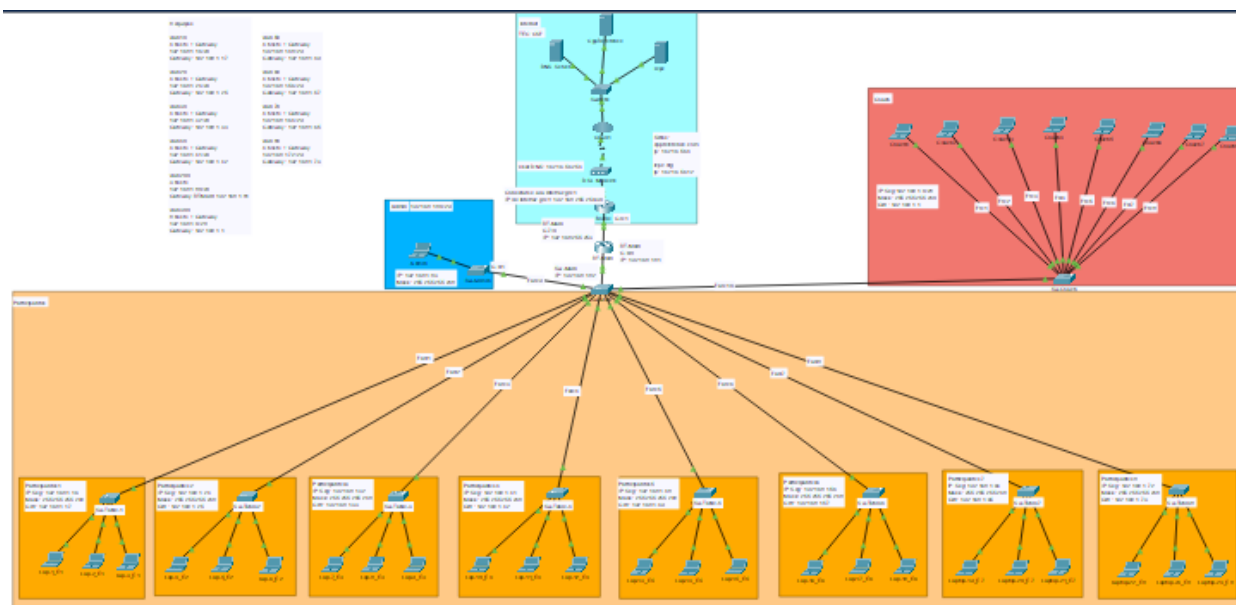


Figura 2 Otra figura de muestra para el índice de figuras



Es el mismo caso para los coaches, cada uno tiene una mesa de 1.47 x 1.19 metros, y una distancia de 1.5 metros entre ellos, sin embargo, el router se encontrará en una mesa separada delante de ellos.

El administrador tendrá su propia mesa donde, de la misma manera, encontraremos su router.

Basándonos en el estándar de cableado estructurado EIA/TIA 568 interconectamos todos nuestros dispositivos usando cables UTP CAT 5 entre conexiones que no excedan los 100 metros. También se buscará colocar dichos cables muy cerca a la pared y proteger con tapetes los segmentos que no se encuentren pegados a la pared.

El RT-Main y el SW-Main serán montados en el rack que ya se encuentra dentro de las instalaciones de multicanchas.

### 3.5. Configuración y pruebas de conectividad

#### **Pruebas de conectividad:**

**Admin acceso remoto, vía SSH a Sw-Main (Ver apéndice 1.1)**

**Admin acceso remoto, vía SSH a RT-Main (Ver apéndice 1.2)**

**Ping de Admin a RT-Main (Ver apéndice 1.3)**

**Ping de Admin a Coaches (Ver apéndice 1.4)**

**Ping de Admin a Equipo1 (Ver apéndice 1.5)**

**Ping de Admin a Equipo2 (Ver apéndice 1.6)**

**Ping de Admin a Equipo3 (Ver apéndice 1.7)**

**Ping de Admin a Equipo4 (Ver apéndice 1.8)**

**Ping de Admin a Equipo5 (Ver apéndice 1.9)**

**Ping de Admin a Equipo6 (Ver apéndice 1.10)**

**Ping de Admin a Equipo7 (Ver apéndice 1.11)**

**Ping de Admin a Equipo8 (Ver apéndice 1.12)**

**Ping de Coach a Equipo1 (Ver apéndice 2.1)**

**Ping de Coach a Equipo2 (Ver apéndice 2.2)**

**Ping de Coach a Equipo3 (Ver apéndice 2.3)**

**Ping de Coach a Equipo4 (Ver apéndice 2.4)**

**Ping de Coach a Equipo5 (Ver apéndice 2.5)**

**Ping de Coach a Equipo6 (Ver apéndice 2.6)**

**Ping de Coach a Equipo7 (Ver apéndice 2.7)**

**Ping de Coach a Equipo8 (Ver apéndice 2.8)**



**Ping de Coach a RT-Main (Ver apéndice 2.9)**  
**Conexión a internet desde Coach (Ver apéndice 2.10)**

**Ping de Equipo1 a su Gateway (Ver apéndice 3.1)**  
**Ping de Equipo1 a RT-Main (Ver apéndice 3.2)**  
**Conexión a internet desde Equipo1 (Ver apéndice 3.3)**

**Ping de Equipo2 a su Gateway (Ver apéndice 4.1)**  
**Ping de Equipo2 a RT-Main (Ver apéndice 4.2)**  
**Conexión a internet desde Equipo2 (Ver apéndice 4.3)**

**Ping de Equipo3 a su Gateway (Ver apéndice 5.1)**  
**Ping de Equipo3 a RT-Main (Ver apéndice 5.2)**  
**Conexión a internet desde Equipo3 (Ver apéndice 5.3)**

**Ping de Equipo4 a su Gateway (Ver apéndice 6.1)**  
**Ping de Equipo4 a RT-Main (Ver apéndice 6.2)**  
**Conexión a internet desde Equipo4 (Ver apéndice 6.3)**

**Ping de Equipo5 a su Gateway (Ver apéndice 7.1)**  
**Ping de Equipo5 a RT-Main (Ver apéndice 7.2)**  
**Conexión a internet desde Equipo5 (Ver apéndice 7.3)**

**Ping de Equipo6 a su Gateway (Ver apéndice 8.1)**  
**Ping de Equipo6 a RT-Main (Ver apéndice 8.2)**  
**Conexión a internet desde Equipo6 (Ver apéndice 8.3)**

**Ping de Equipo7 a su Gateway (Ver apéndice 9.1)**  
**Ping de Equipo7 a RT-Main (Ver apéndice 9.2)**  
**Conexión a internet desde Equipo7 (Ver apéndice 9.3)**

**Ping de Equipo8 a su Gateway (Ver apéndice 10.1)**  
**Ping de Equipo8 a RT-Main (Ver apéndice 10.2)**  
**Conexión a internet desde Equipo8 (Ver apéndice 10.3)**

## Configuraciones:

### RT-Main Config

```

!
version 12.2 // (Default) Sin cambios
no service timestamps log datetime msec // (Default) Sin cambios
no service timestamps debug datetime msec // (Default) Sin cambios
service password-encryption // Oculta las contraseñas de la configuración usando un cifrado Vigenere
!
hostname RT-Main // Configuración nombre del dispositivo
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0 // Contraseña encriptada para el comando enable
!
!
ip dhcp excluded-address 192.168.1.17 //Excluir las gateways del dhcp para no ser asignadas
ip dhcp excluded-address 192.168.1.25 //Excluir las gateways del dhcp para no ser asignadas
ip dhcp excluded-address 192.168.1.33 //Excluir las gateways del dhcp para no ser asignadas
ip dhcp excluded-address 192.168.1.41 //Excluir las gateways del dhcp para no ser asignadas
ip dhcp excluded-address 192.168.1.49 //Excluir las gateways del dhcp para no ser asignadas
ip dhcp excluded-address 192.168.1.57 //Excluir las gateways del dhcp para no ser asignadas
ip dhcp excluded-address 192.168.1.65 //Excluir las gateways del dhcp para no ser asignadas

```

```

ip dhcp excluded-address 192.168.1.73 //Excluir las gateways del dhcp para no ser asignadas
ip dhcp excluded-address 192.168.1.1 //Excluir las gateways del dhcp para no ser asignadas
!
ip dhcp pool EQUIPO1 //Asigna automáticamente los parámetros de IP y la máscara de esta subred
network 192.168.1.16 255.255.255.248 // Ingresas la IP y máscara para esta subred
default-router 192.168.1.17 // Asignas la gateway de esta subred
dns-server 162.16.56.254 // Ingresas la IP del dns-server
ip dhcp pool EQUIPO2 //Asigna automáticamente los parámetros de IP y la máscara de esta subred
network 192.168.1.24 255.255.255.248 // Ingresas la IP y máscara para esta subred
default-router 192.168.1.25 // Asignas la gateway de esta subred
dns-server 162.16.56.254 // Ingresas la IP del dns-server
ip dhcp pool EQUIPO3 //Asigna automáticamente los parámetros de IP y la máscara de esta subred
network 192.168.1.32 255.255.255.248 // Ingresas la IP y máscara para esta subred
default-router 192.168.1.33 // Asignas la gateway de esta subred
dns-server 162.16.56.254 // Ingresas la IP del dns-server
ip dhcp pool EQUIPO4 //Asigna automáticamente los parámetros de IP y la máscara de esta subred
network 192.168.1.40 255.255.255.248 // Ingresas la IP y máscara para esta subred
default-router 192.168.1.41 // Asignas la gateway de esta subred
dns-server 162.16.56.254 // Ingresas la IP del dns-server
ip dhcp pool EQUIPO5 //Asigna automáticamente los parámetros de IP y la máscara de esta subred
network 192.168.1.48 255.255.255.248 // Ingresas la IP y máscara para esta subred
default-router 192.168.1.49 // Asignas la gateway de esta subred
dns-server 162.16.56.254 // Ingresas la IP del dns-server
ip dhcp pool EQUIPO6 //Asigna automáticamente los parámetros de IP y la máscara de esta subred
network 192.168.1.56 255.255.255.248 // Ingresas la IP y máscara para esta subred
default-router 192.168.1.57 // Asignas la gateway de esta subred
dns-server 162.16.56.254 // Ingresas la IP del dns-server
ip dhcp pool EQUIPO7 //Asigna automáticamente los parámetros de IP y la máscara de esta subred
network 192.168.1.64 255.255.255.248 // Ingresas la IP y máscara para esta subred
default-router 192.168.1.65 // Asignas la gateway de esta subred
dns-server 162.16.56.254 // Ingresas la IP del dns-server
ip dhcp pool EQUIPO8 //Asigna automáticamente los parámetros de IP y la máscara de esta subred
network 192.168.1.72 255.255.255.248 // Ingresas la IP y máscara para esta subred
default-router 192.168.1.73 // Asignas la gateway de esta subred
dns-server 162.16.56.254 // Ingresas la IP del dns-server
ip dhcp pool ENTRENADORES //Asigna automáticamente los parámetros de IP y la máscara de esta
subred
network 192.168.1.0 255.255.255.240 // Ingresas la IP y máscara para esta subred
default-router 192.168.1.1 // Asignas la gateway de esta subred
dns-server 162.16.56.254 // Ingresas la IP del dns-server
ip dhcp pool ADMIN
network 192.168.1.84 255.255.255.252
default-router 192.168.1.85
dns-server 162.16.56.254

```

```

!
!
!
no ip cef // (Default) Sin cambios
no ipv6 cef // (Default) Sin cambios
!
!
!
username cisco secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
!
!
!
ip ssh version 2
no ip domain-lookup // Deshabilitar búsqueda automática de DNS
ip domain-name miempresa.com
!
!
!
!
!
!
!
interface Serial0/0 // (Default) Sin cambios
no ip address // (Default) Sin cambios
clock rate 2000000 // (Default) Sin cambios
shutdown // (Default) Sin cambios
!
interface Serial1/0 // (Default) Sin cambios
no ip address // (Default) Sin cambios
clock rate 2000000 // (Default) Sin cambios
shutdown // (Default) Sin cambios
!
interface Serial2/0 // (Default) Sin cambios
no ip address // (Default) Sin cambios
clock rate 2000000 // (Default) Sin cambios
shutdown // (Default) Sin cambios
!
interface GigabitEthernet6/0 // (Default) Sin cambios
no ip address // (Default) Sin cambios
duplex auto // (Default) Sin cambios

```

```

speed auto // (Default) Sin cambios
!
interface GigabitEthernet6/0.10 // Creación de las vlans
encapsulation dot1Q 10 // Estándar para el método de etiquetado para las vlans
ip address 192.168.1.17 255.255.255.248 // Gateway de la interfaz
!
interface GigabitEthernet6/0.20 // Creación de las vlans
encapsulation dot1Q 20 // Estándar para el método de etiquetado para las vlans
ip address 192.168.1.25 255.255.255.248 // Gateway de la interfaz
!
interface GigabitEthernet6/0.30 // Creación de las vlans
encapsulation dot1Q 30 // Estándar para el método de etiquetado para las vlans
ip address 192.168.1.33 255.255.255.248 // Gateway de la interfaz
!
interface GigabitEthernet6/0.40 // Creación de las vlans
encapsulation dot1Q 40 // Estándar para el método de etiquetado para las vlans
ip address 192.168.1.41 255.255.255.248 // Gateway de la interfaz
!
interface GigabitEthernet6/0.50 // Creación de las vlans
encapsulation dot1Q 50 // Estándar para el método de etiquetado para las vlans
ip address 192.168.1.49 255.255.255.248 // Gateway de la interfaz
!
interface GigabitEthernet6/0.60 // Creación de las vlans
encapsulation dot1Q 60 // Estándar para el método de etiquetado para las vlans
ip address 192.168.1.57 255.255.255.248 // Gateway de la interfaz
!
interface GigabitEthernet6/0.70 // Creación de las vlans
encapsulation dot1Q 70 // Estándar para el método de etiquetado para las vlans
ip address 192.168.1.65 255.255.255.248 // Gateway de la interfaz
!
interface GigabitEthernet6/0.80 // Creación de las vlans
encapsulation dot1Q 80 // Estándar para el método de etiquetado para las vlans
ip address 192.168.1.73 255.255.255.248 // Gateway de la interfaz
!
interface GigabitEthernet6/0.200 // Creación de las vlans
encapsulation dot1Q 200 // Estándar para el método de etiquetado para las vlans
ip address 192.168.1.81 255.255.255.248 // Gateway de la interfaz
!
interface GigabitEthernet6/0.300 // Creación de las vlans
encapsulation dot1Q 300 // Estándar para el método de etiquetado para las vlans
ip address 192.168.1.1 255.255.255.240 // Gateway de la interfaz
!
interface GigabitEthernet7/0 // Interfaz
ip address 192.168.255.253 255.255.255.252 // Gateway de la interfaz

```

```
duplex auto // (Default) Sin cambios
speed auto // (Default) Sin cambios
!
interface GigabitEthernet8/0
no ip address // (Default) Sin cambios
duplex auto // (Default) Sin cambios
speed auto // (Default) Sin cambios
shutdown // (Default) Sin cambios
!
interface GigabitEthernet9/0 // Interfaz
ip address 192.168.1.1 255.255.255.240 // Gateway de la interfaz
duplex auto // (Default) Sin cambios
speed auto // (Default) Sin cambios
!
router rip // (Default) Sin cambios
!
ip classless // (Default) Sin cambios
ip route 0.0.0.0 0.0.0.0 192.168.255.254 // Configurar ruta estática
!
ip flow-export version 9 // (Default) Sin cambios
!
!
!
banner motd $ // Mensaje de banner que se mostrará al inicio de la sesión remota
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMWWNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNW
WMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMWNXXXKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKXX
XNNWWMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMWNXXXKKK0O00KKKKKKKKOod0KKKKKKOdoOKKKKKKKKK0O0KKK
XXNWWMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMWNXXXKKK0xl:cdOKKKKKKKK0o.;cccc;.dKKKKKKKKKOd::ox0KKKXXNWM
MMMMMMMMMMM
MMMMMMMWXXKKKKOd'. c0KKKKKKKKk, ;OKKKKKKKKO:
.'cxOKKKXNWMMMMMMMM
MMMWWXKKK0kl' ,x0KKKKKKKOl. .l0KKKKKKK0d' .'lkKKKKXWMMMMMM
MMWNKKKKOl. .;clcc;,. .;cclc;,. .lOKKKKNWMMM
MMWXKKKKk; ;kKKKKXWMM
MWNKKKKk; ;OKKKKNMM
MWXKKK0o. .oKKKKXWM
MWXKKKOl. .o0KKKXWM
MWXKKKKx. 'xKKKKXWM
MMWXKKK0o. .o0KKKXWMM
MMMNXXXKKK0d' .'... ... .'...' ,d0KKKXWMMM
MMMMWNKKKKOl' .l000Oxc';oxkkd:. .cdkkxo;.cx0000c. 'lOKKKKNWMMMM
```

```

MMMMMWXKKKKOo;...kKKKK000KKKKK0kc.
 ckKKKKKK0OKKKKKk;...dOKKKXXWMMMMMM
MMMMMMMMWNXKKK0kdloxO0KKKKKKKKKKK0d'
'x0KKKKKKKKKKK0kdoldO0KKKXNWMMMMMMMM
MMMMMMMMMMMMWNXXKKK0OO00KKKKKKKKKKK0x;...kKKKKKKKKKKKK00OO0KKK
XXNWWMMMMMMMMMMMM
MMMMMMMMMMMMMMMMWNNXXKKKKKKKKKKKKKKKKKOkOKKKKKKKKKKKKKKKKKK
XXNNWWMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMWWNNNXXXXXKKKKKKKKKKKKKKKKKKXNNN
WWMMMMMMMMMMMMMMMMMMMMMMMMMMMM

```

-----

El acceso a este dispositivo es solo para usuarios autorizados, si usted no  
está expresamente autorizado, por favor desconéctese inmediatamente.  
Los accesos no autorizados están en contra de la ley, y pueden estar  
sujetos a penas criminales o civiles.

\$

!  
!  
!  
!  
!

line con 0 // Ingresa al modo de configuración de la consola

password 7 0822455D0A16 // Definición de la contraseña para acceder por la consola

logging synchronous // Sincronizar mensajes no solicitados y depurar salidas

login // Comprobación de la contraseña en la consola

!

line aux 0 // (Default) Sin cambios

!

line vty 0 4 // Acceso a la interfaz telnet

password 7 0822455D0A16 // Asignación de contraseña

login local // Confirmación y habilitación de la contraseña

transport input ssh // Se hace uso del protocolo SSH

line vty 5 15 // Creación de sesión de administración fuera de la banda de dispositivos - Config VTY

password 7 0822455D0A16 // Asignación de contraseña

login local // Confirmación y habilitación de la contraseña

transport input ssh // Se hace uso del protocolo SSH

!

!

!

end // (Default) Sin cambios

## Configuración del Sw-Main (Switch de los participantes):

### Switch - Main

```

!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw-Main //Configuración del nombre establecido al dispositivo - Main
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0 //Contraseña encriptada
!
!
!
ip ssh version 2 //Se configura a la versión 2 de SSH
ip domain-name miempresa.com
!
username cisco secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
spanning-tree mode pvst //Comunicación STP en todas las VLAN - protocolo de red capa 2 (modelo OSI)
spanning-tree extend system-id //Valor del puente en el BID para identificar la VLAN
!
interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/2
  switchport access vlan 20
  switchport mode access
!
interface FastEthernet0/3
  switchport access vlan 30
  switchport mode access
!
interface FastEthernet0/4
  switchport access vlan 40
  switchport mode access
!
interface FastEthernet0/5

```



```
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 70
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 80
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 200
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 300
switchport mode access
!
interface FastEthernet0/11
switchport mode trunk
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
```

```
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
switchport mode access
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan200
ip address 192.168.1.82 255.255.255.248
!
ip default-gateway 192.168.1.81
!
banner motd $ // Mensaje de banner que se mostrará al inicio de la sesión remota
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMWWNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNW
WMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMWWWNNXXXKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKXX
XNNWWMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMWNNXXKKK0O00KKKKKKKKKOod0KKKKKKOdoOKKKKKKKKK0O0KKK
XXNWWMMMMMMMMMMMMMMMMMM
MMMMMMMMMMWNXXKKK0xl:cdOKKKKKKKK0o.:cccc,..dKKKKKKKKK0d::ox0KKKXXNWM
MMMMMMMMM
MMMMMMWWXXKKK0dc'. c0KKKKKKKKk, ;OKKKKKKKKO:
.'cxOKKKXNWWMMMMMM
MMMWWXKKK0kl' ,x0KKKKKKK0l. .l0KKKKKKK0d' .'lkKKKKXWMMMMM
MMWNKKKKOl. ,.:clcc:, ,.:cclc:, .lOKKKKNWMMM
MMWXKKKKk; ;kKKKKXWMM
MWNKKKKk; ;OKKKKNMM
MWXKKK0o. .oKKKKXWM
MWXKKK0l. .o0KKKXWM
MWXKKKKx. 'xKKKKXWM
MMWXKKK0o. .o0KKKXWMM
MMMNXXKKK0d' .'.,... .. .'.,' ,d0KKKXWMMM
MMMMWNKKKKOl' .l000Oxc':oxkkd:. .cdkkxo:,cx0000c. 'lOKKKKNWMMMM
```

```

MMMMMWXKKKKOo;...kKKKK000KKKKK0kc.
.ckKKKKKK00KKKKKk;...:dOKKKXXWMMMMMM
MMMMMMMMMMWNXKKK0kdloxO0KKKKKKKKKKK0d'
'x0KKKKKKKKKKK0kdoldO0KKKXNWMMMMMMMM
MMMMMMMMMMMMMMWNXXKKK0OO00KKKKKKKKKKK0x;.;kKKKKKKKKKKKK00OO0KKK
XXNWWMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMWNNXXKKKKKKKKKKKKKKKKKOkOKKKKKKKKKKKKKKKKKK
XXNNWWMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMWWNNNXXXXXKKKKKKKKKKKKKKKKKKXKXXXXXNNN
WWMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM

```

-----

El acceso a este dispositivo es solo para usuarios autorizados, si usted no  
 esta expresamente autorizado, por favor desconectese inmediatamente.  
 Los accesos no autorizados estan en contra de la ley, y pueden estar  
 sujetos a penas criminales o civiles. \$

!  
!  
!

```

line con 0 //Ingreso al modo configuración de la consola
password 7 0822455D0A16 //Asignación de contraseña
logging synchronous //Sincronización de mensajes no solicitados - Reanuda el registro
login // Confirmación y habilitación de la contraseña

```

!

```

line vty 0 4 //Acceso a la interfaz telnet
password 7 0822455D0A16 //Asignación de contraseña
login local // Confirmación y habilitación de la contraseña
transport input ssh // Se hace uso del protocolo SSH

```

```

line vty 5 15 // Creación de sesión de administración fuera de la banda de dispositivos - Config VTY
password 7 0822455D0A16 //Asignación de contraseña
login local // Confirmación y habilitación de la contraseña
transport input ssh // Se hace uso del protocolo SSH

```

!  
!  
!  
!

end

# Capítulo 4

## 4. Evaluación de resultados

Introspección sobre el diseño final de la red para el concurso del ICPC dentro del campus Santa Fe.

### 4.1. Problemáticas enfrentadas durante la etapa de solución del reto

Generación de múltiples iteraciones del diseño de la red, por errores durante el desarrollo de los requerimientos y observaciones por parte del socio formador. En los primeros diseños de redes, realizamos una deficiente distribución de las redes, ya que varios equipos estaban dentro de la misma y habría problemas de seguridad. También exceso de routers, planteamos hub's que fueron finalmente cambiados a switch's administrables y no administrables. El penúltimo diseño nos percatamos que teníamos que cambiar la conexión entre el router y los switch's porque enlazaban en el router todos los switch's y eso entorpece la conexión general de la red, entonces cambiamos las conexiones para que entre el Sw-Main, el Sw-Coach y el Sw-Admin estuvieran directamente enlazados.

### 4.2. Evaluación de los objetivos planteados

Cumplimos con el abastecimiento de red para todos los participantes, coaches y administradores, la correcta logística de los espacios dentro del campus y la implementación de los estándares internacionales IEEE.

### 4.3. Evaluación de la propuesta

La propuesta de solución cumple exitosamente con los requerimientos y objetivos planteados, la red de los participantes está segmentada correctamente por equipos que tienen conexión entre ellos y a internet, la red de coaches tiene acceso a los equipos y a internet. La red del administrador tiene acceso a toda la red del concurso y a internet. Cuenta con la instalación física dentro de los estándares IEEE y con las medidas de sana distancia Covid-19.

# Capítulo 5

## 5. Conclusiones y trabajo futuro

Últimas observaciones, descripción de áreas de oportunidad y optimizaciones de la red.

### 5.1. Conclusiones

El diseño cumplió con las expectativas para el cual se formuló el proyecto, implementamos los requerimientos esperados para este proyecto, los diseños físicos y lógicos de la red, haciendo la valoración económica de los dispositivos necesarios para atender a los estándares internacionales vigentes y de esta manera obtener todas las potencialidades de la red a las necesidades del concurso.

### 5.2. Trabajo futuro

Una de las mayores áreas de oportunidad que encontramos en nuestro diseño de red es en él “fault tolerance”, ya que no contamos con una infraestructura muy resistente a daños imprevistos, por lo que en un futuro nos gustaría poder diseñar e implementar una red con un mejor diseño que minimice los riesgos de pérdida de conexión debido a fallas físicas y/o lógicas.

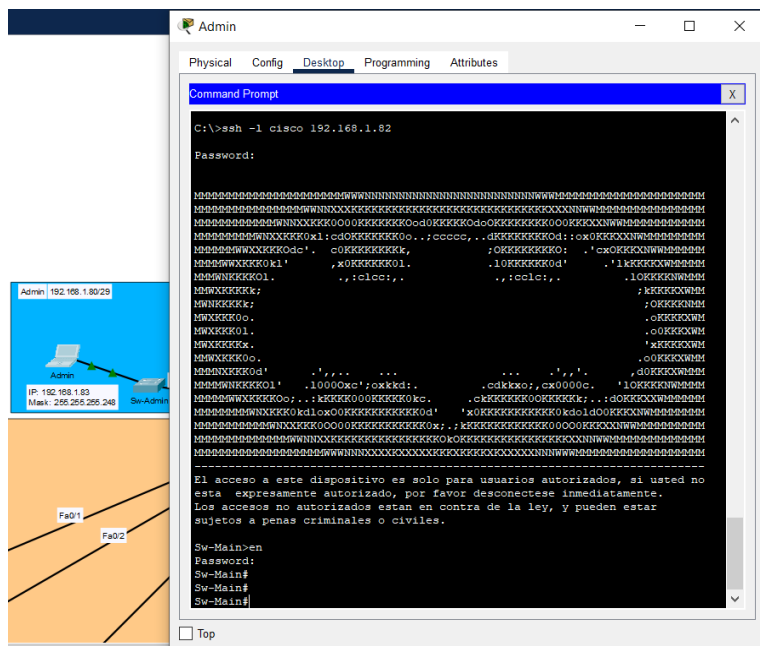
Por ejemplo, actualmente solo estamos trabajando con un router, lo cual no es muy seguro, ya que si este se llega a dañar perderíamos la conectividad de todas las redes, o incluso si una de sus rutas se llegara a dañar se perdería por completo el acceso a esa conexión. En cambio, usando 2 o incluso 3 routers nos aseguraría que en caso de perder acceso a una ruta, o a algún router, siempre se podría tomar una ruta alterna para poder llegar al punto final deseado.

Otra mejora que se podría realizar la restricción de seguridad para que los coaches solamente se puedan conectar con su equipo, y que entre ellos también permanecen asilados.

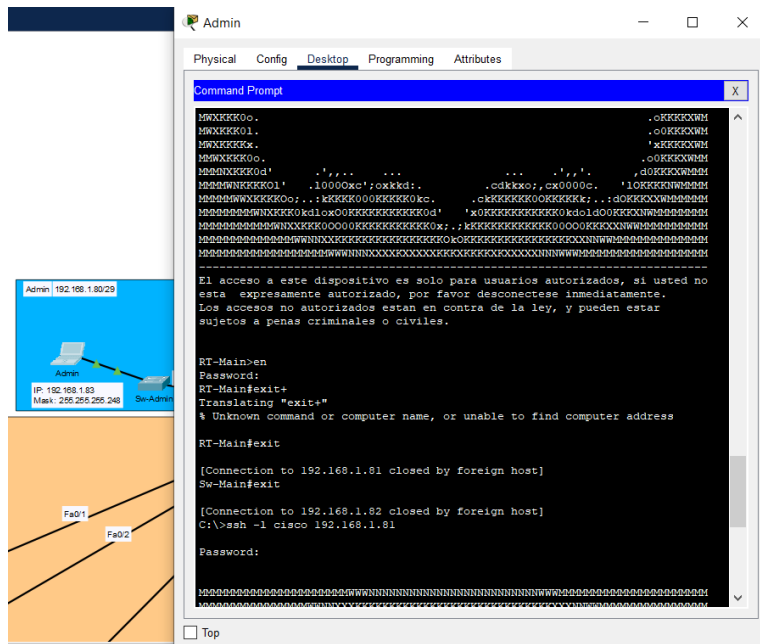
# Apéndices

## Apéndice

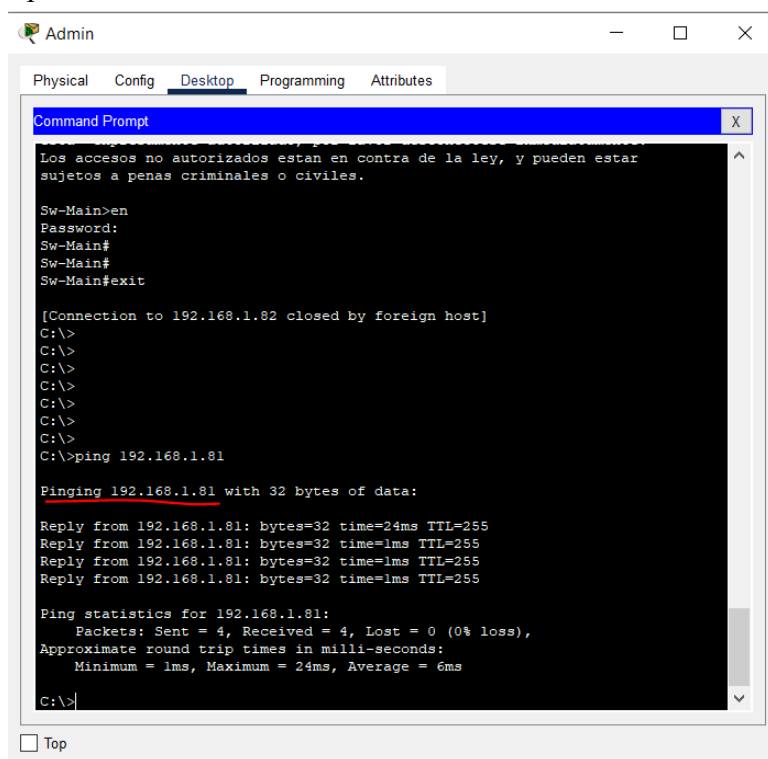
## Apéndice 1.1



## Apéndice 1.2



### Apéndice 1.3



Admin

Physical Config **Desktop** Programming Attributes

Command Prompt

```

Los accesos no autorizados estan en contra de la ley, y pueden estar
sugetos a penas criminales o civiles.

Sw-Main>en
Password:
Sw-Main#
Sw-Main#
Sw-Main#exit

[Connection to 192.168.1.82 closed by foreign host]
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.81

Pinging 192.168.1.81 with 32 bytes of data:

Reply from 192.168.1.81: bytes=32 time=24ms TTL=255
Reply from 192.168.1.81: bytes=32 time=1ms TTL=255
Reply from 192.168.1.81: bytes=32 time=1ms TTL=255
Reply from 192.168.1.81: bytes=32 time=1ms TTL=255

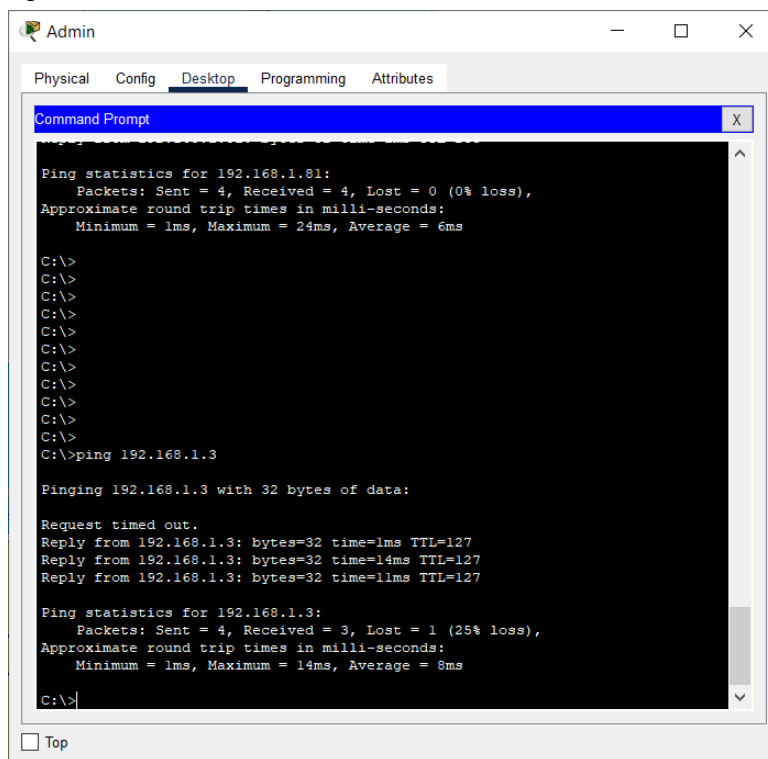
Ping statistics for 192.168.1.81:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 24ms, Average = 6ms

C:\>

```

☐ Top

### Apéndice 1.4



Admin

Physical Config **Desktop** Programming Attributes

Command Prompt

```

Ping statistics for 192.168.1.81:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 24ms, Average = 6ms

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=1ms TTL=127
Reply from 192.168.1.3: bytes=32 time=14ms TTL=127
Reply from 192.168.1.3: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 8ms

C:\>

```

☐ Top

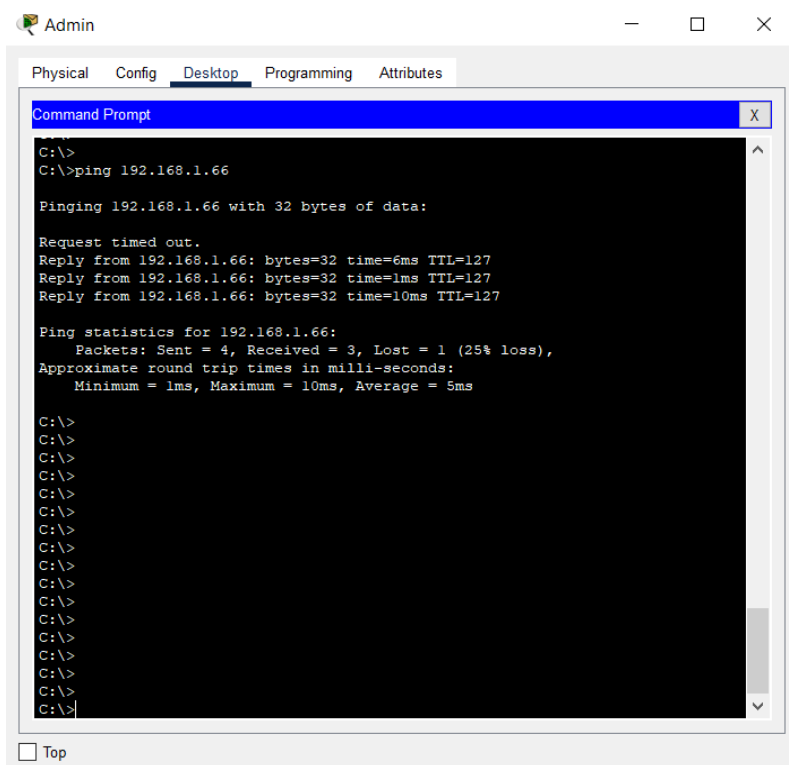








## Apéndice 1.11



The screenshot shows a network configuration window titled "Admin" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the execution of a ping command to 192.168.1.66. The output indicates a successful ping with 32 bytes of data, showing a request timed out, followed by three successful replies from 192.168.1.66 with varying times and TTL values. Ping statistics show 4 packets sent, 3 received, and 1 lost (25% loss), with round trip times ranging from 1ms to 10ms.

```
C:\>
C:\>ping 192.168.1.66

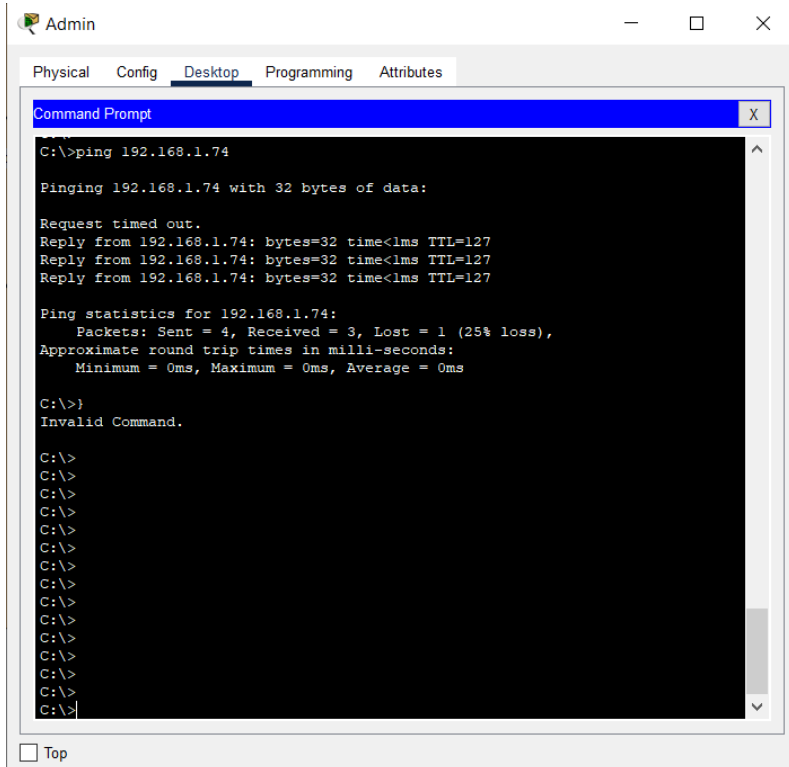
Pinging 192.168.1.66 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.66: bytes=32 time=6ms TTL=127
Reply from 192.168.1.66: bytes=32 time=1ms TTL=127
Reply from 192.168.1.66: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 5ms

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

## Apéndice 1.12



The screenshot shows a network configuration window titled "Admin" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the execution of a ping command to 192.168.1.74. The output indicates a successful ping with 32 bytes of data, showing a request timed out, followed by three successful replies from 192.168.1.74 with varying times and TTL values. Ping statistics show 4 packets sent, 3 received, and 1 lost (25% loss), with round trip times ranging from 0ms to 0ms. Below the ping results, the user enters an invalid command, resulting in an "Invalid Command." message.

```
C:\>ping 192.168.1.74

Pinging 192.168.1.74 with 32 bytes of data:

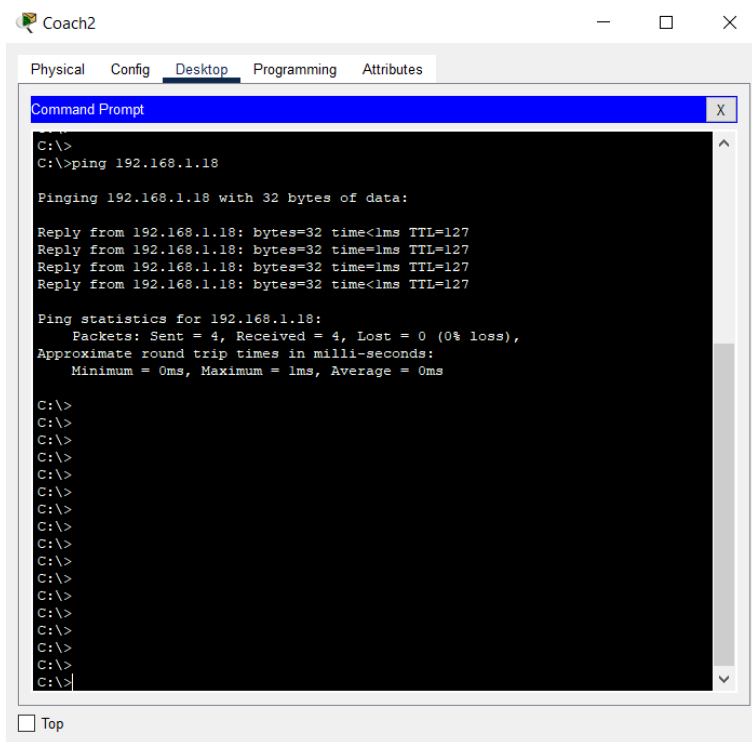
Request timed out.
Reply from 192.168.1.74: bytes=32 time<1ms TTL=127
Reply from 192.168.1.74: bytes=32 time<1ms TTL=127
Reply from 192.168.1.74: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.74:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>}
Invalid Command.

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

## Apéndice 2.1



The screenshot shows a Coach2 virtual machine window with a 'Desktop' tab selected. Inside the desktop is a 'Command Prompt' window. The command prompt shows the execution of the command 'ping 192.168.1.18'. The output indicates that four packets were sent and received successfully with 0% loss. The round trip times are all less than 1ms.

```
C:\>
C:\>ping 192.168.1.18

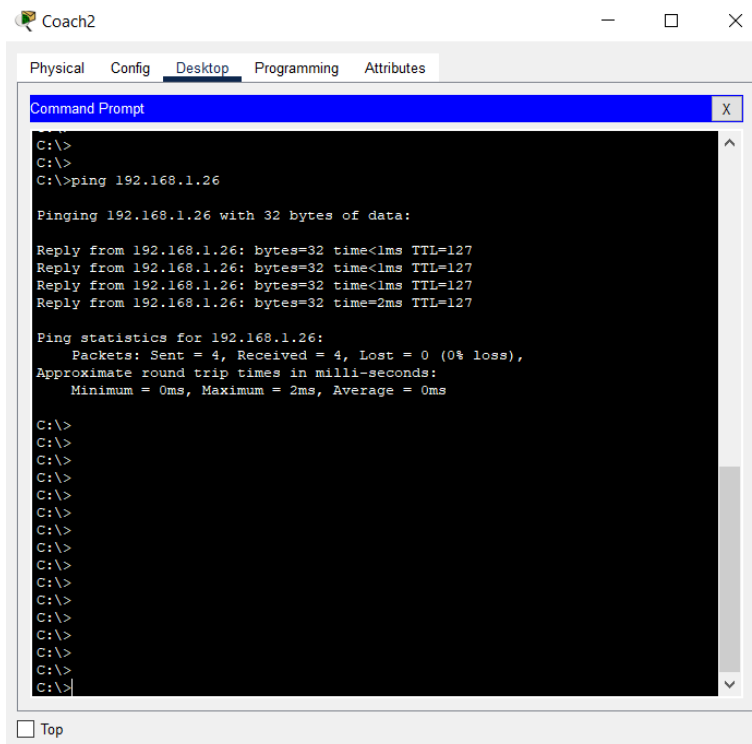
Pinging 192.168.1.18 with 32 bytes of data:

Reply from 192.168.1.18: bytes=32 time<1ms TTL=127
Reply from 192.168.1.18: bytes=32 time<1ms TTL=127
Reply from 192.168.1.18: bytes=32 time<1ms TTL=127
Reply from 192.168.1.18: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

## Apéndice 2.2



The screenshot shows a Coach2 virtual machine window with a 'Desktop' tab selected. Inside the desktop is a 'Command Prompt' window. The command prompt shows the execution of the command 'ping 192.168.1.26'. The output indicates that four packets were sent and received successfully with 0% loss. The round trip times are all less than 2ms.

```
C:\>
C:\>
C:\>ping 192.168.1.26

Pinging 192.168.1.26 with 32 bytes of data:

Reply from 192.168.1.26: bytes=32 time<1ms TTL=127
Reply from 192.168.1.26: bytes=32 time<1ms TTL=127
Reply from 192.168.1.26: bytes=32 time<1ms TTL=127
Reply from 192.168.1.26: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.1.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

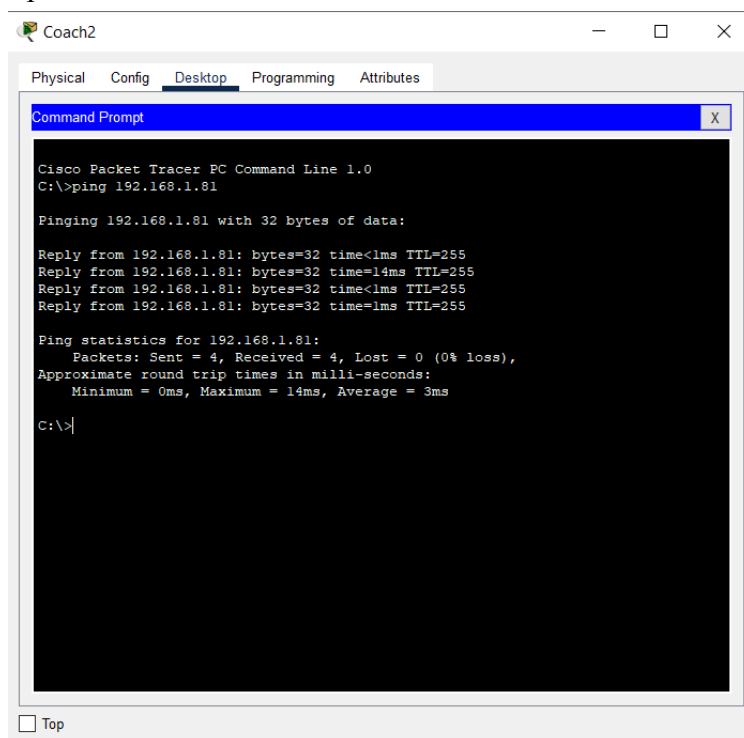
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```



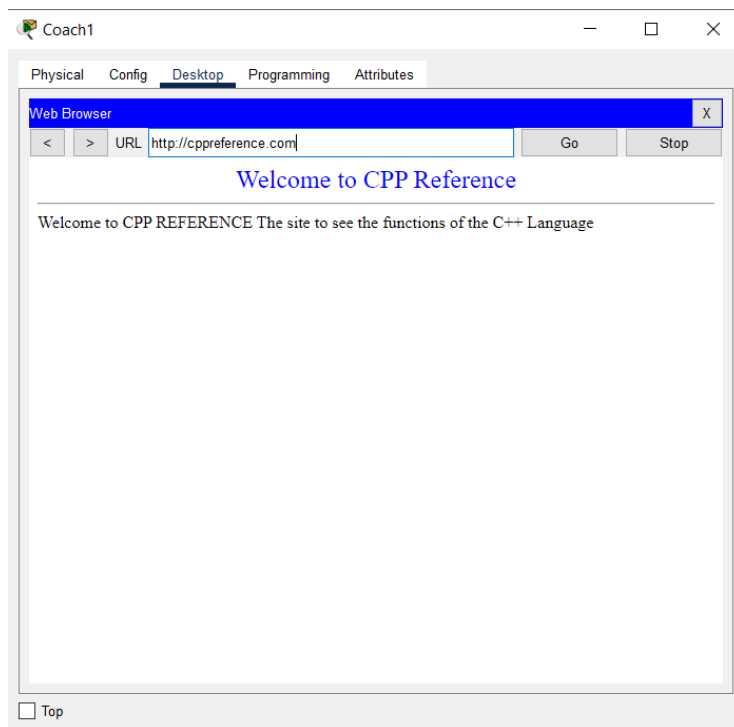




## Apéndice 2.9



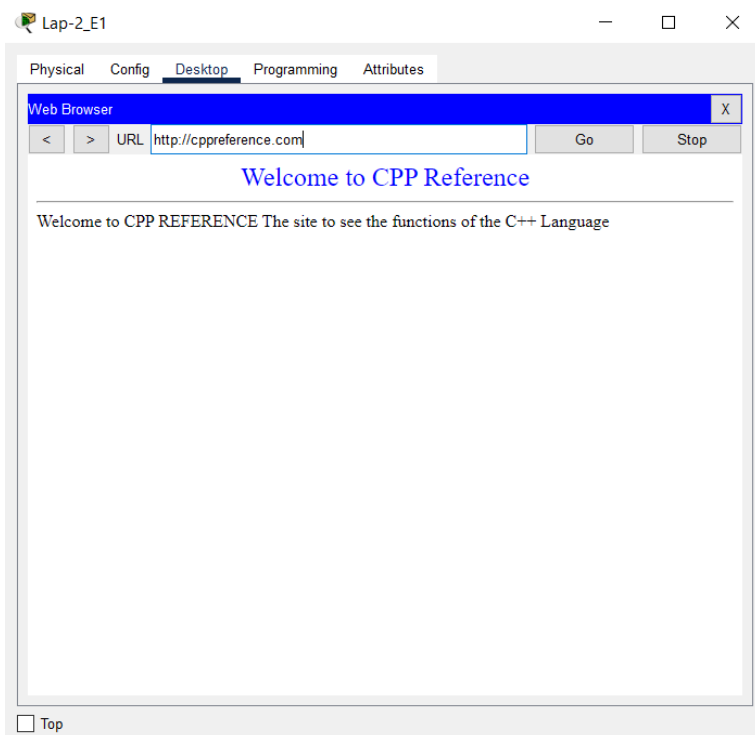
## Apéndice 2.10



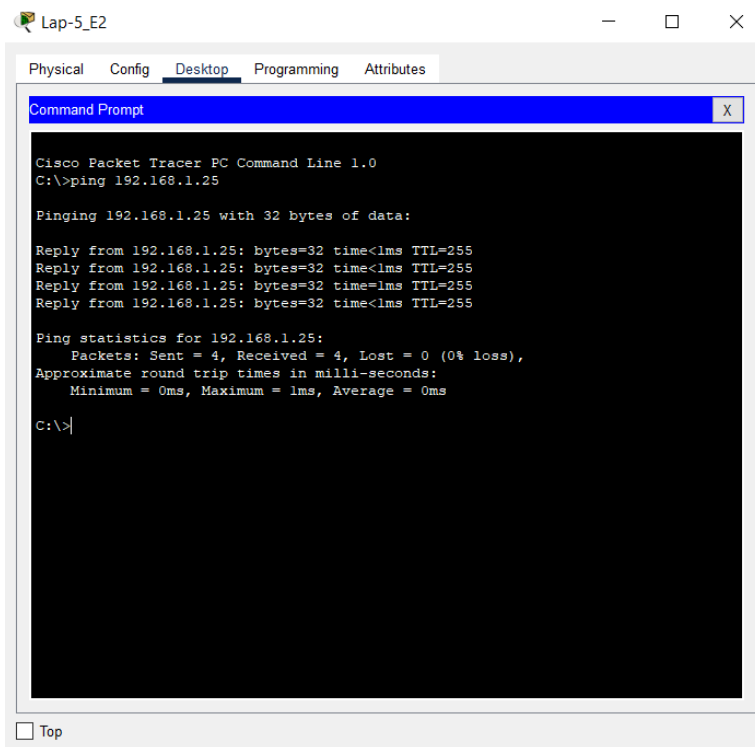




### Apéndice 3.3

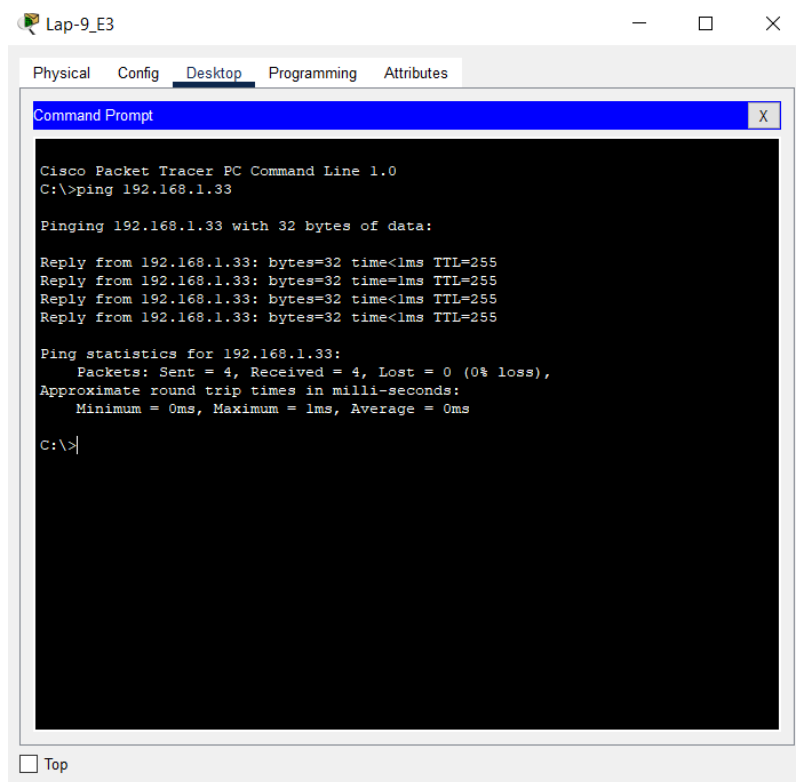


### Apéndice 4.1

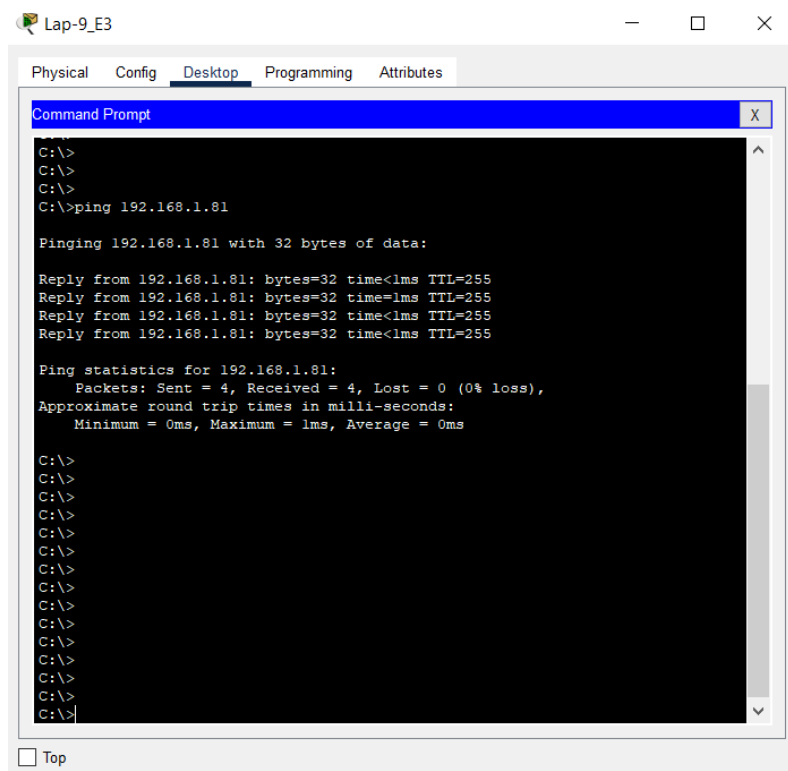




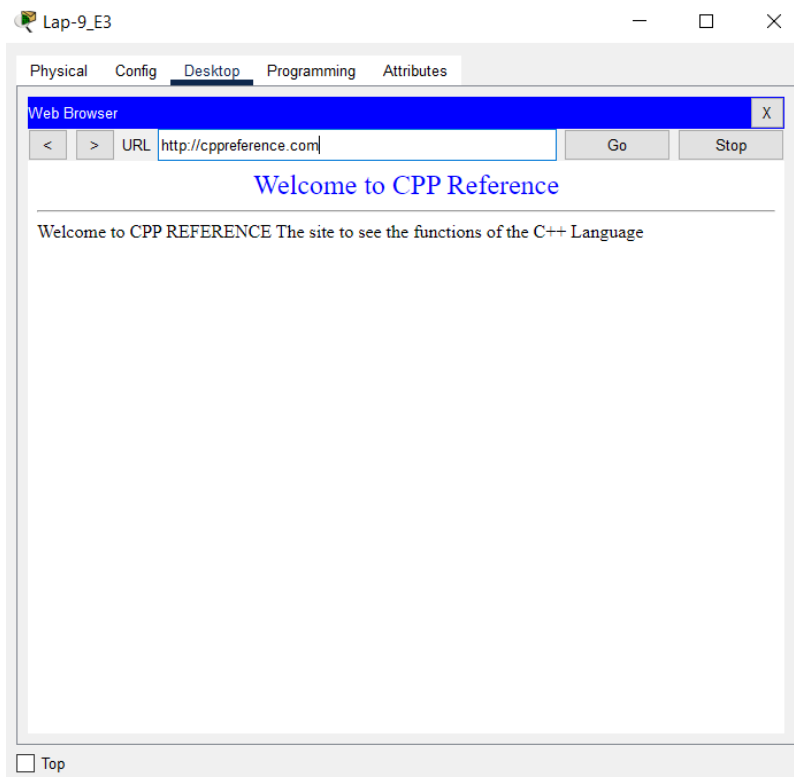
## Apéndice 5.1



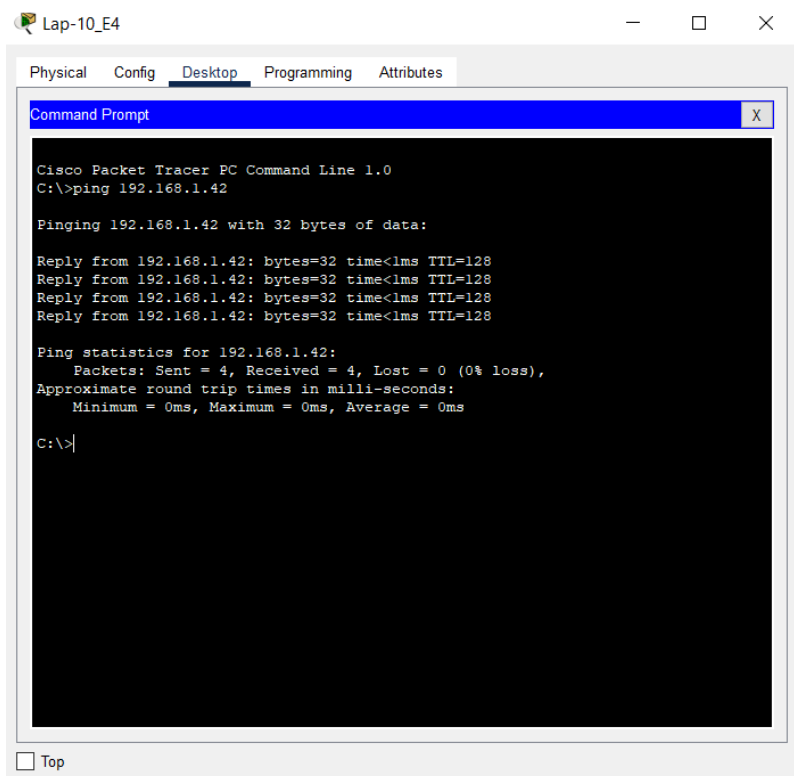
## Apéndice 5.2



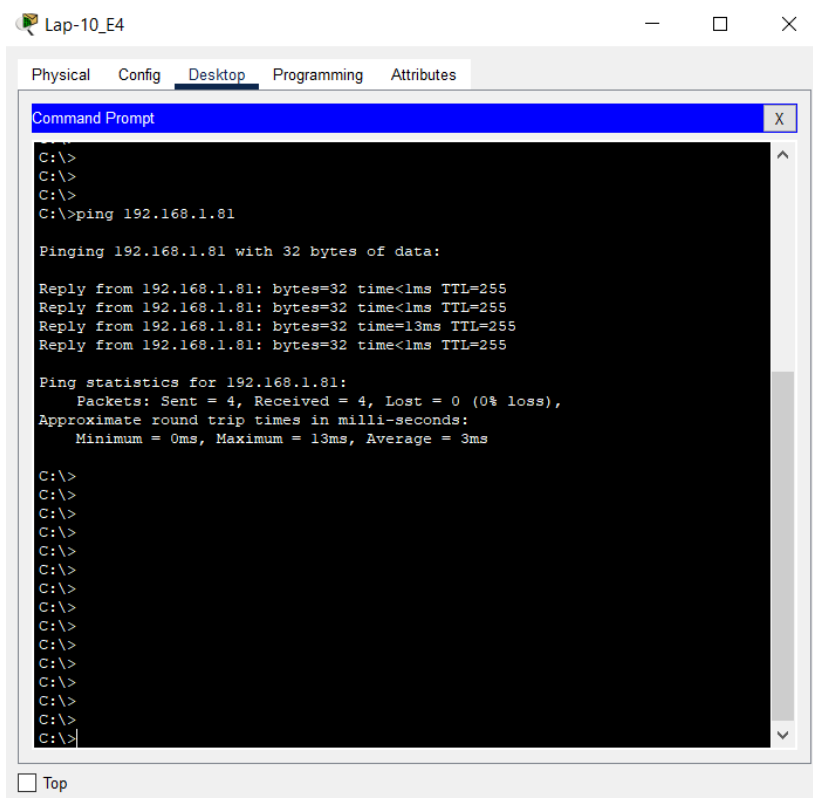
## Apéndice 5.3



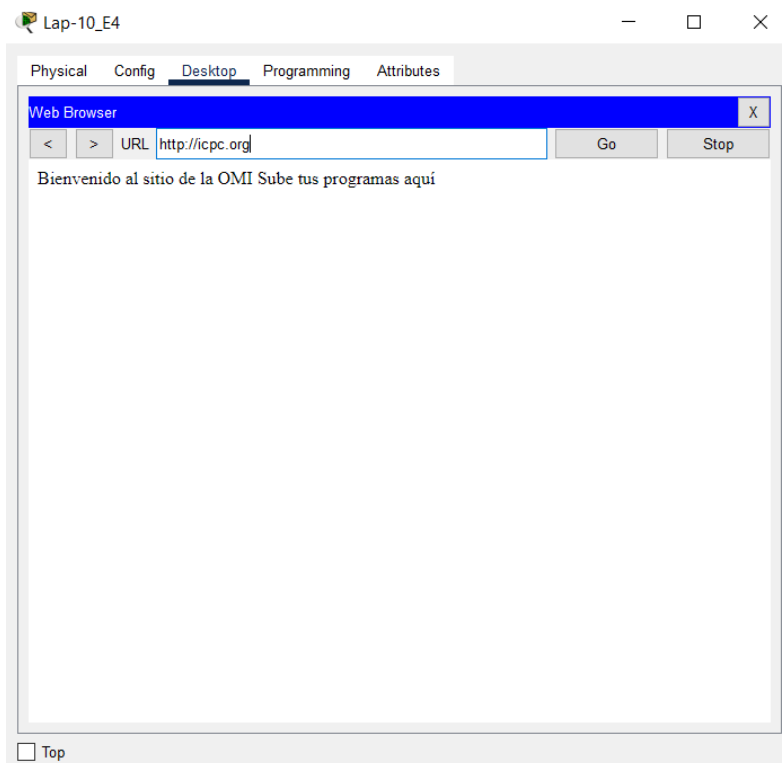
## Apéndice 6.1



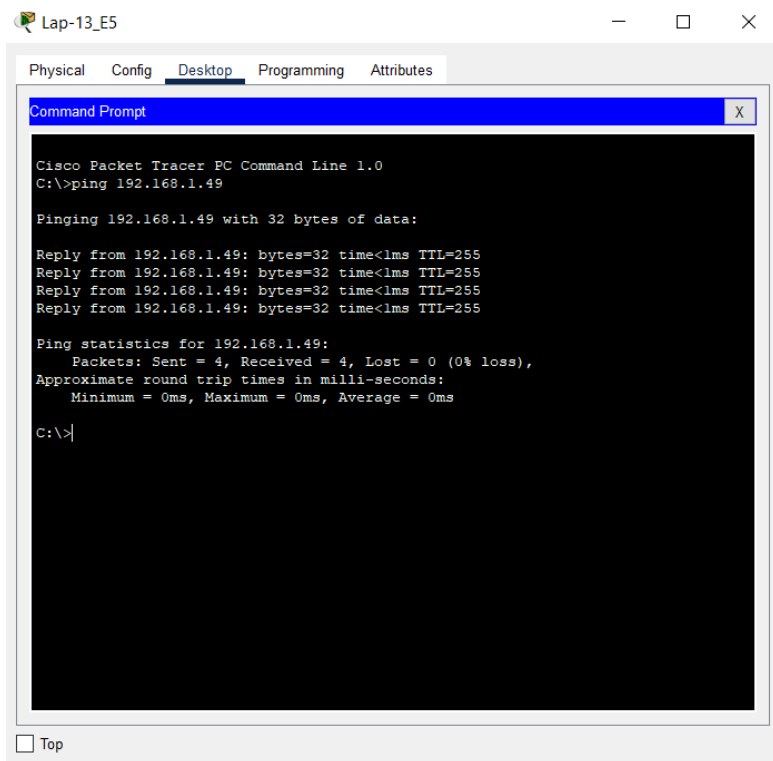
## Apéndice 6.2



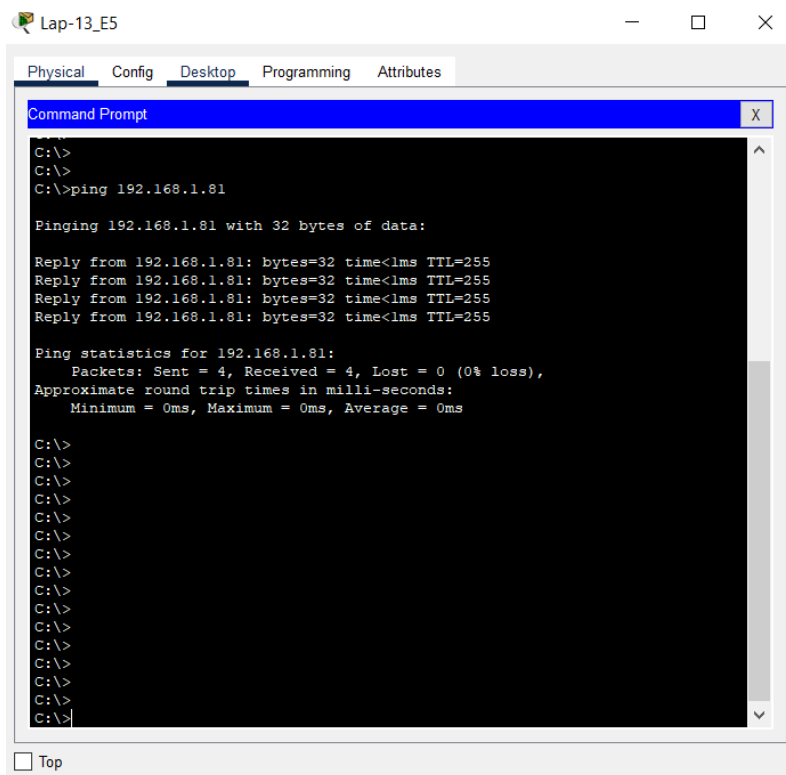
## Apéndice 6.3



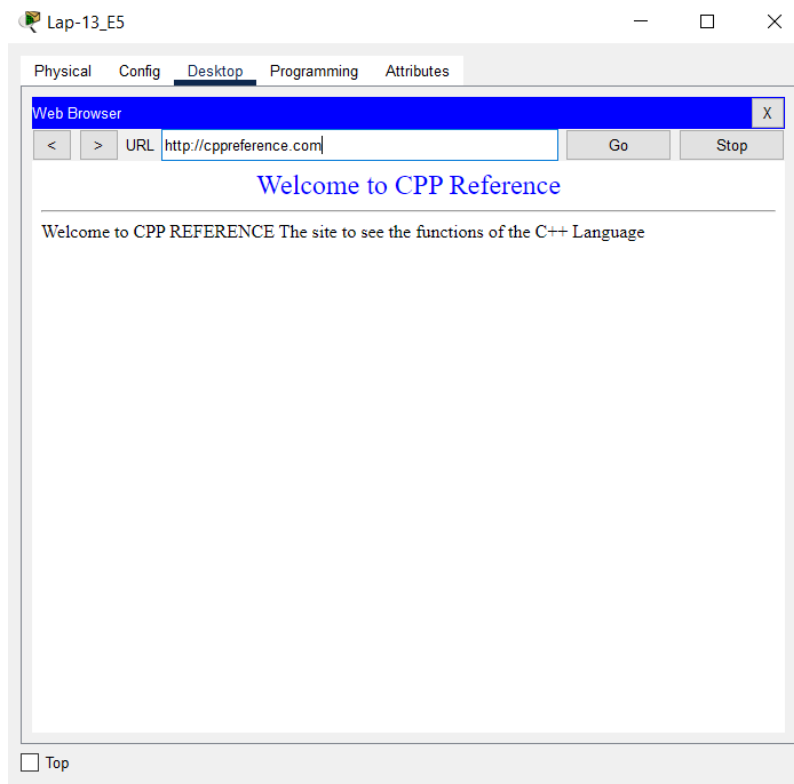
## Apéndice 7.1



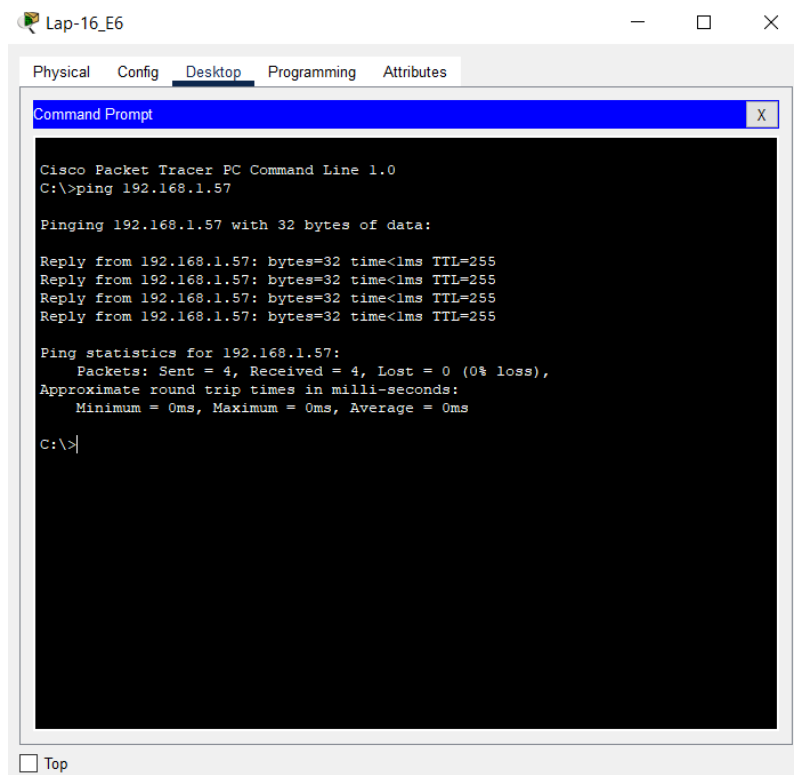
## Apéndice 7.2



### Apéndice 7.3

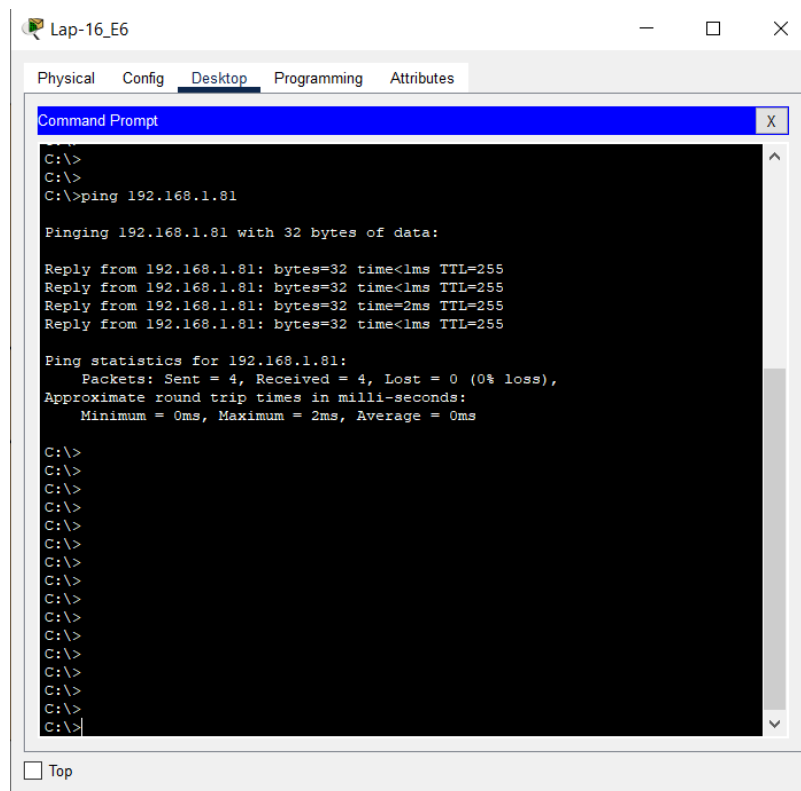


### Apéndice 8.1

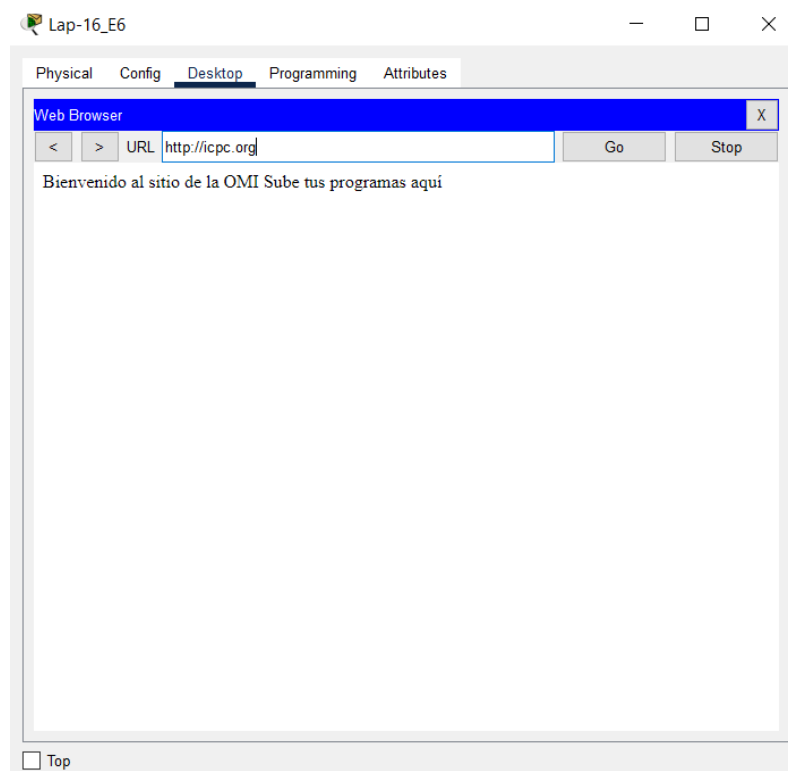




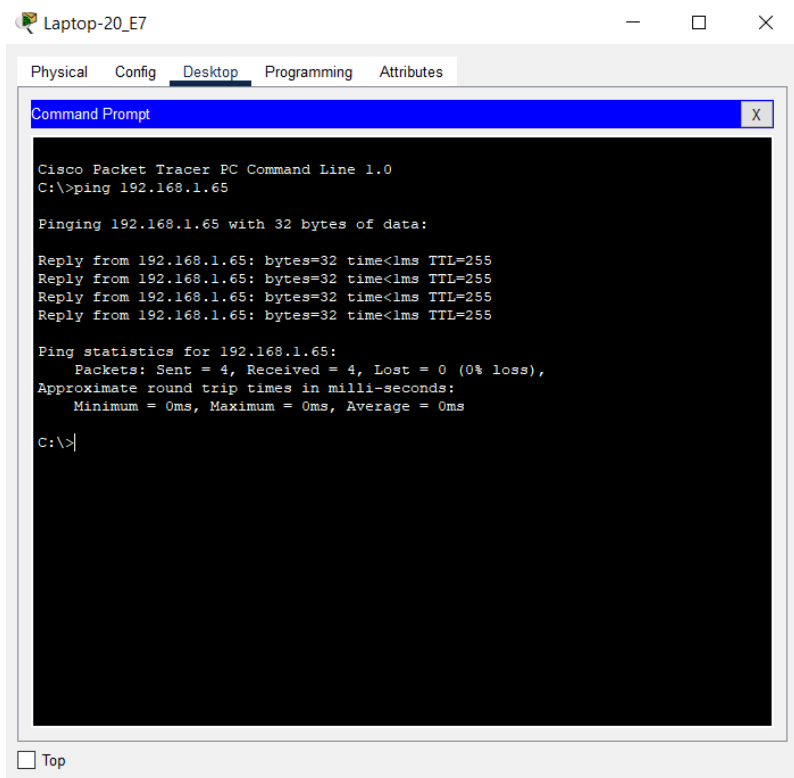
## Apéndice 8.2



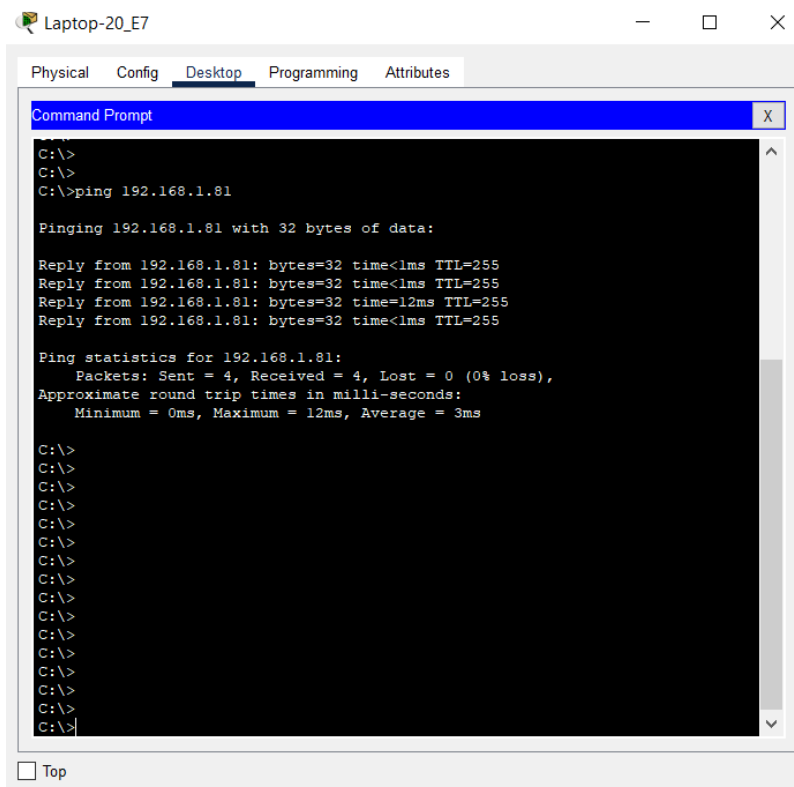
## Apéndice 8.3



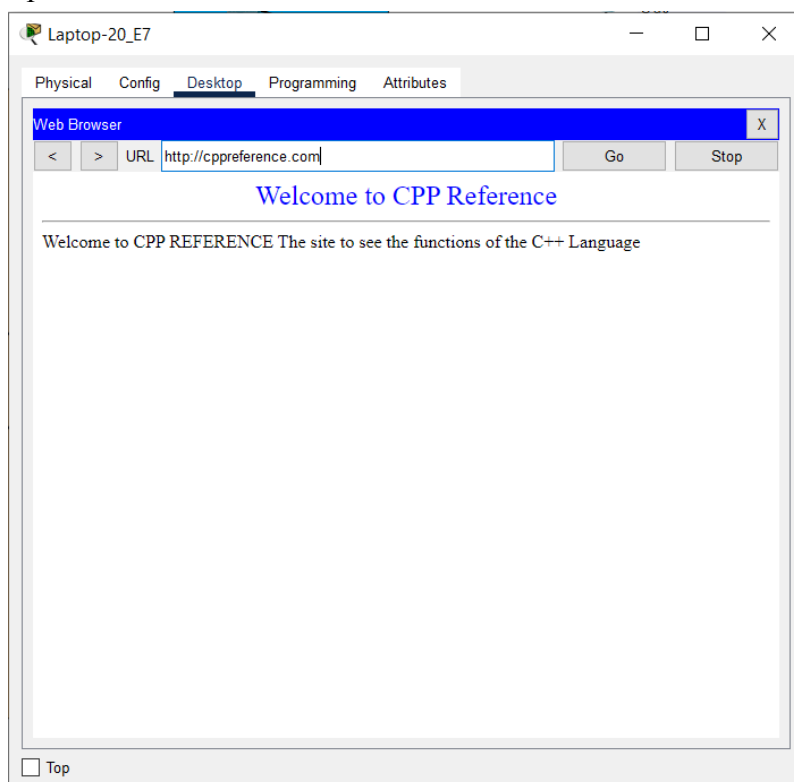
## Apéndice 9.1



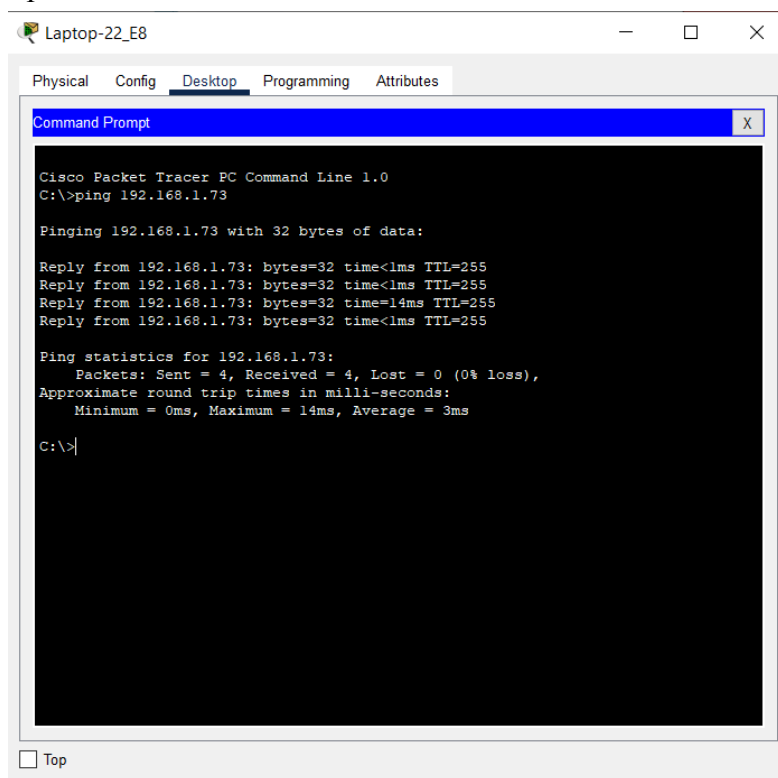
## Apéndice 9.2



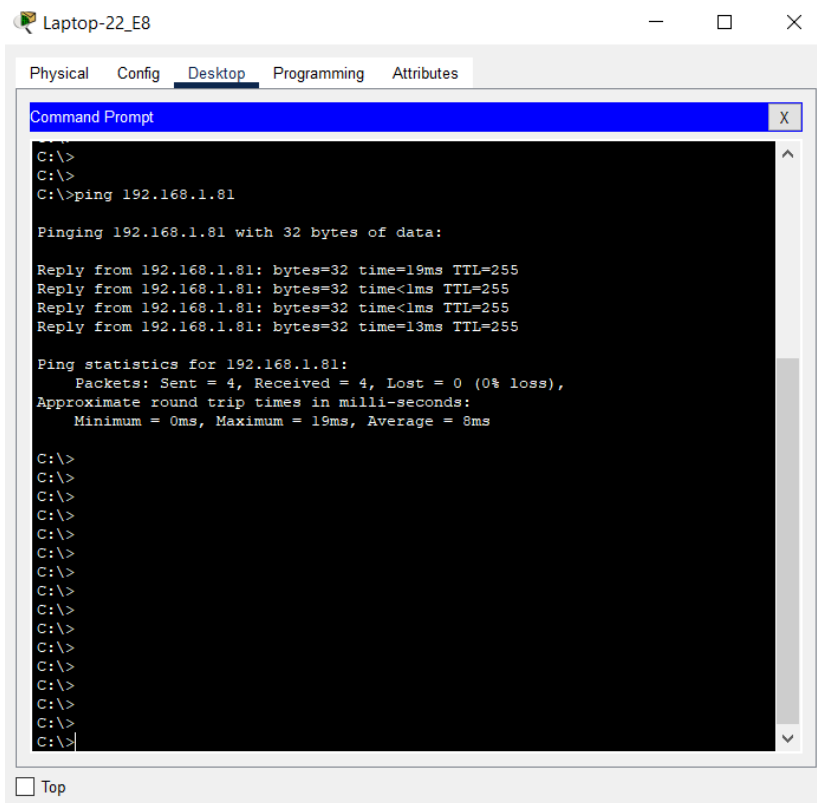
## Apéndice 9.3



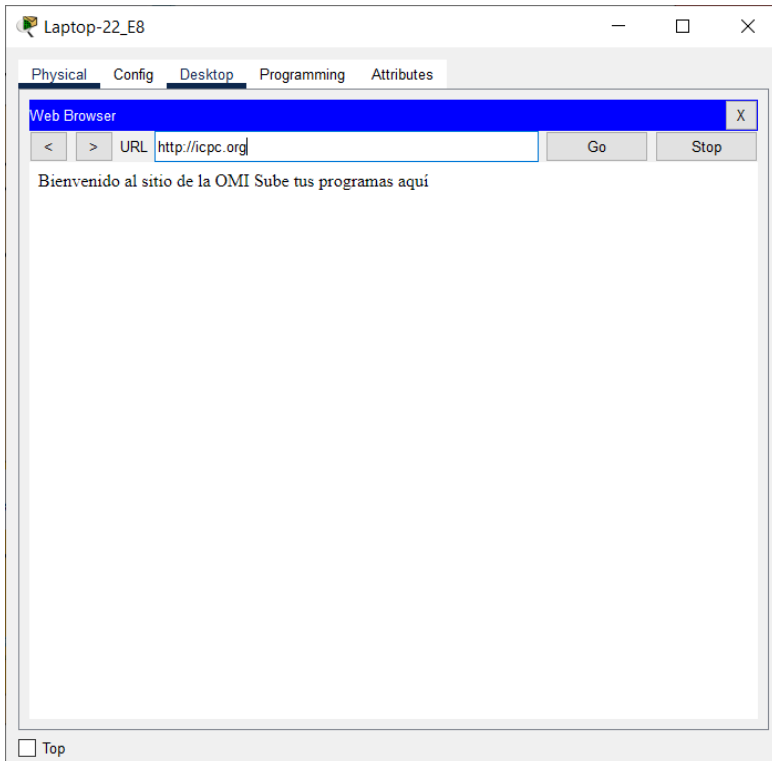
## Apéndice 10.1



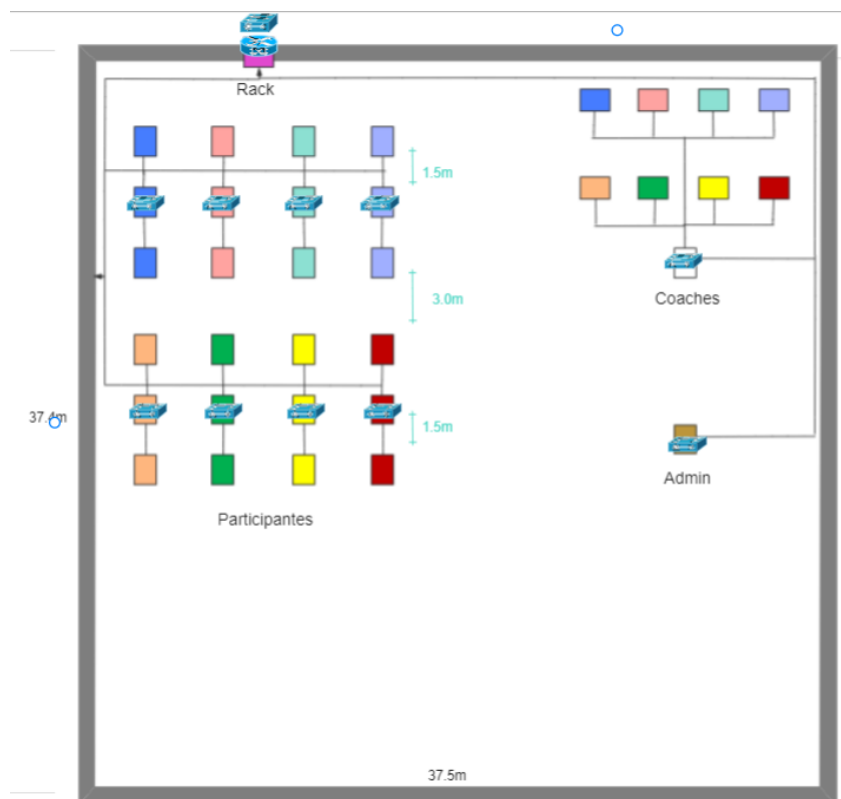
## Apéndice 10.2



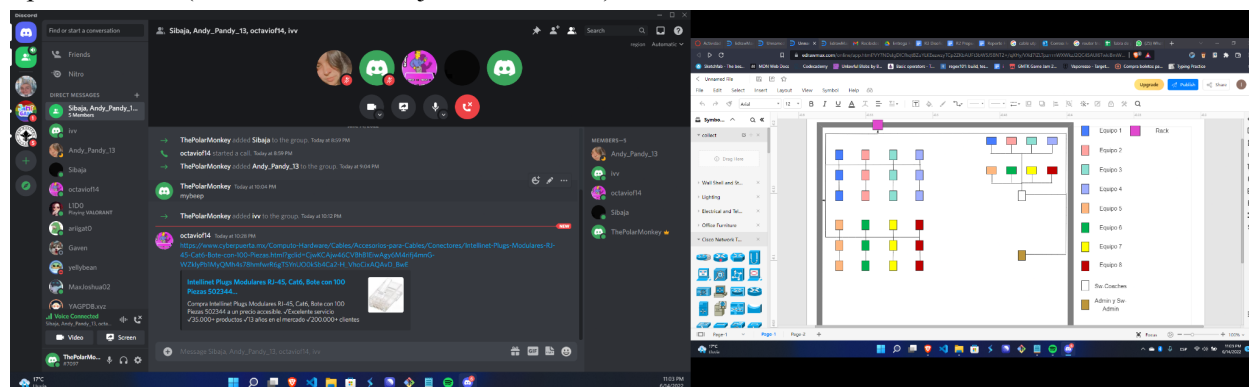
## Apéndice 10.3



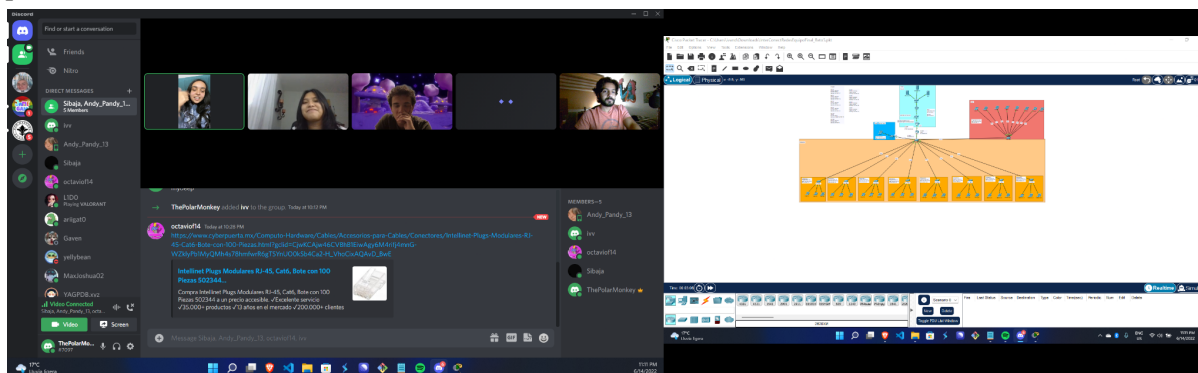
## Apéndice 11.0



## Apéndice 12.1 (Evidencia de Trabajo Colaborativo)



## Apéndice 12.1



# Glosario

## Glosario de términos

### DHCP

El Protocolo de configuración dinámica de host (DHCP) es un protocolo cliente/servidor que proporciona automáticamente un host de Protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada.

### HUBS

Es un dispositivo que funciona como punto de conexión para todos los dispositivos dentro de un LAN. Debido a que forman parte de la capa 1 del modelo de OSI, los hubs no tienen manera de distinguir puertos individuales por lo que a la hora de enviar una señal, ésta se manda a todos los puertos del hub.

### IP

Una dirección IP (Internet Protocol) es una dirección única que identifica a un dispositivo en Internet o en una red local.

### LAN

Es un conjunto de dispositivos que se encuentran conectados dentro de una zona física específica. Una LAN (Local Area Network) puede ser pequeña o grande, desde ser la red de una pequeña casa, hasta una red empresarial la cual contenga miles de usuarios y dispositivos.

**UTP**

Cable de par trenzado no apantallado o no blindado (Unshielded Twisted Pair) : Contiene pares trenzados sin blindar que se utilizan para diferentes tecnologías de redes locales.

**VLAN**

Virtual LANs son grupos de dispositivos, los cuales se encuentran conectados a 1 o más LANs que están configurados para comunicarse entre sí, como si estuvieran enlazados por el mismo cable. Debido a que las VLANs se encuentran en puertos lógicos y no físicos, son extremadamente flexibles.

**ICPC**

International Collegiate Programming Contest.

**SWITCHES**

Son dispositivos que conectan varios dispositivos en la misma red dentro de una zona física específica. Un switch permite a los dispositivos conectados compartir información y comunicarse entre sí.

**PING**

Packet Inter-Network Groper es un comando que manda un pedido a través de la red a un dispositivo específico. Un ping exitoso da como resultado una respuesta de vuelta del dispositivo especificado hacia el dispositivo que originó el ping.

**ROUTER**

Los enrutadores proporcionarán nivel de red o conectividad terciaria en el modelo OSI (interconexión de sistemas abiertos), mientras que los switches proporcionan conectividad secundaria en este modelo.

**INFRAESTRUCTURA.**

Se refiere a todos los recursos que conforman a una red.

**IEEE**

Institute of Electrical and Electronic Engineers

**CLI**

Short command line interface, CLI es la interfaz que se puede encontrar dentro de los dispositivos de red, tales como los routers y switches. Esta interfaz permite el manejo y control del dispositivo.

**EXEC**

Exit or Access Next Mode.

**SSH**

SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación.

**TELNET**

Telecommunication Network es un protocolo de red TCP/IP que es utilizado para establecer conexiones remotas con otros ordenadores, servidores, y dispositivos con un sistema compatible en el acceso mediante este sistema de comunicación.

**ETHERNET**

Es un tipo de topología de red de área local (LAN) soportado en el sistema operativo i5/OS. En i5/OS, Ethernet proporciona soporte para el estándar de Digital Equipment Corporation, Intel Corporation y Xerox (Ethernet Versión 2) y el estándar IEEE 802.3.

**SUBNETTING**

El Subnetting o subneteo es la técnica de subdividir una gran red IP física en varias redes lógicas más pequeñas, de forma que cada una de estas subnets funcionen como una red individual respecto a envíos y recepción de paquetes, aunque sigan perteneciendo a una misma red principal y a un mismo dominio.

**DNS**

Domain Name System es el directorio telefónico de Internet. Las personas acceden a la información en línea a través de nombres de dominio como nytimes.com o espn.com. Los navegadores web interactúan mediante direcciones de Protocolo de Internet (IP). El DNS traduce los nombres de dominio a direcciones IP para que los navegadores puedan cargar los recursos de Internet

**VTY**

Virtual Teletype (VTY) es una interfaz de línea de comandos (CLI (Command Line Interface)) creada en un router y utilizada para facilitar la conexión con el demonio a través de Telnet, un protocolo de red utilizado en las redes de área local. Para conectarse a un VTY, los usuarios deben presentar una contraseña válida.

**GATEWAY**

Gateway hace referencia a una puerta de enlace que funciona como un marco de comunicación de datos. Actúa como un puente entre diferentes redes.



## TCP

TCP (Protocolo de Control de Transmisión, por sus siglas en inglés Transmission Control Protocol) es un protocolo de red importante que permite que dos anfitriones (hosts) se conectan e intercambien información.

# Bibliografía

## Bibliografía

*Catalyst 3560 Switch Command Reference.* (n.d.).

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\\_46\\_se/command/reference/cr1/intro.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_46_se/command/reference/cr1/intro.pdf)

*Cisco DNA Center - Device 360 for Wireless LAN Controller and Access Point in Cisco*

*DNA Center Assurance.* (2022, February). Cisco.

<https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html>

*¿Cómo funciona un switch?* (2021, September). Cisco.

[https://www.cisco.com/c/es\\_mx/solutions/small-business/resource-center/networking/network-switch-how.html](https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/network-switch-how.html)

*Gateway: ¿Qué es y para qué sirve?* - AlaiSecure - España. (2021, December 14).

AlaiSecure - España. <https://alaisecure.es/glosario/gateway-que-es-y-para-que-sirve/>

(2022).Geek-University.com.

[https://geek-university.com/what-is-a-network-hub/#:~:text=A%20network%20hub%20serves%20as,\(except%20the%20incoming%20port\).](https://geek-university.com/what-is-a-network-hub/#:~:text=A%20network%20hub%20serves%20as,(except%20the%20incoming%20port).)

*IBM Docs.* (2021, April 14). Ibm.com.

<https://www.ibm.com/docs/es/i/7.2?topic=standards-ethernet-networks>

José Antonio Castillo. (2019, January 20). *Telnet qué es y para qué sirve* 【 *La más completa* 】【. Profesional Review; Profesional Review.

<https://www.profesionalreview.com/2019/01/20/telnet-que-es/>

KeepCoding. (2022, March 14). *¿Qué es Subnetting?* | *KeepCoding Tech School.*

KeepCoding Tech School.

<https://keepcoding.io/blog/que-es-subnetting/#:~:text=El%20Subnetting%20o%20subneteo%20es,principal%20y%20a%20un%20mismo%20dominio.>

*Ping - Definition and details.* (2022). Paessler.com; Paessler.

<https://www.paessler.com/it-explained/ping>

*¿Qué es DNS?* | *Nociones básicas.* (2022). Cloudflare.

<https://www.cloudflare.com/es-es/learning/dns/what-is-dns/>

*TCP - Glosario | MDN.* (2020, December 11). Mozilla.org.  
<https://developer.mozilla.org/es/docs/Glossary/TCP>

Techopedia. (2011, October 21). *Virtual Teletype (VTY)*. Techopedia.com; Techopedia.  
<https://www.techopedia.com/definition/1884/virtual-teletype-vty>

What is CLI. (2022). *What is CLI?* Computerhope.com.  
<https://www.computerhope.com/jargon/c/cli.htm>

*What Is Network Infrastructure? - Gigamon Blog.* (2019, March 6). Gigamon Blog.  
<https://blog.gigamon.com/2019/03/06/what-is-network-infrastructure/#:~:text=Network%20infrastructure%20comprises%20hardware%20and,up%20a%20system's%20network%20infrastructure.>