



# FACULTAD DE INGENIERIA

REDES DE DATOS SEGURAS

## Proyecto 1

Planeación, optimización y rediseño de una red cableada

Alumnos

- Garrido Czacki Mario Horacio
- Romero Andrade Cristian
- Romero Andrade Vicente

Profesor: Ing. Edgar Martinez Meza



## Índice

<b>1. Resumen</b>	<b>2</b>
<b>2. Objetivos</b>	<b>2</b>
2.1. Objetivo General . . . . .	2
<b>3. Entrevista</b>	<b>2</b>
<b>4. Escenario</b>	<b>5</b>
<b>5. Desarrollo</b>	<b>6</b>
5.1. Diseño Físico . . . . .	6
5.2. Estimaciones . . . . .	7
5.2.1. Estimacion de días y costos . . . . .	7
5.3. Propuesta . . . . .	9
<b>Siglas</b>	<b>17</b>
<b>Glosario</b>	<b>17</b>
<b>Índice de tablas</b>	<b>19</b>
<b>Índice de figuras</b>	<b>19</b>



## 1. Resumen

El cableado estructurado ha surgido y mejorado con el pasar del tiempo como una opción de establecer redes de área local LAN más estables, seguras y veloces que han de solventar gran cantidad de inconvenientes de conexión, intrusiones y tráfico lento, entre otros problemas que deben enfrentar los diseñadores de red.

En este proyecto se plantea el cableado de la segunda planta del Instituto de Geografía (IGG), tratando de una excelente cotización con excelente calidad-precio para el cableado, la instalación de los equipos con sus configuraciones correspondientes. tomando en cuenta el tiempo de vida de la futura red.

## 2. Objetivos

### 2.1. Objetivo General

Elaborar la Planeación, optimización y rediseño de la red Cableada interna del Instituto de Geografía (IGG) de la UNAM. El diseño de la red abarcará aspectos físicos y lógicos (cableado estructurado y direccionamiento lógico), así como la aplicación de los conceptos estudiados en los temas 3 y 5 de la materia de Redes de Datos Seguras.

## 3. Entrevista

Como requerimiento se nos pide hacer una entrevista a un experto sobre el área de redes para profundizar más en nuestra solución de la reestructura de la red del segundo piso de la IGG. En esta entrevista tenemos a José Palacios, Administrador de red en Padilla y Asociados:

### ¿Cuáles son los estándares que utilizas en el día a día en tu trabajo?

Pues es una pregunta muy amplia, realmente un poco de todo. Como en la empresa a mi no me toca hacer la instalación ya que contratan gente externa para eso, pues me toca más la parte del troubleshooting y software. Lo que si te toca de a ley es hacer un patch cord entonces el T568A y T568B si podría decir que los uso. Aún así a mi me toca ver la parte más lógica de la administración por lo que me tocan muchos estándares de encriptación como AES, OpenPGP, RSA, etc...

Por otro lado también veo bastante la parte inalámbrica por lo que pues WPA2 para las redes inalámbricas, Bluetooth para cuando a alguien no le funcionan los headsets por interferencia y otros de ese estilo. Por la parte administrativa pues SSH, SFTP, NAT, DHCP, etc...

### ¿Cuáles son las políticas de uso de la red que administras?

Realmente somos muy laxos para los tipos de contenido que nuestros empleados pueden ver en sus computadoras. Incluso si están en el Face mientras saquen el trabajo no hay mucho problema. Lo que si es que hemos tenido algunos incidentes y son los que nos llevó a poner reglas. Te puedo decir las principales:

- Bloqueo de sitios pornográficos — Obviamente vienes al trabajo a trabajar, entonces no hay razón para andarlos viendo.
- Bloqueo de protocolos P2P — Esto viene de que teníamos unos empleados que hacían uso excesivo de la red a altas horas de la noche. Cuando fuimos a investigar sus computadoras estaban encendidas descargando películas...Yo no se por que lo tenían que hacer en el trabajo cuando se



supone que no tienen tiempo para verlas pero ahí estaban, y cuando se enteraron los jefes de que estaban usando la red para piratería hasta los corrieron, pero por parte de la administración de red desde ahí los bloqueamos.

- Uso responsable de datos — Esto está mal dicho, es más bien privacidad de datos de la empresa. Básicamente es estar vigilando la cantidad de datos de subida externos a la red interna. Si alguien necesita subir documentos a la nube los metemos a un servidor dentro de la red que sirve como ventana para cuando los quieran ver desde fuera, pero es más difícil de sacar información así.
- No permisos de instalación en las máquinas de la empresa — No es tanto por desconfianza en los empleados, es más bien que luego los pueden engañar y te pueden meter un backdoor o algo del estilo. En mayor o menor medida les instalamos lo que nos pidan si lo necesitan para el trabajo, pero si nos andan pidiendo que un cliente de tienda de videojuegos pues ya no, claro.
- No reenviar correos externos en el servicio interno de correo electrónico — En sí tenemos todo un sistema muy cerrado de mensajería interna y todo mensaje que provenga de fuera de una lista de contactos se trata como sospechoso, pero no falta el que reenvía un correo cadena o alguna otra cosa. A parte de que reenviar algún correo de un cliente está mal por violar su privacidad, pueden haber vectores de ataque por correo electrónico que lleguen a las máquinas internas de la empresa y no queremos eso.
- No responder a todos — Tuvimos que deshabilitar esta función en los servidores de correo de la empresa, y aunque se quejen algunos no era padre tener que ver que a todo mundo le llegara un — Recibido, gracias. Porque un directivo manda un correo a toda la empresa y no falta la persona que quiere responder...Se hacía mucho SPAM y por eso ya no puedes hacerlo.
- No guardar archivos personales en la nube de la empresa — No somos millonarios aunque nos gustaría, por lo que no podemos guardar las fotos de las vacaciones con la familia en 2013. No nos metemos mucho, pero si hay auditorías periódicas nada más viendo los nombres de los archivos que suben para saber si alguien está abusando. Ya si quieren les regalo un USB, tengo muchos pero las reglas son reglas.

#### **¿Qué podrías remarcar para la parte de administración de redes?**

Si te gusta hay de dos, o te encuentras con cosas padres o con dolores de cabeza. Por mi parte apenas andamos haciendo el deployment de la nube interna y me he dado una divertida haciendo que funcione bien, y cuando ves que tu trabajo se va volviendo la columna vertebral de la empresa pues es muy padre.

Por la parte no tan padre es el soporte técnico. No puedo esperar a que las tablets sean lo suficientemente buenas como para deshacernos de las impresoras, se traban, se derrama la tinta, se queda atorado el buffer de documentos o a veces simplemente no quieren conectarse a la red. Luego no falta el desesperado que quiere imprimir si o si y manda el mismo documento muchas veces y luego ves una biblia de diapositivas de PowerPoint repetidas. Por suerte ya no se estila usar el Fax, porque esos también tenían muchos problemas. Incluso nos llegaban a mandar hojas enteras en negro para acabarse la tinta y que dejaran de imprimir, y en esos tiempos era más complicado.

#### **¿Me podrías resumir un poco el funcionamiento de tu red?**

Pues mira, primero que nada tienes un firewall FortiGate 5001E que se dedica a bloquear accesos que no queremos. A parte de eso por cualquier otro caso todos los usuarios cuentan con firewalls en sus propias computadoras ya sea en sitio o propiedad de la empresa. Claro que a parte de todo un



antivirus por cualquier cosa. Con eso y las políticas de no instalación ni permisos de administrador más o menos puedes asegurar que no van a pasar amenazas de equipo en equipo.

Como pusimos la nube interna tuvimos que contratar otro servicio de fibra para tener redundancia. Nos sale caro pero por lo que esta pasando por el COVID fue una muy buena inversión que hicimos el año pasado. En sí la nube interna digamos que está muy aislada por ambos lados. Tienes un portal web que deja hacer login y tener acceso limitado a archivos sensibles por fuera, y teníamos implementado que usaras un VPN para poder subir archivos a ella. Tuvimos que darle computadoras de la empresa a algunos empleados que no tenían ya que el VPN solo lo configuramos en esas y nos ayuda a mantener la red de la empresa relativamente segura mientras no estamos en sitio.

Volviendo a la configuración de bloqueo de la que te hablé hace rato nuestra red dentro de la empresa te maneja bloqueo a nivel DNS para los sitios bloqueados. A nivel máquina tienes algo a lo que le podrías llamar un rootkit, pero básicamente es un programa que corre en el anillo cero de la computadora y tiene permisos para todo, y se asegura que no puedas hacer varias cosas. También tenemos algunos programas que se dedican a bloquear protocolos como el P2P del que te hablaba antes instalados en cada computadora propiedad de la empresa.

Por parte del monitoreo de la red tenemos un Zabbix con el que nos podemos meter a ver el tráfico dentro de la red de la empresa. Obviamente con esto del COVID pues resulta monótono porque dentro de la empresa como tal no hay tanto tráfico, y tenemos otro sistema separado para la nube.

#### **¿Como es el mantenimiento de la red?**

Pues por ahora es más sencillo entre comillas. Las autoridades regionales ya no están dejando que te transportes si no es urgente por lo que solo he ido al sitio un par de veces a verificar el estado de los servidores, hay otros empleados que sí están más tiempo. Lo que sí tengo mucho más ahora es monitoreo, como todo el negocio depende de la nube por ahora tenemos que estar muy pendientes de tener disponibilidad lo más cercana posible al 100 % y cuidarnos bastante de los ataques. Hemos tenido intentos de ataques de denegación de servicio, pero pues contratamos un servicio para el front que lo puede librar, por lo que no hizo más que alentar un poco la entrada a la interfaz.

En una situación más convencional el mantenimiento iría si mucho a la parte de monitorear y soportar la nube, pero las responsabilidades se irían también a la red como tal. Entonces pues ahí me toca monitorear todo lo que es tráfico, revisar cableados en las computadoras fijas y ayudar a los empleados cuando estos desean hacer alguna modificación a su equipo.



## 4. Escenario

La red que se implementará abarca el edificio Principal del Instituto de Geografía (IGG). Es necesario tener las siguientes consideraciones:

- El enlace de acometida principal deberá ser con tecnología de fibra óptica y se tomará desde el anillo de red UNAM, nota éste ya existe.
- En el edificio Principal existen dos Terrazas en la que no se puede realizar el cableado, sin embargo se necesita conectividad.
- También existen áreas donde no se puede realizar cableado pero se necesita conectividad. (Revisar en los planos)
- Los cuartos de telecomunicaciones el MDF y los IDF's sólo pueden instalarse en áreas permitidas, éstos deben estar conectados a través de fibra óptica, entre cada uno de los IDF's y el MDF.
- Los cubículos son ocupados por un investigador y sus becarios y las áreas más grandes llamadas peceras albergan varios becarios. Considere el número de nodos adecuado para cada área y las direcciones IP que se van a requerir.
- En caso de que haya más de un área de trabajo por piso deberá aplicar direccionamiento lógico VLSM y poner las IPs correspondientes a cada área.



## 5. Desarrollo

Lo primero a efectuar antes de realizar ninguna operación previa, es comprobar toda la instalación sobre la cual se va a efectuar el montaje de la red. En este caso el segundo piso del edificio del *Instituto de Geografía (IGG) de la UNAM*. Nos piden lo siguiente:

- El cableado de ochenta nodos de red con CAT 6a o superior.
- Patch cords de categorías 6a o superiores de 24 a 48 puertos.
- Cableado de Fibra optica de *doce hilos*, con cotización propia.
- Dos racks.
- Correcto enrutamiento de lo IPs.
- Dos switch de cuarenta y ocho puertos 10G a un rango de (390W, 450W).
- Cuatro access points

### 5.1. Diseño Físico

En la figura 1 Podemos apreciar la ubicación de los racks de telecomunicaciones y las áreas de trabajo. También se nos proporciona un plano a detalle donde se encuentran especificadas las ubicaciones de las rosetas y de algunos access points, como un estimado de maquinas a interconectar. En la siguiente sección (5.3) se muestra un plano con el cableado ya estructurado.

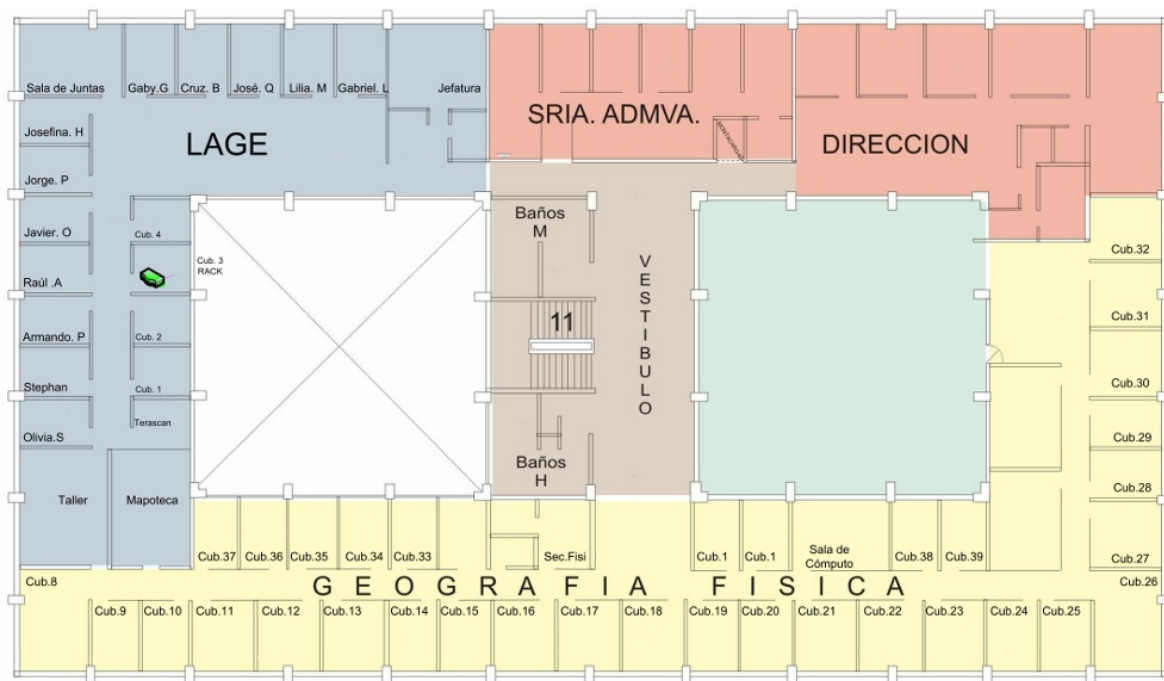


Figura 1: Distribución de la segunda planta



## 5.2. Estimaciones

### 5.2.1. Estimacion de días y costos

Producto/ Referencia	Descripción	Cantidad	Unidad	Valor Unitario	Valor Total
	Subsistema área de trabajo y Salidas de datos				\$74,649.15
	Jack RJ45 Mini.com® CAT 6a	85	unidad	\$250.00	\$21,250.00
	Placa de pared de cuatro Entradas (Tapa y caja)	85	unidad	\$599.99	\$50,999.15
	Patchcord 6a	80	unidad	\$30.00	\$2,400.00
	Subsistema horizontal				\$5,300.00
	Cable UTP de Datos Cat 6a	1	305 [m]	\$5,300.00	\$5,300.00
	Subsistema Gabinete de Telecomunicaciones				\$15,200.00
	Cable UTP de Datos Cat 6a	3	unidad	\$1,600.00	\$4,800.00
WMPHF2E	Organizador Horizontal Frontal 2ur	4	unidad	\$900.00	\$3,600.00
WMPVF45E	Organizador Vertical Frontal 2ur	4	unidad	\$1,700.00	\$6,800.00
	Fibra Óptica				\$57,767.99
	Fibra Óptica 12 hilo 70 metros, Multimodo 50/125	70	metro	\$450.00	\$31,500.00
FLCSMCXAQY	Conector Simplex pre-pulido lc Opticam® multimodo 50/125	24	unidad	\$602.00	\$14,448.00
FAP12WBRDDLZ	Panel de adaptadores de fibra LC 10 Gig OM3/OM4 cargado con doce adaptadores de fibra optica LC 10Gig duplex multimodo	1	unidad	\$5,000.00	\$5,000.00
FAP6WAQDLC	Panel de 6 Adaptadores de Fibra Óptica LC 10Gig OM3/OM4 Dúplex Multimodo	1	unidad	\$1,750.00	\$1,750.00
FXE3-10M3Y	Jumpper de Fibra Duplex lc-lc 50/125 m (om3/om4)	1	3 [m]	\$869.99	\$869.99
FHD-2UFCE	Distribuidor de fibra de 2U	1	unidad	\$4,200.00	\$4,200.00
	Equipos y Dispositivos				\$208,497.00
WAP581-B-K9	Access Point Cisco	4	unidad	\$5,700.00	\$22,800.00
WS-C2960X-48TS-L	Switch CISCO 48 puertos	2	unidad	\$67,899.00	\$135,798.00
WS-C2960X-24S-L	Switch CISCO 24 puertos	1	unidad	\$49,899.00	\$49,899.00
				Total	\$361,414.14

Tabla 1: Cotización, Productos





Nombre	Duración
☐ ● Proyecto	33
☐ ● Alistamiento Previo	5
● Análisis de Estructura	1
● Calculo de cantidades de Obra	2
● Definición de Red y Datos de la estructura	2
● Inicio de actividades	0
☐ ● Montaje de sistemas de portacables y ductos	9
● Perforaciones entre placas	3
● Instalaciones de Bandejas y Canaletas	6
☐ ● Instalación de Red	19
● Tendido de Cable UTP	10
● Instalaciones de Salidas Lógicas	2
● Adecuaciones de Gabinetes	2
● Marcado de los Subsistemas	1
● Instalaciones de los dispositivos	1
● Configuración y pruebas de conectividad (direccionamiento de IP)	3
● Entrega	0

Figura 2: Cronograma

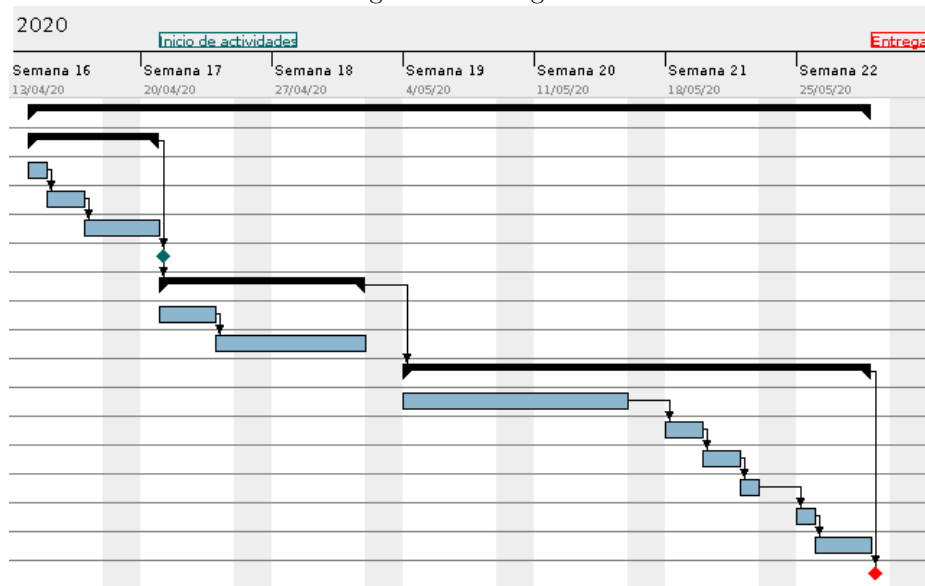


Figura 3: Cronograma Gráfico

Como vemos en la figura 2 la instalación de la red para el segundo piso consta de **33** días laborales añadiendo un costo de mano de obra de \$300,000,00MXN.

Por lo tanto, el costo para instalar la red en el segundo piso del IGG es a un aproximado de \$661,414,14MXN — SEISCIENTOS SESENTA Y UN MIL CUATROCIENTOS CATORCE 14/100 MXN.



### 5.3. Propuesta

Considerando las necesidades de la red del segundo piso, y reconociendo las distintas áreas de trabajo, se identificaron tres subredes pertinentes para su cableado. Hay que notar que aunque nuestros switches tienen capacidades para más nodos, estas se mantendrán latentes para posibles expansiones en la red si llegan a ser necesarias, y solo se considerarán los 80 nodos planteados inicialmente.

- Geografía Física: Es la zona por mucho más grande, y por ende la que requiere más soporte de equipos. A esta subred le asignaremos una capacidad de 40 nodos.
- LAGE: Identificamos las necesidades de esta zona, y decidimos asignarle 22 nodos.
- Área Administrativa (Zona conjunta Dirección y Secretaría Administrativa): Consideramos que por su cercanía física y de necesidades, una sola subred puede cubrir ambas. A esta subred le asignaremos 18 nodos.

Ahora que definimos las necesidades de nuestras subredes, realizaremos las divisiones de las IP. Consideraremos nuestra IP base a 177.164.4.0.

#### Geografía Física

A esta la conoceremos como la subred 0. Ya que decidimos asignarle 40 nodos, requeriremos un número de nodos posibles potencia de dos. Por lo tanto esta red tendrá  $2^6 - 2 = 62$  hosts.

Empezaremos la descripción de la subred:

- Máscara modificada: 255.255.255.192 o /26
- Segmento: 177.164.4.0
- Direcciones asignables: 177.164.4.1 – 177.164.4.62
- Broadcast: 177.164.4.63

#### LAGE

A esta la conoceremos como la subred 1. Ya que decidimos asignarle 22 nodos, requeriremos un número de nodos posibles potencia de dos. Por lo tanto esta red tendrá  $2^5 - 2 = 30$  hosts.

- Máscara modificada: 255.255.255.224 o /27
- Segmento: 177.164.4.64
- Direcciones asignables: 177.164.4.65 – 177.164.4.94
- Broadcast: 177.164.4.95

#### Área Administrativa

A esta la conoceremos como la subred 2. Ya que decidimos asignarle 18 nodos, requeriremos un número de nodos posibles potencia de dos. Por lo tanto esta red tendrá  $2^5 - 2 = 30$  hosts.

- Máscara modificada: 255.255.255.224 o /27
- Segmento: 177.164.4.96



- Direcciones asignables: 177.164.4.97 – 177.164.4.126
- Broadcast: 177.164.4.127

En este caso no requerimos subredes de enlace ya que la conectividad entre las subredes es dentro del mismo router.

Una vez configurada la red en PacketTracer para su prueba, se puede ver así:

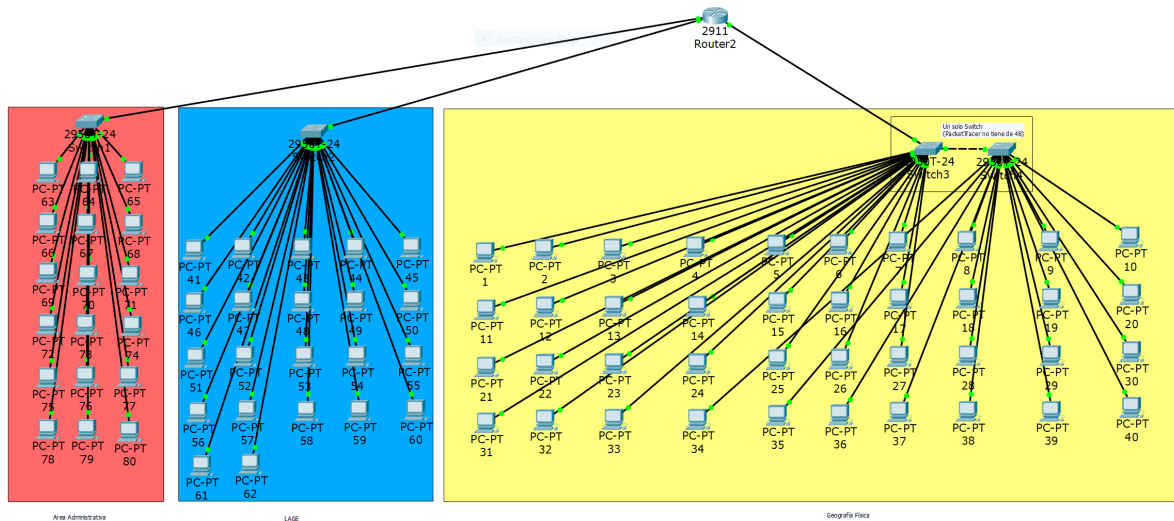


Figura 4: Topología de la red.

Debe notarse que decidimos usar dos switches de 24 puertos y uno de 48 por los requerimientos de cada subred. Sin embargo, PacketTracer no tiene switches de 48 puertos incluidos, por lo que lo sustituimos por dos switches de 24 puertos en cascada. Esto en la práctica no sucedería porque procuraríamos tener el hardware necesario, pero fue necesario hacer esta sustitución para poder probar la configuración de la red. Los colores de los recuadros corresponden a la zona en la que se encuentran los equipos dado el siguiente diagrama:



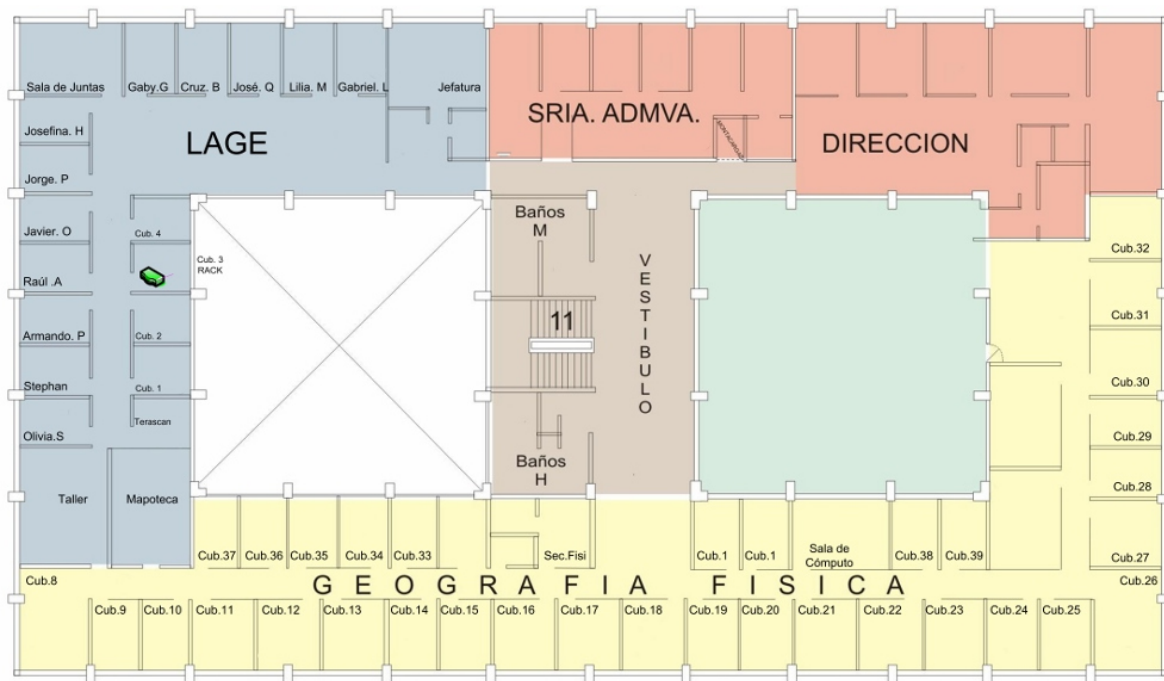


Figura 5: Diagrama de las zonas del segundo piso.

## Configuración

Para realizar la simulación, se tuvo que configurar el equipo de manera que se respetaran las subredes necesarias. A continuación daremos ejemplos de como se realizó la configuración para cada zona:

### Geografía Física

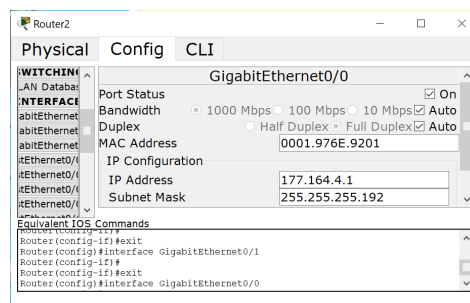


Figura 6: Configuración del puerto del router para esta subred (dirección IP y máscara de subred)



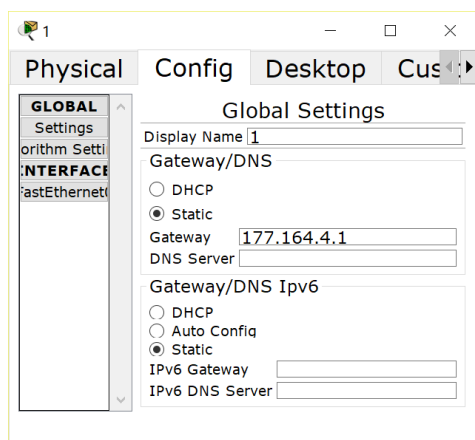


Figura 7: Configuración de Gateway para un equipo de la subred

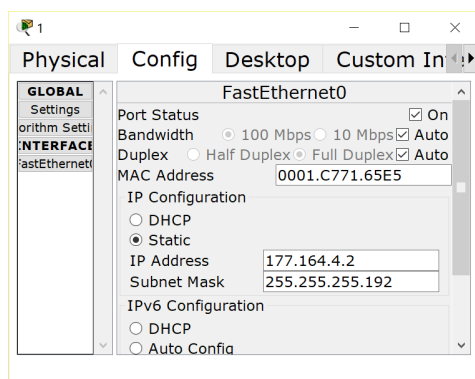


Figura 8: Configuración de dirección IP y máscara de subred para un equipo de la subred

## LAGE

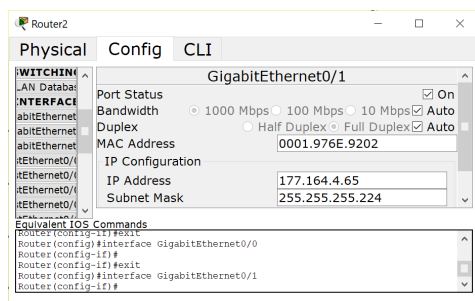


Figura 9: Configuración del puerto del router para esta subred (dirección IP y máscara de subred)



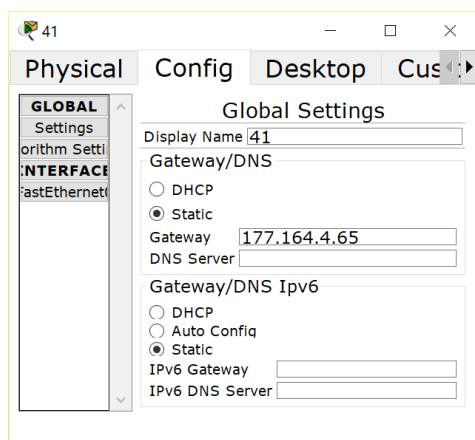


Figura 10: Configuración de Gateway para un equipo de la subred

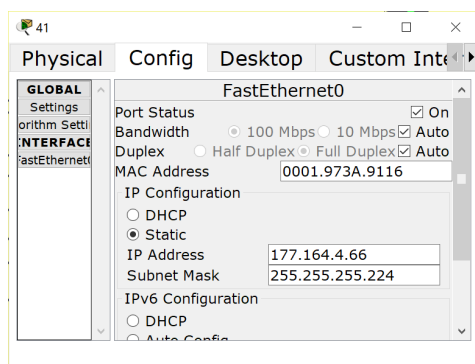


Figura 11: Configuración de dirección IP y máscara de subred para un equipo de la subred

## Área Administrativa

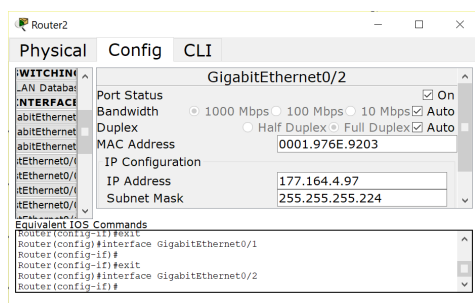


Figura 12: Configuración del puerto del router para esta subred (dirección IP y máscara de subred)



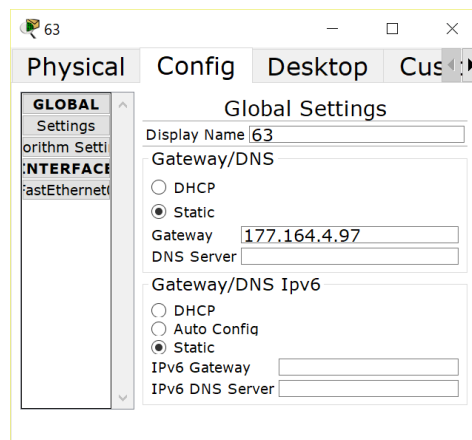


Figura 13: Configuración de Gateway para un equipo de la subred

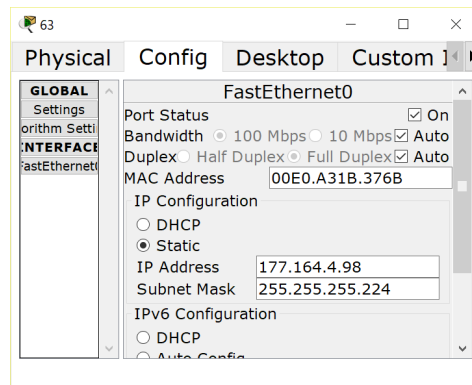


Figura 14: Configuración de dirección IP y máscara de subred para un equipo de la subred

## Pruebas de conectividad

Tras generar la red, se hicieron varias pruebas para demostrar la correcta configuración de las subredes. Como se podrá ver, se probaron todos los casos de conectividad dentro y fuera de las subredes.

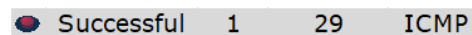


Figura 15: Prueba de hacer un ping de un equipo en la subred 0 a otro en la subred 0.

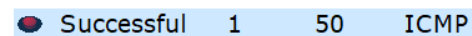


Figura 16: Prueba de hacer un ping de un equipo en la subred 0 a otro en la subred 1.




	Successful	16	74	ICMP
---	------------	----	----	------

Figura 17: Prueba de hacer un ping de un equipo en la subred 0 a otro en la subred 2.


	Successful	45	59	ICMP
---	------------	----	----	------

Figura 18: Prueba de hacer un ping de un equipo en la subred 1 a otro en la subred 1.


	Successful	54	3	ICMP
---	------------	----	---	------

Figura 19: Prueba de hacer un ping de un equipo en la subred 1 a otro en la subred 0.

	Successful	58	76	ICMP
---	------------	----	----	------

Figura 20: Prueba de hacer un ping de un equipo en la subred 1 a otro en la subred 2.

	Successful	80	63	ICMP
---	------------	----	----	------

Figura 21: Prueba de hacer un ping de un equipo en la subred 2 a otro en la subred 2.


	Successful	79	9	ICMP
---	------------	----	---	------

Figura 22: Prueba de hacer un ping de un equipo en la subred 2 a otro en la subred 0.


	Successful	69	42	ICMP
---	------------	----	----	------

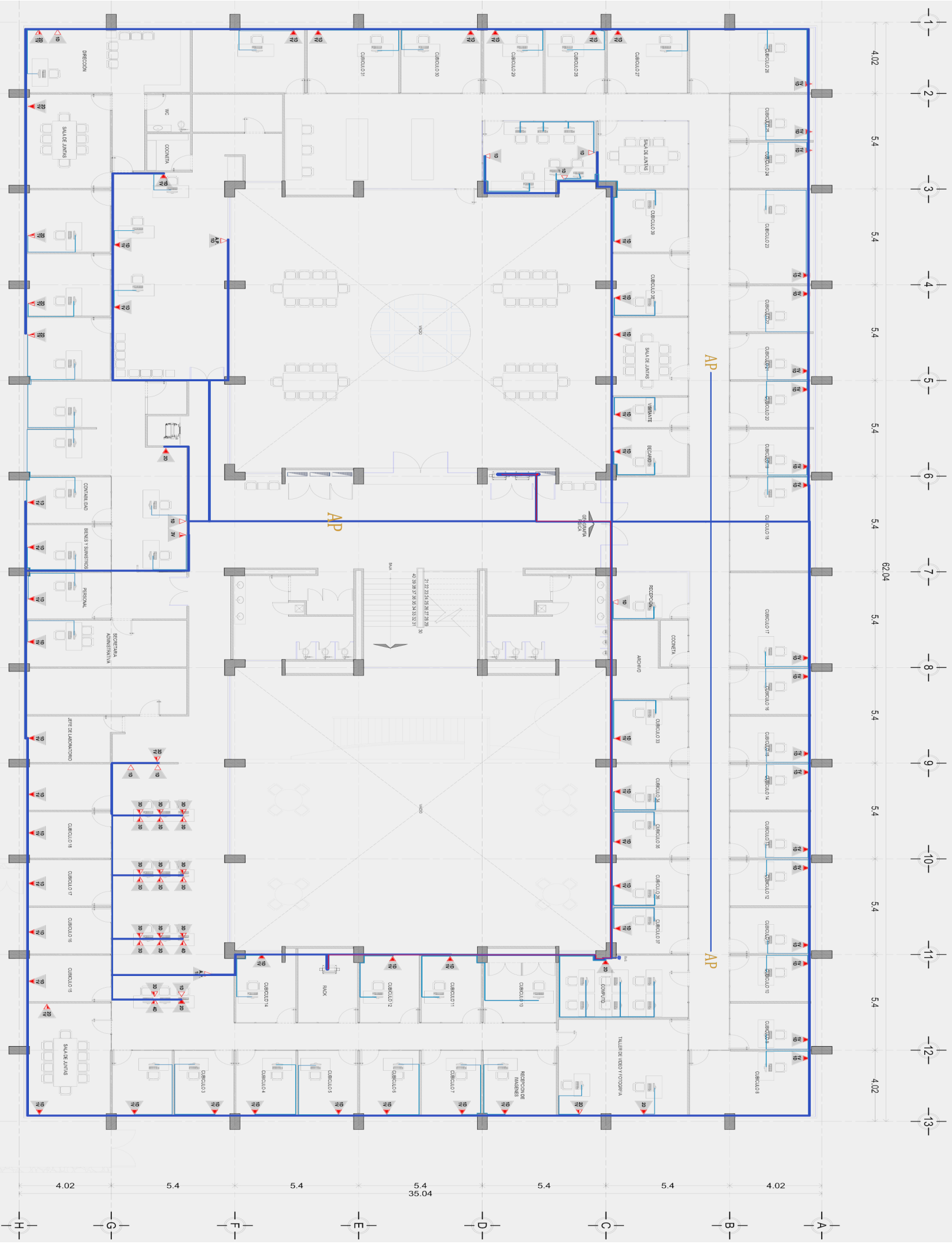
Figura 23: Prueba de hacer un ping de un equipo en la subred 2 a otro en la subred 1.

Como se puede notar, la configuración es correcta ya que es posible tanto generar comunicación en la misma subred, así como pasar esa comunicación al router que tiene puertos como Gateway de las otras subredes, lo que permite un correcto enrutamiento de la información. Si se deseara limitar estos accesos por políticas de acceso, podríamos recurrir a firewalls en el router para evitar la intercomunicación directa entre equipos de las distintas subredes.

A continuación se muestra una imagen a escala del piso con su respectivo cableado, donde la fibra óptica (color rojo) entra por el backbone y donde los IDF's se conectan en estrella con el MDF.







## Siglas

### I

**IDF** Intermediate Distribution Frame–Marco de distribución intermedia. 5, 15

**IGG** Instituto de Geografía. 2, 5, 6, 8

### L

**LAN** Local Area Network–Red de área local. 2

### M

**MDF** Main Distribution Facility–Instalación principal de distribución. 5, 15

### U

**UNAM** Universidad Nacional Autonoma de México. 2, 5, 6

### V

**VLSM** Variable Length Subnet Mask–Máscaras de Subred de Tamaño Variable. 5

## Glosario

### A

**access point** Se trata de un dispositivo utilizado en redes inalámbricas de área local (WLAN -Wireless Local Area Network), una red local inalámbrica es aquella que cuenta con una interconexión de computadoras relativamente cercanas, sin necesidad de cables, estas redes funcionan a base de ondas de radio específicas. El Access Point entonces se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios.. 6

### C

**cableado estructurado** El concepto de cableado estructurado es tender cables deseñal en un edificio de manera tal que cualquier servicio de voz, datos, vídeo, audio, tráfico de Internet, seguridad, control y monitoreo esté disponible desde y hacia cualquier roseta de conexión del edificio. Esto es posible distribuyendo cada servicio a través del edificio por medio de un cableado estructurado estándar concables de cobre o fibra óptica. Esta infraestructura es diseñada, o estructurada para maximizar la velocidad, eficiencia y seguridad de la red. Ninguna inversión en tecnología dura más que el sistema de cableado, que es la base sobre la cual las demás tecnologías operarán.. 2

### P

**patch cord** Los racks (que también se conocen como cabinas o bastidores) se hallan en los centros de datos que disponen de muchos servidores. El correcto armado de la estructura es esencial para el funcionamiento de los equipos, ya que los cables deben organizarse de manera adecuada para lograr las conexiones.. 6



**R**

**rack** Los racks (que también se conocen como cabinas o bastidores) se hallan en los centros de datos que disponen de muchos servidores. El correcto armado de la estructura es esencial para el funcionamiento de los equipos, ya que los cables deben organizarse de manera adecuada para lograr las conexiones.. 6

**roseta** Es la entrada hembra de un JACK RJ45, tiene la función de interconectar dispositivos electrónicos de red (servidores, switch, router, equipos de cómputo, etc.).. 6

**W**

**WPA** WPA (acceso inalámbrico protegido) es una solución de seguridad inalámbrica (wifi) ofrecida por WiFi Alliance para solucionar las carencias de WEP. WPA2 está basada en el nuevo estándar 802.11i. 2



## Índice de tablas

1. Cotización, Productos . . . . .	7
------------------------------------	---

## Índice de figuras

1. Distribución de la segunda planta . . . . .	6
2. Cronograma . . . . .	8
3. Cronograma Gráfico . . . . .	8
4. Topología de la red. . . . .	10
5. Diagrama de las zonas del segundo piso. . . . .	11
6. Configuración del puerto del router para esta subred (dirección IP y máscara de subred)	11
7. Configuración de Gateway para un equipo de la subred . . . . .	12
8. Configuración de dirección IP y máscara de subred para un equipo de la subred . . . . .	12
9. Configuración del puerto del router para esta subred (dirección IP y máscara de subred)	12
10. Configuración de Gateway para un equipo de la subred . . . . .	13
11. Configuración de dirección IP y máscara de subred para un equipo de la subred . . . . .	13
12. Configuración del puerto del router para esta subred (dirección IP y máscara de subred)	13
13. Configuración de Gateway para un equipo de la subred . . . . .	14
14. Configuración de dirección IP y máscara de subred para un equipo de la subred . . . . .	14
15. Prueba de hacer un ping de un equipo en la subred 0 a otro en la subred 0. . . . .	14
16. Prueba de hacer un ping de un equipo en la subred 0 a otro en la subred 1. . . . .	14
17. Prueba de hacer un ping de un equipo en la subred 0 a otro en la subred 2. . . . .	15
18. Prueba de hacer un ping de un equipo en la subred 1 a otro en la subred 1. . . . .	15
19. Prueba de hacer un ping de un equipo en la subred 1 a otro en la subred 0. . . . .	15
20. Prueba de hacer un ping de un equipo en la subred 1 a otro en la subred 2. . . . .	15
21. Prueba de hacer un ping de un equipo en la subred 2 a otro en la subred 2. . . . .	15
22. Prueba de hacer un ping de un equipo en la subred 2 a otro en la subred 1. . . . .	15
23. Prueba de hacer un ping de un equipo en la subred 2 a otro en la subred 1. . . . .	15

