Pymes On Line
Su aliado estratégico en tecnología e innovación

Santiago de Cali, Julio 26 de 2024

Señores

INTENALCO EDUCACION SUPERIOR

Atn. Dr Neyl Grisales Arana Rector

Atn. Dr Ricardo Perdomo Mosquera Técnico administrativo Supervisor

ASUNTO: AUDITORIA DE RED, REVISION DE PUNTOS DE RED, INCLUYENDO EQUIPOS DE RED.

Se realizo la revisión de todos los puntos de datos ubicados en los pisos: 1, 2, 3, 4, 5 y salas de cómputo. Donde se identifican los puntos de red, Backbone, Access point y equipos administrativos (equipos de cómputo, impresoras y teléfonos). A continuación, se detalla en cada uno de los switches su respectiva configuración.

Al realizar la revisión de switch, al encontrarse que el firewall de estos se encontraba desactualizado se procedió con la actualización de 17 switch a la última versión de su firewall respectivo. Aunque esto no estaba constatado en el contrato

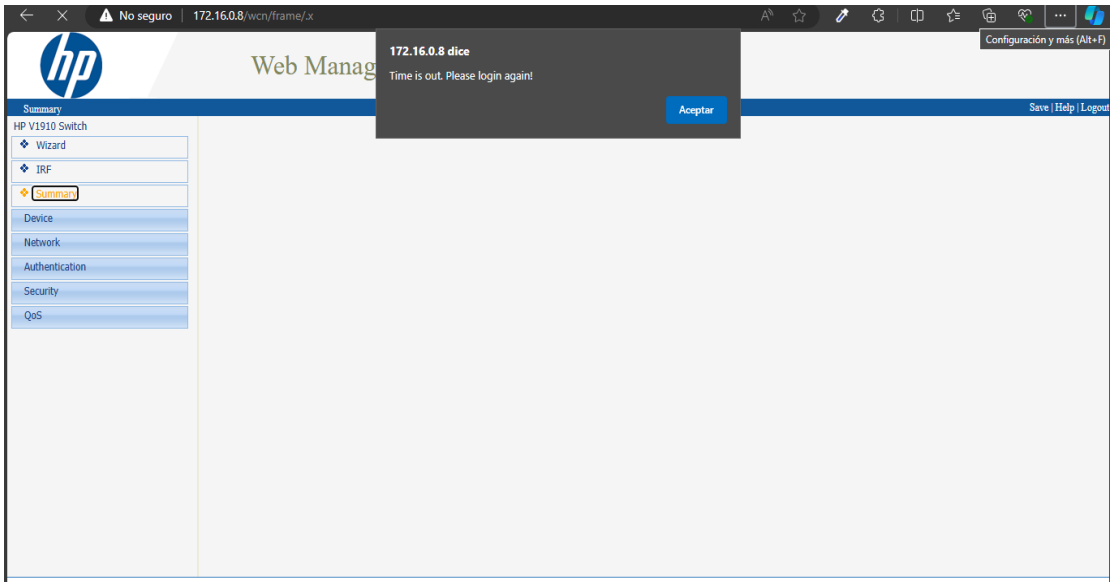
UBICACIÓN	SWITCH	IP	PUERTOS EN TRUNK	PUERTOS EN ACCESS	VLAN
PISO 1	**CISCO SG 220-50 OFICINA MANTENIMIENTO**	172.16.3.243	PUERTO:1-50	0	VLAN 1 Y 200
PISO 1	**CISCO SG 220-50 BIBLIOTECA**	172.16.3.245	PUERTO:26,46,48-50	PUERTO:1-25,-27-45	VLAN 100 Y 200
PISO 1	**TP-LINK TL-SG3452**	172.16.2.154	0	0	VLAN 400 Y 1
PISO 2	**HP V1910 24G**	172.16.0.8	0	0	N/A
PISO 3	**CISCO SG 220-50**	172.16.3.248	PUERTO:1-50	0	VLAN 1 Y 200
PISO 4	**CENTRO PRINCIPAL DE CABLEADO CISCO SG 220-50**	172.16.3.249	PUERTO:1-27,29, 31-42,44-50	PUERTO:28,30,43	VLAN 1,200 Y 400
PISO 4	**CENTRO PRINCIPAL DE CABLEADO SALAS – CISCO SG 250-26**	172.16.3.240	PUERTO:1,10,20,25	PUERTO:11-19,21-24,26-50	VLAN 400
PISO 4	**SWITCH SALA SISTEMAS 1: SG250-50**	172.16.8.24	PUERTO: 50	PUERTO:1-49	VLAN 1
PISO 4	**SWITCH GABINETE SERVIDORES**	172.16.2.110	PUERTO: 50	PUERTO: 2,25	VLAN 1 Y 400
PISO 4	**SALA SISTEMAS 2: SG250-26**	172.16.8.22	PUERTO: 26	PUERTO:1-25	VLAN 1
PISO 4	**SALA SISTEMAS 3: SG250-26**	172.16.8.28	PUERTO: 26	PUERTO:1-25	VLAN 1
PISO 4	**SALA SISTEMAS 4: SG250-26**	172.16.8.30	PUERTO: 25	PUERTO:1-24-26	VLAN 1

PISO 4	**SALA SISTEMAS 5: SG250-26**	172.16.8.20	PUERTO: 26	PUERTO:1-25	VLAN 1
PISO 4	**SALA SISTEMAS 6: SG250-26**	172.16.8.21	PUERTO: 26	PUERTO:1-25	VLAN 1
PISO 4	**SALA SISTEMAS 7: SG250-26**	172.16.8.32	PUERTO: 26	PUERTO:1-25	VLAN 1
PISO 5	**CISCO SG 220-50 AUDITORIO**	172.16.3.246	PUERTO:1-50	0	VLAN 1 Y 200
PISO 5	**CISCO SG 220-50 OFICINA TALENTO HUMANO**	172.16.3.247	PUERTO:1,46-50	PUERTO: 2-45	VLAN 1 Y 200

SWITCH PISO 2 - HP V1910 24G

Dirección IP: 172.16.0.8

No es posible realizar configuración de redes VLAN debido a fallas conexión mediante la web del switch



Nota: Al ingresar el código de acceso, se produce un error a pesar de que el código sea correcto. Además, el sistema se desconecta en un lapso de 5 segundos después de intentar el acceso.

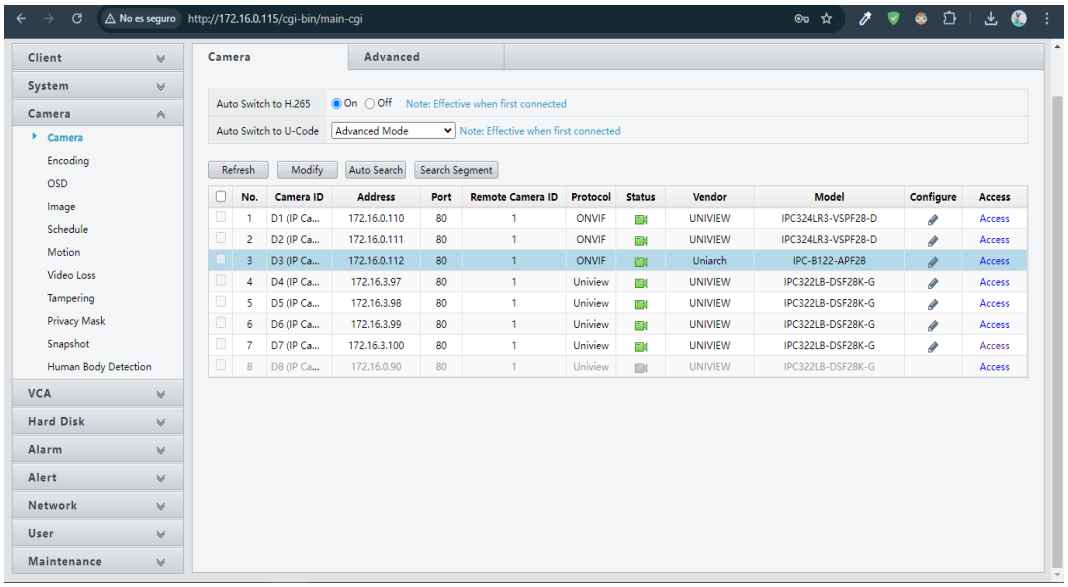
Ubicación	Centros de cableado	Switch	Routers	AP	Eq. Computo sala	Equipos admi.	Equipos biblioteca	Servidores	Tableros inteligentes	Cámaras
Piso 1	3	3	0	5	22	25	18	0	1	32
Piso 2	1	1	0	3	0	0	0	0	8	8
Piso 3	1	1	0	3	0	2	0	0	0	10
Piso 4	9	10	3	4	155	7	0	6	1	18
Piso 5	2	2	0	4	0	41	0	0	1	15
TOTAL	16	17	3	19	177	75	18	6	11	83

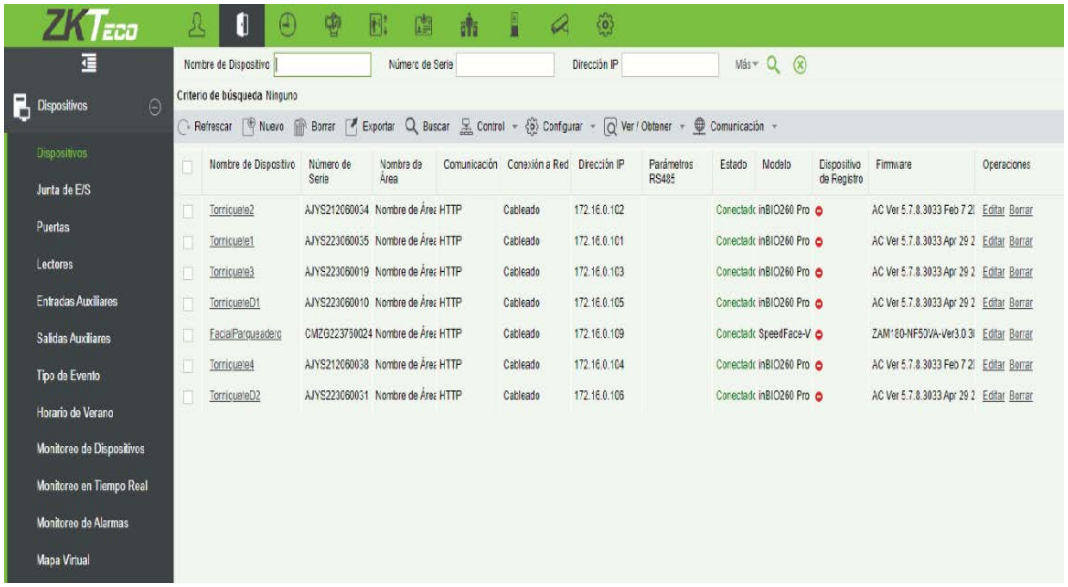
SEGMENTACIÓN DE RED DE DATOS

El direccionamiento de la red de la institución está constituido de la siguiente forma:

CONFIGURACION REDES CONEXIÓN						
RED	DHCP	DIRECCION DE RED	MASCARA	PUERTA ENLACE	DNS	DNS
ADMINISTRATIVA:	**172.16.2.25/150**	172.16.0.1/22	255.255.252.0	172.16.0.1	200.110.169.20	200.110.169.27
VLAN 400 SALAS	**172.16.8.20/250**	172.16.8.1/24	255.255.255.0	172.16.8.1	200.29.96.24	200.29.104.24
VLAN 100 BIBLIOTECA	**172.16.20.10/250**	172.16.20.1/24	255.255.255.0	172.16.20.1	200.29.96.24	200.29.104.24
VLAN 200 RED WIFI ESTUDIANTES	**172.16.16.10/172.16.17.10**	172.16.16.1/22	255.255.252.0	172.16.16.1	200.29.96.24	200.29.104.24
CLARO		190.144.141.10/30	255.255.255.242	190.144.141.9	190.157.8.33	
Emcali:		200.29.117.154/29	255.255.255.248	200.29.117.153	200.29.96.24	200.29.104.24
Mediacommerce:		190.121.134.55/28	255.255.255.240	190.121.134.50	200.110.169.20	200.110.169.27

UBICACIÓN	CENTRO CABLEADO	TOTAL, DE PUNTOS DE DATOS
PISO 1	SC 1	42
PISO 1	BIBLIOTECA	47
PISO 1	EXTENSION	59
PISO 1	MONITOREO	48
PISO 2	CUARTO ELECTRICOS	35
PSIO 3	CUARTO ELECTRICOS	40
PISO 4	CENTRO CABLEADO PRINCIPAL	48
PISO 4	SALA 1	46
PISO 4	SALA 2	23
PISO 4	SALA 3	23
PISO 4	SALA 4	22
PISO 4	SALA 5	23
PISO 4	SALA 6	22
PISO 4	SALA 7	23
PISO 4	JURIDICO	23
PISO 5	SC 5-1	48
PISO 5	SC 5-2	86
PISO 5	TS 1	6
	TOTAL	664





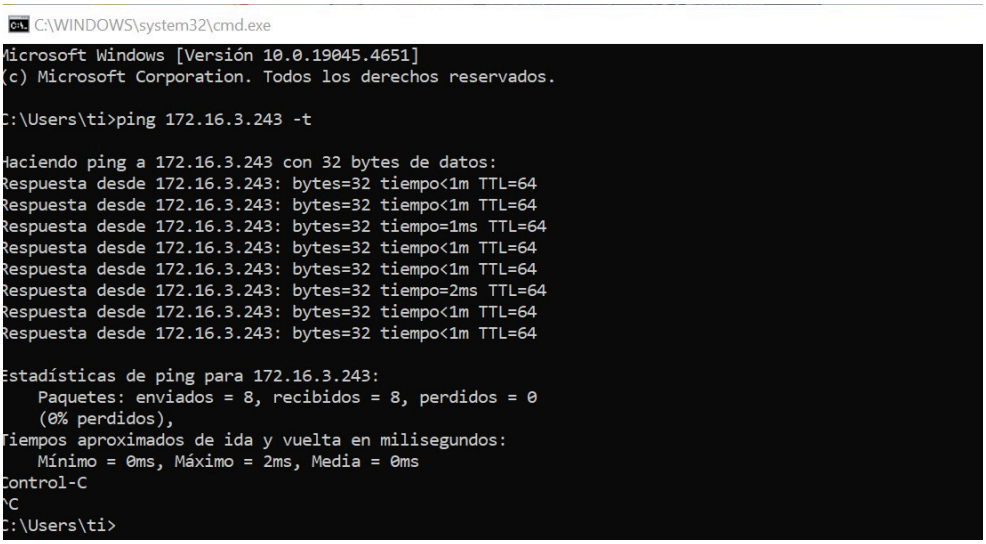
3. PRUEBAS DE LATENCIA

Definición de latencia en una red de datos, muestra en el tiempo que tarda los datos en transferirse a través red, entre mayor sea el retardo latencia será alta y al menor retardo menor latencia. La latencia ideal para comunicación en tiempo real, debe ser menor a 50 milisegundos, menos de 20 milisegundos se considera ideal. Se realizaron a través de comando ping que nos devuelve el tiempo que se tarda de un paquete a otro según la IP pruebas

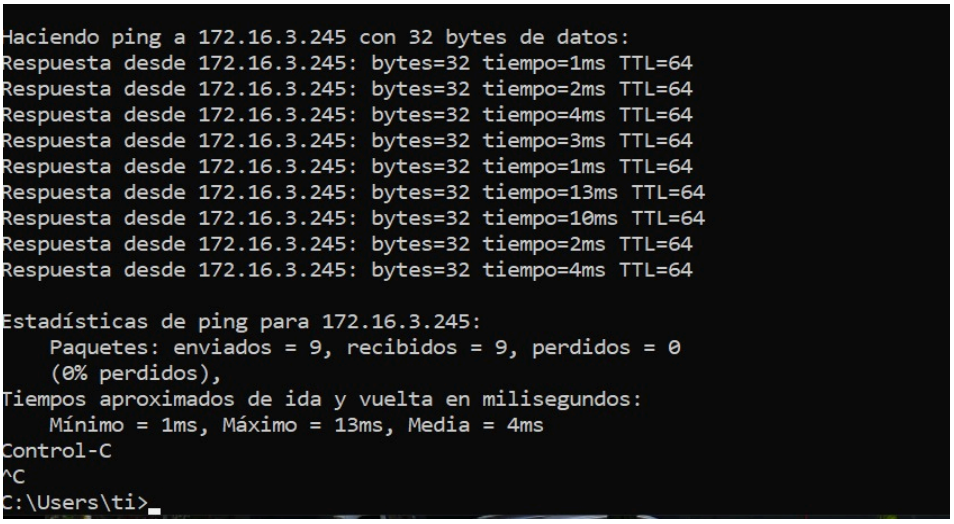
CENTRO DE CABLEADO	IP	LATENCIA	IMAGEN	OBSERVACION
Centro de cableado principal	172.16.3.243	1 milisegundo	SWITCH PISO 1	Bueno
Centro de cableado principal	172.16.3.245	1 milisegundo	SWITCH BIBLIOTECA	Bueno
Centro de cableado principal	172.16.2.154	1 milisegundo	SWITCH EXTENCION	Bueno
Centro de cableado principal	172.16.0.8	1 milisegundo	SWITCH PISO 2	Bueno
Centro de cableado principal	172.16.3.248	1 milisegundo	SWITCH PISO 3	Bueno

Centro de cableado principal	172.16.3.249	1 milisegundo	SWITCH SALAS PISO 4	Bueno
Centro de cableado principal	172.16.3.240	1 milisegundo	SWITCH PRINCIPAL PISO 4	Bueno
Centro de cableado principal	172.16.8.24	1 milisegundo	SWITCH AUDITORIO PISO 5	Bueno
Centro de cableado principal	172.16.8.22	1 milisegundo	SWITCH TALENTO HUMANO	Bueno
Centro de cableado principal	172.16.8.28	1 milisegundo	SWITCH SALA SISTEMAS 1	Bueno
Centro de cableado principal	172.16.8.30	1 milisegundo	SWITCH SALA SISTEMAS 2	Bueno
Centro de cableado principal	172.16.8.20	1 milisegundo	SWITCH SALA SISTEMAS 3	Bueno
Centro de cableado principal	172.16.8.21	1 milisegundo	SWITCH SALA SISTEMAS 4	Bueno
Centro de cableado principal	172.16.8.32	1 milisegundo	SWITCH SALA SISTEMAS 5	Bueno
Centro de cableado principal	172.16.3.246	1 milisegundo	SWITCH SALA SISTEMAS 6	Bueno
Centro de cableado principal	172.16.3.247	1 milisegundo	SWITCH SALA SISTEMAS 7	Bueno
Centro de cableado principal	190.121.134.50	1 milisegundo	CÁMARA IP	Bueno
Centro de cableado principal	200.29.117.153	1 milisegundo	GATEWAY MEDIACOMMERCE	Bueno
Centro de cableado principal	190.144.141.9	1 milisegundo	GATEWAY EMCALI	Bueno
Centro de cableado principal	172.16.3.216	2 milisegundos	GATEWAY CLARO	Bueno
Centro de cableado principal	172.16.3.3	2 milisegundos	DINSTAR	Bueno
Centro de cableado principal	172.16.0.4	1 milisegundo	SERVIDOR ARCHIVO	Bueno
Centro de cableado principal	172.16.0.7	7 milisegundo	SERVIDOR TELEFONIA	Bueno

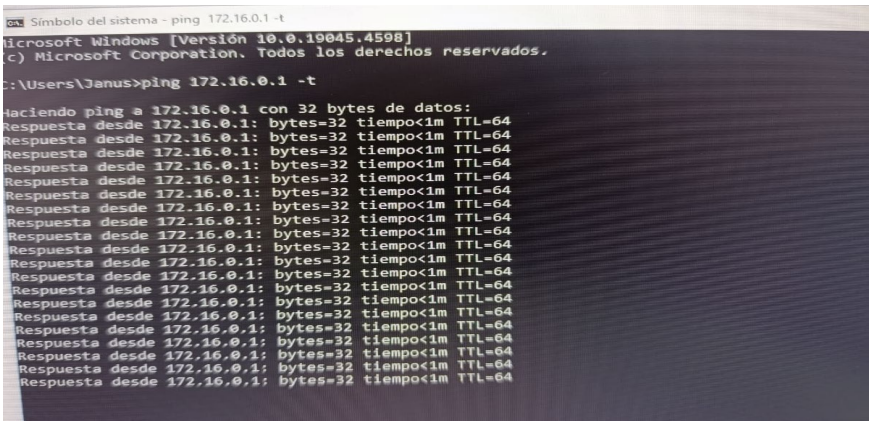
SWITCH PISO 1



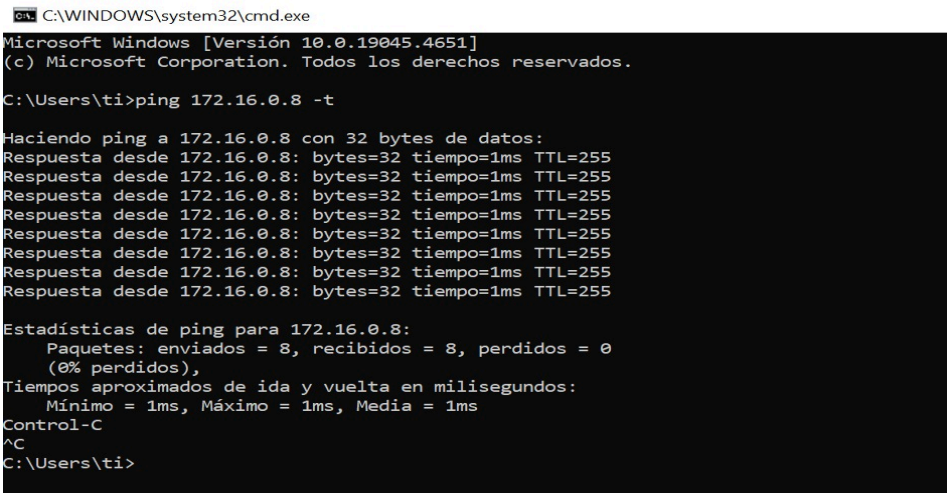
SWITCH BIBLIOTECA



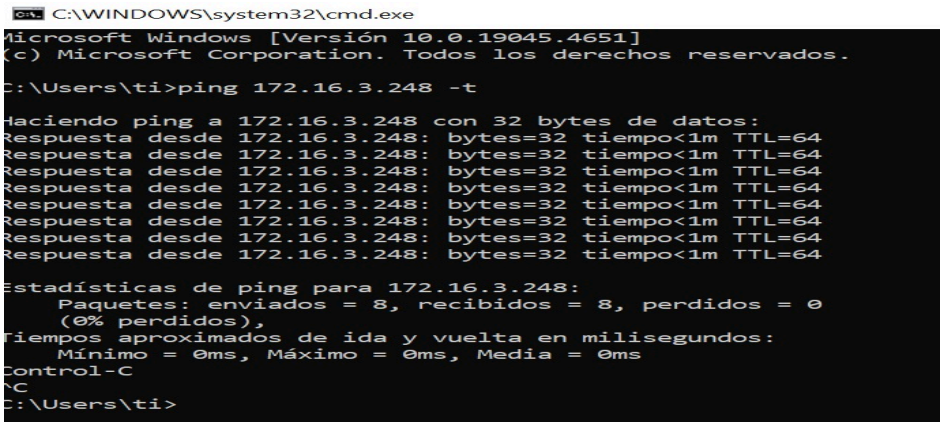
SWITCH EXTENSION



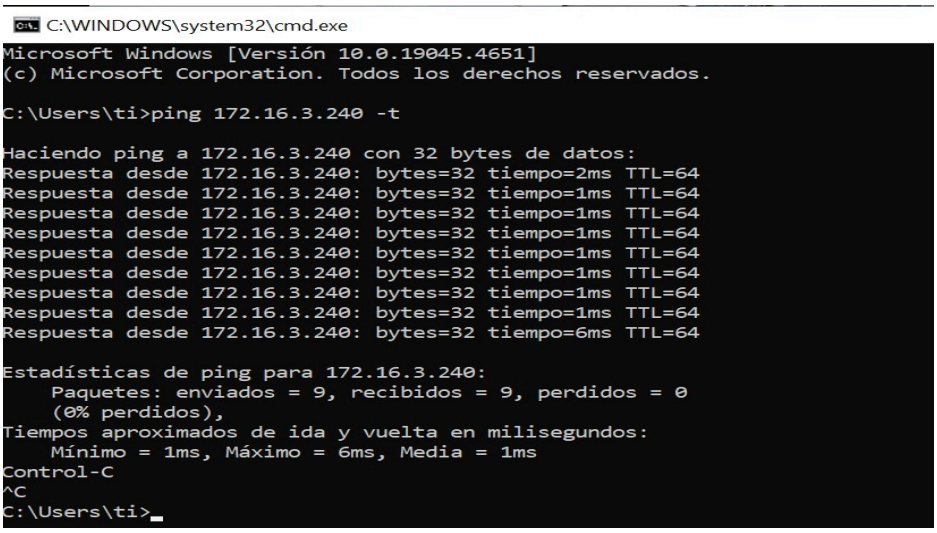
SWITCH PISO 2



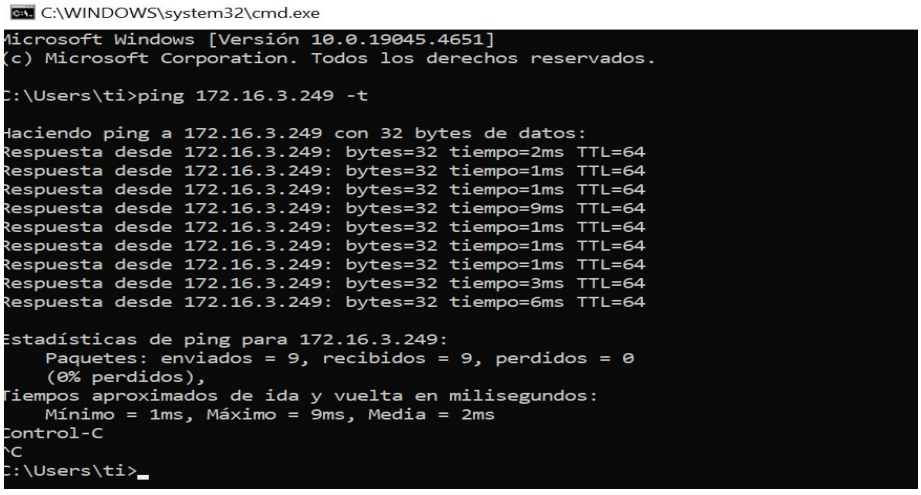
SWITCH PISO 3



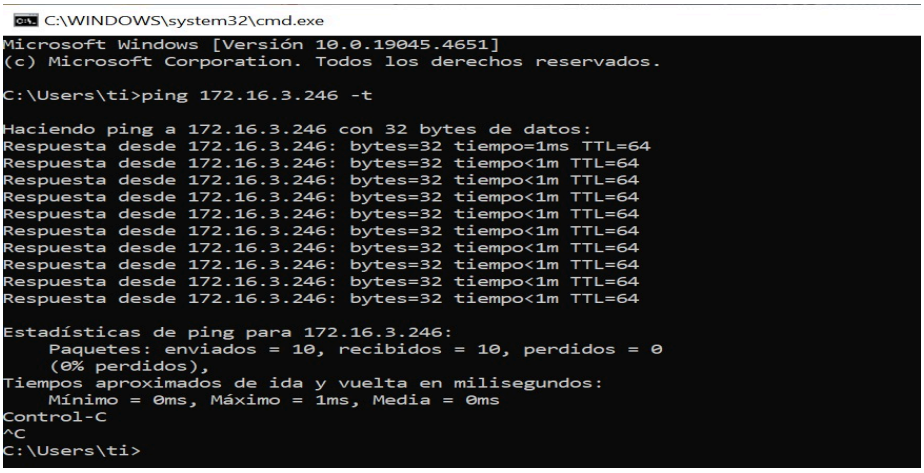
SWITCH SALAS PISO 4



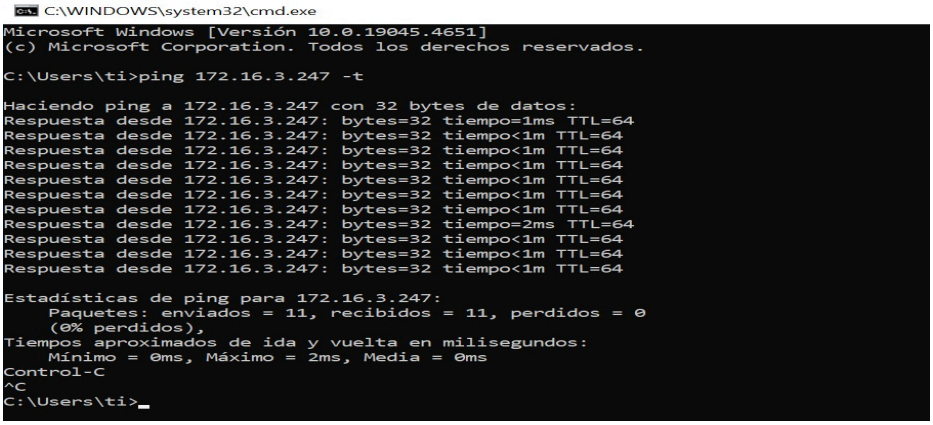
SWITCH PRINCIPAL PISO 4



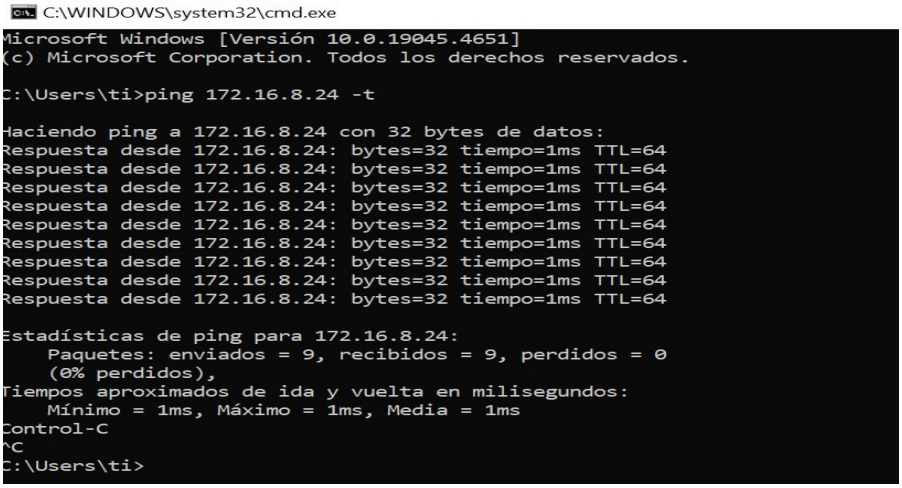
SWITCH AUDITORIO PISO 5



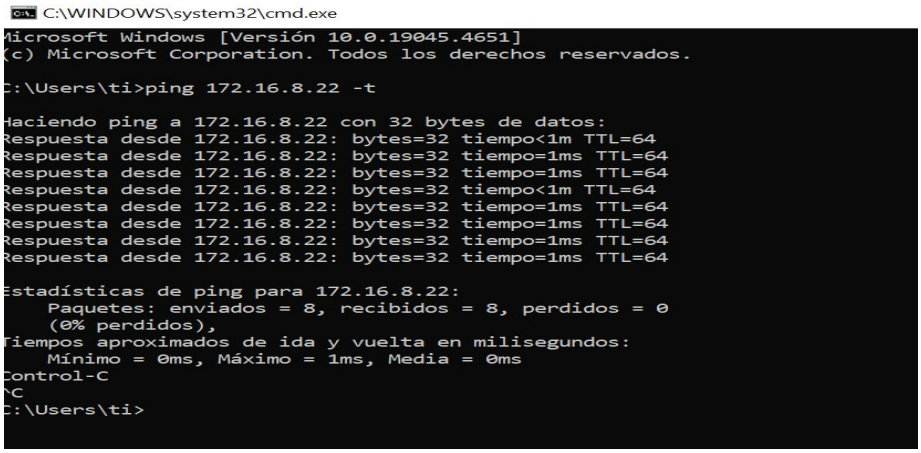
SWITCH TALENTO HUMANO PISO 5



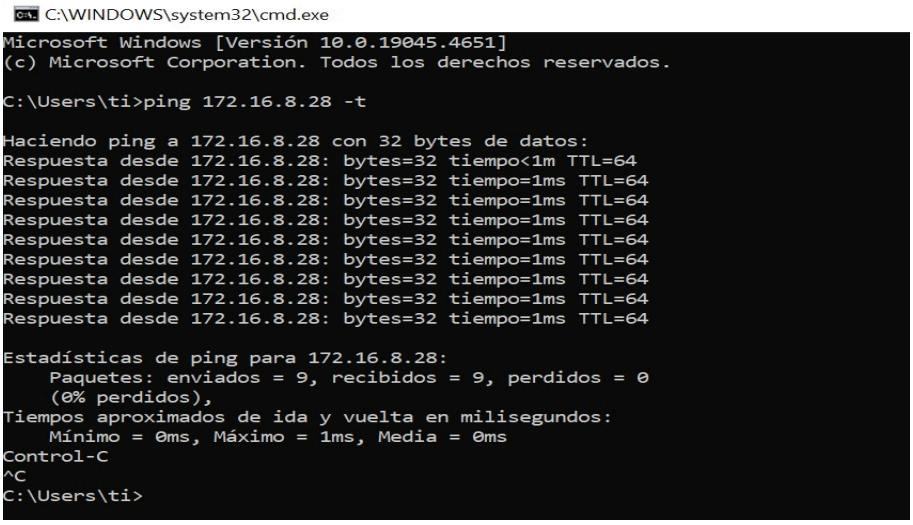
SWITCH SALA SISTEMAS 1



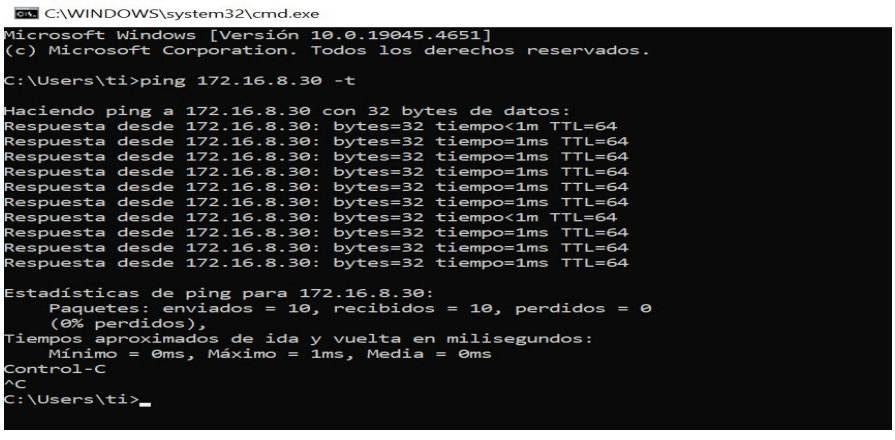
SWITCH SALA SISTEMAS 2



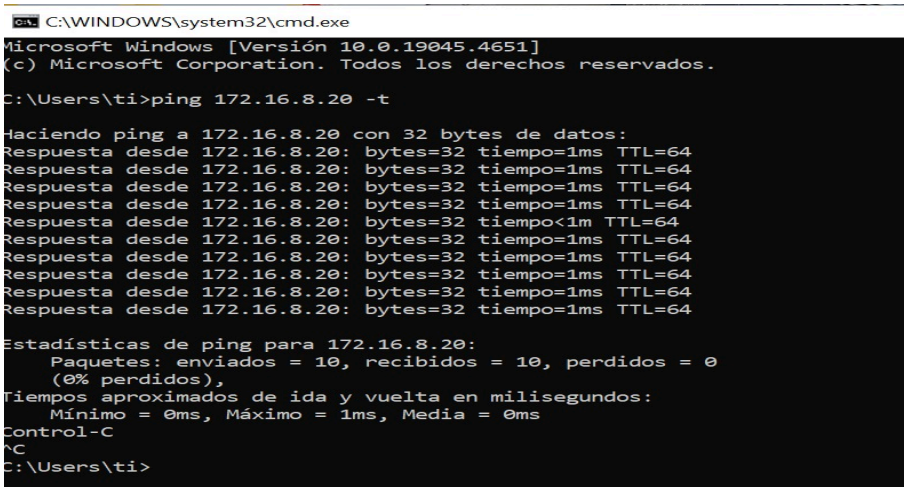
SWITCH SALA SISTEMAS 3



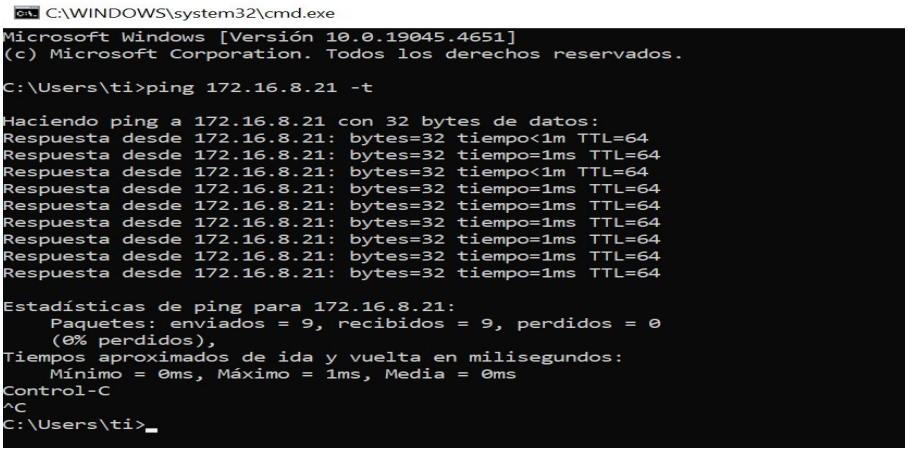
SWITCH SALA SISTEMAS 4



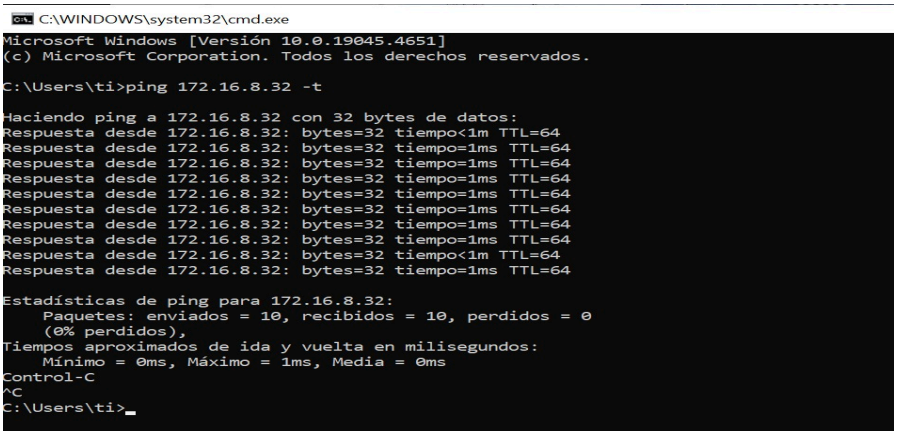
SWITCH SALA SISTEMAS 5



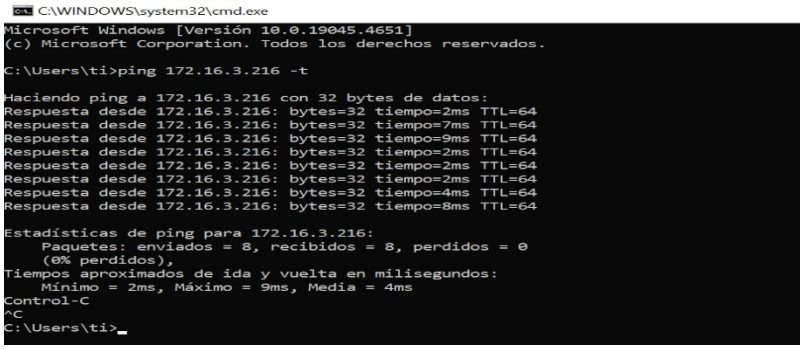
SWITCH SALA SISTEMAS 6



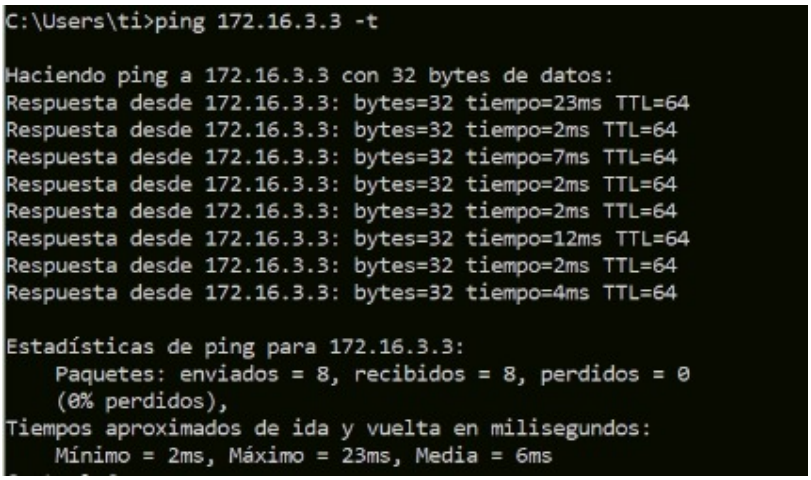
SWITCH SALA SISTEMAS 7



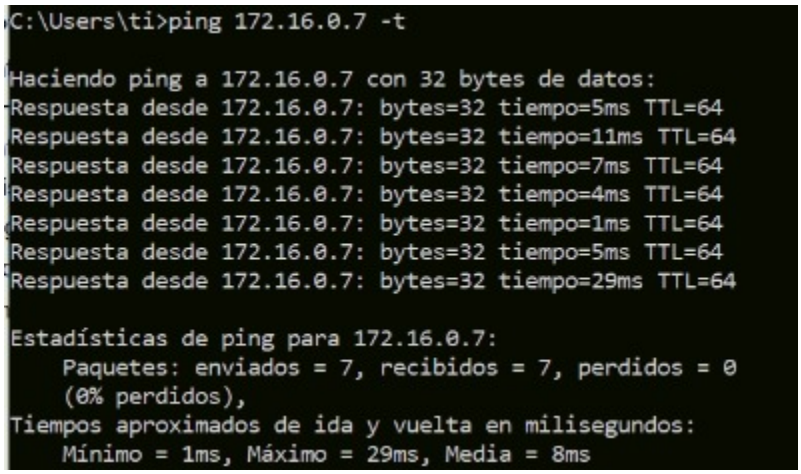
PRUEBA LATENCIA CÁMARA IP



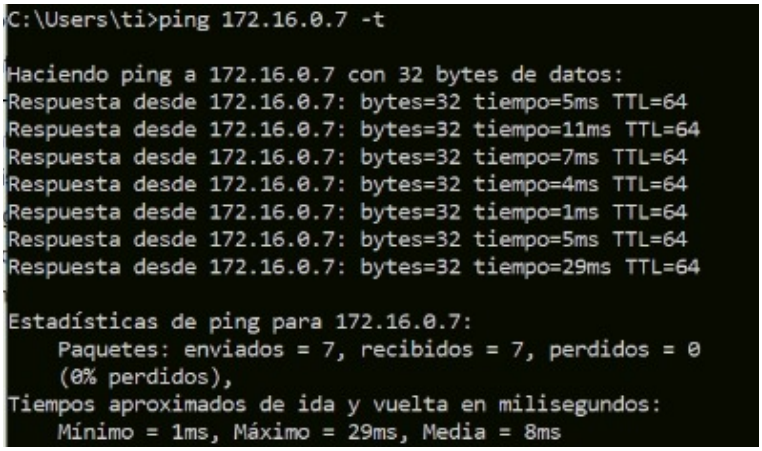
DINSTAR



SERVIDOR ARCHIVO



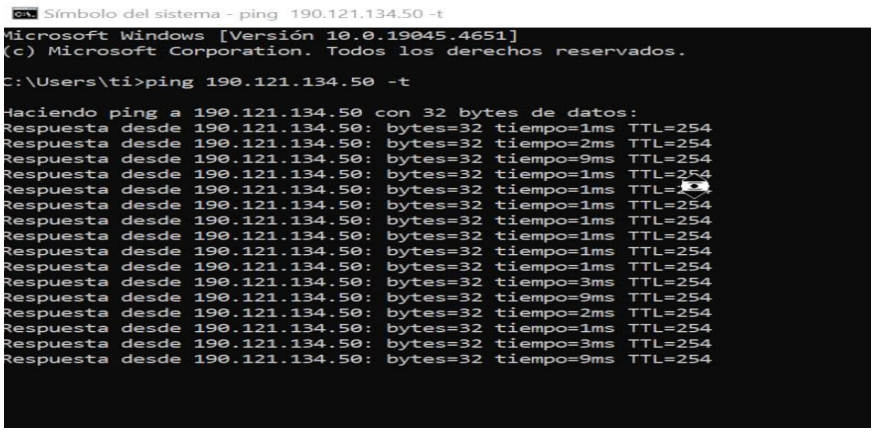
ELAXTIX SERVIDOR TELEFONIA

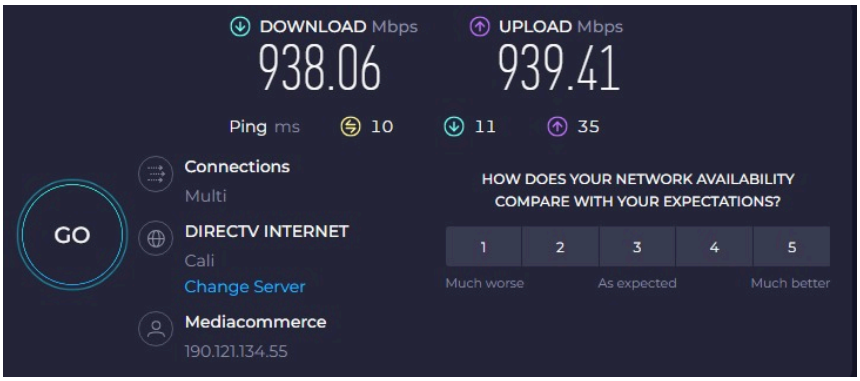


Se realizaron pruebas de carga, descarga y latencia en cada uno de los Gateway de los proveedores (Claro, Emcali y Mediacommerce) en donde se obtuvieron los siguientes resultados:

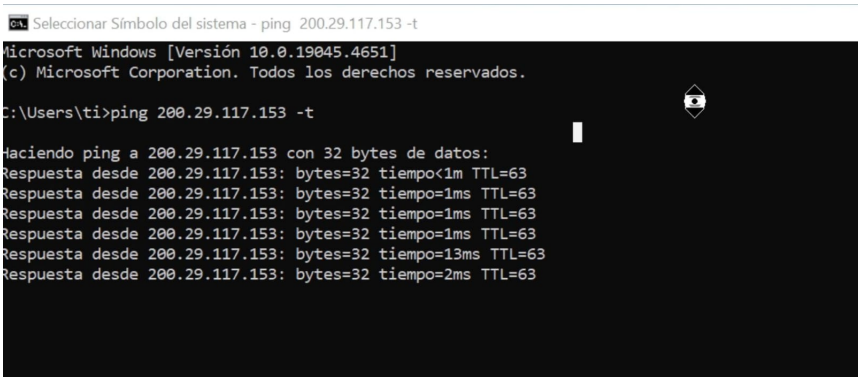
CONEXIÓN A INTERNET			
ROUTER	PROVEDOORES	TIPO	MEGAS
1	EMCALI	DEDICADO	1000
2	MEDIA COMERC	DEDICADO	1000
3	CLARO	BANDA ANCHA	300

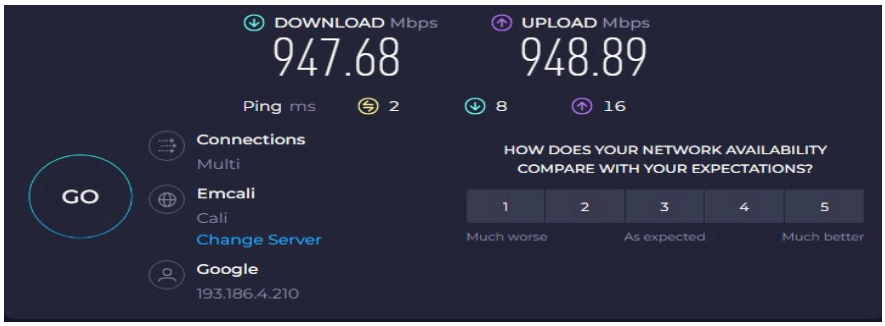
GATEWAY MEDIACOMMERCE



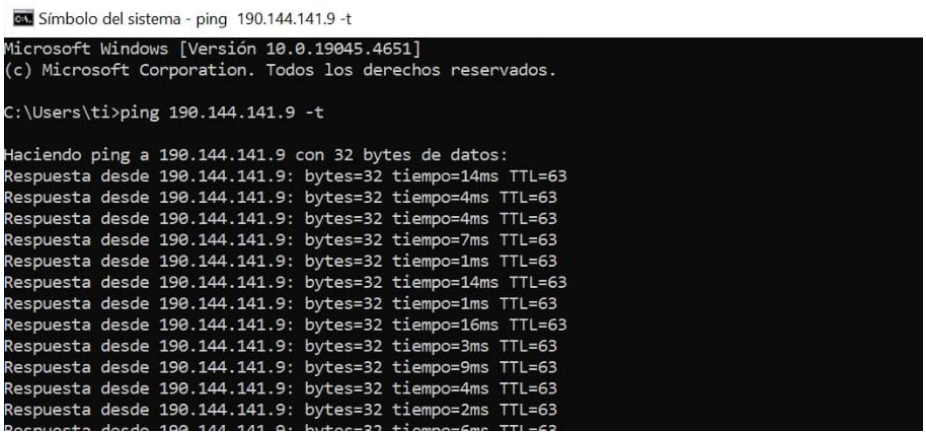


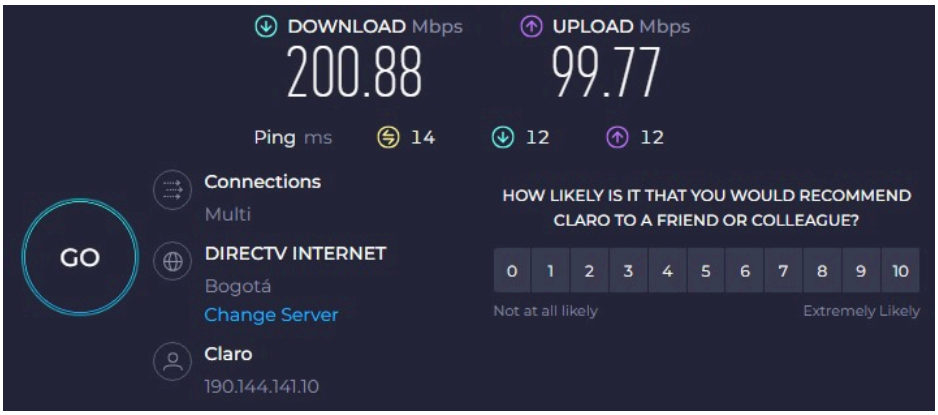
GATEWAY EMCALI





GATEWAY CLARO





Se puede concluir que el estado latencia es óptimo ya que es menor a 50 milisegundos con un estándar de 10 milisegundos.

4. ESCANEO DE PUERTOS

Se realizo el escaneo de puertos con el software IP PORT SCCANER donde se evidencio lo siguiente:

SEGMENTOS 172.16.0.1/172.16.3.254

NOMBRE	IP	PUERTOS	DETALLE	OBSERVACION
SOPHOS	172.16.0.1	22	Servicio Secure Shell	
		25	Simple Mail Transfer Protocol	
		53	Resolución de nombres por DNS	
SERVIDORARCHIVO	172.16.0.4	23	Servicio Telnet	
		80	Protocolo de Transferencia de HiperTexto	
		135	epmap	
		139	NETBIOS Servicio de sesiones	
		445	SMB a través de TCP/IP	
*.servicios.intenalco.edu.co	172.16.0.6	53	Resolución de nombres por DNS	
		80	Protocolo de Transferencia de HiperTexto	
		443	HTTPS	
SERVIDOR DE TELEFONIA	172.16.0.7	22	Servicio Secure Shell	
		25	Simple Mail Transfer Protocol	
		80	Protocolo de Transferencia de HiperTexto	
		110	Post Office Protocol v3 para	
		143	Internet Message Access Protocol	
		443	HTTPS	
		993	IMAP a través de SSL/TLS	
		995	POP3 a través de SSL/TLS	
SRVDOMINIO.intenalco.local		53	Resolución de nombres por DNS	

	172.16.0.10	80	Protocolo de Transferencia de HiperTexto	
		88	Sistema de autenticación de red	
		135	epmap	
		139	NETBIOS Servicio de sesiones	
		389	Lightweight Directory Access Protocol	
		443	HTTPS	
		445	SMB a través de TCP/IP	
		464	Modificación de contraseña para Kerberos	
		593	Mapa de Ep RPC HTTP	
		636	LDAP a través de SSL/TLS	
Apache HTTP Server Test Page powered by CentOS	172.16.0.13	21	Conexión FTP	
		22	Servicio Secure Shell	
		25	Simple Mail Transfer Protocol	
		53	Resolución de nombres por DNS	
		80	Protocolo de Transferencia de HiperTexto	
		110	Post Office Protocol v3 para	
		143	Internet Message Access Protocol	
		443	HTTPS	
		465	Autenticado SMTP sobre TLS/SSL	
		587	Message Submission Agent	
		993	IMAP a través de SSL/TLS	
		995	POP3 a través de SSL/TLS	
Equipo sin identificar	172.16.0.15	21	Conexión FTP	
		25	Simple Mail Transfer Protocol	
		53	Resolución de nombres por DNS	
		110	Post Office Protocol v3 para	
		143	Internet Message Access Protocol	
		465	Autenticado SMTP sobre TLS/SSL	
		587	Message Submission Agent	
		993	IMAP a través de SSL/TLS	
		995	POP3 a través de SSL/TLS	
NPI16BB44	172.16.3.117	21	Conexión FTP	
		23	Servicio Telnet	
		80	Protocolo de Transferencia de HiperTexto	
		443	HTTPS	
		515	Servicios de impresión Line Printer Daemon	

		631	Internet Printing Protocol	

SEGMENTOS 172.16.8.0/254

NOMBRE	IP	PUERTOS	DETALLE	OBSERVACION
Sophos Ltd	172.16.8.1	22	Servicio Secure Shell	
		25	Simple Mail Transfer Protocol	
		53	Resolución de nombres por DNS	
Cisco Systems, Inc	172.16.8.20	80	Protocolo de Transferencia de HiperTexto	
Cisco Systems, Inc	172.16.8.21	80	Protocolo de Transferencia de HiperTexto	
Cisco Systems, Inc	172.16.8.22	80	Protocolo de Transferencia de HiperTexto	
Cisco Systems, Inc	172.16.8.24	80	Protocolo de Transferencia de HiperTexto	
Cisco Systems, Inc	172.16.8.28	80	Protocolo de Transferencia de HiperTexto	
Cisco Systems, Inc	172.16.8.30	80	Protocolo de Transferencia de HiperTexto	
Cisco Systems, Inc	172.16.8.32	80	Protocolo de Transferencia de HiperTexto	
DESKTOP-SCO1OVR	172.16.8.193			
DESKTOP-PCRI1T7	172.16.8.199			

SEGMENTOS 172.16.16.0/254

NOMBRE	IP	PUERTOS	DETALLE	OBSERVACION
Sophos Ltd	172.16.16.1	22	Servicio Secure Shell	
		25	Simple Mail Transfer Protocol	
		53	Resolución de nombres por DNS	

SEGMENTOS 172.16.20.0/254

NOMBRE	IP	PUERTOS	DETALLE	OBSERVACION
Sophos Ltd	172.16.16.1	22	Servicio Secure Shell	
		25	Simple Mail Transfer Protocol	
		53	Resolución de nombres por DNS	
BIBLIOTECA9	172.16.20.12	135	epmap	
		139	NETBIOS Servicio de sesiones	
		445	SMB a través de TCP/IP	
BIBLIOTECA	172.16.20.14	80	Protocolo de Transferencia de HiperTexto	
		135	epmap	
		139	NETBIOS Servicio de sesiones	
		445	SMB a través de TCP/IP	
NPI153A8D	172.16.20.15	21	Conexión FTP	
		23	Servicio Telnet	
		80	Protocolo de Transferencia de HiperTexto	
		443	HTTPS	
		515	Servicios de impresión Line Printer Daemon	
		631	Internet Printing Protocol	

5. Análisis de topología

Intenalco cuenta con una topología de red que cumple con los estándares internacionales de red: TIA-568A y TIA-568B.

De acuerdo a esta norma el cableado de la red de datos de Intenalco es categoría 6 el cual es un cable trenzado de cuatro pares que permite velocidades de hasta mil megabytes por segundo y permite un rango de frecuencia de transmisión de 250 MHz de voz, video y datos.

La topología instalada de red es jerárquica de estrella lo que significa que parte de un centro principal de cableado y se divide en subcentros de cableado por piso, en algunos casos especiales algunos pisos se encuentran dos o tres subcentros de cableado, como es el caso del piso 1,4 y 5. Cuenta con cableado horizontal, el cableado va desde los subcentros de cableado o los centros de datos que se encuentran debidamente identificados.

Cableado vertical este cableado va desde centro principal de cableado a los subcentros de cableado que se define como Backbone este cableado es de categoría 6, con excepción Backbone piso 1 y extensión que es de categoría 6A

Se realizo el mapeo de los puntos y se evidencio que, en muchos puntos al realizar obra civil y de pintura, no se encontraban con la marcación debida, a lo cual se realizó la marcación correspondiente. Este procedimiento no hacía parte de este contrato. Para que así la administración de la red sea más dinámica y se tengan identificado claramente cuando se tenga una falla.

Observación

Una vez realizado el mapeo de los puntos de red se observó que 16 puntos de 664 lo cual equivalente al 2,4% de la totalidad de los puntos tenían debido a que por obras civiles y de pintura se han visto averiados.







A continuación, se detalla en un Excel (puntos de datos) el mapeo de cada punto y ubicación respectiva para su fácil administración donde se define claramente la interconexión de equipos a la red de datos dejando claramente documentado este punto. El cual será anexado junto a este documento.



PUNTOS INTENALCO
final.xlsx

6. Políticas de seguridad:

Al configurar las políticas de seguridad del firewall Sophos, se aplicaron las siguientes medidas:

1. Filtrado de tráfico: Permite bloquear aplicaciones, puertos y direcciones IP. Sophos, con su experiencia, ya cuenta con las posibles vulnerabilidades de tráfico predeterminadas para garantizar mayor seguridad en la red. Algunas de las categorías bloqueadas incluyen:

- Protocolos de red no seguros
- Aplicaciones de mensajería instantánea
- Redes sociales y sitios de entretenimiento
- Contenido malicioso
- Aplicaciones de VoIP no autorizadas
- Acceso a puertos no utilizados

2. Prevención de intrusiones: Utiliza sistemas de detección y prevención de intrusiones (IDS/IPS) mediante:

- Monitoreo en tiempo real
- Detección basada en firmas
- Análisis basado en comportamiento
- Reglas personalizables
- Informes y registro
- Filtrado web
- Integración con otras soluciones de seguridad

3. Control de aplicaciones: Permite gestionar y restringir el uso de aplicaciones específicas en la red, mejorando la seguridad y el rendimiento.

4. VPN y acceso remoto: Proporciona políticas para conexiones seguras a través de redes privadas virtuales, asegurando que solo los usuarios autorizados puedan acceder a la red. Se configuraron ocho VPN para el acceso remoto seguro:

- intenalco
- intenalco01
- intenalco02
- intenalco03
- intenalco05
- pymes.online
- soporte

5. Filtrado web: Controla el acceso a sitios web y contenido en línea, bloqueando aquellos que son considerados peligrosos o inapropiados. Los tipos de filtrado incluyen:

- Contenido
- URL
- Protocolo
- Tráfico en tiempo real
- Aplicaciones
- Usuarios
- Horas
- Informes y análisis

6. Protección contra malware: Integra funciones de detección y bloqueo de malware para proteger la red de amenazas. Los métodos de protección incluyen:

- Detección de firmas
- Análisis de comportamiento
- Análisis de tráfico en tiempo real
- Protección contra ransomware
- Exploits
- Botnets
- Rootkits
- Spyware
- Adware
- Sandbox

7. Registro y monitoreo: Permite registrar y monitorear el tráfico de la red para detectar comportamientos sospechosos y realizar auditorías de seguridad. Se observó que las aplicaciones con mayor consumo son:

- Facebook
- TikTok
- Facebook games
- Descarga de software sospechoso
- Bits
- Plataformas de streaming
- Aplicaciones móviles

Es necesario verificar si este consumo está relacionado con actividades diarias o trabajos de clase. De no ser así, se debe restringir para garantizar el buen funcionamiento de la red. Se recomienda realizar un monitoreo constante de las páginas en Sophos para identificar riesgos, lo cual debe hacerse diariamente.

8. Seguimiento a dispositivos conectados: Realizar un seguimiento a los dispositivos conectados por DHCP a la red administrativa, tanto PC como móviles, asegurándose de que pertenezcan a funcionarios y no a terceros que hayan compartido la contraseña. Esto ayuda a identificar posibles intrusos conectados por este medio.

Todo esto se verificó con el firewall Sophos y quedó configurado para mantener una red segura. Es crucial realizar un seguimiento diario, ya que cada día surgen nuevas amenazas y algoritmos de hackeo. Se deben generar nuevas

reglas personalizadas en el firewall cuando se detecten estos riesgos. Las conexiones deben realizarse a través de VPN seguras y no mediante software de acceso remoto para evitar posibles vulnerabilidades.

7. Análisis de protocolos

El protocolo utilizado en la red de datos de Intenalco es TCP/IP IPV4 el cual se encuentra sementado en las siguientes redes:

CONFIGURACION REDES CONEXIÓN						
RED	DHCP	DIRECCION DE RED	MASCARA	PUERTA ENLACE	DNS	DNS
ADMINISTRATIVA:	**172.16.2.25/150**	172.16.0.1/22	255.255.252.0	172.16.0.1	200.110.169.20	200.110.169.27
VLAN 400 SALAS	**172.16.8.20/250**	172.16.8.1/24	255.255.255.0	172.16.8.1	200.29.96.24	200.29.104.24
VLAN 100 BIBLIOTECA	**172.16.20.10/250**	172.16.20.1/24	255.255.255.0	172.16.20.1	200.29.96.24	200.29.104.24
VLAN 200 RED WIFI ESTUDIANTES	**172.16.16.10/172.16.17.10**	172.16.16.1/22	255.255.252.0	172.16.16.1	200.29.96.24	200.29.104.24

En la actualidad se presentan problemas de conexión debido a que muchas veces se les asignan a los equipos de direcciones que pertenecen al rango que se encuentran en DHCP y entran en conflicto. Por lo tanto, es importante tratar que los equipos que pertenecen a la institución cuenten con IP fijas para evitar estos conflictos que se presentan máxime utilicen direcciones de IP que sean de switch, servidores los cuales generan problemas debido a duplicidad de IP

La red no presenta cuellos de botella y problemas de direccionamiento IP, pero es importante que equipos de trabajo como switch, router, equipos de trabajo tengan sus direcciones IP bien definidas y no sean reutilizadas en otros equipos para así tener un buen funcionamiento de los mismos.

No se evidencian problemas de rendimiento en la red local en cuanto a la conectividad, pero sí se observa que el canal de internet cuenta con dos conexiones dedicadas de 1000 Mbps cada una, proporcionadas por los proveedores Emcali y Mediacomerce. Ambas conexiones ofrecen un máximo de entre 900 y 930 Mbps, sumando un total de 1860 Mbps de canal dedicado. Adicionalmente, Claro proporciona una conexión de banda ancha con 300 Mbps de descarga y 150 Mbps de subida.

Teniendo en cuenta que un servicio de internet óptimo hoy en día necesita entre 2 y 3 Mbps para asegurar una conexión adecuada para videoconferencias, correos, redes sociales, trabajos de edición, entre otros, y que los funcionarios administrativos utilizan hasta 5 Mbps debido a sus diversas tareas, la institución ha decidido que el canal de Mediacomerce se destine a la red administrativa. Esta red conecta a los administrativos desde sus estaciones de trabajo (computadoras, tabletas, celulares, entre otros) y también incluye los servidores internos, cámaras de videovigilancia, telefonía IP, sistemas de control de acceso, entre otros. Este canal cuenta con 930 Mbps con una relación de reutilización de 1:1, lo que garantiza una conexión dedicada y eficiente.

Para garantizar la óptima productividad, se estima que cada usuario requiere entre 3 y 5 Mbps, dependiendo de las actividades que realicen. Promediando el ancho de banda, el número de usuarios o equipos que podrían acceder sería entre:

- 930 Mbps / 3 Mbps = 310 usuarios.

En el caso de que solo los usuarios estuvieran conectados a internet, pero considerando que diferentes aplicaciones, software y servidores también requieren conexión, se distribuye el ancho de banda en un 60% para los usuarios y un 40% para los equipos que lo necesiten. Esto resultaría en:

- 60% de 930 Mbps = 558 Mbps para usuarios.
- 558 Mbps / 3 Mbps = 186 usuarios conectados.

La red administrativa cuenta con conexiones cableadas a los puntos de datos y conexión a la red vía Wifi. El Wifi administrativo puede asignar hasta 100 direcciones IP. Hay 75 puestos de trabajo conectados por cable y aproximadamente 30 portátiles conectados por Wifi para los docentes. Esta distribución es suficiente para el uso administrativo, siempre y cuando cada usuario se conecte con un solo dispositivo.

Sin embargo, se ha evidenciado que los funcionarios no solo utilizan sus puestos de trabajo, sino también sus dispositivos móviles, lo que podría sobrepasar la capacidad instalada de la red administrativa. Por lo tanto, es necesario controlar la cantidad de dispositivos conectados por cada funcionario para evitar sobrecargar la red. Por ejemplo, si cada funcionario utiliza su puesto de trabajo y además conecta su celular, se sobrepasaría la capacidad instalada.

Recomendación

- Controlar la conexión de dispositivos a la red administrativa de los funcionarios que solo se utilicen los dispositivos que tienen o que hacen parte de la producción diaria de los funcionarios por ejemplo controlar la conexión de celulares, tabletas, portátiles cuando el funcionario cuenta ya con una conexión asignada esto se puede analizar con un sistema de validación de equipos de plataforma o Hotspot.
- Analizar el consumo que requiere el personal de audio visuales, diseño y redes sociales

El canal de Emcali cuenta con 930 Mbps con una relación de reutilización 1:1, permitiendo una conexión dedicada. La distribución del ancho de banda se realiza de la siguiente manera:

- Biblioteca: 60 Mbps, lo que permite 20 equipos (60 Mbps / 3 Mbps por equipo). Actualmente, la biblioteca cuenta con 18 equipos.
- Red de salas: 465 Mbps, lo que permite 155 conexiones (465 Mbps / 3 Mbps por equipo).
- Wifi para estudiantes: 405 Mbps, lo que permite 203 conexiones (405 Mbps / 2 Mbps por conexión), ya que los estudiantes solo realizan consultas por internet.

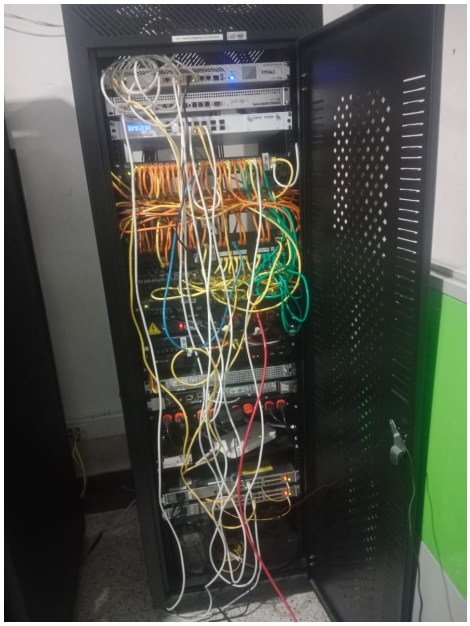
El canal de Claro, de 300 Mbps, se utiliza como respaldo en caso de caída de cualquiera de los canales de internet y mantiene activa la red de estudiantes, permitiendo aproximadamente 150 conexiones adicionales por Wifi (300 Mbps / 2 Mbps por conexión).

La configuración de los proveedores de internet está balanceada de tal manera que, si un proveedor falla, el otro lo reemplaza. Aunque esto disminuye la utilidad del recurso, permite el funcionamiento continuo.

8. Recomendaciones

1. reparar 16 puntos de datos que presentan fallas porque han dañado los Jack categoría 6 en los puestos de trabajo estos deben remplazarse y Re poncharse, con sus respectivas pruebas de conectividad

2. Los Backbone existentes actualmente en cable categoría 6 se cambien por fibra óptica multimodo de seis hilos para tener un Backup en caso de falla y aumentar la velocidad de transmisión entre equipos activos y el ancho de banda que en la actualidad es de 250mhz a máximo 2 TB o 2ghz
3. El Switch cisco instalados en los subcentros de cableado y Switch hp cuentan con puertos SFT de fibra óptica, al momento de adquirir las tarjetas SGP para los switches existentes
4. El firewall Sophos que existe actualmente junto con su licenciamiento presentan desactualización tecnológica y el fabricante solo lo tendrá activo hasta el año 2025 por esta razón se debe cambiar este equipo en el año 2025 y adquirir nuevas licencias
5. En el centro principal de cableado debe de reorganizarse puesto que en la actualidad para realizar conexiones se han utilizado de 3 metros



6. Las antenas Unifi LR también presentan desactualización tecnológica por eso a futuro estas deben ser actualizadas para tener una mejor conexión wifi.
7. El personal de sistemas debe contar con equipo de mapeo de puntos y la herramienta requerida para brinda soporte en caso de falla.
8. Recomendación aumento en el canal de la red de estudiantes que permita la conexión de por lo menos la conexión del 50% de los estudiantes por vía wifi es decir 900mg más en canal dedicado. En la conexión por wifi de estudiantes es importante controlar la conexión de un dispositivo por estudiante ya que así evitamos minimizar la velocidad de conexión del recurso.
9. Basado en este estudio, realizar el estudio para pasar de IPV4 a IPV6
10. Bloqueo del acceso de la red internet de Intenalco por software como Anydesk, TeamViewer, entre otros
11. Realizar monitoreo constante del uso de aplicaciones estableciendo políticas y condiciones para su uso en (redes sociales, plataformas, etc.)
12. Verificar el ancho de banda entregado por el proveedor, certificando que este sea mínimo 930mgb
13. Crear un rango de IPS para los nuevos equipos, y manteniendo actualizado el cuadro de equipos conectados.
14. Establecer rango de direccionamiento de IP de acuerdo a la cantidad de equipos que se desean conectar de acuerdo al recurso de red y no extralimitar el uso ya que causan cuellos de botella
15. Configurar conexiones seguras a través de VPN por externos a la red INTENALCO

16. Se recomienda realizar interconexión en centro de cableado con patch cord de fibra óptica y tarjetas SFTP.
17. Actualizar el software de sistema operativo de los servidores exitentes
18. Actualizar firewall de los equipos activos existentes
19. En la red administrativa todos los equipos deben estar debidamente identificados, sobre todo los que acceden por wifi.
20. Es importante recalcar que el dispositivo se debe monitorear constantemente y actualizar a nuevas politicas personalizadas si es necesario debido a que dia dia hay nuevas vulnerabilidades

9. Capacitación del personal

Se realizo la capacitación al personal del TI de INTENALCO: Ing. Lucero Chamorro, Ing. Edilberto Ruiz García y Jorge Luis Dorado, en lo referente a la administración, configuración, operación e informes del firewall Sophos XS310Z10ZZRCCA. Donde se revisaron todas las opciones con las que cuenta el equipo del presente el contrato.

La capacitación fue realizada por el ingeniero Yefri Marchena, certificado y representante de la casa matriz de Sophos. La sesión tuvo una duración de tres horas y media, durante las cuales se abordaron diversos temas y se resolvieron las dudas e inquietudes planteadas por los participantes.

Durante la capacitación, se abordaron los siguientes temas clave:

1. **Informes de consumo de aplicaciones:** Cómo monitorear y analizar el uso de aplicaciones para optimizar el rendimiento y la gestión de recursos.
   Informes de ataques: Identificación y análisis de intentos de intrusión y actividades maliciosas para fortalecer la seguridad de la red.
2. **Políticas de acceso a aplicaciones web:** Implementación de controles para gestionar quién puede acceder a aplicaciones web y cómo se puede acceder a ellas.
3. **Bloqueo de puertos:** Técnicas y razones para cerrar puertos específicos en la red para prevenir accesos no autorizados y mejorar la seguridad.
4. **Creación de reglas y políticas de bloqueo**: esta opción permite crear en el firewall las reglas para permite el acceso o bloque de los diferentes tipos de paginas
5. **Enrutamiento de redes LAN con redes WAN:** menú que permite de las locales o LAN a las redes WAN o de acceso a internet.
6. **Configuración de conexiones seguras a través de VPN**. Esta opción permite las conexiones utilizando VPN para conexiones de acuerdo a los niveles de seguridad y generar conexiones seguras
7. **Configuración de calidad de servicio QoS:** Permite la configuración de las redes para garantizar la calidad del servicio.
8. **Asignación de IP estática por Host MAC**: Administración y manejo de direcciones IP por la direccion MAC de las tarjetas de red: Esta opción permite asignar de acuerdo a la mal de la tarjeta de red una dirección IP es decir que cada la MAC se detectada por firewall se le asigna la misma direccion IP automáticamente. Asignación de direcciones IP estáticas basadas en la dirección MAC de los dispositivos para una gestión de red más estable y predecible.
9. **Copia de seguridad y firmware:** Creación, restauración y configuración de copias de seguridad del firewall. Permite la actualización del firewall, realizar copias de seguridad y restauración de las mismas.

10. **Visor de registros:** Opción que permite hacer el monitoreo y seguimiento de las actividades que suceden en el firewall generando filtros para establecer cambios o modificaciones que permitan un correcto funcionamiento.
11. Preguntas y resolución de inquietudes por parte los participantes.
12. Grabación de la capacitación que se realiza entrega a los participantes de la capacitación

Se realizará programación con Sophos para capacitación de certificación de manera virtual el cual tendrá duración de cuatro días.

11. Análisis de disponibilidad y redundancia

En el caso de la redundancia a los canales de internet la institución cuenta con el canal de Mediacomerce se destine a la red administrativa. Esta red conecta a los administrativos desde sus estaciones de trabajo (computadoras, tabletas, celulares, entre otros) y también incluye los servidores internos, cámaras de videovigilancia, telefonía IP, sistemas de control de acceso, entre otros. Este canal cuenta con 930 Mbps con una relación de reutilización de 1:1, lo que garantiza una conexión dedicada y eficiente.

Para garantizar la óptima productividad, se estima que cada usuario requiere entre 3 y 5 Mbps, dependiendo de las actividades que realicen. Promediando el ancho de banda, el número de usuarios o equipos que podrían acceder sería entre:

- 930 Mbps / 3 Mbps = 310 usuarios.

En el caso de que solo los usuarios estuvieran conectados a internet, pero considerando que diferentes aplicaciones, software y servidores también requieren conexión, se distribuye el ancho de banda en un 60% para los usuarios y un 40% para los equipos que lo necesiten. Esto resultaría en:

- 60% de 930 Mbps = 558 Mbps para usuarios.
- 558 Mbps / 3 Mbps = 186 usuarios conectados.

El canal de Emcali cuenta con 930 Mbps con una relación de reutilización 1:1, permitiendo una conexión dedicada. La distribución del ancho de banda se realiza de la siguiente manera:

- Biblioteca: 60 Mbps, lo que permite 20 equipos (60 Mbps / 3 Mbps por equipo). Actualmente, la biblioteca cuenta con 18 equipos.
- Red de salas: 465 Mbps, lo que permite 155 conexiones (465 Mbps / 3 Mbps por equipo).
- Wifi para estudiantes: 405 Mbps, lo que permite 203 conexiones (405 Mbps / 2 Mbps por conexión), ya que los estudiantes solo realizan consultas por internet.

El canal de Claro, de 300 Mbps, se utiliza como respaldo en caso de caída de cualquiera de los canales de internet y mantiene activa la red de estudiantes, permitiendo aproximadamente 150 conexiones adicionales por Wifi (300 Mbps / 2 Mbps por conexión).

La configuración de los proveedores de internet está balanceada de tal manera que, si un proveedor falla, el otro lo reemplaza. Para garantizar la continuidad del servicio. En caso de presentarse falla con cualquiera de los tres proveedores priorizando el que tiene mayor consumo de ancho de banda.

12.Optimizacion de la configuracion de red.

Se realizo la verificacion de los dispositivos de red 1:1 inciando por el firewall sophos, switch, servidores, antenas.

Ubicación	Centros de cableado	Switch	Routers	APP	Servidores
Piso 1	3	7	0	5	1
Piso 2	1	1	0	3	0
Piso 3	1	1	0	3	0
Piso 4	9	11	3	5	5
Piso 5	2	5	0	4	0
TOTAL	16	25	3	20	6

Se evidenció que los dispositivos se encontraban con sus firewalls desactualizados, los cuales fueron actualizados a la última versión del fabricante. También se realizó una revisión de la configuración de cada uno de los puertos de los equipos y de las VLAN que debían pasar por ellos, configurándolos de forma correcta.

Asimismo, se evidenció que las antenas Unifi LR, modelo con el que cuenta actualmente la institución, presentan desactualización tecnológica, ya que el fabricante no realiza actualizaciones de software y ya no se encuentran en el mercado. Por lo tanto, estas antenas deben ser reemplazadas.

Además, se identificó que las licencias de Sophos incluidas en el contrato estaban vencidas. Este procedimiento se realizó, quedando actualizadas y configurando el dispositivo para habilitar todos sus servicios. Se informó que el firewall con el que cuenta actualmente la institución saldrá del mercado en el año 2025 por desactualización tecnológica, debido a que el fabricante no volverá a producir licencias para este equipo. Por tal razón, el equipo físico debe ser reemplazado.

13. Analisis de calidad QoS

El firewall sophos no contaba con la configuracion de calidad QS este fue configurado de la siguiente manera para la red administrativa se creo la politica QS donde se establecio el ancho de banda seria sin limite a traves del proveedor Mediacommerce

La red de salas se establecio un ancho de banda de 400mgb para 155 equipos exitentes con un promedio de 3kb por usuario garantizando internet para todos los equipos de sala a traves del proveedor Emcali

La red de biblioteca se establecio un ancho de banda de 60 mgb con promedio 3mgb por equipo para 18 equipos existentes a traves del proveedor Emcali

La red wifi estudiantes se establecio un ancho de banda de 470 mgb con promedio 3kilobytes por usuario garantizando internet para todos los equipos de sala a traves del proveedor Emcali. De un total de 335 usuarios con un promedio de 2mg por usuario

14. Auditoría de cumplimiento normativo

Intenalco cuenta con una topología de red que cumple con los estándares internacionales de red: TIA-568A y TIA-568B.

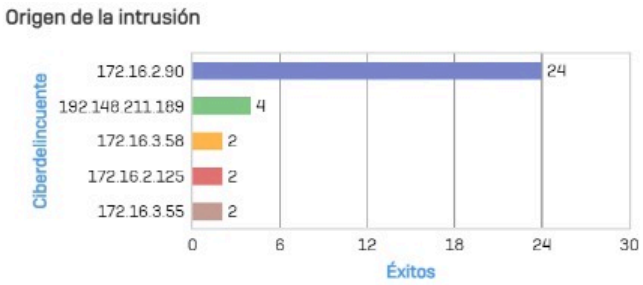
De acuerdo a esta norma el cableado de la red de datos de Intenalco es categoría 6 el cual es un cable trenzado de cuatro pares que permite velocidades de hasta mil megabytes por segundo y permite un rango de frecuencia de transmisión de 250 MHz de voz, video y datos.

La topología instalada de red es jerárquica de estrella lo que significa que parte de un centro principal de cableado y se divide en subcentros de cableado por piso, en algunos casos especiales algunos pisos se encuentran dos o tres subcentros de cableado, como es el caso del piso 1,4 y 5. Cuenta con cableado horizontal, el cableado va desde los subcentros de cableado o los centros de datos que se encuentran debidamente identificados.

Cableado vertical este cableado va desde centro principal de cableado a los subcentros de cableado que se define como Backbone este cableado es de categoría 6, con excepción Backbone piso 1 y extensión que es de categoría 6A

15. Revision firewall

Se realizo la revision del firewall para verificar posibles ataques en la infraestructura de intenalco en el año 2024 es de 38 ataques es un porcentaje muy bajo teniendo en cuenta que una red que tiene acceso a estudiantes o ataques externos como minimo recibe 150 intentos diarios. Se evidencia que los ataques se han hecho desde paginas ubicadas 5 de españa, 2 de estados unidos y el resto no identificados porque se encuentran reservados.. Es importante realizar la verificacion de este tipo de intrucciones en firewall el cual se encuentra configurado para repelerlas a traves de la herramienta wedserverprotection de sophos el cual cancela el posible ataque evitando la penetracion a la red.



Ciberdelincuente	Exitos
172.16.2.90	24
192.148.211.189	4
172.16.3.58	2
172.16.2.125	2
172.16.3.55	2



Víctima	Exitos
172.16.8.13	5
172.16.8.12	4
172.16.20.10	4
172.16.8.16	4
172.16.8.32	3

16. Monitoreo red de datos

Para el monitoreo de la red de datos. La institucion solo cuenta con la opcion de informe firewall sophos el cual permite el monitoreo de aplicaciones, amenazas, trafico de la red y accesos a la misma, en la opcion informes y bloqueos, que genera informacion confiable y eficiente para la toma de medicion de datos adicionalmente para el monitoreo de la red datos intenalco no cuenta con sotfware licenciados para hacerlo por tal razon se intalacion de los siguientes sotfware en el servidor principal

- IP SCANNER ADVANCE: realiza un monitoreo de los equipos conectados en las redes que se testeen,
- IP PORT SCANNER: Permite el escaneo de una red especifica de los puertos. Para buscar vulnerabilidades o puertos abiertos en los diferentes dispositivos que se encuentran en la red.
- WIRESHARK: es una herramienta de análisis de protocolos de red que permite capturar y examinar datos que circulan en una red en tiempo real. Es muy útil para diagnosticar problemas de red, analizar el tráfico

y entender cómo se comunican los dispositivos. Con su interfaz gráfica, puedes ver detalles de cada paquete, filtrar información y realizar análisis profundos de la actividad de la red.

17. Evaluación de la arquitectura de red:

Realizar el estudio para la Implementación de IPv6 en la Red de Intenalco

La evaluación de la arquitectura se realiza en el punto 21 con las recomendaciones respectivas. Intenalco cuenta con un firewall Sophos, referencia: XS310Z10ZZRCAA y SS310Z10ZZRCCA, donde se encuentra configurada la protección de acceso a los datos de la institución de acuerdo con la licencia.

Se han establecido políticas de seguridad tanto para la red LAN como para la WAN, incluyendo políticas de acceso a la red local. También se ha restringido el acceso de software de acceso remoto como TeamViewer, AnyDesk, AnyViewer, entre otros. Las conexiones que se realizan por la red WAN se llevan a cabo a través de VPN para garantizar mayor seguridad. El firewall repele ataques de hackers, proporcionando un sistema de protección de la información robusto.

Es crucial realizar un monitoreo constante de posibles ataques desde otros países y posibles ataques en la red local. Se deben analizar los puertos abiertos y restringirlos para disminuir dichos ataques. La red está segmentada en una VLAN independiente para no permitir el acceso de estudiantes y visitantes a la red administrativa, así como a las salas de computo y usuarios de la biblioteca. La vulnerabilidad presente es en la red administrativa, ya que esta cuenta con acceso a los equipos activos de la infraestructura de Intenalco.

Dado que los usuarios se validan con una única contraseña que a menudo comparten, es importante que estas validaciones para la red administrativa por WiFi o DHCP se establezcan con usuarios restringidos y sus respectivas contraseñas. Este acceso debe ser asignado a usuarios específicos para identificar posibles vulnerabilidades. Por ejemplo, si a un funcionario administrativo se le asigna un portátil, se le entregará un usuario y una contraseña para la red WiFi, y se registrará la IP asignada al equipo para conocer al responsable del mismo. Si este funcionario comparte la contraseña del WiFi con otras personas, estas podrían acceder a la red administrativa y ejecutar programas para acceder a la información institucional, lo que representa una vulnerabilidad latente.

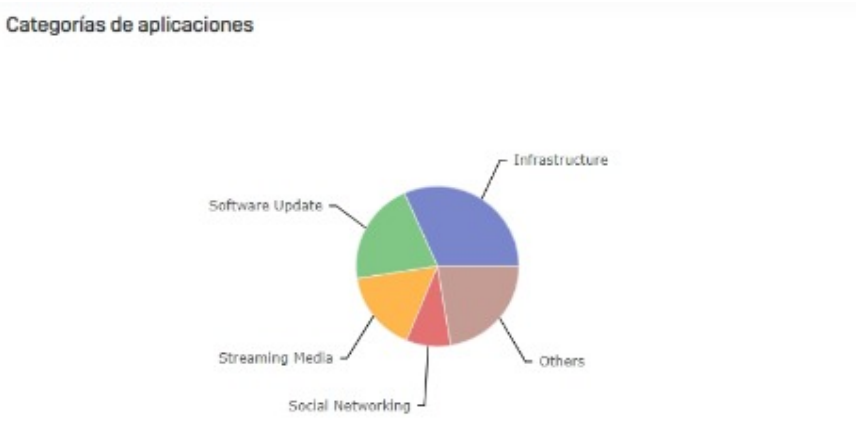
La solución para esto sería asignar direcciones IP por la MAC respectiva del equipo. Al realizar el escaneo de la red, se observa que tanto funcionarios administrativos como personas externas están conectados a la red por WiFi, lo que compromete la seguridad. Por lo tanto, es necesario que todo funcionario o equipo que se conecte a la red administrativa sea identificado, ya que es la red a la cual desean acceder personas externas.

18. Analisis de banda

De acuerdo a la revision realizada en firewall sophos y verificando el consumo de las aplicaciones mas utilizadas desde el 30 de junio a la fecha actual periodo de vacaciones se evidencia lo siguiente:

Aplicaciones	Descripción	Consumo
Actualizaciones de Windows	análisis de 30 junio a 31 de julio	96gb
Facebook	análisis de 30 junio a 31 de julio	57.8gb
YouTube	análisis de 30 junio a 31 de julio	49.1gb
Instagram	análisis de 30 junio a 31 de julio	32.2gb
WhatsApp	análisis de 30 junio a 31 de julio	31gb

Netflix	análisis de 30 junio a 31 de julio	15.7gb

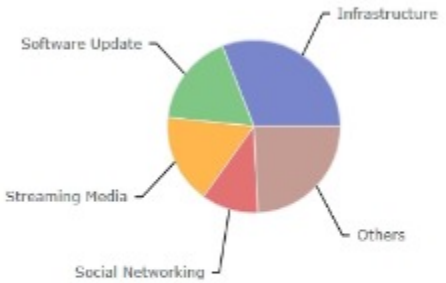


Categoría	Bytes	Porcentaje
Infrastructure	118.41 GB	31.69 %
Software Update	77.73 GB	20.8 %
Streaming Media	60.9 GB	16.3 %
Social Networking	33.02 GB	8.84 %
Others	83.62 GB	22.38 %

Analasis Abril-mayo

Aplicaciones	Descripción	Consumo
Actualizaciones de Windows	Abril-Mayo	684.5gb
Facebook	Abril-Mayo	383.6gb
YouTube	Abril-Mayo	325.9gb
Instagram	Abril-Mayo	204.4gb
WhatsApp	Abril-Mayo	221.8gb
Canva	Abril-Mayo	28.46b
Netflix	Abril-Mayo	22.6gb

Categorías de aplicaciones



Categoria	Bytes	Porcentaje
Infrastructure	1.24 TB	30.94 %
Software Update	715.78 GB	17.4 %
Streaming Media	689.5 GB	16.76 %
Social Networking	439.33 GB	10.68 %
Others	995.66 GB	24.21 %

Se realizo un analisis en un periodo con estudiantes y un analisis de cuando los estudiantes estaban en vacaciones.

FECHA	INFRAESTRUCTURA (CAPA DE SEGURIDAD PROTOCOLOS DE SOCKET, DNS)	ACTUALIZACIONES WINDOWS	PLATAFORMAS DE STREAMING (YOUTUBE, NETFLIX, ETC)	REDES SOCIALES	OTRAS (NAVEGACIÓN)
ABRIL-MAYO	30,94%	17,40%	16,60%	10,68%	24,21%
JUNIO 30- JULIO	31,69%	20,81%	16,30%	8,84%	22,38%

La informacion anterior monitoriar en la seccion de informes de Sophos aplicaciones y wed

Como se puede notar el consumo de internet en redes sociales es alto maxime que en el periodo que se encontraban estudiantes el consumo es del 10.68% y en el periodo donde no se encontraban estudiantes es del 8.84% con esto se puede evidenciar que este alto consumo se da en la red administrativa. El consumo en navegacion, conexión en aplicaciones y otras se puede evidenciar que son tambien realizadas por lo funcionarios ya que la diferencia son muy bajas.

Es importante establecer un procedimiento de actualizaciones de windows o desactivar las mismas con el fin de hacerlas programadas verificando cuales son utiles y cuales pueden causar problemas en la red de datos.

Se debe verificar en streaming el uso de plataformas como: NETFLIX, AMAZON, HBO Y YOUTUBE. Porque con estudiantes y sin estudiantes el consumo es alto.

19. Auditoria de politicas de seguridad.

Se realizo la revision de las politicas de seguridad tal como se indica en el punto 6 del presente informe y se ajustaron de acuerdo a los requerimientos. Es importante recalcar que el dispositivo se debe monitorear constantemente y actualizar a nuevas politicas personalizadas si es necesario debido a que dia dia hay nuevas vulnerabilidades

20 Configuracion de Firewall

DISPOSITIVOS LICENCIAS FILTRACIÓN

Número de serie Número de licencia	Nombre del cliente	Familia	Descripción del Producto	Dispositivo registrado (fecha de registro)	Estado de la licencia (fecha de finalización)	Número de contrato
L0015563828	INSTITUTO TECNICO NACIONAL DE COMERCIO SIMON RODRIGUEZ	Seguridad de red/UTM	Protección XG 310 Xstream	Registrado el 27/04/2023	Activo 23/03/2025	02310198

21. De acuerdo al diagnostico realizado a la red de datos se suguiere lo siguiente:

1. Activar QoS para mejorar la calidad del servicio de internet.

   buscando mejorar el rendimiento de la red de datos se realizo la configuracion del Qos como se indica en el punto 13 del presente informe

2. Configurar conexión seguras atraves de vpn por externos a la red intenalco.

   Se activan los usuarios VPN para conexiones externas. En la capacitacion se le indica al personal de TI como crear nuevas conexiones.

3. Deshabilitar la conexión de software de acceso remoto como: Anydesk, Teamviewer, RealVNC, Getscreen.me, AnyViewer.
4. Asignar direciones DHCP por mac para tener control de quipos existentes de la red.
5. Realizar monitoreo constante en el firewall por opcion de visor de registros.
6. Realizar el siguimiento en el firewall en el menu de informe aplicaciones y de acuerdo al consumos habilitar o restringir el consumo de las mismas. Como se puede obervar en el punto 18.
7. Configurar en el DNS de directorio activo 172.16.0.10 en los DNS del area administrativa para mejorar el recurso de la misma
8. Realizar mantenimiento a la infraestructura de la red de datos como: Switch, servidores, etc. Cada año para alargar la vida util de los mismos.
9. Verificar continuamente el enrutamiento de las redes LAN Y WAN
10. Verificar el trafico en el firewall de paquetes
11. Actualizar el software de sistema operativo de los servidores exitentes
12. Actualizar firewall de los equipos activos existentes
13. Verificar las politicas y actualizarlas según sus necesidades
14. Verificar continuamente el sophos si se presentan ataques desde que ciudad o pais y crear reglas para desminuir dichos ataques.

15. Monitorear los puertos abiertos en la red de datos y restringir el acceso desde la red wan de los puertos como: puerto 80,443,8080,8443: http, 20-21 FTP, 22 SSH, SMB 139,137,445, DNS 53, TELNET 23, SMTP 25, TFTP 69.

Se realizo la implementacion de los puntos anteriores.

22. Topologia de la red actual.

La topologia de red actual de intenalco es una topologia jerárquica de estrella lo que significa que parte de un centro principal de cableado y se divide en subcentros de cableado por piso, en algunos casos especiales algunos pisos se encuentran dos o tres subcentros de cableado, como es el caso del piso 1,4 y 5. Cuenta con cableado horizontal, el cableado va desde los subcentros de cableado o los centros de datos que se encuentran debidamente identificados.

Cableado vertical este cableado va desde centro principal de cableado a los subcentros de cableado que se define como Backbone este cableado es de categoría 6, con excepción Backbone piso 1 y extensión que es de categoría 6ª. Como se evidencia en el diagrama (RED INTENALCO) de acuerdo al analisis, mediciones y latencia se evidencia que la red presenta un funcionamiento optimo. Se realiza entrega un cuadro de la topologia de acuerdo al punto 5. Tambien se puede observar en el documento vicio anexado como (TOPOLOGIA RED INTENALCO)

TOPOLOGIA DE RED INTENALCO.vsdx

RED DE INTENALCO.vsdx

Desde cada gabinete se encuentra el cableado horizontal a las estaciones de trabajo. Para mejorar la topologia de red se requiere:

1. Que los backbones de los pisos de categoria 6 se cambien por fibra optica seis hilos multimodo

Backbone Centro cableado	Piso 1
Backbone Centro cableado	Biblioteca
Backbone Centro cableado	Piso 2
Backbone Centro cableado	Piso 3
Backbone Centro cableado	SALAS
Backbone Centro cableado	Piso 5
Backbone Centro cableado	Camaras
Backbone piso 1	Extension
Backbone piso 1	Monitoreo
Backbone piso 2	Camaras
Backbone piso 5	Oficina profesionales

2. Tarjetas SFTP para cada uno de los switch donde salen los backbone de fibra optica.
3. Cambio de equipo activo por desactualizacion tecnologica

FIREWALL SOPHOS
ANTENAS Unifi LR

4. Interconexion de equipos activos en centro de cableado con patch cord de fibra optica y tarjetas SFTP . La conexión por fibra optica garantiza que la conexión de equipos activos de hasta dos GHZ mejorando la velocidad de transmision.

23. Entrega del Licenciamiento para el firewall

Pymes On Line
SU ALIADO ESTRATÉGICO EN TECNOLOGÍA E INNOVACIÓN

Santiago de Cali, 24 julio 2024

Señores
INTENALCO EDUCACION SUPERIOR
Atn Ingeniera Lucero Chamorro
Área TI

Ref. Entrega de Licenciamiento Sophos

Reciba un cordial saludo.

De acuerdo a lo establecido en la ficha tecnica que hace parte del CONTRATO DE SUMINISTROS No 200.17.001-INT-SEL-ABR-2024 CELEBRADO ENTRE LA INSTITUTO TECNICO NACIONAL DE COMERCIO SIMON RODRIGUEZ Y PYMES ON LINE SAS. item No 23. Referente a la Entrega del licenciamiento para el firewall

DESCRIPCION ELEMENTO	Especificación	Cantidad
XG310 XSTREAM PROTECTION RENEWAL	XS310Z10ZZRCAA	1
XG310 WEBSERVER PROTECTION RENEWAL	SS310Z10ZZRCAA	1

Se realiza la entrega del respectivo licenciamiento y posterior activación en la consola de sophos como se observa a continuación.


DISPOSITIVOS LICENCIAS FILTRACIÓN

Número de serie Número de licencia	Nombre del cliente	Familia	Descripción del Producto	Dispositivo registrado (fecha de registro)	Estado de la licencia (fecha de finalización)	Número de contrato
L0015563826	INSTITUTO TECNICO NACIONAL DE COMERCIO SIMON RODRIGUEZ	Seguridad de red/UTM	Protección XG 310 Xstream	Registrado el 27/04/2023	Activo 23/03/2025	02310198

Se anexa el Documento Licencia emitido por Sophos con la información de las licencias suministradas

ENTREGA	RECIBE
Bernardo Saavedra Gutierrez Representante Legal Pymes On Line SAS Nit 900.440.998-7	Lucero Chamorro Supervicion- Ingeniera TI INTENALCO Nit. 800248004

Atentamente.



Bernardo Saavedra

Gerente - Pymes On Line

+57 304 5770507

bernardo@pymesonline.co

Carrera 23 #57-49 Cali